Data collection survey for promoting the cooperation between public and private sector in cybersecurity in the ASEAN and the Indo-Pacific region

Final Report

February 2026

Japan International Cooperation Agency (JICA)

Deloitte Touche Tohmatsu LLC

Deloitte Tohmatsu Cyber LLC

GP
JR
26-010

Countries for the Survey

Table of Contents

Figures

Tables

List of Abbreviations

Abbreviation	Full Form
AD	Active Directory
AI	Artificial Intelligence
AJCCA	ASEAN Japan Cybersecurity Community Alliance
AJCCBC	ASEAN-Japan Cybersecurity Capacity Building Centre
ASEAN	Association of Southeast Asian Nations
ASM	Attack Surface Management
BGP	Border Gateway Protocol
BSSN	Badan Siber dan Sandi Negara
CASB	Cloud Access Security Broker
CII	Critical Information Infrastructure
CRC	Cybersecurity Regulatory Committee
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DJID (SDPPI)	Directorate General of Resources and Equipment of Post and Information Technology
DPA	Data Privacy Act
DX	Digital Transformation
EDR	Endpoint Detection and Response
EMC	Electromagnetic Compatibility
FIRST	Forum of Incident Response and Security Teams
FQDN	Fully Qualified Domain Name
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GovNet	Government Network
GUI	Graphical User Interface
ICS	Industrial Control Systems
ICSCoE	Industrial Cyber Security Center of Excellence
ICT	Information and Communication Technology
idCARE.UI	Indonesia Cyber Awareness and Resilience Center of Universitas Indonesia
idNSA	Indonesia Network Security Association
IDS	Intrusion Detection System
IPA	Information-technology Promotion Agency
IPS	Intrusion Prevention System
IR	Incident Response
ITE	Information and Electronic Transactions
JICA	Japan International Cooperation Agency
KOMINFO	Ministry of Communication and Information Technology
MFA	Multi-Factor Authentication
MIC	Ministry of Information and Communications
MoPS	Ministry of Public Security
MPLS	Multi-Protocol Label Switching
NCERT	National Computer Emergency Response Team
NCIAC	National Cybersecurity Inter-Agency Committee
NCO	National Cybersecurity Office
NCSA	National Cyber Security Agency
NCSC	National Cyber Security Committee
NCSP	National Cybersecurity Plan
NDA	Non-Disclosure Agreement
NISC	National center of Incident readiness and Strategy for Cybersecurity
NTC	National Telecommunications Commission
ODA	Official Development Assistance

OJT	On the Job Training
OSINT	Open Source Intelligence
OT	Operational Technology
PDP	Personal Data Protection
PH-CERT	Philippine Computer Emergency Response Team
Playbook	Incident Response Playbook
PoC	Proof of Concept
RDP	Remote Desktop Protocol
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network
SIEM	Security Information and Event Management
SNI	Standar Nasional Indonesia
SOC	Security Operation Center
SSH	Secure Shell
STI	Science, Technology and Innovation
TISA	Thailand Information Security Association
VNA	Vietnam News Agency
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response

Chapter 1 Survey Summary

This report demonstrates and investigates the feasibility of deploying Japanese companies' products and services locally, as well as the current state and challenges in the industrial systems (OT), from multiple perspectives. It aims to strengthen public-private partnerships in the cybersecurity field within the ASEAN and Indo-Pacific regions. Through PoC projects and workshops in the target countries, we identified the technological capabilities and local adaptability of Japanese cybersecurity products, as well as the institutional and operational gaps evident in the industrial systems sector and the needs on the ground.

Chapter 2: Survey Background describes the current situation where threats in cyberspace are expanding due to advancing digitalization, and damage is becoming more severe due to inadequate systems and personnel shortages in developing countries.

Chapter 3: Survey Overview explains the overall survey process. This process employed multifaceted methods, including information gathering on Japanese companies' cybersecurity products and services, PoC projects in the target countries, and workshops in the industrial systems sector, targeting the nine ASEAN countries and Mongolia.

Chapter 4: Information on Japanese Cybersecurity Products summarizes the characteristics, local deployment status, and PoC project outcomes of cybersecurity products and services operating within Japan. Information gathering was conducted on cybersecurity products and services deployed within Japan, collecting and organizing information on 315 products from 63 Japanese companies. Furthermore, from the target countries (ASEAN 9 countries and Mongolia), Indonesia, Thailand, and the Philippines were selected. Subcontracting for the investigation, including proof-of-concept projects, was awarded to three companies: Internet Initiative Japan Inc. (Indonesia), Amiya Corporation (Thailand), and Macnica, Inc. (Philippines). Through the proof-of-concept projects with local government agencies and critical infrastructure operators, we specifically investigated the effectiveness and competitiveness of Japanese cybersecurity products and services in the target countries from perspectives including operational efficiency, risk reduction, regulatory compliance, local suitability, personnel proficiency, and operational burden.

Chapter 5: Cybersecurity Measures for Industrial Systems (OT) summarized findings on the gap between institutional frameworks and field implementation in the OT sector, as well as common operational challenges. This was achieved by conducting OT security workshops targeting government agencies and critical information infrastructure operators in the surveyed countries: Thailand, the Philippines, and Indonesia.

Chapter 6: Recommendations and Summary reports on the outcomes of this survey, including the content of discussions with JICA, the three companies implementing the PoC project, and Nagoya Institute of Technology (a national university corporation that conducted the OT workshop), as well as recommendations and conclusions based on this survey.

Chapter 2 Survey Background

With the advancement of digitalization, people, goods, money, organizations—including administrative agencies—and infrastructure systems are increasingly connected in cyberspace, and the risks associated with cybersecurity are also becoming more severe. In many developing countries, insufficient cybersecurity response frameworks and capabilities, coupled with a shortage of skilled personnel, are amplifying these risks. Consequently, severe incidents are occurring globally: damage from ransomware attacks that have wreaked havoc worldwide; critical infrastructure (energy, finance, communications, healthcare, etc.) suffering serious damage; confidential information leaks through supply chains; social disruption caused by disinformation; and personal information breaches. Against this backdrop, numerous development cooperation agencies and governments are providing support to strengthen cybersecurity capabilities in developing countries. This serves as a safeguard for each nation in advancing digital societies within developing countries and aims to enhance regional cybersecurity at the regional level to mitigate the cross-border impact of cyber threats.

The Government of Japan formulated the "Basic Policy on Capacity Building Support for Developing Countries in the Field of Cybersecurity[1]" in 2021. From the perspective of reducing international cybersecurity risks, it is advancing international cooperation in areas such as critical infrastructure protection, countermeasures against cybercrime, international rule-making, promotion of confidence-building measures, and human resource development. Furthermore, the Japan-ASEAN Cybersecurity Policy Meeting[2], led by Japan, will add an "Industry-Government-Academia Session" starting in fiscal year 2024, emphasizing collaboration with industry and academia. Based on the above policy, JICA implements cybersecurity capacity building for government officials and critical infrastructure operators in developing countries through technical cooperation projects such as the "Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services[3]"

Under these circumstances, while implementing such cooperation, there is an expectation to leverage the knowledge and experience of Japanese companies and research institutions. This applies not only to enhancing cybersecurity response capabilities for national governments but also to strengthening cybersecurity measures for critical infrastructure operators. However, JICA's past initiatives have involved limited collaboration with industry and academia. Consequently, JICA does not have a sufficient grasp of Japanese companies interested in providing cybersecurity-related products overseas or expanding their operations in this field.

[1] Cybersecurity Strategy Headquarters https://www.cyber.go.jp/pdf/policy/kokusai/cs-tojyokokushien2021.pdf (in Japanese).
[2] Ministry of Economy, Trade and Industry 18th ASEAN-Japan Cybersecurity Policy Meeting Held
[3] JICA Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services | ODA Project Website

Chapter 3 Survey Overview

3.1. Survey Purposes

JICA has formulated a "Cybersecurity Cluster Strategy" that positions "Realizing a Free and Secure Cyberspace[4]" as a key theme under its global agenda of "Promoting Digitalization," and is implementing capacity building for government officials and critical infrastructure operators in developing countries. Furthermore, while JICA recognizes the importance of leveraging private-sector technology to solve challenges, the utilization of Japanese companies' and research institutions' expertise and experience in the cybersecurity field remains limited. The overseas expansion of products by companies and the accumulation of track records have not sufficiently progressed. Against this backdrop, this survey examined the initiatives of Japanese private companies, research institutions, and universities in the cybersecurity field within Japan, while also exploring the potential for expansion into ASEAN countries.

3.2. Scope of Survey

3.2.1Scope of Project Implementation

This investigation was conducted to examine the items outlined in the subsequent section "3.2.2 Method of Work Implementation" and to prepare reports and other documents. The candidate countries for investigation were the nine ASEAN nations (Indonesia, Cambodia, Singapore, Thailand, the Philippines, Brunei, Vietnam, Malaysia, Laos) and Mongolia.

3.2.2Methods of Project Implementation

This survey was conducted in three phases: planning, implementation, and results compilation. During the implementation phase, activities were conducted in parallel: collecting information on Japanese security companies and products, conducting proof-of-concept projects for Japanese company products, and gathering information on cybersecurity measures for industrial systems (OT). The overall process followed the workflow outlined below.

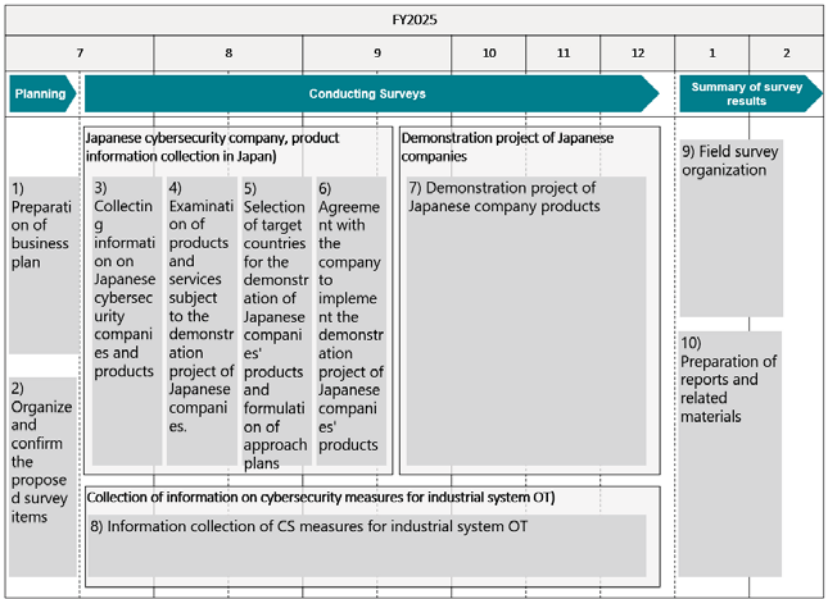


Figure 1 Workflow of the Survey

[4] JICA digital_text.pdf (in Japanese)

Table 1 Tasks and Descriptions of The Survey

No.	Item	Activity Description
(1)	Creation of business plan documents	A work plan for this survey was prepared and confirmed with the Office for STI and DX, Governance and Peacebuilding Department.
(2)	Organization and confirmation of survey items	・ Collection of information on Japanese cybersecurity companies and products, as well as PoC projects for Japanese company products (Japanese and local). ・ Collection of information on cybersecurity measures for industrial systems (OT) (local).
(3)	Japanese cybersecurity companies and product information collection	Conducted surveys on cybersecurity products and services available in Japan that may be useful for emerging economies, especially for governments and critical infrastructure. Information was collected through interviews with stakeholders, and a long list was compiled.
(4)	Examination of candidate companies and services for Japanese enterprise PoC projects	Based on the list created in (3), examined candidate companies and services for PoC projects.
(5)	Selection of target countries for the PoC projects for Japanese company products and formulation of an approach plan	Selected candidate companies for Japanese enterprise PoC projects based on the examination in (4), and formulated pilot plans.
(6)	Agreement with implementation partners for the PoC projects for Japanese company products	Conducted agreements with candidate companies selected in (5), and established survey plans.
(7)	Implementation of Japanese enterprise PoC projects	Conducted Japanese enterprise PoC projects as per the survey plan.
(8)	Information collection on cybersecurity measures for industrial systems (OT)	Amid rising importance of OT cybersecurity measures in ASEAN and other regions, collected information on trends in OT cybersecurity measures in these areas, and confirmed the results of local survey activities.
(9)	Organization of survey results	Organized survey results from (7) and (8), confirming completion of survey activities.
(10)	Creation of reports and related materials	Created final reports and related materials.

During the survey implementation phase, the information gathering and PoC project for Japanese corporate products proceeded with the selection of PoC companies and the advancement of corporate PoC activities, based on product information collection and the selection of target countries.

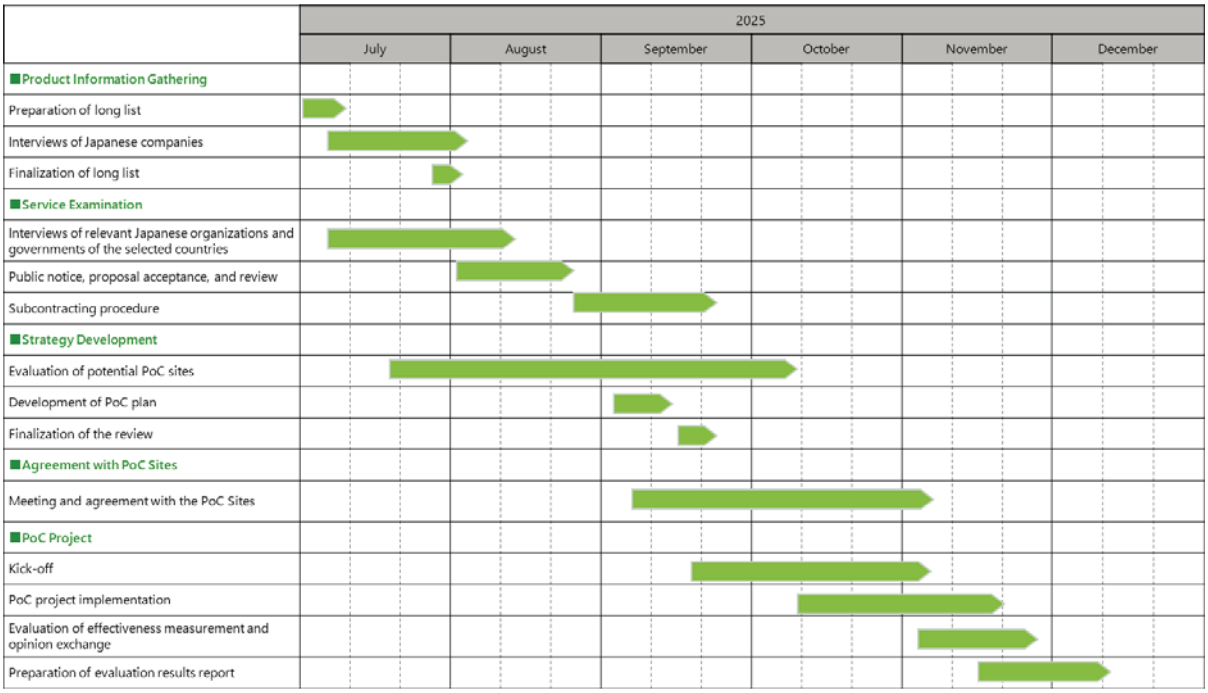


Figure 2 Detailed Schedule of the Project for Information Collection and PoC of Japanese Companies' Products

In gathering information on cybersecurity measures for industrial systems (OT), the core activity involved conducting workshops in the three target countries.

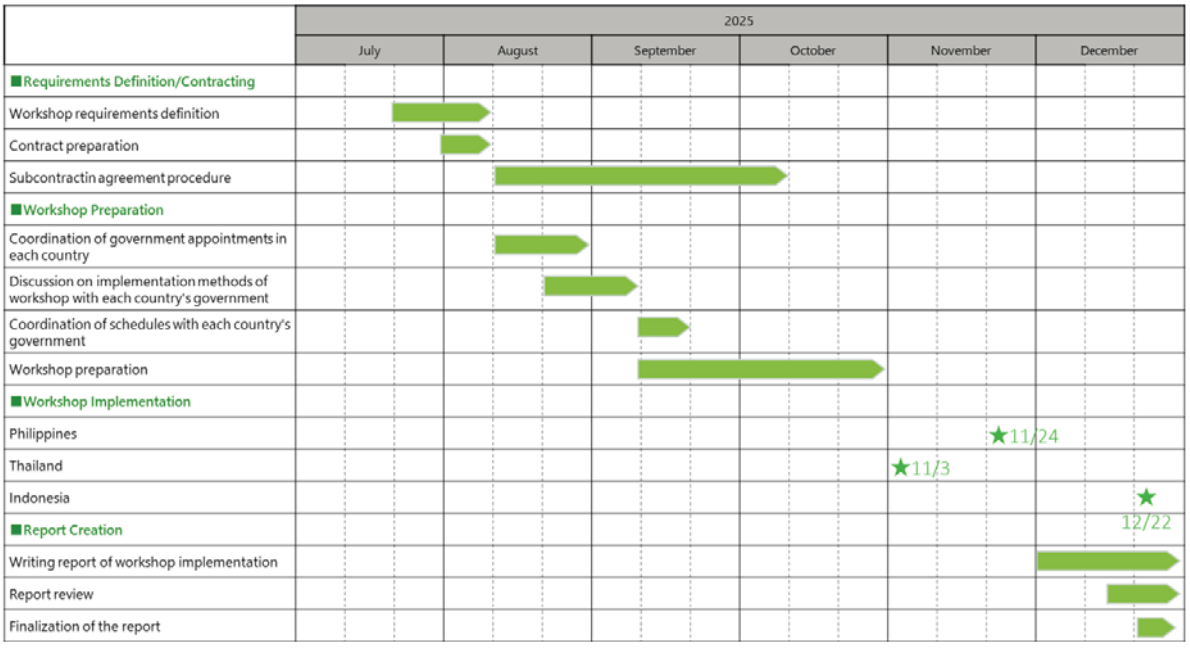


Figure 3 Detailed Schedule for Information Collection on Cybersecurity Measures for Industrial Systems (OT)

3.3. Survey Implementation Schedule

The survey period is from July 1, 2025, to February 27, 2026.

Chapter 4 Information on Japanese Cybersecurity Products

4.1. Overall Overview

This project examines the potential for deploying Japanese cybersecurity products and services in the ASEAN region. It evaluates their effectiveness, sustainability, and suitability for local conditions through PoCs with local government agencies and critical infrastructure operators. Japan has accumulated advanced security technologies and expertise through public-private partnerships. The core objective is to leverage these assets to address the growing cyber risks accompanying the digitalization progress in ASEAN countries. Particularly in developing nations, risks such as ransomware attacks, critical infrastructure breaches, and personal data leaks are becoming increasingly evident. However, institutional frameworks and human resource development remain inadequate. Therefore, PoC projects were advanced based on the Japanese government's policy and JICA's capacity-building programs.

The selection of target countries was based on four indicators: (1) Japan government/JICA cooperation history, (2) companies' interest in overseas expansion, (3) nominal GDP, and (4) the Global Cybersecurity Index (GCI), [5] leading to the selection of Indonesia, Thailand, and the Philippines. Analysis of each country's national strategies and legal frameworks confirmed the critical importance of protecting critical infrastructure and complying with personal information protection laws.

A desk study of Japanese cybersecurity products and services confirmed that Japanese security vendors operate across diverse fields including network monitoring, endpoint protection,[6] ASM,[7] zero trust,[8] cloud security, AI/automation, vulnerability assessment, CSIRT support, [9] and education/training. They also possess extensive implementation experience with government agencies and critical infrastructure and are actively expanding overseas into ASEAN countries.

Product and service selection for the PoC project involved multifaceted evaluation of effectiveness against local challenges, organizational structure, legal compliance, infrastructure integration, and operational feasibility. Three companies were selected: Internet Initiative Japan Inc. (Indonesia), Amiya Corporation (Thailand), and Macnica, Inc. (Philippines). In actual local operational environments, verification focused on log monitoring and anomaly detection (SIEM[10]), remote access management (Zero Trust/privileged ID management), and ASM to assess operational efficiency, risk reduction, and long-term sustainability. Compliance with local laws, data protection and privacy requirements, infrastructure integration, and the operational proficiency of local staff were also evaluated.

The results confirmed that Japanese products are effective for enhancing local security and sufficiently meet local needs and regulations. In the ASEAN market, characterized by a shortage of specialized personnel and high operational burdens, the importance of AI, automation, cloud-based services, and operational support systems was reaffirmed. Going forward, sustainable market expansion is anticipated through compliance with international standards, flexible adaptation to local regulations, collaboration with local partners, and support for human resource development.

This project demonstrated that Japanese cybersecurity products and services possess competitiveness and reliability in global markets, including ASEAN, establishing foundational insights and model cases for overseas expansion.

---

[5] Refer to the Global Cybersecurity Index 2024. The GCI is a global metric developed by the International Telecommunication Union (ITU) that evaluates countries' cybersecurity capabilities and ranks them across five domains: legislation, technology, organization, capacity building, and cooperation.

[6] Security measures to protect endpoints such as PCs and smartphones from cyberattacks and malware.

[7] Attack Surface Management: A methodology for identifying and managing publicly accessible assets on the internet to reduce the risk of external attacks.

[8] A security model that constantly verifies all access, both inside and outside the network.

[9] CSIRT stands for Computer Security Incident Response Team, an organization specializing in responding to, investigating, and recovering from cybersecurity incidents.

[10] Security Information and Event Management: A system that integrates and manages multiple logs to support threat detection and analysis.

4.2. Selection of Target Countries for Verification of Japanese Corporate Products

In selecting target countries, four key criteria were established as particularly important for enhancing the effectiveness and sustainability of international cooperation projects in the cybersecurity field: A) Japan's cooperation track record (in cybersecurity), B) Japanese corporate preferences, C) nominal GDP, and D) maturity level in the Global Cybersecurity Index (GCI).

A) The country's cooperation track record refers to the existence and content of cooperation projects accumulated to date between Japanese government agencies (NCO[11], Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, etc.) or JICA and the partner country. Specifically, the concrete cybersecurity-related cooperation track record of JICA listed in Table 2 serves as a foundation for advancing further collaboration with the target country and is also an important factor in increasing the likelihood of project success.

[11] National Cybersecurity Office (abbreviated as NCSO). In July 2025, based on the Cabinet Secretariat Organization Order, the Cabinet Cyber Security Center was reorganized, and the National Cybersecurity Office was established within the Cabinet Secretariat.

Table 2 Cybersecurity Initiatives Implemented by Japanese Government Agencies (Since 2020)

Country	Project Name	Main Entity	Support entity	Period	Project Overview	Counterpart Organization(s)
Indonesia	Project for Human Resources Development for Cyber Security Professionals	JICA	Technical cooperation	May 2019 – May 2024	Partnering with the University of Indonesia to train cybersecurity professionals, develop open-source tools, and strengthen collaboration with other countries, including Mongolia.	Ministry of Information and Communications; University of Indonesia
Vietnam	Project on capacity building for cyber security in Vietnam	JICA	Technical cooperation	June 2019 – November 2021	Focusing on the Information Security Bureau under the Ministry of Communications: enhancing capacity to respond to cyberattacks, supporting measures for children's online protection, and conducting awareness-raising activities.	Information Security Bureau, Ministry of Information and Communications
Mongolia	Project for Development of Human Resources in Cybersecurity	JICA	Technical cooperation	January 2023 – December 2026	Strengthening cybersecurity education and workforce development through industry–academia–government collaboration to promote a secure digital society in Mongolia.	Ministry of Digital Development and Communications; Mongolian University of Science and Technology, School of Information and Communication Technology
ASEAN Countries (Thailand)	Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services	JICA, Ministry of Internal Affairs and Communications, Ministry of Foreign Arriairs	Technical cooperation	March 2023 – February 2027	Conducting cybersecurity training and exercises for government officials and critical infrastructure organizations in ASEAN member states at the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC), which was established by the Government of Japan together with the Government of Thailand.	National Cyber Security Agency (NCSA); relevant agencies in ASEAN member states.
Cambodia	Project for Improvement of Cyber Resilience	JICA	Technical cooperation	May 2023 – October 2026	Focusing on the ICT Security Bureau within the Ministry of Posts and Telecommunications, we conduct assessments and provide seminars to	Ministry of Posts and Telecommunications; General Department of ICT; ICT Security Bureau

Country	Project Name	Main Entity	Support entity	Period	Project Overview	Counterpart Organization(s)
					enhance cybersecurity capacity, and strengthen inter-organizational collaboration on cybersecurity between the Bureau, critical information infrastructure (CII) sectors, and other government ministries.	
Philippines	Project for Improvement of Cyber Resilience	JICA	Technical cooperation	October 2023 – September 2025	To enhance the cybersecurity capacity of the Cybersecurity Bureau of the Philippines' Department of Information and Communications Technology (DICT), we support training, public awareness and outreach activities, and stronger collaboration with critical infrastructure sectors.	Cybersecurity Bureau, Department of Information and Communications Technology (DICT)
Indonesia, Cambodia, Philippines	JICA Overseas Technical Training "Cyber Defense Exercise" for Indonesia, Cambodia and the Philippines	JICA	Training	January 2025 – February 2025	Conducting cybersecurity training for Indonesia, Cambodia, and the Philippines; design cyberattack-defense exercises and train the personnel who conduct them to strengthen each country's technical capabilities. This effort is carried out in cooperation and coordination with JICA's ongoing cybersecurity-related projects.	Indonesia: Ministry of Information and Communications (MIC) Philippines: Department of Information and Communications Technology (DICT) Cambodia: Ministry of Post and Telecommunications (MPTC)

B) The intentions of Japanese companies reflect the overseas expansion needs and strategies of Japanese firms in the cybersecurity field. By selecting target countries where companies have a desire to expand, the know-how and knowledge accumulated through PoC projects can be leveraged for future in-house expansion.

C) Nominal GDP[12] serves as an indicator of the economic scale of the surveyed countries. Countries with larger nominal GDPs are considered to have larger markets and greater capacity for investment in ICT infrastructure and cybersecurity. In countries experiencing significant economic growth, demand for cybersecurity measures is increasing alongside digitalization, suggesting potential spillover effects from cooperative projects.

D) The Global Cybersecurity Index (GCI) maturity level is an international indicator that comprehensively evaluates each country's preparedness in cybersecurity policies, legal frameworks, infrastructure, human resources, and other areas. Countries with a GCI score of moderate or higher are expected to have a solid foundation already in place, making more effective project implementation feasible.

Based on these four axes, Indonesia received the highest overall evaluation among the countries assessed in Table 3. Thailand, the Philippines, and Vietnam followed as the next highest-ranked countries. From among these, the Philippines and Thailand were selected as target countries for investigation, taking into comprehensive consideration the intentions of Japanese companies, their cooperation track records, and the institutional environments of each country.

[12] World Bank Grope GDP.pdf

Table 3 Assessment for the Selection of Target Countries

Criteria	◎：JICA Technical Cooperation Support ○：Government Agency Projects in Japan △：ASEAN-Japan Cybersecurity Policy Council, etc. ×： No track record	◎： Wide intention ○： Partial intention ×： No intention	◎： 1st ~ 4th place ○： 5th ~ 7th place ×： 8th~10th place	◎T1：Role-modeling ○T2：Advancing △T3：Establishing ×T4：Evolving ×T5：Building			5: Top priority 4: High priority 3: Medium priority 2: Low priority 1: Non-priority	
Country	ODA recipients	A) Cooperation of cybersecurity with Japan	B) Intention of Japanese companies	C) GDP Millions of US dollars)	D) GCI rating			Overall Rating Target Country Priority
					Overall rate	Score	Area	Priority / Reasen
Indonesia	Yes	Cybersecurity Human Resource Development Project JICA)	There are many manufacturing industries	World No. 16 / Target Country No. 1 $1,371,171	T1 100	20 20 20 20 20	Law Technology Organization Capacity Corporation	5 / No concerns about A~D
Philippines	Yes	Cybersecurity Capacity Building Project JICA)	High need for English-speaking countries cybersecurity content	World No. 33 / Target Country No. 4 $437,146	T2 93.49	20 19.11 19.51 17.17 17.7	Law Technology Organization Capacity Corporation	4 / A~D There is no major concern; D is slightly inferior compared to other countries.
Vietnam	Yes	Cybersecurity Capacity Building Project JICA)	There are many manufacturing industries Some companies are cautious	World No. 34 / Target Country No. 5 $429,717	T1 99.74	20 20 20 19.74 20	Law Technology Organization Capacity Corporation	4 / There is no major concern in either A~D Some companies are cautious about B C is slightly inferior to the top
Thai	Yes	ASEAN-Japan Capacity Enhancement Program Strengthening Project on Cybersecurity and Digital Trust Services JICA)	Many foreign products and manufacturing industries Pro-Japanese	World No. 26 / Target Country No. 2 $514,969	T1 99.22	20 20 19.22 20 20	Law Technology Organization Capacity Corporation	4 / There is no major concern in either A~D Although A is the implementing country, it is for the entire ASEAN region, so the priority has been lowered.
Malaysia	Yes	Non-Secretary States in the Japanese Government's Projects	Some companies have local bases	World No. 37 / Target Country No. 6 $399,705	T1 98.82	20 20 18.82 20 20	Law Technology Organization Capacity Corporation	3 / A has no track record of JICA's technical cooperation projects, and there are concerns about the local government's cooperation in the investigation.
Mongolia	Yes	Cybersecurity Human Resource Development Project JICA)	No special comments	World No. 121 / Target Country No. 8 $20,325	T3 56.36	19.18 6.64 13.62 10.43 6.49	Law Technology Organization Capacity Corporation	3 / A has a track record of JICA technical cooperation projects, and there are concerns about B~D
Cambodia	Yes	Cybersecurity Human Resource Development Project JICA)	Many French products	World No. 42/ Target Country No. 7 $363,494	T4 37.02	11.82 4.56 8.3 6.12 6.22	Law Technology Organization Capacity Corporation	2 / A has a track record of JICA technical cooperation projects, there are concerns about B~D, D is inferior to Mongolia, GCI is inferior
Laos	Yes	Non-Secretary States in the Japanese Government's Projects	The presence of Chinese companies is strong	World No. 134/ Target Country No. 9 $15,843	T4 33.74	10.38 6.18 5.52 2.05 9.61	Law Technology Organization Capacity Corporation	1 / A~D are of concern.
Singapore	No	Non-Secretary States in the Japanese Government's Projects	The market is mature	World No. 30/ Target Country No. 3 $501,428	T1 99.86	20 20 20 19.86 20	Law Technology Organization Capacity Corporation	1 / Not a country eligible for ODA assistance
Brunei	No	Non-Secretary States in the Japanese Government's Projects	The market is small	World No. 138/ Target Country No. 10 $15,128	T3 70.38	17.2 14.89 11.35 10.76 16.18	Law Technology Organization Capacity Corporation	1 / Not a country eligible for ODA assistance

Particularly in countries with extensive past cooperation with JICA (countries with high A-axis scores), there is a high potential for rapid coordination with local government agencies, enabling smooth information gathering and stakeholder coordination during surveys and project implementation. This led to the conclusion that the feasibility of this project is enhanced. Considering this, regarding Vietnam, on February 28, 2025, the national management and oversight responsibilities for cybersecurity were transferred from the Ministry of Information and Communications (MIC) to the Ministry of Public Security (MoPS). Ten administrative procedures, including business permits and import permits for cybersecurity products and services, now fall under MoPS jurisdiction.[13] Considering the project period, coordination with the new competent authority is expected to require a certain amount of time. Establishing a sufficient cooperative framework within the project period may be difficult. Therefore, the priority of these countries as survey targets was lowered. Furthermore, for Singapore and Brunei, which are not ODA recipient countries, the priority as survey targets was also lowered, in line with the objectives of ODA projects.

4.3. National Strategies and Legal Regulations in the Survey Countries

The national strategies and legal regulations in each survey country are as follows.

4.3.1 National Strategies and Legal Regulations Related to Cybersecurity in Indonesia

(1) National Strategy

[13] Vietnam News Agency (VNA) Cybersecurity protection function handed over to public security ministry

Indonesia has positioned the strengthening of cybersecurity as a key priority in its national strategy. To systematically advance cybersecurity as a national security issue, the government enacted Presidential Regulation (Perpres) No. 47/2023 in 2023.[14] The pillars of the strategy are as follows:

- Strengthening Cybersecurity Governance:
  Centralize the oversight and coordination of cybersecurity policy under the National Cybersecurity and Cryptography Agency (BSSN). Establish collaborative frameworks with ministries, local governments, and critical infrastructure operators.
- Protecting Critical Information Infrastructure:
  Enhance protection for critical infrastructure in sectors such as energy, finance, communications, transportation, and healthcare. Require critical infrastructure operators to meet minimum cybersecurity standards and fulfill incident reporting obligations.
- Improving Incident Response Capabilities:
  Establish rapid response systems (CSIRT establishment and coordination) for cyberattacks and data breaches. Promote incident recording, analysis, and sharing.
- Human Resource Development and Awareness:
  Expand cybersecurity workforce development programs. Strengthen awareness campaigns for citizens and businesses.
- International Cooperation:
  Promote information sharing, joint training, and technical cooperation with international organizations like ASEAN and other nations.

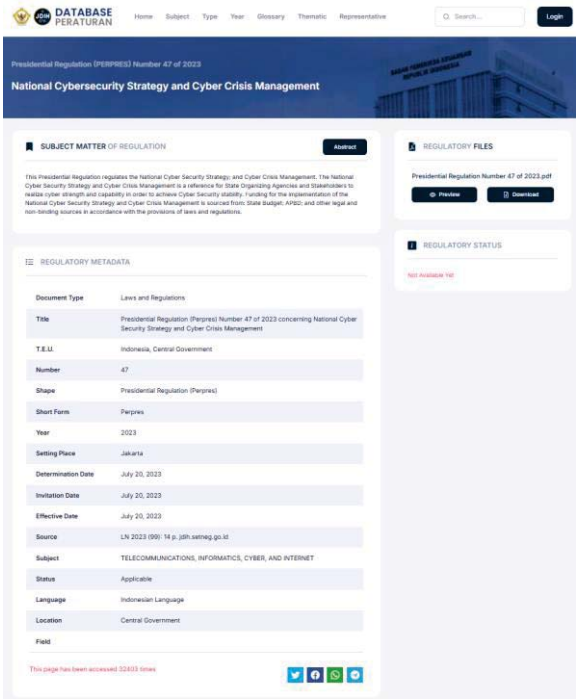


Figure 4 Indonesian Audit Board (BPK) Legal Information System Website

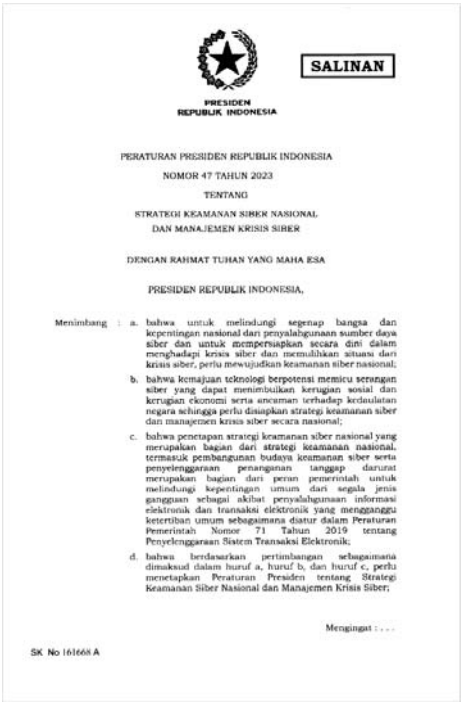


Figure 5 Presidential Regulation (Perpres) No. 47/2023

(2) Legal Regulations

A) Cybersecurity Law (Electronic Information and Transactions Law (ITE Law) (No. 11/2008) [15])

i. Overall Overview

This is the fundamental law regulating cybercrime and electronic transactions. It provides the legal framework for combating cybercrime and conducting e-commerce, while also

[14] Indonesian Audit Board (BPK) PERPRES No. 47 Tahun 2023
[15] Indonesian Audit Board (BPK) UU No. 11 Tahun 2008

strengthening personal data protection and responses to data breaches.

ii. Definition of Critical Information Infrastructure

The National Cyber and Cryptography Agency (BSSN), central to Indonesia's cybersecurity policy, defines critical information infrastructure in BSSN Regulation No. 8/2020 as information systems, networks, and assets that are vital for national security, economic stability, and the maintenance of public health and safety. Disruption, damage, or destruction of these systems would cause significant impact on society and the nation.

iii. Sectors of Related Critical Information Infrastructure

BSSN and related guidelines designate the following sectors as critical information infrastructure:

- Government and administrative agencies (national data centers, resident databases, etc.)
- Energy sector (power management systems, oil and gas operational networks, etc.)
- Financial services (banking systems, payment infrastructure, securities trading systems, etc.)
- Communications and Information Sector (Telecom Carrier Networks, Internet Backbone Facilities, etc.)
- Healthcare (Hospital Information Systems, Medical Databases, etc.)
- Transportation and Logistics (Air Traffic Control Systems, Rail Control Systems, Port Systems, etc.)
- Water Resources and Water Supply
- Food Supply Management Systems
- Defense and Public Safety Systems

B) Legal Regulations to Note for Sales in the Country

i. Personal Data Protection Law (PDP Law) (Law No. 27/2022) [16]

Indonesia's PDP Law, enacted in 2022, strictly mandates personal data protection, security measures, and incident response. As cybersecurity products are critical tools for supporting compliance with these laws, key points for sales include explaining PDP Law-compliant features, confirming local regulations, and assisting customers with compliance.

ii. Export-Related Regulations

Regarding the export of cybersecurity products to Indonesia, the following Indonesian regulations are primarily relevant:

- Communication Equipment Certification[17]:
  When exporting cybersecurity products, type certification (DJID (SDPPI) [18] certification) from Indonesia's Ministry of Communication and Information Technology (KOMINFO) [19] or obtaining SNI (Indonesian National Standard) [20] certification may be required. Additionally, SDPPI certification is mandatory for devices with wireless functionality (e.g., Wi-Fi-enabled firewalls).[21]
- Cryptographic Technology Regulations:
  In Indonesia, cryptographic technology may require authorization from BSSN.[22] Specifically, when providing such technology to government agencies or critical infrastructure, BSSN approval or additional review may be required.
- Import Permit:

[16] Indonesian Audit Board (BPK) UU No. 27 Tahun 2022

[17] General Incorporated Foundation Japan Quality Assurance Organization インドネシア | 国際認証サービス | 電気製品・医療機器・車載機器の認証・試験 | 日本品質保証機構（JQA） (in Japanese)

[18] In January 2025, the SDPPI (Information and Communications Resources Standards Agency) was renamed the DJID (Digital Infrastructure Agency). See インドネシア -「SDPPI」から「DJID」へ、無線認証当局の名称変更」 | ニュースリリース | JQA (in Japanese)

[19] In October 2024, the name was changed from KOMINFO (Ministry of Information and Communication) to KOMDIGI (Ministry of Communication and Digital). See インドネシア -「SDPPI」から「DJID」へ、無線認証当局の名称変更」 | ニュースリリース | JQA (in Japanese)

[20] Indonesian National Standardization Agency (BSN) https://bsn.go.id

[21] Indonesian Audit Board (BPK) Permenkominfo No. 3 Tahun 2024

[22] Indonesian Audit Board (BPK) Peraturan BSSN No. 8 Tahun 2020

Certain cybersecurity products may require an Import Permit or prior registration.[23]

4.3.2 National Strategies and Legal Regulations Related to Cybersecurity in Thailand

(1) National Strategy

Cybersecurity policy is positioned as central to national security and development in the Kingdom of Thailand National Strategy (2018–2037).[24] The National Security Strategy promotes the development of specialized personnel and the utilization of advanced technologies and big data to prepare for diverse threats, including cyberattacks. It establishes an integrated response system involving collaboration between the government, private sector, citizens, and international organizations. Emphasis is also placed on international cooperation and strengthening information infrastructure, with efforts to establish a nationwide information collection and analysis system in collaboration with ASEAN countries and others. The Competitiveness Enhancement Strategy identifies digital, AI, and data sectors as growth industries, advancing the strengthening of digital infrastructure including science, technology, and logistics. In the administrative sector, it enhances policy transparency and effectiveness by providing swift, transparent services through digital technology and establishing a nationwide monitoring and evaluation system for strategy implementation. Furthermore, efforts are being made to develop human resources through lifelong learning and digital platforms, and to advance the digitalization of society. Through these measures, the Kingdom of Thailand aims to realize a safe and resilient digital society by comprehensively promoting threat response capabilities, industrial promotion, administrative reform, and human resource development, all centered on cybersecurity.

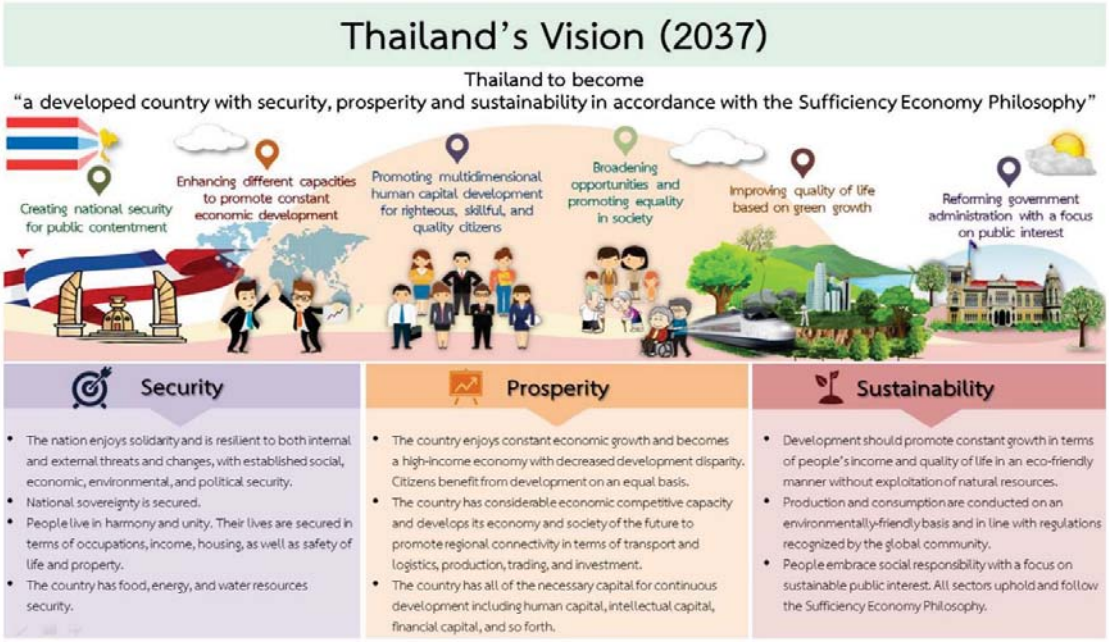


Figure 6 Thailand's Vision 2037

(2) Legal Regulations

A) Cybersecurity Act (B.E. 2562 (2019))[25]

i. General Overview

The Kingdom of Thailand's Cybersecurity Act establishes a framework to protect government and private information systems from cyber threats affecting national security and public order. The Act defines cybersecurity maintenance as encompassing all preventive, countermeasure, and risk mitigation measures against domestic and international threats, which include unlawful intrusion into computers and data. The National Cybersecurity Committee (NCSC), the

[23] Ministry of Trade of the Republic of Indonesia Peraturan - JDIH Kementerian Perdagangan RI, JETRO view_interface.php (in Japanese)

[24] Thai National Strategy Office National_Strategy_Summary.pdf

[25] Thai Ministry of Digital Economy and Society 3572-Cybersecurity-Act-B-E-2562--2019-

Regulatory Commission (CRC), and the Secretariat have been established to undertake policy formulation, standard setting, monitoring, and response support. Policies aim at integrated management, capacity building, protection of critical information infrastructure, cooperation, human resource development, awareness raising, and legal development. Related organizations are obligated to develop standards and codes of practice aligned with these policies. The Secretariat serves as the coordinating body, handling information sharing, training, standard development support, and incident response. Each organization is required to register responsible officers, comply with standards, conduct annual risk assessments and response planning, and promptly report major incidents. Depending on the severity of the threat, the CRC may direct information gathering or technical measures, and penalties are imposed for violations.

ii. Definition of Critical Information Infrastructure
Under Article 3 of this Act, critical information infrastructure is defined as computers or computer systems used by government agencies or private organizations in their operations related to the maintenance of infrastructure that contributes to national security, public safety, the security of the national economy, or the public interest.

iii. Sectors of Related Critical Information Infrastructure
Pursuant to Article 49 of this Act, the Committee has the authority to determine, through notification, which organizations constitute critical information infrastructure, along with their characteristics and conditions.

（1） National Security
（2） Critical Public Services
（3） Banking and Finance
（4） Information Technology and Telecommunications
（5） Transportation and Logistics
（6） Energy and Utilities
（7） Public Health
（8） Other Sectors Designated by the Committee

B) Legal Regulations to Note for Sales in the Country

i. Personal Data Protection Act B.E. 2562 (2019) [26]
Thailand's Personal Data Protection Act (PDPA) applies not only to businesses collecting, using, or disclosing personal data within Thailand, but also to foreign businesses handling personal data within Thailand (Section 5). Personal data refers to all information that can directly or indirectly identify an individual, excluding information concerning deceased persons (Section 6). The roles of data controllers and processors are clearly defined (Section 6). When transferring personal data outside Thailand, explicit consent from the data subject or other lawful basis is required if the destination country does not provide an equivalent level of protection to the PDPA (Section 28). Data subjects are granted rights including access, rectification, erasure, and restriction of use (Sections 30-34). Obtaining consent is generally mandatory for the collection, use, and disclosure of personal data; processing without consent is unlawful (Section 19). Violations of these rules may result in administrative fines of up to 5-million-baht, criminal penalties, and civil damages (Section 84, Section 79, Section 77). Businesses operating in Thailand are required to establish a compliance framework for the PDPA.

ii. Export-Related Regulations
Regarding the export of cybersecurity products to Thailand, the following Thai regulations are primarily relevant:

- Export and Import of Goods Act, B.E. 2522 (1979) [27]
  This Act stipulates that all goods imported or exported may be subject to restrictions such as export/import bans, licensing requirements, obligations to submit quality/origin certificates, payment of levies, or clearance at designated ports, based on notifications from

[26] Thai Ministry of Digital Economy and Society 3577-Personal-Data-Protection-Act-B-E--2562--2019-
[27] World Trade Organization Import Licensing Notification Portal

the Minister of Commerce for reasons including national security, economic stability, and public interest. Violations are subject to severe penalties. Therefore, when exporting cybersecurity products from Japan, it is crucial to thoroughly verify beforehand whether the items fall under the scope of the Act, confirm the necessary permits, licenses, and documents, and review the latest notifications from the Ministry of Commerce and related agencies to ensure proper procedures are followed.

- Control of Item in Relation to the Proliferation of Weapons of Mass Destruction Act B.E. 2562[28]
  Thailand manages the transfer of items and technologies that could be used for the proliferation of weapons of mass destruction (WMD) based on international requirements such as UN Security Council resolutions. This law regulates dual-use products (those with both civilian and military applications) that can be diverted for WMD-related purposes, managing them based on designated lists, notifications, and catch-all provisions. Cybersecurity products may also fall under this scope depending on their functions and intended use, making clear clarification of product specifications and applications crucial in practice.
- The Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services, B.E. 2553（2010）[29]
  This law establishes the National Broadcasting and Telecommunications Commission (NBTC) of Thailand, defines its authority, and regulates wireless communication equipment, broadcasting equipment, and telecommunications services. The NBTC sets technical standards and type approval for wireless communication equipment, assigns frequencies, mandates certification label display, and ensures the safety of equipment in the market and the proper use of radio waves. Furthermore, notifications and regulations issued by the NBTC detail procedures for type approval, required documentation, testing standards, labeling requirements, and penalties. Certification is conducted based on the NBTC website and notifications. Even cybersecurity products must comply with NBTC regulations if they possess wireless communication functions as a prerequisite for sale.

4.3.3 National Cybersecurity Strategy and Legal Framework in the Philippines

(1) National Strategy

The Philippines has positioned strengthening cybersecurity as a key national priority to establish itself as a leader in the digital domain. To create a secure digital space nationally, it formulated the National Cybersecurity Plan (NCSP 2023-2028)[30] in 2024. It advocates protecting critical infrastructure in sectors such as power, telecommunications, finance, transportation, and healthcare; safeguarding networks of public institutions, including military organizations; and securing supply chains. Furthermore, it conducts awareness and educational activities for both the public and private sectors to enable citizens to utilize digital technologies with confidence. The plan outlines the following as its primary framework:

- Enhancing Government Network Defense:
- Strengthening defenses for the Government Network (GovNet) through the introduction of IDS/IPS, secure BGP, and passive elements to protect over 3,900 national and local agencies. Additionally, through the reorganization of the Cybersecurity Bureau, we will strengthen the National Computer Emergency Response Team (NCERT) and establish a new National Security Operations Center (NSOC). This will enable the creation of a “National Cyber Threat Database” cataloging threat types, vulnerabilities, and countermeasures. Concurrently, we will collaborate with private sector entities to enhance network segmentation protection.
- Cybersecurity Talent Capacity Building

[28] Department of Trade Negotiations (DTN), Ministry of Commerce, Thailand กรมเจรจาการค้าระหว่างประเทศ | Department of Trade Negotiations

[29] Thai Ministry of Digital Economy and Society The Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services, B.E. 2553（2010）

[30] Philippine Department of Information and Communications Technology (DICT) NCSP 2023-2028 - FINAL-DICT

Designate October as "Cybersecurity Awareness Month," with all ministries and agencies conducting cyber hygiene activities. Advance advanced education and research through the reestablishment of the ICT Academy and the Cybersecurity Center of Excellence. Update occupational classifications, establish qualification standards, and promote the recognition of industry certifications as public service qualifications. Foster talent through scholarships, international training programs, and participation in domestic and international hackathons.

- Establishment of Cross-Agency Policy Framework
  Strengthen the National Cybersecurity Inter-Agency Committee (NCIAC) as a cross-agency coordination body to facilitate policy alignment and dispute resolution. Advance a presidential order for Critical Information Infrastructure (CII) protection, support legislation for mandatory incident disclosure and protection of security researchers, expand bilateral and multilateral international cooperation, and incorporate international standards.

To achieve the above three items, NCSP has explicitly outlined the following six items as its main pillars.[31]

- Enactment of the Cybersecurity Act:
  Focuses on strengthening the legal system and policy framework for cybersecurity, aiming to establish clear laws and regulations to protect against online threats.
- Protection and Defense of Critical Information Infrastructure (CII):
  Efforts to safeguard critical systems such as power grids, financial services, and transportation from cyberattacks. Includes measures like vulnerability assessments, incident response plans, and cybersecurity certifications. Examples include mandating cybersecurity audits for banks and requiring critical infrastructure operators to implement and maintain intrusion detection systems.
- Proactive Defense in Cyberspace:
  This emphasizes the importance of taking preemptive action against threats rather than reacting passively. It includes measures to identify and prevent threats before damage occurs. A key element of this pillar is the establishment of a National Cybersecurity Operations Center to support monitoring and incident response.
- Strengthening Cybersecurity Talent:
  Recognizing that effective cybersecurity requires a robust talent base, this pillar fosters an environment where experts develop skills and capabilities through scholarships and education/training via cybersecurity Centers of Excellence like Lumify Work Philippines.
- Public Cybersecurity Awareness and Education:
  To disseminate cybersecurity best practices, awareness campaigns (such as National Cybersecurity Month) and educational programs will be implemented, aiming to empower everyone to protect themselves from online threats.

[31] Philippine Department of Information and Communications Technology (DICT) Achieving Cyber Resilience via the National Cyber Security Plan | Lumify Work Philippines

Figure 4. NCSP 2023-2028 Results Framework

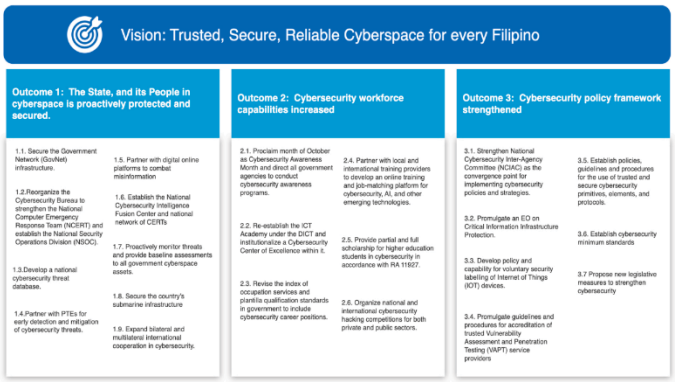


Figure 7 Framework of the Philippine National Cybersecurity Plan (NCSP) 2023–2028

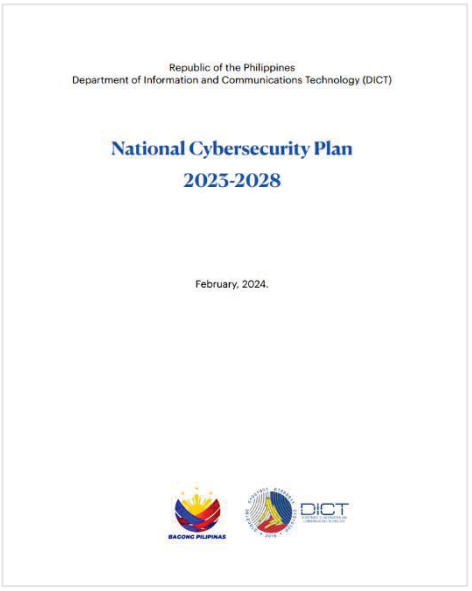


Figure 8 Philippine National Cybersecurity Plan (NCSP) 2023–2028

(2) Legal Regulations

A) Cybercrime Prevention Act of 2012, Republic Act No. 10175[32]

i. Overview

This Act provides the legal framework for preventing and prosecuting crimes in cyberspace. It defines illegal access, data interference, and system interference as cybercrimes and establishes the basis for operational cooperation and enforcement. It is positioned as the fundamental law for addressing online misconduct. In practice, it is used in conjunction with other laws such as the E-commerce Act (RA 8792) and also serves to complement cybercrime responses to online services by both public and private entities.

ii. Definition of Critical Information Infrastructure

Article 3 of this Act explicitly defines critical information infrastructure as computer systems and assets (including physical and virtual) that are essential for the continuity of services vital to the functioning of society and the economy, and whose disruption or destruction could have a significant impact on national security, the economy, or public safety and health.

iii. Relevant Critical Information Infrastructure Sectors

This Act does not list specific industry sectors that qualify as CIIs. Instead, Article 3 comprehensively covers fields providing services essential to society and the economy. Which sectors qualify as CIIs is determined based on the criterion of whether the systems or assets in that field, if stopped or destroyed, would cause "serious impact" on national security, the economy, or public safety and health. Thus, sectors of high public importance and criticality are targeted. Meanwhile, Article 3 of the Law on the Prevention, Prohibition, and Punishment of Terrorism (Republic Act No. 11479) [33] states that critical infrastructure includes, but is not limited to, assets or systems affecting telecommunications, water and energy supply, emergency services, food security, fuel supply, banking and finance, transportation, radio and television, information systems and technology, and chemical and nuclear sectors.

B) Legal Regulations to Note for Sales in the Relevant Country

i. Data Privacy Act, Republic Act No.10173 : DPA[34]

[32] The Official Gazette Republic Act No. 10175 | Official Gazette of the Republic of the Philippines

[33] The LAWPHil Project Republic Act No. 11479

[34] National Privacy Communication Republic Act 10173 - Data Privacy Act of 2012 - National Privacy CommissionNational Privacy Commission

Enacted in 2012, the Philippines' DPA establishes a strict compliance framework not only for entities processing personal information within the Philippines, but also for processing using domestically located equipment and for processing the personal information of Filipino citizens. This aims to protect individual privacy while ensuring the free flow of information for innovation and growth. While certain exemptions apply when processing information collected abroad under foreign laws within the Philippines, obligations for information security measures are imposed on the domestic portion. The DPA establishes "transparency," "legitimate purpose," and "proportionality" as fundamental principles of processing, requiring compliance with these principles. As cybersecurity products are critical tools supporting compliance with these laws, key points for sales include explaining DPA-compliant features, confirming local regulations, and supporting customer compliance.

ii. Export-Related Regulations

Regarding the export of cybersecurity products to the Philippines, the primary Philippine regulations applicable are as follows.

(3) NTC Certification[35] :

All electronic devices utilizing telecommunications equipment and wireless communications require approval from the National Telecommunications Commission (NTC). This ensures they do not adversely affect other electronic devices or communication networks within the Philippines (Electromagnetic Compatibility: EMC) and comply with technical standards. This applies to many electronic devices, including telecommunications equipment, wireless devices, Bluetooth devices, and radio frequency-based wireless equipment, requiring prior verification.[36]

(4) Import Permit:

Certain cybersecurity products may require an Import Permit or prior registration.

4.4. Information on Japanese Products and Overseas Expansion Status

For cybersecurity products and services offered in Japan, information as of July 2025 was collected, primarily from company websites, focusing on products and services deemed useful for developing countries (for governments and critical infrastructure). This survey item was structured into three categories: "Company Information," "Product/Service Information," and "Implementation Track Record with Governments or Critical Infrastructure." and "Implementation Track Record with Governments or Critical Infrastructure." Company information included headquarters location, capital, local offices, and overseas expansion status, clearly indicating the company's business foundation and regions of operation. Product/service information organized delivery methods, multilingual support, key functions, and features, detailing specific service contents. Implementation track record documented cases of adoption by government agencies and critical infrastructure operators.

Table 4 Survey Items for Japanese Cybersecurity Companies and Products

Category	Survey Item	Summary Description
Company Information	Company Name	Name of the company providing the product/service
	Headquarters Location	City/region where the company's headquarters is located
	Capital	Capital amount of the company; serves as a benchmark for company scale and business
	Company Overview	Brief introduction of the company's industry, main business content, and features

[35] National Telecommunication Commision National Telecommunications Commission - National Capital Region
[36] National Telecommunication Commision Wireless Data Networks And Devices

Category	Survey Item	Summary Description
	Company URL	Official website URL of the company
	Legal Entity Type	Legal entity type of the company (e.g., Japanese corporation, overseas corporation)
	Local Bases	Presence and locations of bases in the target survey region.
	Overseas Expansion Record	Presence of overseas business development and achievements
	Overseas Expansion Record (Region-wise)	Status of development by region (e.g., Thailand, Indonesia, etc.)
	Overseas Expansion Record Sources	Sources and URLs related to overseas expansion records
	Notes	Other special notes or additional information
Product/Service Information	Product/Service Category	Product/service category (e.g., monitoring, web server protection, access control)
	Product/Service Name	Official name of the product/service
	Product/Service Overview	Brief explanation of the main functions and features of the product/service
	Delivery Method	Delivery format (e.g., cloud-based, on-premises, hybrid, etc.)
	Multilingual Support Languages	Presence or absence of multilingual support and supported languages
	Product URL	Product or service website URL
Government/CII Introduction	Government Implementation Record	Representative implementation cases and case studies for government agencies
	Critical Infrastructure Implementation Record	Representative implementation cases for critical infrastructure sectors (e.g., electricity, gas, water, transportation, communications)

Based on the above survey items, we conducted research on cybersecurity products and services offered within Japan. As a result, we collected information on 315 products and services from 63 companies in total, compiling them into a long list. Security vendors operating in Japan provide products and services across diverse fields, including network monitoring, endpoint protection, web application protection, access management, authentication and identity management, vulnerability assessment, data protection, and IoT security. Furthermore, multiple delivery models exist, including cloud-based, on-premises, and hybrid, catering to a wide range of needs regardless of company size or industry. Additionally, numerous operational support services are available, such as threat intelligence, cyber exercises, CSIRT operational support, penetration testing, security consulting, and education/training. Multilingual support and the establishment of overseas offices are progressing, building a framework to serve both Japanese and international customers.

(1) Characteristics of Corporate Information

Security vendors operating in Japan include a mix of major Japanese IT companies, specialized vendors, and foreign-affiliated global enterprises. Their capitalization and corporate structures vary significantly. Regarding overseas expansion, numerous examples of establishing bases or forming local partnerships have been confirmed across the globe, including ASEAN countries (Singapore, Thailand, Vietnam, Indonesia, Philippines, etc.), North America, Europe, the Middle East, and Africa. A key characteristic is that many companies have established service delivery frameworks not only for the Japanese market but also for the global market through multilingual support, establishing local subsidiaries, and partner agreements.

(2) Technical Features of Products and Services

Many products and services were identified as addressing advanced domains such as integrated monitoring (SOC, SIEM), endpoint defense (EDR/XDR), zero trust, cloud security, threat intelligence, SASE,[37] ASM, and AI/automation technologies. These products predominantly reflect the latest technological trends, including threat detection and operational efficiency through AI and automation, cloud-native security, sandbox-based threat analysis, authentication and identity management via API integration, and IoT security design. They are characterized by a wide range of delivery models—cloud-based, on-premises, and hybrid—enabling flexible implementation tailored to company size and industry. Additionally, operational support services are robust, including vulnerability assessments, penetration testing, cyber exercises, CSIRT operational support, security consulting, and education/training. This comprehensive support extends beyond mere product sales to strengthen overall operational frameworks.

(3) Characteristics of Implementation Records in Government and Critical Infrastructure

Numerous cases were confirmed where products and services from many vendors have been implemented in government agencies, local governments, critical infrastructure such as power, gas, water, and transportation, financial institutions, and educational institutions. Implementation is particularly prominent in government agencies and critical infrastructure for areas such as integrated monitoring (SOC, SIEM), EDR/XDR, Zero Trust, WAF, CASB, DDoS countermeasures, and authentication/ID management. These implementation records demonstrate that security services are widely utilized as a foundation for ensuring the safety of social infrastructure and countering cyberattacks. A key characteristic is the progress of adoption across a broad range of public and critical infrastructure sectors, regardless of region or industry.

4.5. Interviews with Candidate Companies for Verification of Japanese Corporate Products

Based on the long list, preliminary interviews were conducted from late July to early August 2025 with nine companies possessing cybersecurity products/services in Japan and having a presence in the ASEAN region or expressing interest in international expansion. These interviews confirmed each company's business activities, track record and willingness for local expansion, budgetary challenges, and the existence of local connections. The interviews revealed concerns regarding costs within the budget allocated for this survey, as well as variations in the strength of local sales structures among the companies. A summary of the interview results is provided below.

4.5.1 Amiya Corporation

(1) Company Overview

Amiya Corporation[38] (hereinafter referred to as Amiya) is a company primarily focused on the security, information and communications, and software fields. It has 202 employees (as of December 2025, including temporary staff and contractors) and a capital of 62.47 million yen (as of September 2025). Established in December 1996, the company is headquartered in Chuo Ward, Tokyo. Its core business involves the development and sales of security solutions, including the integrated log management product “ALog”.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

ALog[39] is an integrated log management (SIEM[40]) product featuring proprietary log translation technology and AI-powered anomaly detection. It automatically collects logs from diverse IT systems, enabling easy management and analysis without requiring specialized knowledge. With over 6,000 deployments in Japan and overseas combined, it boasts the top market share in Japan's domestic SIEM sector.

[37] Secure Access Service Edge: A new architecture that integrates network functions and security functions in the cloud.
[38] Amiya Company Overview | Corporate Information | AMIYA Corporation.
[39] Amiya ALog Series | Services | AMIYA Corporation.
[40] SIEM (Security Information and Event Management) is a system designed to centrally aggregate logs and data output from firewalls, IDS/IPS, proxies, and other sources. By combining and performing correlation analysis on this data, it aims to monitor networks and detect incidents such as cyberattacks and malware infections.

Key features include: ① Automation (automatic collection regardless of on-premises/cloud deployment, extensive templates/plugins), ② AI-powered log mapping (flexible adaptation with only time format definition, automatic regular expression extraction), ③ Alert notifications & report analysis (automatic reports via template selection, instant alerts[41]), ④ AI risk scoring[42] (automatic analysis of deviations from normal patterns to score risk levels), ⑤ Patented translation/conversion logic (converts logs for readability, accuracy, and compactness, compressing data size to 1/200th), ⑥ Low cost (billed based on post-conversion data size, significantly cheaper than Western competitors), ⑦ Agentless approach[43] (deployable without burdening existing systems), ⑧ Support for diverse communication protocols (SMB[44], SSH[45], Syslog[46], WebAPI[47]).

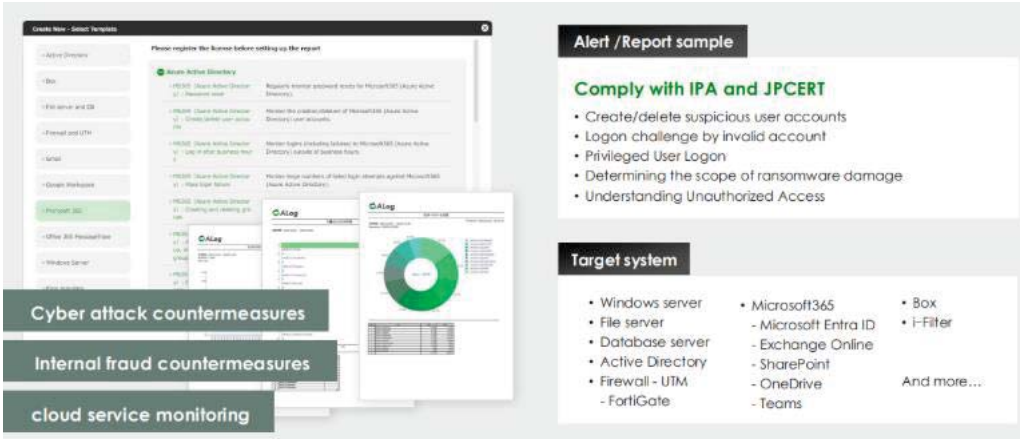


Figure 9 Image of Alert Notification and Report Analysis by Alog

(3) Status of Overseas Business Expansion

We are expanding our business primarily in ASEAN (Thailand, Vietnam, Singapore, Malaysia, Indonesia), as well as in Taiwan, China, the UK, and the US. We establish bases through local agents and partners, and have also established local technical support systems. In ASEAN countries, we have a track record of implementation with major infrastructure operators, including deliveries to Malaysian government agencies, a major Indonesian automotive company, and major Taiwanese financial institutions and government agencies. Overseas sales have steadily increased: 57 transactions in 2022, 64 transactions in 2023, and 72 transactions in 2024.

4.5.2 Internet Initiative Japan Inc.

(1) Company Overview

Internet Initiative Japan Inc.[48] (hereinafter referred to as IIJ) is a company primarily engaged in the telecommunications industry, with 5,221 employees (as of 2025, consolidated) and capital of ¥23,037 million (as of 2025). Established in December 1992, its headquarters are located in Fujimi, Chiyoda-ku, Tokyo. Its business activities encompass a wide range of services, including Internet access

[41] An alert is a warning message that notifies the responsible personnel when the system detects an abnormality or risk.
[42] A system that uses technologies such as AI to quantify (score) the risk level of detected events and operations, extracting and notifying high-priority risks.
[43] Agentless monitoring is a method of collecting information using standard communication protocols (e.g., SMB, SSH, Syslog) without installing dedicated software (agents) on the monitored systems.
[44] This is a communication protocol for sharing files, printers, and other resources between computers running Windows and other operating systems. It is also used for log collection.
[45] SSH (Secure Shell) is a communication protocol for securely performing remote access and data transfer over a network, primarily used for collecting logs from Linux systems and network devices.
[46] Syslog (System Logging Protocol) is a standard communication protocol for sending log information from network devices and servers. It is supported by many devices and is used for automating log management.
[47] An API (Application Programming Interface) is a mechanism that enables software to exchange functions and data. It is used for tasks such as retrieving logs from cloud services.
[48] IIJ Corporate Data | About IIJ | IIJ.

services, WAN services, and network-related services; network and system construction, operation, and maintenance; and the development and sale of telecommunications equipment.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

Safous Privileged Remote Access[49] is software that provides integrated secure remote access and privileged account management for critical internal and industrial systems. Unlike traditional VPNs (Virtual Private Networks), it significantly enhances security levels by verifying users and devices each time based on zero-trust communication over the internet, granting access to business systems with the minimum necessary privileges. Recent large-scale ransomware attacks are said to stem from two primary causes: exploiting VPN vulnerabilities and the leakage or misuse of privileged accounts. Safous achieves an approach that simultaneously mitigates these two major risks.

Key features include: ① Zero-Trust Architecture (a mechanism that "constantly verifies" users and devices without relying on VPNs), ② Secure Management of Privileged Accounts (protecting passwords in a Vault, temporarily issuing permissions when needed, and automatically revoking them afterward), ③ Agentless Connectivity (secure access via web browser without installing dedicated software on user devices), ④ Multi-Factor Authentication (MFA), ⑤ Least Privilege Access Control (pre-registering which systems users can access, the scope of operations permitted, the time periods allowed, and required approvals), ⑥ Session Recording and Auditing (recording video and logs of who performed what actions on which systems and when).

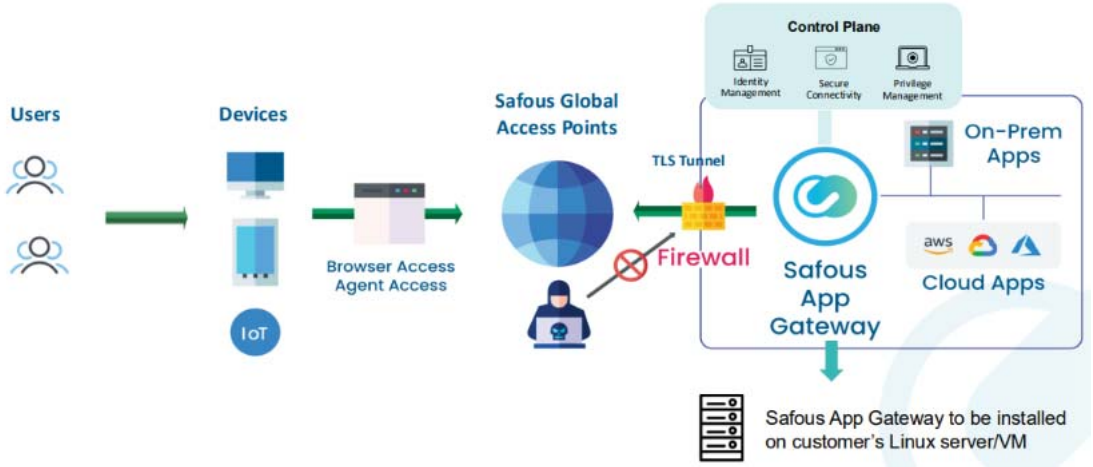


Figure 10 Overview Image of Safous Privileged Remote Access

(3) Status of Overseas Business Expansion

We are expanding our business operations in ASEAN (Thailand, Indonesia, etc.). Our presence is established through local agents and partners, with local technical support systems also in place. We have a track record of deployments with critical infrastructure operators across ASEAN countries, including deliveries to Thailand's National Research Institute, a major Indonesian financial institution, and an Indonesian food manufacturing company. Overseas sales and deployments of Safous Privileged Remote Access have reached a total of approximately 2,500 licenses. Going forward, the company plans to expand the introduction of security products into IT/OT hybrid environments according to local needs.

4.5.3 Macnica, Inc.

(1) Company Overview

Macnica, Inc.[50] (hereinafter referred to as Macnica) is a technology trading company dealing in

[49] IIJ IIJ Safous 特権リモートアクセス - ゼロトラストセキュリティに基づいたセキュアアクセスサービス (in Japanese)
[50] Macnica Company Profile - Company Information -Macnica.

semiconductors, electronic components, cybersecurity, and related fields. As of March 2025, it has 5,071 employees and a capital of ¥11,194,260,000. Founded in 1972, its headquarters are located in Yokohama City. Its core business involves the import, export, sales, development, and processing of electronic components such as semiconductors and integrated circuits, as well as the development, import, export, and sales of electronic equipment and their peripheral devices and accessories.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

Macnica ASM[51] (Attack Surface Management) is a service that identifies and assesses externally exposed assets from an attacker's perspective using publicly available information on the internet. This service is conducted using a "passive scanning method" (a method that investigates based on publicly available information without directly placing a load on the target system).

The service delivery flow is as follows. First, in ① Domain Investigation, we extract and discover not only officially published domains but also related domains unknown to the organization. This is achieved by specifying keywords such as registrant names, email addresses, and phone numbers, and leveraging open-source data like reverse Whois and certificate information. Next, in ② Subdomain, FQDN, and IP Investigation, we broadly explore externally exposed systems—such as subdomains and IP addresses—starting from the discovered domains. Finally, ③ Risk investigation identifies vulnerabilities present in the discovered assets. Using known vulnerability databases and patent-pending technologies, it verifies the services and products running on each IP, along with open ports, to uncover vulnerabilities exploitable from outside. The main features are the following three points.

A) Comprehensive Discovery of Publicly Exposed Assets: Utilizing OSINT (Open Source Intelligence) to identify assets publicly available on the internet through both automated and manual methods
B) Noise Removal and Accuracy Improvement: Analysts visually verify and exclude third-party assets and false positives (noise) introduced during extraction to create the final list
C) Attacker-Perspective Risk Assessment: Analysts identify and notify critical vulnerabilities (high-severity vulnerabilities) among those discovered for the assets. These are vulnerabilities most likely to directly lead to major incidents (events causing damage), such as ransomware attacks.

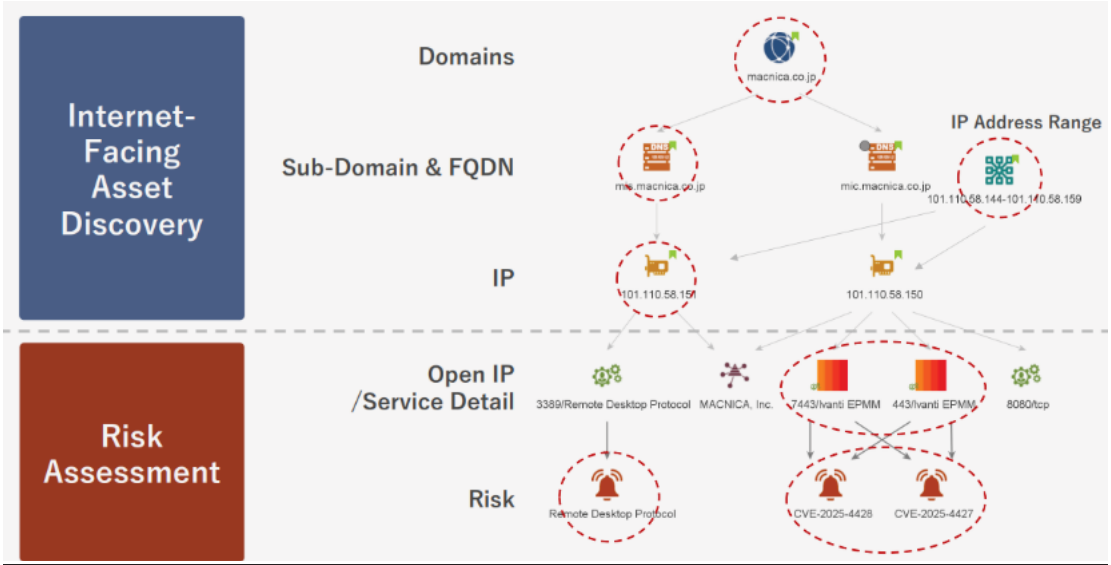


Figure 11 Image of Macnica ASM Investigation Process

(3) Status of Overseas Business Expansion

Macnica ASM has been implemented at approximately 60 companies in Japan, including critical

[51] Macnica Macnica Attack Surface Management - Security Business -Macnica

infrastructure providers, but as of December 2025, it has no implementation track record with overseas companies. The group has connections to ASEAN countries (including Thailand, the Philippines, and Indonesia) and has overseas subsidiaries in Singapore, China, Taiwan, South Korea, Hong Kong, the United States, the United Kingdom, Brazil, India, and Thailand.[52] While expanding sales channels in collaboration with group companies, the product domains and offerings vary by local subsidiary. Furthermore, within the cybersecurity distribution business, the local subsidiary Netpoleon Solutions Pte Ltd. possesses strong connections in Thailand, the Philippines, and Indonesia—the target countries for this initiative.

4.5.4 Trend Micro Inc.

(1) Company Overview

Trend Micro Inc.[53] (hereinafter referred to as Trend Micro) is a cybersecurity company that develops and sells security-related products for computers and the Internet. It has 6,869 employees (as of December 2024) and a capital of ¥19,926 million (as of December 2024). Founded in October 1989 by Taiwanese entrepreneurs, its headquarters are located in Shinjuku Ward, Tokyo. Its primary business is the development and sale of security-related products and services for computers and the internet.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

Deep Discovery Inspector (DDI)[54] is a security appliance that visualizes threats lurking within an organization's internal network and detects suspicious communications such as targeted attacks and information-stealing malware. DDI performs behavioral analysis based on communication packet information, featuring capabilities such as detecting suspicious behavior and applications of concern on the network, identifying connections to C&C servers, and performing dynamic file analysis via sandboxing. In a typical deployment, a mirror port is configured on the core switch, allowing DDI to analyze a copy of the traffic passing through the core switch. This minimizes deployment effort and reduces network impact in the unlikely event of a DDI failure.

DDI feeds detection information back to Trend Micro's managed cloud console, enabling integrated management with logs from other solutions. This contributes to visualizing the full attack picture and reducing customer management and operational burdens. Additionally, Trend Micro offers Trend Service One Complete, a solution operation support service provided by security analysts, which includes monitoring of the cloud console. If customers cannot upload detection status to the cloud console due to their circumstances, they can log into the DDI and directly check the console to view detection information. In this case, on-site visits can be made to access the console, allowing for detailed support and rapid response while directly confirming the situation.

(3) Status of Overseas Business Expansion

Indonesia, Thailand, and the Philippines, which are target countries for the survey, have Trend Micro sales offices with sales representatives and engineers stationed there. In countries with sales offices, there is a track record of selling solutions including DDI, and these are often deployed primarily to government agencies and critical infrastructure operators (mainly financial institutions) in those countries. Furthermore, the sales model follows the same licensing structure overseas as in Japan, where the first year's software usage fees and hardware support are included as a package upon new purchase. From the second year onward, continued use is possible by paying the DDI software renewal fee.

4.5.5 SYNCHRO Inc.

(1) Company Overview

[52] Macnica Location Information - Company Information -Macnica
[53] Trend Micro 会社概要 | トレンドマイクロ (JP) (in Japanese)
[54] Trend Micro Deep Discovery™ Inspector | トレンドマイクロ (JP) (in Japanese)

SYNCHRO Inc.[55] (hereinafter SYNCHRO) is a company primarily focused on manufacturing and cybersecurity product development. As of January 2026, it has 38 employees and capital of ¥315.17 million. Established in April 2001, its headquarters are located in Chiyoda Ward, Tokyo. Specific business activities include: ① Manufacturing, sales, installation, and maintenance of access control systems centered on the "VPII" series of back-of-hand vein authentication systems; ② Embedding, development, sales, and maintenance of the proprietary IP networking technology "KATABAMI" for various IoT devices; ③ Planning, design, development, and maintenance of solution systems differentiated by total access control from both physical and cyber spaces using ① "VPII" and ② "KATABAMI", based on one-stop engineering practices, and the construction of secure next-generation service platforms.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

The KATABAMI series[56] is a line of Japanese developed cybersecurity products created by SYNCHRO, primarily consisting of the following four products: ① KATABAMI VDP dawn automatically discovers connected devices on a network when installed on inexpensive hardware. ② KATABAMI VDP performs remote vulnerability assessments within office networks (LANs). ③ KATABAMI Isolator safely isolates devices from the network that cannot be patched but must remain operational for business purposes. ④ KATABAMI CRA stores data by establishing communication paths impervious to ransomware intrusion.

Vulnerability Assessment Service ② KATABAMI VDP and its accompanying countermeasure recommendations are characterized by "individualized problem-solving" that goes beyond theoretical generalizations, providing reports based on actual assessments of the target company. The assessment report is created based on the "Common Vulnerability Scoring System (CVSS) v3 Overview" from FIRST (Forum of Incident Response and Security Teams), a globally recognized standard for vulnerability assessment. Furthermore, by individually explaining countermeasures for each vulnerability, it contributes to raising awareness and building security knowledge within the target company. Additionally, storing backup data that can be listed in the event of a cyberattack, such as ransomware, in a remote location (on a separate network, not via VPN) is an effective countermeasure. This service is already available in Japan as ④KATABAMI CRA.

(3) Status of Overseas Business Expansion

In Japan, we have implemented our system in 20 cases, including critical infrastructure sectors such as nuclear-related organizations and newspapers. Overseas sales and implementation achievements include one case with a system development company in Vietnam. Going forward, we aim to expand our business by strengthening partnerships with local critical infrastructure operators in ASEAN. For example, we have connections at the management level with entities such as disaster countermeasure research centers and power plants in Indonesia, and industrial equipment switch manufacturers in the Philippines.

4.5.6 GMO Cybersecurity by Ierae, Inc.

(1) Company Overview

GMO Cybersecurity by Yellare Inc.[57] (hereinafter referred to as GMO) primarily operates in the information and communications industry, with 302 employees (as of 2025) and capital of 100 million yen (as of 2025). Established in February 2013, its headquarters are located in Shibuya Ward, Tokyo. Its main businesses include vulnerability assessments (cybersecurity assessments), penetration testing, security incident/forensics response support, security training/certification support, SOC, security consulting, and the development/operation of the ASM/vulnerability assessment tool "GMO Cyber

[55] SYNCHRO 会社概要・沿革・アクセス – 株式会社 SYNCHRO (in Japanese)
[56] SYNCHRO KATABAMI – 株式会社 SYNCHRO (in Japanese)
[57] GMO 会社情報 | 脆弱性診断（セキュリティ診断）の GMO サイバーセキュリティ by イエラエ (in Japanese)

Attack Net de Diagnosis" and the automated WAF operation service "GMO Cybersecurity WAF Aid," as well as the development/operation of the price survey tool "Price Search." and operation of the ASM/vulnerability assessment tool "GMO Cyber Attack Net de Diagnosis," development/operation of the automated WAF management service "GMO Cybersecurity WAF Aid," and development/operation of the price survey tool "Price Search."

(2) Products with Overseas Expansion Potential and Their Features/Advantages

GMO Cyber Attack Net de Diagnosis ASM[58] is an Attack Surface Management (ASM) tool. It automatically and continuously discovers and identifies an organization's assets exposed on the internet (IP addresses, domains, subdomains, web applications, network devices, etc.), aiming to detect and manage vulnerabilities and misconfigurations. Compared to traditional manual inventory management and spot diagnostics, ASM enables the discovery of risks ahead of attackers through automation and continuous monitoring.

Key features and advantages include: ① Automatic external asset discovery (automatically crawls publicly accessible assets on the internet, enabling detection of assets unknown to the organization), ② Vulnerability and risk assessment (performs vulnerability scans on detected assets, classifies them based on international standards (CVE, CVSS scores), assigns priorities, and provides remediation guidance), ③ Continuous monitoring (detects new exposed assets or configuration changes through regular automated monitoring (weekly/monthly) and provides real-time alert notifications), ④ Reporting and remediation guidance (provides detailed reports on detected vulnerabilities and recommended corrective actions), ⑤ Addressing talent shortages (Enables efficient asset management through ASM automation, even for organizations lacking specialized personnel).

(3) Status of Overseas Business Expansion

Within Japan, we have a proven track record of providing services to over 30 major infrastructure companies, primarily in the information and communications and financial sectors. We have also expanded overseas to Ulaanbaatar, Mongolia. Aiming to expand our business into ASEAN, we maintain top-level connections with companies and government agencies in Indonesia, Thailand, and the Philippines, the countries covered in this survey.

4.5.7 Yamaha Corporation

(1) Company Overview

Yamaha Corporation[59] (hereinafter referred to as Yamaha) is a company primarily engaged in the fields of musical instruments, audio equipment, and related services. Its consolidated employee count is 18,949 (as of 2025), and its capital is ¥28,534 million (as of 2025). Founded in 1887 and established in October 1897, the company is headquartered in Hamamatsu City, Shizuoka Prefecture. It provides over 100 types of musical instruments worldwide, ranging from educational instruments like recorders and pianicas to pianos, guitars, drums, and violins. Additionally, within its network equipment business, it offers and develops products and services related to cybersecurity.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

Yamaha offers router products with a primary focus on security features, including UTM (Unified Threat Management) appliances and routers with security capabilities. The UTX100/UTX200 series targets small to medium-sized businesses. The UTX100 is a UTM appliance that provides all the security functions required by small businesses in a single unit.[60] It enables easy deployment with minimal setup, delivering multiple security measures at a high cost-performance ratio. Beyond the firewall functionality traditionally standard in network security devices, it incorporates application control, URL filtering, intrusion prevention (IPS), antivirus, anti-bot, and anti-spam features to counter

[58] GMO GMO サイバー攻撃ネット de 診断 ASM| GMO サイバーセキュリティ by イエラエ株式会社 (in Japanese)
[59] Yamaha Corporate Profile - About Us - Yamaha Corporation
[60] Yamaha UTX100 特長 (in Japanese)

threats like malware and targeted attacks. The security license includes support services from a dedicated manufacturer support desk, covering configuration assistance and advance replacement. It also provides unified support for combinations with Yamaha routers/switches.

The UTX100/UTX200 incorporates the highly reliable core engine from Check Point while adding Yamaha's unique functional enhancements. This pursuit of Yamaha's distinctive added value results in a product offering greater peace of mind. Currently, Yamaha's cybersecurity products incorporate Check Point's highly reliable core engine while adding Yamaha's unique functional enhancements, providing products that offer greater peace of mind. While contractual agreements utilize Check Point's technology for the core components, Yamaha pursues its own unique added value. Existing products, while lacking deployment records in critical infrastructure, are primarily used in chain store locations such as restaurants and convenience stores.

(3) Status of Overseas Business Expansion

Yamaha's cybersecurity product, the UTM appliance, is not sold overseas. Regarding Japanese sales of network products in general, due to contractual restrictions with Check Point and core engine relationships, overseas sales are not conducted. Japanese sales are handled by SCSK Corporation. Overseas, local sales subsidiaries primarily sell musical instruments and audio systems, along with some switch products (local subsidiaries exist in Indonesia, Singapore, Thailand, the Philippines, Vietnam, Malaysia, Asia, Oceania, North America, Central and South America, Europe, and the Middle East). Regarding future overseas expansion, aside from SCSK Corporation launching select router products in Indonesia, while connections exist with overseas subsidiaries selling musical instruments, no specific plans have been announced.

4.5.8 SCSK Corporation

(1) Company Overview

SCSK Corporation[61] (hereinafter referred to as SCSK) is a specialized subsidiary of the SCSK Group focused on cybersecurity measures, with capital of 50 million yen (100% owned by SCSK Corporation). Established in August 2023, it is headquartered in Koto Ward, Tokyo. Its core businesses include security service development and sales (consulting, vulnerability diagnosis/assessment, training, etc.) and security product sales.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

SCSK excels in product implementation, consulting, and analysis services. In addition to Japanese cybersecurity products, it distributes overseas products as an authorized reseller. BIG-IP (Advanced) Web Application Firewall[62] (hereafter BIG-IP ASM (Application Security Manager)), sold as an agent for F5 Networks, is a Web Application Firewall (WAF) that monitors traffic on ports used by web servers, protecting web applications and the data behind them from malicious users. Web applications with input forms often contain vulnerabilities to some degree. While vulnerability assessments can identify security holes and allow for application fixes, this approach may not be practical in terms of cost and time when dealing with numerous applications. BIG-IP ASM addresses this challenge by deploying in front of the web server. It blocks requests targeting vulnerabilities, protecting the application and the data behind it. Furthermore, when combined with the “SCSK WAF Implementation and Operation Support Service,” based on SCSK's extensive WAF implementation experience and expertise, it enables optimal policy tuning for each site, supporting the construction of more robust web systems.

As part of our track record in deploying critical infrastructure solutions in Japan, we provide services to government agencies and electric power companies. Specifically, we build and deliver SIEM solutions such as Trend Micro's TippingPoint (IPS) and Splunk for government agencies in Japan, and IBM's QRadar for Japanese electric power companies.

(3) Status of Overseas Business Expansion

[61] SCSK 企業情報 – SCSK セキュリティ株式会社 (in Japanese)

[62] SCSK オンプレミス型 WAF「F5 BIG-IP ASM」概要 – SCSK セキュリティ株式会社 (in Japanese)

The SCSK Group maintains an overseas network spanning the United Kingdom, Germany, China, Singapore, Indonesia, Myanmar, and the United States, with a particular strength in providing on-site customer support. Within ASEAN countries, the Group established its overseas subsidiary in Jakarta, Indonesia (SCSK Global Indonesia was founded in 2019).

4.5.9 KDDI Corporation

(1) Company Overview

KDDI Corporation[63] (hereinafter referred to as KDDI) is a major integrated telecommunications company primarily engaged in the telecommunications business. As of March 2025, it had approximately 64,636 employees and a capital of ¥141,852 million. Established in June 1984, its headquarters are located in Chiyoda-ku, Tokyo. Its core businesses include providing mobile phone services under the "au" brand, leased lines, internet service provider (ISP) services, fixed-line telephone services, and satellite phone services.

(2) Products with Overseas Expansion Potential and Their Features/Advantages

KDDI provides operation and monitoring services utilizing commercially available security products. Specifically, through its "KDDI Managed Security Service,[64]" it leverages an automated analysis engine incorporating KDDI's log analysis infrastructure and the expertise of LAC, a KDDI group company specializing in information security. This service delivers the security monitoring and operations essential for a zero-trust environment. By consolidating access to the log analysis platform, security personnel, and operational expertise, organizations can implement zero-trust security without preparing new monitoring systems or human resources. Real-time log analysis and detection operates 24/7/365, analyzing logs and detecting threats in real time, notifying customers of critical alerts. For particularly critical alerts, security analysts provide additional analysis and countermeasure support. Accurate support is also available through an English-language contact point for inquiries from overseas. After implementation, the dashboard provides real-time, intuitive visualization of the security situation through AI analysis and reporting powered by generative AI. This makes it easy to identify endpoints and users with high alert counts. Furthermore, generative AI automatically creates summary reports for specified periods. Both displayed alert information and summary reports can be downloaded at any time, enabling effortless utilization for creating security reports.

(3) Status of Overseas Business Expansion

The group maintains bases in countries across Asia, Oceania, Europe, the Middle East, Africa, North America, and South America. Within the ASEAN region, it has local bases in Cambodia, Indonesia, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam, maintaining strong connections with telecommunications infrastructure providers and power companies in these countries

4.6. Selection Process for Products and Services to Conduct Proof of Concept Projects

4.6.1 Selection Method for Products and Services to Conduct PoC Projects

On August 7, 2025, the public offering guidelines were sent to the9companies that participated in the preliminary interviews, with an application deadline of August 26. The selection of products and services for the PoC project was open to corporations possessing cybersecurity products and services within Japan, and demonstrating both the desire and track record for overseas expansion.

The solicitation guidelines specified Thailand, Indonesia, and the Philippines as the target countries. One organization per country was selected from government-related entities or critical infrastructure operators as the PoC site. The PoC projects were scheduled to be conducted from September 2025 to January 2026. The guidelines required adjustments and improvements to the PoC methods based on local conditions and needs, as well as verification of the effectiveness and sustainability of the products and services from multiple perspectives, including data protection and privacy compliance, integration with local

[63] KDDI Corporate Information | KDDI CORPORATION

[64] KDDI KDDI マネージドセキュリティサービス｜マネージド・アウトソース/ゼロトラスト｜法人向け｜KDDI 株式会社 (in Japanese)

infrastructure, operational feasibility, and ease of technical acquisition. Furthermore, it was a requirement to submit a report detailing the results of the PoC and verification.
The selection policy designated Japanese corporations possessing sufficient technical capabilities and operational capacity in the cybersecurity field, along with organizational structures capable of completing the project within the designated period, as candidates for subcontracting. Furthermore, considering the results of the aforementioned "4.4 Interviews with Candidate Companies for the PoC of Domestic Japanese Products," and given the nature of the PoC project, it was judged that placing heavy emphasis on price competition could lead to a decrease in participating companies. Therefore, after consultation with JICA, a policy emphasizing "selection based on quality" was adopted.
The screening criteria comprehensively evaluated and assessed the following: eligibility for application, suitability for the implementation objectives (alignment with the survey objectives), potential contribution to solving the issues (effectiveness of the proposed products/services against local challenges), validity and feasibility of the PoC plan (specific approach, schedule, structure, and presence of local connections), and reasonableness of the cost estimate. Furthermore, since the difficulty of establishing local connections and organizational structures varies by company, a system was adopted allowing each company to select its preferred country. Evaluation and selection were conducted separately for each country applied for.

4.6.2 Selection Process for Subcontractors Conducting PoC Projects

During the application period, application materials were received from 6 out of 9 companies. Subsequently, the investigation team and JICA conducted evaluations of the applicant companies. The review comprehensively evaluated each company's proposal based on the following criteria: whether the proposal aligns with the project's objectives and local challenges; whether the proposed products/services are effective and can deliver impact on local challenges; whether the PoC plan, schedule, and organizational structure are realistic and feasible; whether connections exist with local government agencies and key infrastructure operators; and whether the cost estimates are reasonable.

Ultimately, three companies (Amiya Corporation, Internet Initiative Japan Inc., and Macnica, Inc.) were selected for participation in each country. Notification of selection was sent to each company on September 5, 2025, and confirmation of their intent to participate in the project was obtained from all companies.

- Amiya Corporation (Thailand)
- Internet Initiative Japan Inc. (Indonesia)
- Macnica, Inc (Philippines)

The primary selection criteria included high evaluations for the feasibility of the PoC plan and the established local implementation framework, the effectiveness of the products and services in addressing local challenges, connections with local government agencies and critical infrastructure operators, competitiveness, sustainability, and uniqueness in overseas markets, and the potential for market entry and social impact through this research project.

4.7. PoC Plans and Results for Products and Services

A kickoff meeting was held with the three companies selected and the survey team, during which the implementation details—such as the formulation of PoC plans in each target country, consensus building with local partners, product introduction and effectiveness measurement, and the preparation of survey reports—were coordinated. The PoC plans and results for the products and services, based on the survey reports submitted by each company, are as follows.

4.7.1 Amiya Corporation (Thailand)

（1） Target Country and Proof of Concept Product/Technology/Service

- Target Country:
  Thailand
- Name of Proof of Concpet Product/Service:
  ALog
- Overview of Product/Service (Features, Functions, Communication Flow, etc.):

ALog is a SIEM product that enables easy management of vast and complex log data collected from

diverse IT systems, even for users without specialized knowledge. This is achieved by combining Amiya's proprietary logtranslation/conversion technology with AI-based anomaly and threat detection. With over 6,000 installations, ALog holds the top share in the domestic Japanese SIEM market. Its automation features allow for automatic log collection from various environments, including cloud and on-premises systems. AI analyzes the logs, assigns risk scores, and provides instant alert notifications in case of anomalies. The patented log translation/conversion compresses and structures logs for easier viewing, significantly reducing data volume and associated costs. ALog uses an agentless architecture, minimizing impact on existing systems for safe and efficient operation.

Additionally, ALog automatically collects logs from various systems without the need for additional software, enabling real-time monitoring and immediate alerting via its dashboard. AI-driven risk detection and automated report generation streamline audits and operations, enhance security, and reduce operational burden. Key features and functions are detailed in section 4.5.1.

■ALog Functional Overview

ALog is a log management product that collects, analyzes, and stores logs from various IT systems.
It parses complex event logs (raw logs) output by hosts and converts/analyzes them into actual user operation patterns (access lo

System Image (Log Collection & Analysis)

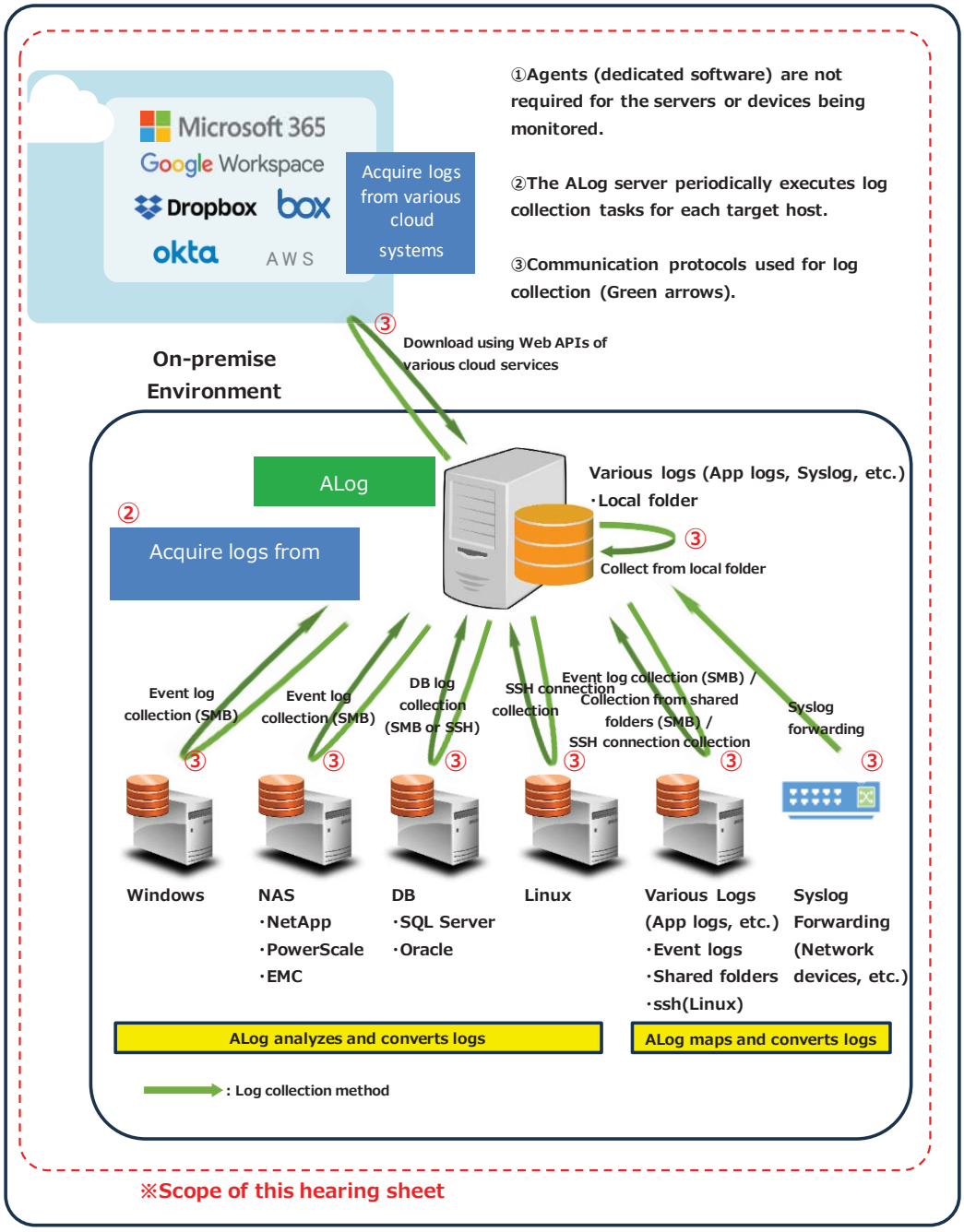


Figure 12　System Image (Log Collection/Analysis)

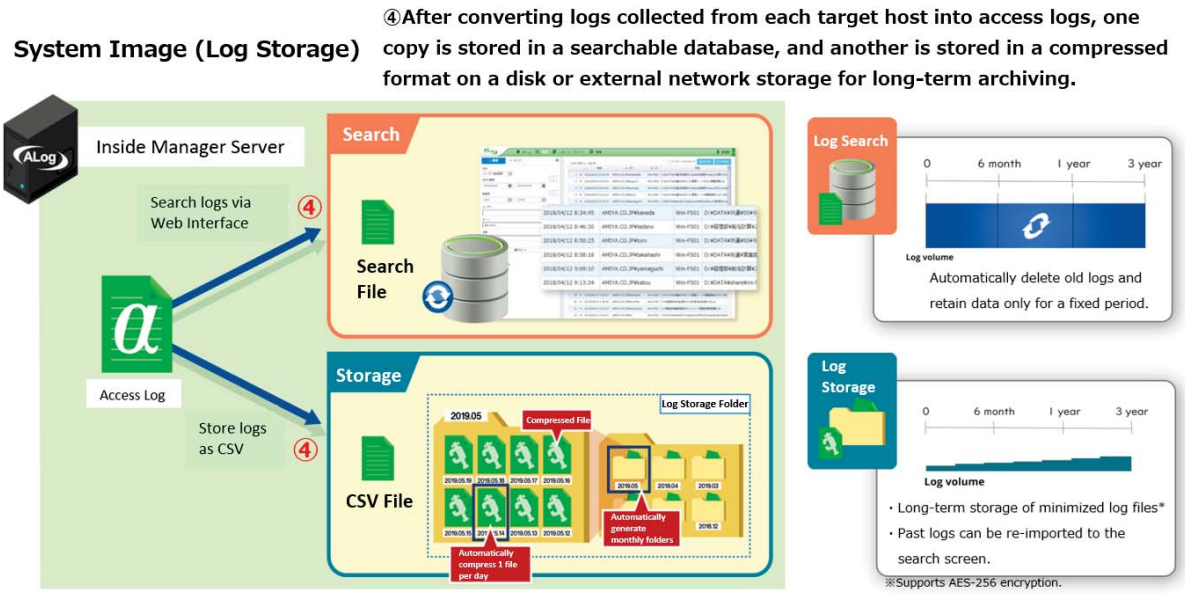


Figure 13　System Image (Log Storage)

- Effectiveness Hypotheses and Expected Outcomes (Quantitative & Qualitative / Short & Long-Term):

With the introduction of ALog, the short-term goal is zero missed detections of critical logs and a 50% reduction in alert detection time, which will be quantitatively evaluated through test scenarios measuring log accuracy and response speed. In the long-term, automating incident response is expected to halve personnel workload, improve operational efficiency by 1,080 hours annually, and increase cyberattack detection rates by over 50%. Comprehensive log collection and AI-based anomaly detection will reduce operational burden and enable faster incident response, contributing to stronger security and improved business continuity.

■Quantitative Outcomes (Short & Long-Term):

【Short-Term】

The short-term goals are zero missed detections of critical logs and a 50% reduction in both the number and average response time for alerts. Evaluation involves test scenarios such as confidential file access, privilege changes, and unauthorized logins, confirming ALog's accurate aggregation and display of logs across defined targets (OS, network devices, cloud services). Pre-deokiyment and post-deployment scenarios are compared to quantitatively assess improvements in alert response time, detection count, and the impact of false positives/negatives, thereby verifying the overall effectiveness of ALog in enhancing operational efficiency and security.

【Long-Term】

By introducing ALog, incident response previously handled by four staff members 24/7/365 can be automated, reducing required personnel by two. The average response time per alert, previously 30 minutes, can be halved through automatic judgment, reducing monthly workload from 180 to 90 hours and achieving an annual efficiency gain of 1,080 hours. Cross-system analysis, previously limited, is now possible, improving cyberattack detection rates by over 50%. Validation uses simulated attack scenarios and customer satisfaction with MDR services for quantitative measurement.

■Qualitative Outcomes

【Short-Term】

ALog enables log collection and visualization from diverse devices, requiring only time format definition. AI automatically extracts regular expression mapping candidates, making log format changes and configurations easy. The AI-powered risk scoring function analyzes data characteristics, visualizing and notifying risks such as unauthorized access or information leakage on a 10-point scale.

Deviations from normal behavior are detected early, allowing for prompt identification of cyberattack signs.

【Long-Term】

By preparing for security incidents, ALog strengthens rapid response and security visualization. Even during incidents, proper log management enables early detection and accurate investigation, facilitating smooth response and preventing delays in business recovery or loss of trust.

（2） Details of the PoC Project

・ Objective

ALog is already sold in Singapore, Malaysia, various Asian countries, Europe, and the US. The aim is to expand into critical infrastructure operators in ASEAN countries, raising the profile of Japanese-made security solutions and contributing to the enhancement of local security visibility. Rapid detection and response to incidents, such as cyberattacks or data leaks due to human error, are crucial. ALog provides efficient detection and response even with limited resources, offering mechanisms to monitor and detect cyberattacks via access and communication logs.

・ Scope and Key Focus Areas:

A) Effectiveness, Sustainability, and Local Adaptability of ALog

① Effectiveness (Cybersecurity and Compliance)
ALog integrates and analyzes logs from PCs, Active Directory, firewalls, etc., enabling early detection of cyberattacks and insider threats, significantly enhancing security. It is compliant with Thailand's Personal Data Protection Act (PDPA), supporting rapid cause identification and evidence preservation as required by law.

② Sustainability (Long-Term Operation Support)
Certified local partners provide ongoing technical support, ensuring stable and long-term operation. Log compression and flexible pricing enable efficient adaptation to business growth and increased log volume.

③ Local Adaptability (Personnel/Skills)
Proprietary log translation technology allows clear, automatic conversion of "who did what, when," even without specialized knowledge, addressing the shortage of local security experts. Both on-premises and cloud versions are available for optimal deployment.

B) Compliance with Regulations, Integration, and Operational Feasibility

ALog supports the 72-hour notification requirement of Thailand's PDPA and enables prompt notification to data subjects. It monitors suspicious account activity, privileged logins, unauthorized access, and ransomware impact, generating sample reports for compliance and operational feasibility.

C) Scope

The PoC includes local deployment and operational verification of ALog, collecting and reporting diverse logs (file access, authentication, network, PC, email, proxy, VPN), and setting alerts for anomalies. This verifies whether a small IT security team can respond quickly and accurately.

・ PoC Method (Items, Methods, Duration, Number of Trips, etc.)

A) Duration and Local Visits

The project team consists of one project manager, one project leader (for project management and negotiation), and one IT engineer from Japan, plus one local IT engineer in Thailand. The PoC lasts 1–2 months, with two local visits (initial setup; mid-to-final adjustment, measurement, and reporting). Daily monitoring and alert response are managed by local staff, with remote support from Japan.

B) Adaptation to Local Environment

ALog is deployed for servers, network devices, storage, and cloud services. Local infrastructure inventory, log output confirmation, and security policy interviews are conducted in advance.

C) Log Collection and Alert Threshold Tuning
Logs for authentication, operations, network, and cloud are collected using ALog's standard templates. Settings are tuned during the PoC, and detection accuracy is verified with simulated events.

D) Evaluation by Investigation Item
Current measures, operation structure, challenges, and background are checked via interviews and document reviews. Local needs and product requests are identified through surveys and interviews, and ALog's effectiveness, sustainability, adaptability, and need alignment are evaluated through tests and interviews. Data protection, integration with local infrastructure, operational usability, technical training, and failure response are also verified.

E) Training for Local Staff
About two hours of online or hands-on training for local IT staff, confirming proficiency in operation and report creation; satisfaction surveys and interviews are conducted after training.

F) Evaluation Metrics and Feedback
Targets include a 50% reduction in average detection time, a 50%+ increase in cyberattack detection, and over 90 hours/month operational workload reduction. Progress and effects are evaluated using quantitative and qualitative indicators, shared weekly and in the final report.

- PoC Schedule
  - ✓ Mid–late September 2025: Formulation of PoC plan
  - ✓ Early–mid October 2025: Selection and finalization of PoC site (including local events)
  - ✓ Mid–late October 2025: Kickoff with PoC site (local visit)
  - ✓ Mid October–early November 2025: Site survey, requirements definition, system selection, audit settings
  - ✓ Late October–late November 2025: ALog deployment, log collection, operational verification (on-site)
  - ✓ Early November–early December 2025: Operational PoC and effect measurement
  - ✓ Early–mid December 2025: Results analysis, report preparation, feedback, training
  - ✓ Late December 2025: Submission of draft report
  - ✓ Mid-January 2026: Submission of final report
  - ✓ Late January 2026: Final report and feedback meeting

（3） Risks and Countermeasures

- External Risks

Delays in local server adjustments or technical issues can be addressed quickly as Amiya engineers and local partners are stationed onsite. The support structure follows the organization shown in Figure 20 (ALog Support Flow).

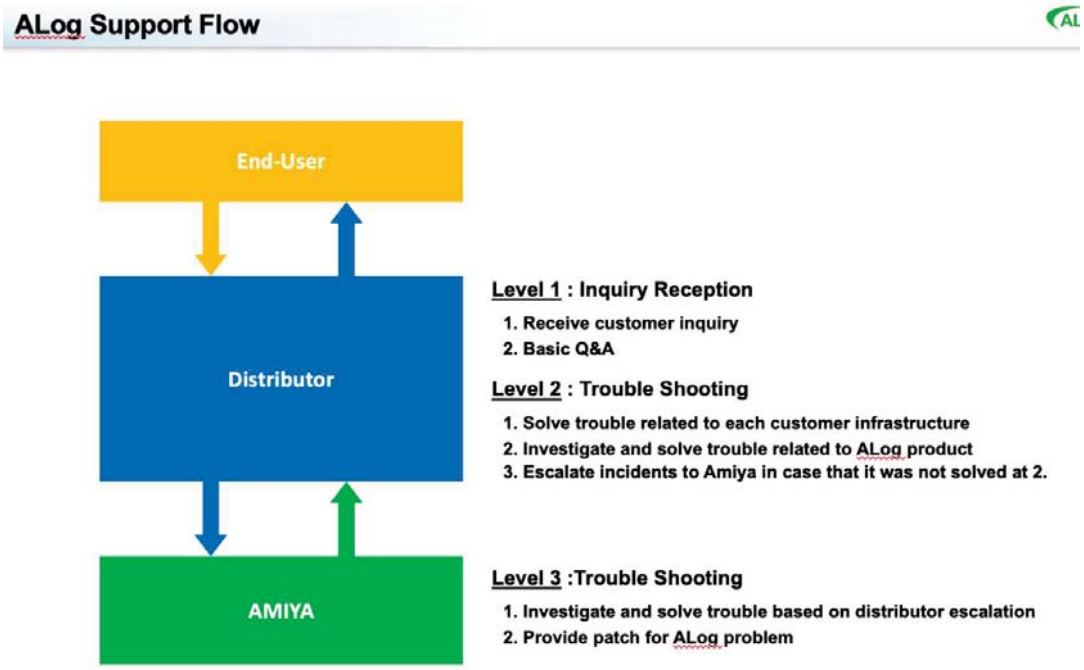


Figure 14 ALog Support Flow

- Regulatory Risks (Cross-border Data, Personal Data, Import/Export)

  A) Cross-border Data
  ALog monitors access logs on local servers only; there is no transmission of data overseas, eliminating cross-border concerns.

  B) Personal Data Protection
  The product complies with local regulations regarding personal data handling.

  C) Import/Export
  Software (ALog and components) is downloaded directly to the local server from Amiya's official website, so there is no need for international shipping or customs procedures.

- Other Considerations

  A) System Operation Risks
  Increased log collection may burden the network or servers, potentially causing delays or data loss. These are managed by adjusting collection intervals, reviewing server specs, and using distributed processing. Temporary log collection suspension due to OS or cloud service changes is addressed with vendor patches and regular verification.

  B) Security Risks
  Log collection requires high-privilege accounts, so usage is restricted and strong password policies are enforced.

  C) Failure/Disaster Risks:
  If the ALog server stops, log collection is interrupted, so regular backups and a rapid recovery framework are necessary. Power or air conditioning issues are managed with UPS and proper rack environments.

  D) Technical Troubles
  Potential issues include hardware failures, network outages, software bugs, data loss, and security incidents.

E) Redundancy/Recovery Measures

Clustering and failover are not standard but regular backups of configuration files and logs allow rapid recovery. Dual storage to external media is also recommended.

（4） Overview of the PoC Site

- Name / Location
  - Organization: Faculty of ICT, Mahidol University
  - Address: 999 Phutthamonthon Sai 4 Road, Salaya, Nakhon Pathom 73170, Thailand
  - Website: https://www.ict.mahidol.ac.th/en/

- Business Activities of the PoC Site

Mahidol University, headquartered in Bangkok, is a national university in Thailand established in 1888 and became a university in 1943. Its predecessor was Thailand's first national medical school, and it has since grown into a comprehensive university with 17 faculties and numerous other organizations. In the QS World University Rankings 2025, Mahidol University ranks second in Thailand. The university operates programs promoting medical innovation in partnership with the Value-Driven Care Center at Siriraj Hospital's Faculty of Medicine. Furthermore, a Cybersecurity Center is scheduled to be established in 2026. If a cyberattack disrupts university operations, there is a high risk of serious consequences such as the leakage of confidential information may occur.

The Faculty of ICT[65] is led by Dean Dr. Pattanasak Mongkolwat, supported by six advisors, four associate deans, and twelve assistant deans, and is organized into six divisions. This PoC was conducted in collaboration with the 17-member Office of Technology Support, with the Technology Infrastructure Division's faculty taking a leading role in the project.

Figure 15 Mahidol University

- PoC Environment

A) Definition of the PoC Environment (Production Environment)

The PoC was conducted in Mahidol University's live production environment, where both faculty and students use the systems daily. Rather than using test data, the project analyzed real access and operation logs from actual business and class activities. This allowed for accurate evaluation of log collection stability and detection accuracy in a real-world operational setting.

B) Equipment and Software Used

The hardware and software specifications used in the PoC are as follows:

Table 5 List of Equipment and Software Used

[65] Mahidol University ICT People – Faculty of ICT, Mahidol U.

Role	Host Name	Details	Remarks
ALog Management Server	ALog Server	OS: Microsoft Windows Server Software: ALog V1.1.5 ALog Syslog Receiver V1.0.3	Collects logs from target servers/devices, analyzes them, and generates alerts and reports.
Target Server #1 AD	AD 1	Windows Server Active Directory	Manages logins and account privileges, and generates related logs.
Target Server #2 AD	AD 2	Windows Server Active Directory	Manages logins and account privileges, and generates related logs.
Target Server #3 AD	AD 3	Windows Server Active Directory	Manages logins and account privileges, and generates related logs.
Target Server #4	File Share	Windows Server	Stores files and generates related logs.
Target Network Device	NW Device	Next-generation firewall for mid-sized branches	Generates logs related to VPNs and Threats, and forwards them to the ALog Management Server.

C) System Architecture and Log Collection Mechanism

The table above shows the system interconnection configuration, and the roles of each device used in this PoC. The area enclosed by the black box denotes the monitored scope (on-premises environment). Users access the system from their PCs via authentication servers, file servers, and network devices. The ALog management server aggregates logs from these servers and network devices, centrally collecting event logs in an agentless manner. Logs from network devices are forwarded in Syslog format. The collected logs are automatically converted and stored within ALog in an easy-to-read format, enabling administrators to search and analyze all logs collectively via a web browser on their PCs.

（5） Cybersecurity Challenges at the PoC Site

- Current Countermeasures

  The Faculty of ICT at Mahidol University conducts joint projects such as a Blood Donation Drive for Siriraj Hospital's Patients with the Faculty of Medicine at Siriraj Hospital and manages a large volume of highly confidential information.

  To maintain confidentiality, all operations are handled in-house, enforcing autonomous management by internal staff without outsourcing.

  Although the university uses shared, centralized security services, there are challenges in achieving detailed visibility into access monitoring and log management at the departmental level. An information leak caused by a cyberattack could severely impact the operation of these joint projects.

- Current Operations and Management

  The Technology Infrastructure Division, comprising 19 members, is responsible for all operations and management. There is no outsourcing. The division includes units for technical equipment, system engineering and maintenance, architecture and landscape, classroom and laboratory support, technical foundation, network management, computer system management, information systems, and audiovisual/digital media development.

- Main Issues and Constraints

The primary issue is budget limitations, making it difficult to purchase new security products. Additionally, faculty members often have to manage IT systems and security in addition to their primary responsibilities, resulting in limited human resources.

- Background
  No major security incidents have occurred in the past, and the current perception is that the security risk is not high.

（6） Needs for Cybersecurity Products and Services

- Types of Needs
  Due to budget constraints, there are currently no plans to introduce new security products or services. The university uses a common platform and internally developed applications. With the Cybersecurity Center planned for 2026, there is an intention to consolidate and centrally manage security measures. In the future, there will likely be a need for security products or services capable of monitoring and managing the common platform, custom applications, and business systems.

- Product/Service Needs
  Although there are no current plans for new deployments due to budget limitations, a solution capable of monitoring custom applications is necessary, as other faculties also use the common platform.

- Basis for Needs
  As other faculties use the common platform, a solution capable of monitoring custom applications is essential.

（7） Verification of Effectiveness, Sustainability, Adaptability, and Needs for Cybersecurity Products/Services

- Effectiveness
  Overview
  ALog demonstrated stable log collection and audit trail management across multiple critical systems, including authentication infrastructure, file sharing, and the network perimeter. During a continuous operation test period—including a long holiday—there were no log losses or collection interruptions, and all major operations (file operations, authentication, privilege changes, external communications) were comprehensively captured and reconstructable.

  Specific Results
  - In the authentication infrastructure (Active Directory), ALog accurately recorded both successful and failed logins and changes to audit policy, confirming its ability to monitor for unauthorized access or insider threats.
  - On the file server, creation, deletion, and renaming of files were tracked per user. Renaming detection is especially effective for ransomware countermeasures, establishing a foundation for anomaly detection.
  - For network boundary defense, traffic and threat logs were centrally managed by ALog, enabling correlation analysis with other products.
  - Predefined risk scenarios (unauthorized login, repeated authentication failures, audit setting changes, renaming/deletion of important files) were all detected and alerted immediately, with zero missed detections (100% detection rate).
  - Of 14 risk logs detected during the PoC, all were appropriately categorized with zero false positives.

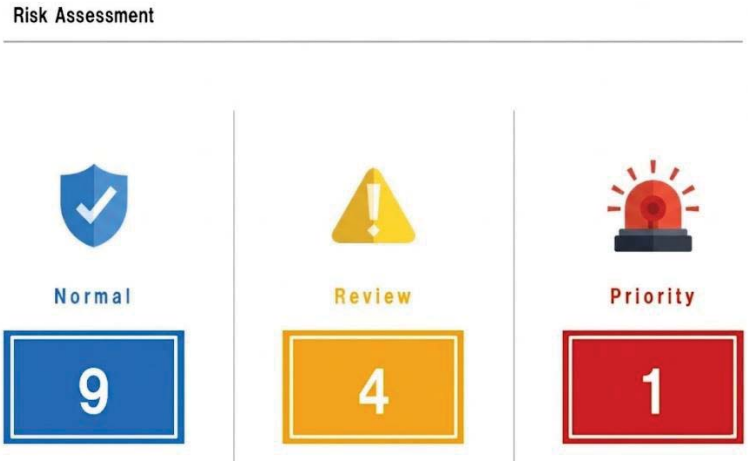


Figure 16 Risk Assessment Results

- The time required for administrators to trace AD/file server operations during incidents was reduced from 120 minutes (previous method) to 5 minutes with ALog—about a 96% reduction in workload. Major efficiency gains were observed in log collection, data interpretation, correlation, and report output.

Evaluation

ALog demonstrated high effectiveness in audit trails and risk detection for critical systems, meeting expectations for log stability, comprehensive operation history, detection accuracy, false positive suppression, integration efficiency, and workload reduction. It is particularly advantageous for organizations with limited personnel and budgets, providing high-precision risk detection and operational efficiency. Local staff evaluated ALog as "very useful," confirming its suitability as a security audit and management platform even in resource-constrained environments.

The PoC also resolved two major issues: dependency on specialized skills and time consumption for log analysis. Previously, translation and correlation of raw logs (which took 120 minutes and required deep knowledge of Windows Event IDs) are now automated; even non-experts can verify facts in just 5 minutes. This 115-minute reduction per case equates to about 192 hours saved annually (assuming 100 investigations/reports per year), freeing up time for advanced security monitoring and training, and improving the university's overall security operations.

- Sustainability

As a result of this PoC, there is very strong interest in the product; however, there are currently no plans for deployment due to the limited budget of the local organization. It is difficult to implement the system with a single department's budget in the short term, and financial adjustments will be a prerequisite for continued use.

Mahidol University maintains an independent, in-house operation model without outsourcing. Because ALog is highly efficient and can significantly reduce the workload of staff, it is likely that long-term operation can be maintained without incurring additional personnel costs.

Furthermore, during the PoC, it was confirmed that basic operations could be managed using only internal resources. However, for handling complex security incidents or system upgrades, establishing a remote support structure with local technical partners will be an important condition for sustainable use.

- Adaptability

ALog enables advanced auditing in the Faculty of ICT's infrastructure division without requiring dedicated security analysts, making it highly compatible with limited local resources and technical foundation. User surveys gave top marks for ALog's GUI and usability, with very

high satisfaction. Even in environments with restrictions on sharing sensitive system information, the automatic mapping feature with external products worked effectively. The PoC achieved a 100% detection rate, confirming ALog's suitability for the local environment.

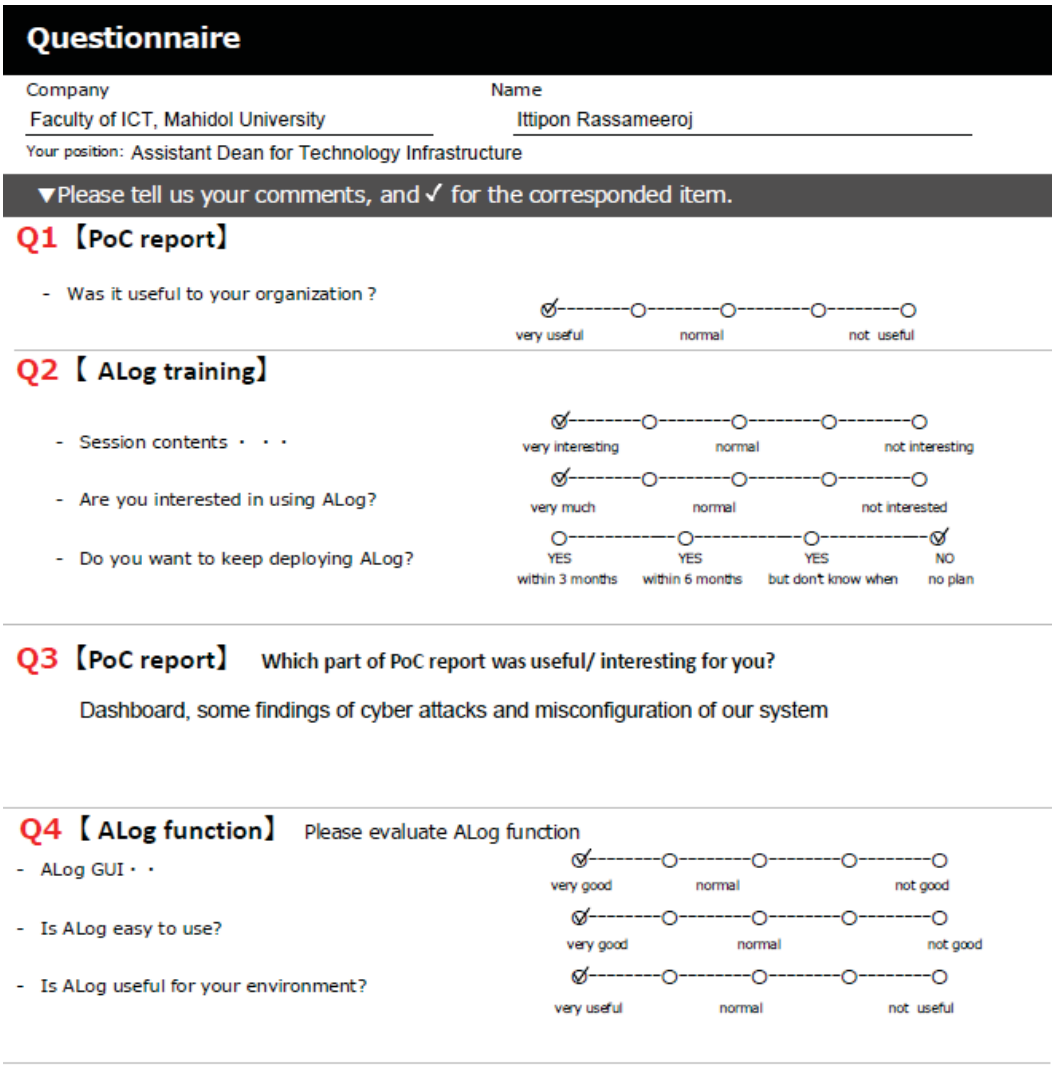


Figure 17 Results of the Evaluation Survey by Mahidol University

- Needs Verification
  Through the PoC, it became clear that ALog aligns with Mahidol University's underlying challenges, such as the current lack of security, detailed data access auditing, and integration with perimeter defense products. In particular, the dashboard function and the detection of cyberattacks and system misconfigurations were evaluated as the most beneficial by on-site staff. While the technical needs at the site are consistent with ALog's functions, further emphasizing ALog's value will be key to promoting its adoption. Overall, ALog was rated as "very useful" and functions as a practical risk visualization platform for the on-site operations staff.

（8） Evaluation of Data Protection and Privacy Compliance in the Target Country and at the PoC Site

- Data Protection (Legal and Regulatory Compliance)

The GDPR[66] is a regulation that strengthens the protection of personal information and privacy in

[66] It stands for "General Data Protection Regulation," which refers to the EU General Data Protection Regulation.

the EU, and as mentioned above, Thailand has also enacted the PDPA (Personal Data Protection Act). ALog is a solution that can comply with Article 25 of the GDPR, "Data protection by design and by default[67]." Specifically, by taking technical and organizational measures, it is possible to ensure the protection of data subjects' rights, such as data minimization and pseudonymization of personal data. Furthermore, since ALog manages data on local servers without cross-border data transfers, there are no concerns about cross-border risks or import/export regulations. These factors enable ALog to build a data protection system that complies with local laws and regulations.

- Data Protection Measures

At the PoC site, critical server groups (e.g., Active Directory) are operated within internal network segments isolated from external networks, and communications with the ALog server are strictly controlled by network devices, keeping the risk of unauthorized external access or data leakage extremely low. Access rights are restricted to authorized personnel only, and the removal of data via recording media is prohibited, thereby mitigating insider-related data leakage risks. For log management, ALog's anti-tampering feature will be enabled in production, ensuring the authenticity of logs. Data retention periods, deletion, and disposal are carried out in accordance with the PoC site's security policy, ensuring proper management.

- Privacy Protection

At the PoC site, personal information is managed appropriately in accordance with local laws. An NDA (Non-Disclosure Agreement) has been signed, and the handling and operation of personal information are clearly defined. The handling of personal and sensitive information is conducted with caution, and notification and obtaining consent from users are thoroughly implemented. Personal information is securely protected based on the privacy policy.

- Privacy Risks

At Mahidol University, a common IT infrastructure is used across all faculties. Data and networks for each faculty are logically separated, so staff from other faculties cannot access them without permission. Controls are also implemented in accordance with Thailand's PDPA.

In addition, the following risks regarding ALog implementation have been verified, and countermeasures have been put in place:

- ✓ Cross-border data transfer risk: Log data is managed in a domestic on-premises environment and is not transferred externally.
- ✓ Data confidentiality risk: While data is stored in plain text during the PoC (trial operation) phase, it will be stored encrypted in production, eliminating risks of leakage or tampering.
- ✓ Administrators abuse risk: Access to the management screen is restricted, and administrator activity is also recorded and audited.
- ✓ Operational (load) risk: The server load caused by log collection does not increase significantly, and there is no impact on operations.

（9） Evaluation of Integration with Local Infrastructure

- Infrastructure Environment

  This PoC was conducted in the production environment at the PoC site. ALog was introduced and integrated without changing the existing network configuration. The monitoring targets were Windows servers (Active Directory and file servers) and network firewalls. For the server layer, logs were collected agentlessly over the SMB protocol, and for the network layer, logs were forwarded via Syslog. The ALog Manager was installed on the on-site virtualization platform. No special agent installation was required, and the system was deployed smoothly using only existing communication port settings and standard privileges.

- Integration

[67] With regard to the handling of personal data, it requires that data protection be incorporated from the outset (at the design stage) and that only the minimum necessary data be processed.

The integration of ALog SIEM with the local infrastructure was completed successfully. Immediately upon deployment, Windows event logs and network device traffic logs were collected without delay. Logs of different formats were normalized into a common format using ALog's standard templates and were centrally managed via the web console. Alert notifications for critical operations also functioned correctly, enabling a transition from conventional individual confirmation tasks to centralized and efficient operations using ALog.

- Issues in Integration
  No technical issues occurred during the PoC period. During the initial setup, communication via SMB and Syslog between the ALog server and monitored targets was confirmed, and necessary port settings were made to resolve any issues. During the operational verification phase, it was defined that ALog is a log management product, not a vulnerability scanner, and CVE responses would be handled through log patterns and alert settings. An operational design was agreed upon, clarifying the division of roles between detection by security products and investigation by ALog.

（１０） Evaluation of Usability and Ease of Technical Mastery

- Usability
  ALog features an intuitive interface suitable for local operation without outsourcing. Log search and aggregation can be easily performed via a browser-based GUI, earning high ratings such as "Very good" from users. During the hands-on exercises in the PoC, administrators were able to receive alert notifications and quickly identify causes or extract audit trails. The dashboard automatically displays "who did what and when," contributing to early detection of anomalies. In user surveys, the dashboard function and the detection of cyberattacks or misconfigurations were also evaluated as beneficial.

- Technical Mastery
  Local staff received training through lectures and hands-on sessions and were able to master the basics of ALog operation in a short period. In practical exercises, they experienced management screen operations, alert handling, and report output, reaching a level where they could detect anomalies within about three hours. The training was rated as "very interesting." Challenges for the future include response drills for incidents and confirming the retention of medium to long-term operational tasks, but since basic operations are easy to learn, further efficiency in technical mastery is expected through video manuals and the expansion of setting templates tailored to local operations.

- User Evaluation
  Surveys of local stakeholders at Mahidol University yielded high ratings such as "very useful" and "very good." The ability to detect signs of attacks or configuration errors without specialized knowledge was particularly appreciated. There is high satisfaction with the product features, but "limited budget" was mentioned as an issue for continued use. Going forward, department-specific and cost-effective implementation methods are desired.

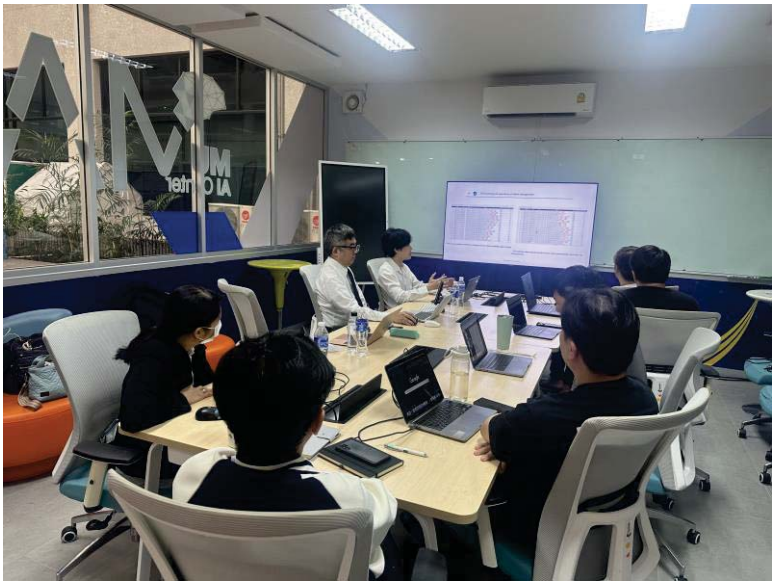


Figure 18　Scene from the PoC Report Meeting with Professors at the Faculty of ICT, Mahidol University

（１１）Recommendations and Summary

- Suggestions and Recommendations

  By further strengthening its current functions, ALog SIEM can differentiate itself from other SIEMs and improve operational efficiency. In particular, automation and templating of log correlation functions, improved alert visibility, implementation of standard action templates, enhanced false positive suppression, and clarification of CVE response support are required. In addition, during introduction and operation, it should be clearly stated that ALog is “not an automatic decision-making SIEM, but a SIEM specialized in visualization and audit trail management,” standardizing integrated report formats, the meaning of thresholds, role sharing with other security products, and communication specifications. This will maximize ALog’s value as a SIEM that enables users to make accurate and rapid decisions in auditing, incident response, and audit trail management.

- Summary

  In the Thai market, ALog SIEM is highly compatible with local cybersecurity challenges, legal regulations, and constraints related to IT personnel and budgets. Its design, which does not require specialized knowledge, overwhelming cost advantage, high affinity with PDPA (Personal Data Protection Act), and the presence of local partners and track record, lower the barriers to introduction and operation. In particular, for sites facing shortages of IT personnel or difficulties in introducing expensive third-party products, ALog is the optimal and realistic choice. It is also easy to deploy in the fields of education, healthcare, and government, and the foundation for market expansion is already in place. Leveraging its extensive achievements in Japan, similar success can be expected in the Thai market.

Figure 19　Photo with Amiya and the Dean and Professors of the Faculty of ICT, Mahidol University

4.7.2 Internet Initiative Japan Inc. (Indonesia)

（1） Target Country and Proof of ConceptProduct/Technology/Service

- Target Country: Indonesia
- Product/Service for Proof-of-Concept:
  Safous Privileged Remote Access (Privileged Remote Access Service)
- Product/Service Overview (Features, Functions, Communication Flow, etc.):
  Safous is a software solution that provides integrated secure remote access and privileged account[68] management for critical internal systems and industrial systems. Instead of traditional VPNs (Virtual Private Networks), Safous is based on zero trust communications[69] over the Internet, which verifies users and devices each time and provides access to business systems with minimum privileges, thereby enhancing security. The main features and functions are described in section 4.5.2.
- Effectiveness Hypothesis / Expected Outcomes (Quantitative & Qualitative, Short-term & Long-term):
  In Indonesia, a major cybersecurity issue is cyberattacks targeting the OT/IT convergence domain. The primary method of these attacks—such as ransomware—involves exploiting vulnerabilities in remote access (including VPNs) to infiltrate systems, then escalating privileges to privileged IDs capable of system modification and altering the system. Furthermore, in the current OT/IT convergence domain, there is no visibility regarding "who performed what task, on which system, at what time, and with whose approval," resulting in an environment that can become a lawless zone.

[68] An account with higher privileges than regular users, such as for system administration or configuration changes. If compromised, it can lead to significant damage.

[69] A security model that operates on the premise of "trust nothing," continuously authenticating and verifying networks and users, and granting only the minimum necessary privileges.

By introducing Safous, those managing critical infrastructure can pre-register which users accessing remotely are allowed to access which systems, for what scope of work, during what time periods, and under whose approval. Additionally, by enforcing MFA (Multi-Factor Authentication) for those registrants, it becomes possible to fully prevent unauthorized access due to impersonation or credential reuse, access to unauthorized systems, actions beyond the permitted scope, and uncontracted work.

Such access management and logging functions, tailored to these needs, are required in any country. While some guidelines and laws exist, Indonesia faces institutional challenges in implementing effective measures, and Safous can help address these issues

■Quantitative Outcomes

【Short-term】

- Zero cyberattacks caused by impersonation or vulnerabilities in VPN devices and remote access
- No congestion issues like those seen with VPNs, while maintaining security
- Security implementation rate (across all target systems)
- Rate of zero trust-based remote connections (remote access via Safous)

【Long-term】

- Zero cyberattacks caused by impersonation or VPN device vulnerabilities in remote access
- Reduced administrative workload for configuration and network settings in response to changes in number of sites and accounts
- Reduced downtime in production facilities (shorter mean time to recovery, improved operation rates)
- Fewer site visits and lower personnel costs due to implementation of remote maintenance at equipment sites

■Qualitative Outcomes

【Short-term】

- Immediate visibility of controls: Access status (login/operation/logout) to critical systems can be visualized per individual, clarifying responsibility
- Establishment of standard rules: Temporary access limited to specific projects, periods, and targets becomes the operational standard, with privileges revoked upon completion
- Immediate audit response: Records of "who, when, where, and what was done" can be provided instantly, reducing the burden of internal and external audits
- Localization of impact: Even in the event of an intrusion, the reachable range is limited, preventing cascading service outages
- Realization of remote operations: Enables status checks and initial response without visiting the site, including remote islands, offshore, and remote areas, improving on-site agility

【Long-term】

- Establishment of a “never stop” operational culture: The principle of granting only the minimum necessary access, only to those who need it and only when needed, becomes the organizational standard, replacing practices of always-open/shared access
- Improved cost structure: Travel, standby, and emergency response costs remain low and stable. Site expansion is possible without increasing personnel
- Sustained audit and regulatory compliance: Evidence stored domestically, and consistent procedures make it easy to maintain ongoing compliance with audits, certifications, and customer inspections
- Expansion of safe digitalization: Additional or updated equipment (Industrial 4.0) can be promoted based on secure connectivity, maintaining an environment where operational risks decrease as connectivity increases
- Enhanced resilience: The cycle of detection, blocking, and recovery matures, continuously reducing both the frequency and impact of major incidents

（２） Contents of the PoC

- Objective of the PoC

In this proof-of-concept, we aim to build an advanced model case and use it as a catalyst to accelerate the adoption of the solution at other sites and similar organizations.

Safous is designed and developed for easy deployment even in regions—particularly in emerging markets—where awareness and organizational structures for security investment are still insufficient. Its core function is "access management," which is the most essential first step in cybersecurity.

Access management is an effective defense against ransomware attacks, which are becoming increasingly severe in ASEAN countries. As OT domains continue to move online, government agencies and critical infrastructure operators, in particular, need to grant access privileges at various levels to their widely distributed key control systems. For these reasons, Safous is highly suitable for such environments.

- Scope of the PoC and Key Focus Areas

In this proof-of-concept, we will examine the following three points:

① Effectiveness, Sustainability, and Local Needs

We will confirm whether the counterpart recognizes the threat of ransomware attacks and the need for secure network connections in IT/OT integrated environments as priority issues. Additionally, we will assess whether there is organizational leadership for introducing solutions to address these challenges, and whether our product’s market price is perceived as reasonable.

② Data Protection and Privacy Compliance

While it has already been confirmed that Safous itself is compliant with local laws and regulations as a product, we will verify the extent to which it can meet the regulatory needs of potential adopters—specifically, whether it sufficiently fulfills the security measures required for critical infrastructure operators under local legislation.

③ Compatibility with Local Infrastructure and Ease of Operation and Technical Adoption

Although the hurdles and lead time for introducing Safous are minimal, when the counterpart is a critical infrastructure operator, it may be necessary to foster understanding among a wide range of internal and external stakeholders due to political and organizational cultural factors. Furthermore, in the OT domain, personnel who are not only unfamiliar with security but also with IT tools themselves may be assigned, so it is important to evaluate the lead time needed for decision-making and skill acquisition.

- PoC Methodology (Items, Methods, Duration, Number of Visits, etc.)

The proof-of-concept (PoC) items are as follows:

- Cybersecurity challenges in the target country and at the PoC site
- Needs for cybersecurity products and services in the target country and at the PoCsite
- Verification of the effectiveness, sustainability, suitability, and needs for cybersecurity products and services in the target country and at the PoC site
- Evaluation of data protection and privacy measures in the target country and at the PoC site
- Evaluation of integration with local infrastructure
- Evaluation of operational usability and ease of technical adoption

Mainly through interviews with the PoC site, information will be collected and evaluated according to the above PoC items. The procedure is as follows:

① Decide on specific PoC sites together with stakeholders and candidates

② In this PoC, since the product evaluation is aimed at future deployment in OT domains of subsidiary companies, the product will initially be introduced into an IT domain with connectivity to the OT domain (an IT/OT integrated area) at BKI. The current status of the systems and infrastructure at the site will be surveyed, and explanations about the product and its implementation methods will be provided to those responsible for cybersecurity in both IT and OT domains.

③ Actual implementation and explanations to users (employees, vendors, etc.)

④ After a certain period of PoC, extensive interviews will be conducted with site management, site leaders, security staff, users, etc., to collect user experience feedback

The evaluation period for the product, from actual implementation to the end of interviews, is expected to be about two months. In addition, two business trips are planned: one after steps 1 and 2, and another after step 4.

- PoC Schedule (including Milestones)

The schedule is as follows:

Early October 2025: Meetings and agreement with the PoC site; survey of the POC site's systems and development of an implementation plan
Mid-October 2025: Kickoff meeting with the counterpart; procurement of installation equipment
Late October 2025: Installation of security products
Early November 2025: Product and operation training for the PoC site team
Early December 2025: Measurement of proof-of-concept effectiveness and exchange of opinions
Late December 2025: Submission of the draft survey report (by the 26th)
Mid-January 2026: Submission of the final survey report (by the 16th)
Late January 2026: Final reporting session and feedback meeting

（３） Risks and Countermeasures

- External Risks：

A decline in the PoC site candidate's willingness to implement the solution due to changes such as a replacement of decision-makers, the introduction restrictions on foreign technologies, or the adoption of similar products, may result in the termination of consideration for deployment.

- Regulatory Risks (Cross-Border Data Transfer / Personal Data Protection / Import and Export)：None of the following apply: cross-border data transfer, personal information protection, or import/export regulations.
- Other Considerations：None

（４） Overview of the PoC Site

- Name and Site Location

Company Name：PT Biro Klasifikasi Indonesia（BKI）
Location：Jl. Yos Sudarso 38-40, Tanjung Priok, Jakarta – 14320

- Business Activities of the PoC Site

The PoC site, BKI, is a state-owned enterprise in Indonesia responsible for ship classification, inspection, and certification. It serves as a core entity ensuring safety in the maritime industry and implementing regulations based on international conventions such as SOLAS[70] and MARPOL.[71] In addition to guaranteeing safety and quality in the maritime sector through its classification, inspection, and certification services, BKI plays a key role in translating requirements based on international conventions and domestic regulations into practical site operations and implementing them in a manner that enables effective oversight.

As part of Indonesia's maritime digitalization initiatives, BKI is promoting the adoption of DX (digital transformation) solutions. As one such initiative, BKI is developing an integrated platform for data collection, monitoring systems, and digital services in the maritime sector (hereinafter referred to as the "Maritime Information Platform") at a newly established data center in the Chikarang area (hereinafter referred to as the "SMV Data Center"). The Maritime Information Platform is expected to handle various types of information, including data on ship operations and equipment usage, coastal

[70] The SOLAS Convention (International Convention for the Safety of Life at Sea) is a treaty that establishes international safety standards for the construction, equipment, and operation of ships. It was adopted by the International Maritime Organization (IMO) with the aim of ensuring the safety of human life at sea.

[71] The MARPOL 73/78 Convention (International Convention for the Prevention of Pollution from Ships) is an international treaty established to prevent marine pollution caused by oil, noxious liquid substances, waste, exhaust gases, and other pollutants from ships. It was adopted by the International Maritime Organization (IMO).

infrastructure operation status, and surveillance footage. As the scope of the platform expands in the future, governance requirements such as access management, activity logging, and log retention will become essential.

The SMV Data Center has just begun operations as a new facility. In anticipation of the future use of the Maritime Information Platform, BKI is gradually standardizing network configurations, organizing asset information (usage, ownership, connection relationships), and developing operational procedures (change management, approvals, audit readiness).

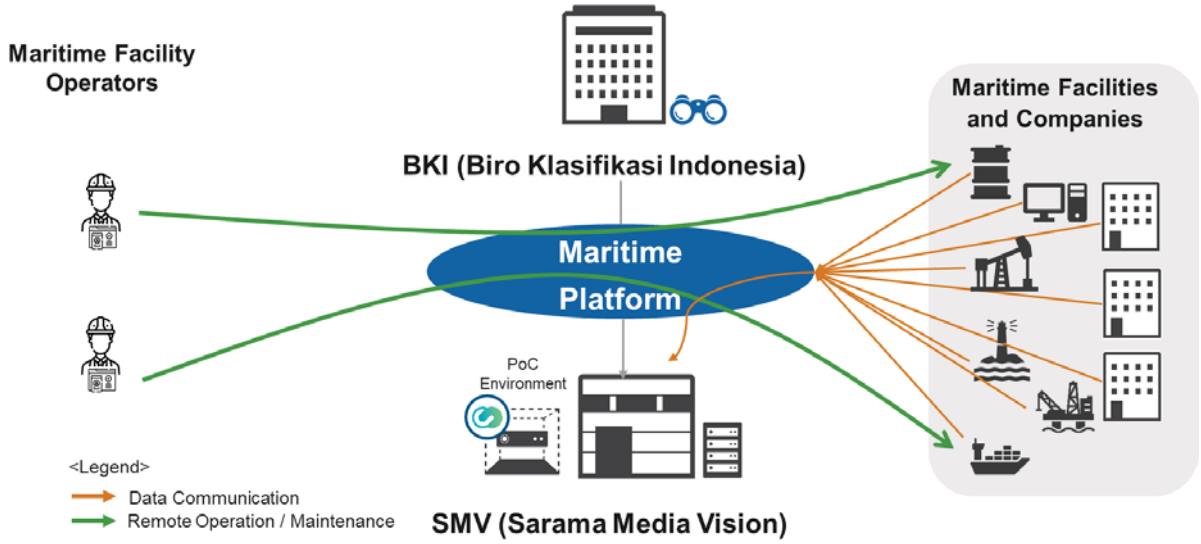


Figure 20　Summary of PoC Partners

- PoC Environment

Initially, the counterpart for this PoC was the Digital TIC Operations Department of BKI, with the plan to introduce Safous into the production environment of the Maritime Information Platform at BKI's newly established SMV Data Center. The aim was to ensure the security of platform operations and data collection from maritime companies. However, for the SMV Maritime Information Platform, the introduction of new products into the production environment requires not only confirmation of technical compatibility but also consideration and approval from a governance perspective—such as clarification of operational responsibility, design of access privileges, log retention policies, and traceability (audit trails) in case of incidents. As these governance requirements are still being developed, it was not possible to implement Safous in the production environment.

Given that these governance controls are still under development, a phased approach involving the creation of a test (staging) environment to pre-validate connectivity requirements and auditability (activity logging and log acquisition) is considered reasonable. Therefore, in this PoC, Safous was introduced into the SMV Data Center's staging environment and its effectiveness was measured.

（５） Cybersecurity Challenges in the Target Country and at the PoC Site

- Current Status of Countermeasures:

As a result of the investigation, it was confirmed that the SMV Data Center is still in the process of establishing its foundational infrastructure as a new facility, and there are several gaps between its current state and the control levels required for the Maritime Information Platform. These gaps indicate that the security level generally expected of a Maritime Information Platform is not being met, and it has become clear that fundamental management measures are broadly lacking.

- Current Operational and Management Structure: Confidential Information
- Key Challenges and Limitations:

It was identified that the current security standards are significantly insufficient to support the advancement of the Maritime Information Platform initiative.

- Background of the Issue:

The background of the issues includes a lack of security awareness, qualitative problems such as the absence of suitable infrastructure engineers, and a shortage of quantitative resources. In terms of cybersecurity regulations, technical standards and procedures for information security management—as well as security audits—have been established, covering data, applications, networks, data center facilities, and operational management systems. Although there is a requirement to continuously implement the "implementation → audit → improvement" cycle, enforcement has not been carried out, and as a result, the adoption of cybersecurity products has not progressed. Furthermore, while the concept of the Maritime Information Platform is advancing, the foundational systems that support it—such as network design, asset management, operational procedures, and audit readiness—are still in a transitional phase. During this transition period, it is difficult to permit remote connections without established controls, resulting in a situation where remote access must be prohibited.

（6） Needs for Cybersecurity Products and Services in the Target Country and PoC Site

- Varieties of Needs:
  - ➢ Establishment of fundamental security measures for the network and data center infrastructure
  - ➢ Enhancement of control levels in preparation for becoming a Maritime Data Center[72]
  - ➢ Visualization and governance of system groups, including legacy assets

These needs are not limited to improving the operational efficiency of a single data center, such as the one used in the current proof-of-concept; rather, they are based on essential governance requirements that will be indispensable for the future operation of a Maritime Information Platform on a national scale.

- Product and Service Needs: Confidential Information
- Background of the Needs:

With regard to product and service needs, the requirements are not merely for improved convenience, but are based on essential control requirements—such as auditability, traceability, and accountability—that are indispensable for the continuous operation of the Maritime Information Platform.

（7） Effectiveness, Sustainability, Suitability, and Verification of Needs for Cybersecurity Products and Services in the Target Country and at the PoC Site

- Effectiveness:
  As a result of the PoC in the staging environment, Safous showed high effectiveness in the following areas:
  ■Quantitative Effects
- Enabled the definition of critical applications and the setting and management of privileged access for administrators
- All connections via Safous were stable, with no observed latency or connection failures
- The introduction of multi-factor authentication eliminated impersonation risks
- Access logs and activity records (session recordings) could be obtained, establishing visibility that was previously nonexistent

■Qualitative Effects
【Short-term】

- Clearly identified who accessed, when, where, and what actions were performed
- Temporary granting and automatic expiration of privileges prevented unnecessary retention of access rights
- Facilitated the presentation of operational audit trails, reducing the burden of audit responses

[72] Although this is not a general term, it is used as is because it is a preferred expression among those involved with BKI.

【Long-term】

- Promoted a shift toward an operational culture of "granting only necessary access to necessary personnel at necessary times"
- Enabled the transition from onsite dependency to flexible operations, including remote first-line support
- Demonstrated adaptability for future vendor governance and multi-site deployment at the Maritime Data Center

- Sustainability:
  Since Safous is agentless, it imposes a low operational burden and can be maintained even with only one administrator. Additionally, because ID and access management are centralized, the system is structured to allow for continued use even after the production environment has been further developed.
- Suitability:
  Safous's access control, approval workflow, and audit trail management are closely aligned with the requirements of the future Maritime Data Center and are highly compatible with the existing culture that emphasizes auditing and traceability.
- Verification of Needs:
  It was confirmed that Safous is capable of addressing all the previously identified issues—such as access management, visibility, and audit response—within the scope of the PoC
  .

The operational model confirmed in this PoC can also be considered effective as a control and audit model that can be deployed across the entire Maritime Information Platform in the future.

（８） Evaluation of Data Protection and Privacy Measures in the Target Country and at the PoC Site

- Data Protection (Regulatory Compliance):
  In Indonesia, information security management and technical standards for electronic government systems (SPBE) [73] have been issued as multiple regulations by BSSN. In particular, the following are the main regulations relevant to the SMV Data Center, which was the subject of this PoC.
  - Peraturan BSSN No.4 Tahun 2021
    This regulation establishes information security management, technical standards, and procedures for SPBE, covering data, applications, networks, data center facilities, and operational management systems.
  - Peraturan BSSN No.8 Tahun 2024
    This regulation defines the technical standards for security audits of SPBE, requiring the continuous cycle of "implementation → audit → improvement."

Safous is equipped with features such as access management, approval workflows, activity recording, and the principle of least privilege, and has been confirmed to have a high level of implementation compatibility with the regulatory requirements for "access control," "authentication management," and "audit trails."

- Data Protection Measures:
  It was confirmed that Safous can effectively supplement most of the fundamental data protection measures required in the data center.
- Privacy Protection:
  The Safous solution used in this PoC handles only the minimum necessary identification information, such as users' email addresses, authentication logs, and activity records. All such

[73] The Electronic Government System (SPBE: Sistem Pemerintahan Berbasis Elektronik) is a national framework established by the Indonesian government to utilize information and communication technology for the electronic implementation of government operations, with the aim of improving the efficiency and transparency of administrative services and internal government processes. It sets guidelines for each ministry and government agency to promote the digitization and interconnection of administrative procedures, data management, public services, and more.

data is stored within the gateway of the deployment site (SMV Data Center) and is not transmitted externally. This structure is compliant with the principles of the Indonesian Personal Data Protection Law (PDP Law), including purpose limitation, protection of data subjects, and access control. From a privacy protection perspective, no structural risks inherent to the product were identified.

- Privacy Risks:
  Confidential Information

（９） Evaluation of Integration with Local Infrastructure

- Infrastructure Environment:
  The SMV Data Center ensures redundancy in power supply and communications in its physical environment, providing sufficient availability.
- Integration:
  In the staging environment, Safous operated stably and was able to control connections for RDP,[74] SSH,[75] and web applications without any issues. The fact that it does not require a special agent demonstrates high compatibility with local environments where there may be many legacy devices[76] on which installing the latest software is difficult.
- Challenges in Integration:
  Safous is a solution designed to ensure the security of the entire network simply and quickly. Through this PoC, no integration issues were identified regarding the implementation of Safous as the foundation of the maritime information platform.

（１０） Evaluation of Usability and Ease of Technical Skill Acquisition

- Usability:

The Safous management console can be operated solely through a web browser, allowing integrated execution of access permission settings, application registration, and session log review. Its ability to quickly establish control even in previously unregulated environments was highly evaluated.

- Technical Skill Acquisition:

Through lectures using the staging environment, the staff were able to quickly learn basic operations such as ID configuration, creation of access conditions, and log review. As initially expected, it was determined that a typical IT administrator would be able to independently operate the system within approximately one week.

- User Evaluation:

Administrators highly appreciated that access control, which had previously been personalized, was streamlined, enabling clearer assignment of work responsibilities and acquisition of operation logs. On the other hand, the establishment of network security measures, such as approval workflows and the introduction of firewalls, has been recognized as a future challenge. Overall, the implementation of Safous demonstrated a clear positive effect on strengthening the local operational framework.

（１１） Recommendations and Conclusion

- Improvement Proposals and Recommendations:

Based on the insights gained through this PoC, we propose the following improvement measures to SMV/BKI:

① Gradual Enhancement of Fundamental Security and Network Control

[74] RDP (Remote Desktop Protocol) is a communication protocol used to operate Windows PCs and servers remotely. In this report, the term refers to the operation of remotely connecting to a Windows server via Safous.

[75] SSH (Secure Shell) is a communication protocol that uses encrypted connections to access servers and devices remotely. In this report, it refers to remote access operations to Linux servers and management servers via the SSH protocol.

[76] This refers to systems or devices that, although introduced some time ago, are still used in current operations. For example, systems or devices like Windows XP, which are no longer supported but are still in use, fall into this category. In OT environments, systems and devices are often prioritized for continuous operation and stability, so frequent upgrades, as seen in IT, are less common. In this report, it refers to equipment in local environments where it may be difficult to install the latest software or agents.

Since the maritime information platform is expected to be connected to multiple OT environments in the future—including ships, ports, coastal infrastructure, and offshore facilities—it is necessary to establish comprehensive network governance. However, rather than implementing everything at once, it is preferable to develop these measures in stages, taking into account the current operational framework and approval processes.

② Visualization of Asset Management and Configuration Information
Confidential Information

③ Standardization of Access Management and Approval Flows
Given operational forms involving multiple internal staff and external vendors, it is important to manage access based on individual IDs, apply the principle of least privilege, and clarify approval flows. Using Safous for access control and acquisition of operation logs is an effective means to implement such operations, and it is desirable to formalize these procedures as standard operational practices going forward.

④ Establishment of Audit Trails and Log Management
As the maritime information platform is expected to become an infrastructure requiring accountability and audit compliance in the future, it is important to establish unified management of audit trails such as access logs, operation records, and approval histories, and maintain the capability to present these records when necessary.

⑤ Development of a Control Model Anticipating Platform Expansion
In anticipation of future expansion, it is effective from a sustainability perspective to establish a common access control and audit model as the foundation, rather than introducing different controls for each individual system.

- Conclusion:

Through this PoC it was confirmed that Safous is an effective means to rapidly achieve access management, visualization, and the establishment of audit trails, even in environments like the SMV Data Center where infrastructure development is still in progress. The evaluation as a PoC phase was sufficient, and feasibility for implementation was demonstrated from both technical and operational perspectives.

Going forward, BKI plans to encourage the adoption of Safous among various maritime companies as part of their security measures. However, there were instances where questions were raised about the possibility of support from the Japanese government or international organizations regarding the introduction of Safous, especially for critical facilities on the platform such as those operated by public institutions related to energy, given the varying levels of management resources and security awareness among platform participants.

Maritime facilities are recognized as critical infrastructure and targets of cyberattacks in Japan as well. It is still fresh in our memory that port functions were suspended in 2023 due to a ransomware-related cyber incident. In response, the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) has continuously issued alerts to operators in the port and maritime sectors, emphasizing the importance of ensuring visibility, access control, and operation logs. In other words, in OT environment security measures, boundary defense and measures based solely on system shutdowns are insufficient; it is necessary to have mechanisms that allow continuous identification and control of "what assets exist, who accessed them, when, and how."

The ID-based access control and audit trail operation model established by Safous is consistent with this approach to OT security. It can serve as a foundational platform that can be expanded horizontally in line with the growing scope of the maritime information platform, not limited to the SMV Data Center. Even as the number of stakeholders and facilities increases, the ability to gradually expand the scope of secure operations while maintaining control and visibility provides important implications for the sustainable and secure operation of the maritime information platform in the future.

4.7.3 Macnica, Inc.（Philippines）

（１） Targeted Country and Proof of Concept Product/Technology/ Service

- Target Country

Philippines

- Name of Proof of Concept Product/Technology
  Macnica Attack Surface Management (ASM)
- Overview of Produc/Service(Feature, Functions, Communication Flow, etc）
  Macnica ASM (Attack Surface Management) is a service that utilizes publicly available information on the Internet to identify and assess externally exposed assets from an attacker's perspective. This service is conducted using a "passive scan" approach, which investigates based on publicly available information without directly placing any load on the target systems.
- Hypotheses of Effectiveness / Expected Outcomes (Quantitative & Qualitative / Short-term & Long-term)
  ■Quantitative Outcomes
  【Short term】
  In the short term, if Macnica ASM is implemented as a proof-of-concept project, the following quantitative outcomes can be expected. First, it is anticipated that a large number of externally exposed assets that were previously unrecognized will be detected. In past cases, more than 1.5 times the number of known IT assets were newly discovered, and it is expected that previously unidentified assets will also be detected in Philippine government agencies and critical infrastructure companies. Next, critical and high-severity vulnerabilities will be identified, enabling immediate actions such as blocking or applying patches. This greatly increases the possibility of preventing incidents before they occur. Additionally, assets and vulnerabilities that require attention will be organized based on the severity of the risk, clearly indicating what should be addressed first in a short period of time. As a result, each organization will be able to quickly develop a roadmap for countermeasures. Furthermore, at the conclusion of the proof-of-concept, the number of detected assets, vulnerabilities, and response status will be quantitatively reported, helping to avoid potential damage.
  【Long term】
  From a long-term perspective (after the official implementation of Macnica ASM), continuous monitoring enables immediate detection of risks associated with new assets or configuration changes, ensuring that the attack surface remains visible at all times. This prevents vulnerabilities from being left unaddressed and leads to a steady decrease in incident occurrence rates. Additionally, as asset inventories and response histories are automatically accumulated, it becomes easier to report to DICT or third-party auditors, and organizations can flexibly respond to future legal requirements or reporting obligations. Furthermore, by replacing manual investigations and external assessments, the annual service fee for ASM enables wide-ranging monitoring, resulting in continuous reductions in incident response costs and human resource requirements. Lastly, by preventing major incidents from occurring, organizations can accumulate the benefits of avoiding potential financial and social losses, leading to long-term cost advantages.
  ■Qualitative Outcomes
  【Short term】
  In the short term, clarifying "what was previously unseen" helps alleviate the anxiety of staff and managers, and contributes to raising awareness and a sense of urgency regarding security throughout the organization. Next, risk assessment by experts eliminates false positives and noise, enabling personnel to focus on important issues. This is expected to reduce operational workload and improve efficiency from the initial stages. Additionally, ASM reports facilitate information sharing among IT departments, management, and external vendors, establishing a foundation for recognizing security as a common organizational issue. Furthermore, through reporting sessions during the proof-of-concept period, stakeholders can enhance their skills and acquire practical knowledge, creating opportunities for interactive learning.
  【Long Term】
  From a long-term perspective (after the official implementation of Macnica ASM), continuous visibility and response will help integrate security into daily operations, reduce dependence on

individual expertise, and foster a culture of "protecting what must be protected." Additionally, the ASM portal enables the status of responses to be visualized both within and outside the organization, making it easier to fulfill accountability. This also contributes to strengthening information sharing with government agencies such as DICT. Furthermore, by sharing reports, information exchange with other organizations and private companies will be promoted, helping to spread best practices and support organizations that may be lagging behind, thereby contributing to the establishment of a collaborative defense system.

（２） Details of the PoC Project

・ Objective

The purpose of this initiative is to conduct a trial of Macnica ASM (External Attack Surface Management: EASM), for government agencies and critical infrastructure operators in the Philippines, to demonstrate its effectiveness and sustainability in addressing the country's cybersecurity challenges. Appropriately applying ASM in a manner suited to local circumstances, Macnica identifies specific benefits that contribute to the realization of a secure cyberspace for the target organizations.

ASM continuously visualizes the external attack surface from an attacker's perspective and prioritizes and notifies risks, enabling effective external attack surface management with minimal operational burden, even for government agencies and critical infrastructure operators with limited personnel and resources. Through this proof-of-concept, our company clarifies the following five evaluation perspectives in the Philippines, based on actual survey results and feedback from participating organizations: (1) effectiveness and sustainability (technological and social suitability, as well as financial sustainability), (2) local needs and acceptance, (3) compliance with data protection and privacy requirements, (4) integration with existing systems and operations, and (5) ease of operation and technical skill acquisition. By doing so, we will consider an implementation model that aligns with institutional and operational requirements, supporting everything from short-term deployment to long-term establishment. Furthermore, throughout the proof-of-concept process, we will highlight key outcomes such as the visualization of unknown assets, reduction of high-risk assets, establishment of remediation processes, and knowledge transfer to local personnel. These results will directly contribute to strengthening the protection of critical infrastructure in the Philippines, while also expanding Japanese solutions as a reproducible deployment model. Through the execution of this proof-of-concept, our company aims to make a meaningful contribution to deepening public-private partnerships and enhancing international competitiveness, as advocated by JICA.

・ Scope and Key Focus Areas

① Effectiveness and Sustainability: In the target organizations, the status of externally exposed assets will be clarified, and the risk reduction effect achieved through ASM will be quantitatively evaluated. Indicators will include the ratio of newly discovered unknown assets and the reduction of high-risk assets.

② Local Needs Compatibility: The proof-of-concept will be conducted based on the priority use cases (high-risk products) defined by our company. Afterwards, we will interview the target organizations to determine if there are any additional risks or requests, they would like to be prioritized for notification, in order to understand local-specific needs.

③ Data Protection and Privacy Compliance: Compliance with the target country's data protection and privacy requirements will be evaluated based on the terms of use for Macnica ASM. No additional technical measures (such as encryption or retention period settings) will be implemented; the evaluation will be limited to confirming compliance on a terms-of-use basis.

④ Operational Process Compatibility: A desk-based review will be conducted to verify whether the entire workflow—from risk notification to asset identification, administrator assignment, and remediation—functions appropriately. During this process, factors on the customer side (such as existing CTEM [Continuous Threat Exposure Management] products, already

implemented cybersecurity devices, and asset management tools) that may influence the workflow will be identified.

⑤ Operational Challenges and Improvement Measures: Through the proof-of-concept, operational challenges and points of concern in the local context will be identified. In consultation with the target organizations, appropriate countermeasures and best practices will be organized and documented.

・ PoC Method (Items, Methods, Duration, Number of Trips, etc)

This proof-of-concept will be carried out in the following sequence: "Preparation → Finalization of Plan → Kick-off (on-site) → Investigation → Preliminary Notification & Remediation Support → Report Preparation & On-site Reporting → Consolidation → Submission & Final Report." The kick-off and investigation reporting sessions at the proof-of-concept sites will be conducted through in-person visits, while other processes will primarily be handled online. Note that this project will not provide ongoing portal access or operational services; instead, the main deliverable will be a written report summarizing the investigation results.

・ PoC Schedule

A. Preparation and Establishment of Proof-of-Concept Structure

From September 5 to October 20, 2025, over a period of approximately one and a half months, preparatory activities will be conducted. These will include concluding business outsourcing contracts and managing progress, holding internal kick-off meetings and preparing related materials, final confirmation and coordination of contractual and compliance requirements, drafting the Memorandum of Understanding (MOU) for cooperation in the proof-of-concept, identifying and obtaining internal agreement on candidate sites for the proof-of-concept, contacting, coordinating with, and finalizing the sites, defining the scope of the investigation, formulating the project plan, and coordinating the structure on the Netpoleon, which is a Macnica's subsidiary in the Philippines.

B. Kick-off and Alignment of Verification Objectives with Relevant Ministries

During the five-day period from October 20 to 24, 2025, a kick-off will be conducted with the relevant ministries.

C. Start of Proof-of-Concept Project (ASM Investigation)

From October 23 to December 5, 2025, over a period of about one month, the following activities will be carried out: organizing seed information, conducting OSINT discovery, analyst verification and noise reduction, risk assessment, prioritization, notification of critical risks and remediation support, and preparation of the draft structure for the report to be delivered to the proof-of-concept sites.

D. Preparation of Investigation Reports for Proof-of-Concept Sites and Report Creation for the Secretariat

From December 8 to December 26, 2025, over a period of about three weeks, the following activities will be carried out: preparation of individual reports for each proof-of-concept site, compliance and translation reviews, conducting on-site reporting sessions, integration and quality checks of the final report, and submission and registration of the final draft on December 26.

E. Submission of Final Report and Reporting Meeting

From January 6 to January 19, 2026, the final report will be written over a period of about two weeks. After that, the final report will be submitted and registered, a completion report will be made, and finally, the results will be presented at the final reporting meeting for JICA.

（３） Risks and Countermeasures

・ External Factor Risk

Contract reviews may be prolonged due to additional confirmation of cross-border clauses; therefore, a draft MOU (Memorandum of Understanding) based on the premise of "not handling personal data" will be proposed. In this proof-of-concept project, the investigation will focus on OSINT (Open-Source Intelligence), and only document reports will be provided. Measures will be taken to ensure that no personally identifiable information is handled at all.

- Regulatory Risks (Cross-border Data Transfer / Personal Data Protection / Import and Export)
  Personal Data Protection Risk: Under the Personal Information Protection Act, it is required to limit the purpose of use of information, minimize its collection, and manage it securely. To address this, the proof-of-concept project will adopt a policy of not collecting any personally identifiable information, and reports will only include information at the organizational or asset level. If personal names are found in sources such as WHOIS, they will be deleted or anonymized. No additional technical mechanisms will be introduced, and compliance will be confirmed based on the terms of use of Macnica ASM.
- Other Consideration
  NA

（4） Overview of PoC site
- Name and Location
  Organization A（Group of National Administrative Agencies）
  Organization B (Major Telecommunications Operator in the Philippines）
- Description of the PoC sites
  【Organization A】
  This group is composed mainly of the central agency responsible for overseeing information and communications policy in the Philippine government, as well as multiple ministries and related government agencies that manage critical infrastructure such as health, energy, transportation, and water. They are responsible for developing digital infrastructure at the national level, formulating cybersecurity strategies, and promoting international cooperation. Since these agencies provide services directly related to citizens'daily lives, the management of external attack surfaces is a critical issue for national security.
  【Organization B】
  Organization B is a private enterprise that provides the largest telecommunications infrastructure in the Philippines, offering a wide range of ICT services including fixed-line communications, mobile communications, and data center services. The company employs approximately 8,000 people and delivers highly available networks to users both domestically and internationally.
- PoC environment
  【Organization A】
  In this proof-of-concept project, the aim is to verify the applicability of ASM (Attack Surface Management) in government agencies by conducting risk assessments on the public assets of Organization Group A (total: 5 institutions). The project also seeks to gain insights for future system design and standardization.
  【Organization B】
  Given the large scale of externally exposed assets such as VPN devices and cloud connectivity services, it was estimated that managing the attack surface is an urgent issue. There have also been reports in the past of cases where the organization was targeted by international cyberattack campaigns, making the visualization of external attack surfaces and risk reduction critical themes directly linked to business continuity. The purpose of this proof-of-concept project is to comprehensively identify the company's externally exposed assets and to verify the potential for improving the vulnerability management process.

（5） Cybersecutity Challenges in the Target Country and at the PoC Site
【Challenges of Organization A】
In Organization A, the lack of unified asset management is particularly evident. The central department does not have direct authority over the assets of each government agency, and management is delegated to each individual agency. Currently, there are no common management manuals or standardized response procedures in place, and domain management is limited to Domain management is limited to handling applications at the time of acquisition. Furthermore, because

operational standards and violation policies related to cybersecurity have yet to be established, the central department is limited to presenting recommendations and has been unable to implement enforceable controls. These structural limitations reduce the visibility of externally exposed assets and increase the risk of unmanaged assets being exploited by attackers.
Secondly, the lack of a well-developed legal framework is also a challenge. Under the current system, cybersecurity-related laws and regulations are limited to basic policies based on national plans, and there is no legal framework that obligates each agency to manage vulnerabilities or respond to incidents. As a result, the effectiveness of countermeasures depends on the discretion of each agency, and it is difficult for the central department to enforce prompt corrective actions.
Thirdly, there is a serious shortage of personnel and an imbalance in skill levels. The central department consists of approximately 79 members, but the skill levels of ICT personnel in each agency are unclear, and there is no standardized skill assessment system in place. Additionally, current human resource development relies on training provided by external organizations, and a systematic education program has not been established. The incident response team comprises about 14 members, but with 10 to 15 incident reports received weekly, the lack of sufficient staff and skills is increasing the operational burden.
Fourth, the concentration of operational workload is a significant challenge. Vulnerability assessment and registration testing, along with incident response operations, have been identified as the most burdensome areas. Vulnerability assessments are primarily conducted manually based on monthly scans, requiring considerable time for reviewing detection results and coordinating with the relevant agencies. Although the standard for incident response is to provide initial contact within 15 minutes of receiving a report, responses from the agencies are often delayed, resulting in significant variation in the time required to resolve incidents.

Finally, delays in technical automation are also noted. Currently, the vulnerability management process utilizes the Integrated vulnerability management tool, but automation of asset management and vulnerability response has not yet been achieved, hindering full visibility of externally exposed assets and rapid response. Furthermore, outdated software and unused equipment are still present, and the removal process for these assets also relies on manual operations.
Overall, while Organization A functions as a core institution responsible for national-level cybersecurity strategy, it continues to face structural challenges in areas such as unified asset management, legal enforcement, human resource development, operational efficiency, and technical automation.

【Challenge of Organization B】

Firstly, there is a challenge in ensuring the completeness of the asset inventory. The company manages a wide range of assets, including its headquarters, multiple group companies, and Internet Service Provider (ISP) business domains, but the current management model is decentralized, with the IT department, network department, and security team each using different tools. The IT and network departments each operate integrated asset management tools (ITSM/ITAM), while the security team uses a log integration system (SIEM) to consolidate information. However, automatically determining the affiliation of domains and IP addresses (i.e., which subsidiary owns which asset) remains difficult. In particular, within the ISP domain, manual grouping is required to identify IP ranges, and full automation has not yet been achieved. Interviews revealed that Organization B described the asset structure as a “complex tree structure,” confirming that improving the accuracy of asset management is the top priority.
Secondly, the high operational workload is particularly notable. The SOC maintains a 24/7/365 monitoring system, concentrating tasks such as vulnerability scanning, alert response, report creation, and evidence collection. Especially when zero-day vulnerabilities are discovered, additional investigations and emergency responses are required, significantly increasing the burden on personnel resources. According to interviews, the organization maintains uninterrupted 24/7/365 monitoring, even during weekends and nighttime hours, requiring continuous shift work. Additionally, report creation and evidence collection involve a large amount of manual work, further

increasing the operational burden. While the development of automation playbooks and SIEM integration is underway, many tasks still rely on manual processes at present.
Thirdly, the complexity of regulatory compliance is a significant challenge. The company adheres to international standards such as ISO 27001 and PCI DSS (payment Card Industry Data Security Stadard) ; however, PCI DSS compliance in a multi-tenant environment requires a dedicated SaaS configuration when introducing ASM, which imposes constraints on operational design. Furthermore, because inventories are decentralized across group companies, it is difficult to quickly consolidate information during audits or incident responses. It was also noted that regulatory changes, such as the extension of log retention periods or the introduction of new regulations, may increase operational burdens in the future.
Overall, while Organization B demonstrates a high level of maturity in external attack surface management, challenges remain in areas such as ensuring asset inventory completeness, reducing operational workload, and improving regulatory compliance efficiency. These issues stem from the decentralized management model and the large scale of operations. For future improvement, further advancement in automation and strengthening of information consolidation processes will be necessary.

（6） Needs for Cybersecurity Producst and Services in the Target Country and at the PoC Site

【General needs for Sybersecurity producsts and services】

In the Philippines, while cybersecurity is becoming an increasingly important issue, serious challenges remain, such as outdated infrastructure, limited resources, and insufficient awareness of cybersecurity. These vulnerabilities make the country more susceptible to cyber threats such as ransomware attacks, phishing, and data breaches. The importance of robust cybersecurity measures is growing in response to these threats. The Philippine cybersecurity market is expected to grow by 13% and reach $387.1 million by 2028. The impact of the pandemic, as well as the accelerated use of digital payments and fintech platforms, is also contributing to this trend, with software sales projected to reach $1.26 billion by 2028. For new market entrants, there is demand in areas such as information and network security, IT auditing, consulting, digital forensics, threat intelligence, and software development.[77]

【Local needs of Organization A】

The local needs of Organization A are focused on strengthening the visibility of the external attack surface in relation to the consideration of introducing Macnica ASM, enhancing vulnerability management, improving operational efficiency, and raising the quality of reports to support decision-making. Firstly, since the central department does not have asset management authority and management is delegated to each agency, it is difficult to gain a comprehensive understanding of all externally exposed assets. Therefore, the highest priority is the exhaustive detection, classification, and enhanced visibility of assets through ASM implementation.

Secondly, the current vulnerability assessment relies on monthly scans conducted with the integrated vulnerability management tool, which imposes limitations on detection accuracy and response speed. ASM is expected to supplement these missing functions, provide immediate notifications of zero-day vulnerabilities, and clarify the scope of impact.

Thirdly, under the current system, vulnerability assessments and various incident responses involve a significant amount of manual work. With 10 to 15 incidents escalated from each agency on a weekly basis, the burden on human resources is substantial. The introduction of Macnica ASM is expected to automate detection results, improve the accuracy of alerts, and thereby enhance operational efficiency and incident prevention.

Fourthly, there is a strong demand for improving the quality of reports to support decision-making. In order to persuade each agency and ensure the implementation of corrective actions, reports must not only provide technical evidence but also include information that is easily understood by

[77] International Trade Association Philippines - Digital Economy

decision-makers. In particular, it is expected that reports will clearly explain the reasons for critical risks and feature enhanced visual elements. By integrating ASM information into the existing reporting process, it will be possible to create an environment where decision-makers can make prompt and appropriate judgments.
Additionally, a common and important need for Organization A is countermeasures against website defacement by hacktivists. Organization A has the responsibility to ensure the accuracy and reliability of information disseminated to citizens and related agencies, and the occurrence of website defacement poses a serious risk that directly impacts the authority and social credibility of a national institution. Stakeholders have commented that "website defacement detection is a critical factor in maintaining the organization's authority, and thorough countermeasures are essential."
This situation is compounded by a chronic shortage of cybersecurity personnel. Organization A is considering expanding its incident response team to around 30 members, but it has been confirmed that there is a shortage of personnel with the necessary skills, presenting challenges in recruitment and training. Notably, this issue represents a structural need that is common throughout the Philippine market as a whole.

【Local Needs of Organization B】

The needs of Oraganization B, in relation to considering the introduction of Macnica ASM, were mainly discussed around functional requirements, operational improvements, UI/notification features, report quality, integration, and regulatory compliance.

The first identified need is API integration of Macnica ASM with SIEM and SOAR,[78], support for code management, and selective use of automated testing features for each asset. Additionally, license purchase via AWS Marketplace, tenant management, and rapid vulnerability notification and alert functions were confirmed as important features.
Secondly, stemming from dissatisfaction with current tools, there is a strong demand for automation of asset management and classification. Specifically, manual grouping and classification of subdomains and IP addresses is cumbersome, IP identification in the ISP domain is difficult, and the process of excluding false positives is burdensome. Moreover, delays in vulnerability detection and insufficient notification content (such as the number of affected assets and detailed information being provided only via email) were also pointed out as areas for improvement.

Thirdly, in terms of operational improvements expected after ASM introduction, immediate detection and notification when assets are added, visualization of serverless and cloud assets, faster response to zero-day vulnerabilities, and improved reliability and accuracy of alerts were mentioned. Automation and integrated management of detection results to reduce the SOC team's workload, as well as ensuring reusability through code management tool, are also important needs.
Fourthly, regarding UI and notification features, there is a demand for an intuitive and easy-to-use interface, such as dashboards that allow users to instantly grasp asset status and risks, immediate alert notifications, automatic alerts when assets are added or risks are detected, and grouping and filtering functions. It is also necessary to clearly display detailed alert information (such as the number of affected assets and recommended actions). However, since Organization B develops and integrates its own dashboards, there is not a strong demand for the Macnica ASM UI itself.
Fifthly, there is a need for evidence-based reports that are easy for IT and business departments to understand, reporting of assets not detectable by existing tools, prioritized lists of vulnerabilities and risks, and automatic report generation. In particular, listing FQDNs, IPs, open ports, providing evidence of critical risks, and including PoC are emphasized. For regulatory compliance, independent operation and vendor risk assessment are required to maintain PCI DSS.
Overall, the central needs are strengthening the visibility of the external attack surface, reducing operational workload through automation and integration, improving UI and report quality, and responding to regulatory requirements.

[78] Security Orchestration, Automation and Response: A platform that automates cybersecurity operations, enabling security teams to respond to threats quickly.

（７） Verification of the Effectiveness, Sustainability, Suitability, and Needs of Cybersecurity Products and Services in the Target Country and at the PoC Site

- Effectiveness

  During the proof of concept (PoC), the effectiveness of external attack surface visualization was confirmed.

  Thanks to the Macnica ASM reports, Organization A was able to identify assets and risks related to VPN and firewall devices that had previously gone unnoticed, and also received early warnings about the React2Shell threat.

  Meanwhile, at Organization B, although the management of the external attack surface was already mature due to their advanced SOC system, the Macnica ASM reports served as a means to verify that accuracy and confirmed that there were virtually no unidentified assets.

  Additionally, the information on the React2Shell[79] threat helped reaffirm the importance of zero-day response, demonstrating the value of the threat intelligence provided by ASM.

  On the other hand, this evaluation was limited to report submissions, and the real-time detection capabilities and portal functions of ASM were not verified.

Table 6 Risk Detection Results in Organization A

Risk level	Number of risk alerts * Number of hosts in ()	Remarks
Critical	14 Alerts (3 IPs)	Vulnerability with extremely high risk. These are frequently exploited by attackers and can allow them to break into networks. Immediate action is required.
High	13 Alerts (7 IPs)	External exposure of ports that are easy targets for attackers, such as RDP (3389/tcp) and SMB (445/tcp).
Medium	116 Alerts (83 IPs)	Port exposure for FTP, SSH, SNMP, LDAP, SQL, etc. Not necessarily immediately fatal but generally should not be exposed to the Internet.
	96 Alert (78 IPs)	Server running unsupported software (Apache, PHP, MySQL, etc.) that has not been updated for several years.
Products requiring attention (products that are easy targets for attackers)	25 IPs	VPN devices and Exchange Servers that are open to the outside world. As these are common attack targets, it is necessary to ensure that they are always updated to the latest version.

[79] React2Shell: A general term for vulnerabilities in which an attacker exploits unintended JavaScript execution paths on a website, ultimately leading to the execution of OS commands (shell execution).

Table 7 Distribution of number of risks in Organization A

Item ¥Target	Central Department	Agency 1	Agency 2	Agency 3	Agency 4
Critical	4(1)	10(2)	0	0	0
High	1(1)	5(2)	1(1)	6(1)	0
Medium	39(29)	57(46)	43(30)	73(45)	0
Total	44	72	44	79	0

Table 8 Risk Detection Results of Vulnerability Assessment in Organization B

Item	Research results	Notes
Number of domains	54 domains	Total number of domains, such as xxx.ph
Number of Fully Qualified Domain Name (FQDN)	1907	Number of Fully Qualified Domain Name (FQDN) (Fully Qualified Domain Name (FQDN)) associated with the above domains for which name resolution (IP address identification) was possible
Number of IP address	1026	Number of subdomains or Fully Qualified Domain Name (FQDN) associated with IP address in the investigation process
Number of Netblocks	3601 #	Number of IP address ranges identified as highly likely to be owned by the target organization

Table 9 Risk Distribution Across the Subsidiaries Associated with Organization B

Item ¥Target	Head Office	Subsidiary 1	Subsidiary 2	ISP business related
Number of domains	54	14	2	95
Number of Fully Qualified Domain Name (FQDN)	1907	255	30	968
Number of IP address	1026	136	43	1195
Number of Netblocks	※3601	1	0	Not tabulated

*Most of IP addresses contained in this Netblock are provided to other companies as ISPs and are not hosts managed by Organization B. Therefore, IP address under Netblock was excluded from the investigation.

- Sustainability

  Regarding sustainability, both organizations assessed that it is possible to incorporate the information provided by ASM into their existing reporting processes.

  In Organization A, integration into monthly reports is straightforward, and the information provided by Macnica ASM can be utilized to complement the existing framework. On the other hand, a shortage of human resources and skills remains a challenge, making it necessary to establish training programs for ASM operation.

  From a cost perspective, Organization A has secured a budget of 39 million pesos (approximately 103.5 million yen) for its existing integrated vulnerability management tools, so the introduction of Macnica ASM is within the financially acceptable range. However, it is necessary to consider procurement process constraints, such as requirements for public bidding or direct contracts (for amounts under 2 million pesos).

  In Organization B, Macnica ASM can be integrated into the existing SOC framework and is expected to enhance automation through API integration with Splunk and SOAR. However, since the current API integration capabilities of Macnica ASM are limited, additional feature development will be necessary. From a cost perspective, the introduction of ASM can be accommodated within the existing budget, so financial barriers are minimal.

  In addition, the following deficiencies were identified during this evaluation.

  - The real-time detection capabilities and automation features of ASM have not yet been demonstrated
  - Full automation of asset classification and false positive exclusion has not yet been achieved.
  - The quality of reports has not been optimized for the decision-making level.

  Both strategic and technical measures need to be considered. On the strategic side, it is important to formulate and disseminate operational guidelines for practitioners who lack security expertise, establish product training programs for developing operational personnel, and enhance reporting through visualization and executive-focused information. On the technical side, it is necessary to strengthen automation features for asset classification and false positive exclusion, as well as to develop API integration with SIEM and SOAR.

  In the overall assessment, Macnica ASM is effective for visualizing external attack surfaces and providing threat intelligence, and its swift response to provision of information on zero-day vulnerabilities. However, the fact that real-time detection and operational integration have not yet been demonstrated remains a challenge.

  Regarding sustainability, both organizations have low financial and regulatory barriers, making long-term operation feasible. By advancing standardization, integration feature development, and training program establishment, ASM’s adaptability and competitive advantage in overseas markets can be expected.

- Compatibility

  Although the outcome of this proof-of-concept was limited to report submission, the content demonstrated a certain degree of compatibility with local needs. Specifically, the report comprehensively covered risk information related to critical products (such as VPN devices, firewalls, and Exchange Servers), and the early notification regarding the React2Shell threat was highly valued. In addition, the asset detection results clarified the existence of previously unidentified assets in Organization A, and served as a basis for verifying the accuracy of existing asset management in Organization B.

  - Lack of immediacy: Notifications were limited to the time of report submission and did not ensure real-time responsiveness.
  - Unclear operational integration: Specific methods for integration with the current framework, such as API linkage orcode management tool, have not been defined.
  - Lack of report persuasiveness: Visual elements for decision-makers and clear indication of risk prioritization are insufficient.

To meet these needs, possible improvements include the formulation of operational standardization guidelines at the strategic level and the provision of report templates that take local legal and regulatory requirements into account. Technical measures may involve internal automation of asset classification and false positive exclusion, as well as the development and enhancement of API integration functions with SIEMand SOAR. It is necessary to improve report quality by considering easier-to-understand visualizations, clear indication of risk prioritization, and the addition of executive summaries.

- Needs verification

Regarding needs verification, the following local needs were identified as common to both organizations based on the interview results.

- Complete visualization of externally exposed assets and early detection of previously unidentified assets.
- Rapid notification and clear identification of impact scope for zero-day threats (e.g., React2Shell).
- Report quality that ensures compliance with legal and regulatory requirements (such as National Cybersecurity Plans, PCI DSS, etc.).
- Automation features aimed at reducing operational workload (asset classification, false positive exclusion).
- Persuasive reports for decision-makers (visualization, clear indication of risk response priorities).

In Organization A, underdeveloped legal frameworks and a shortage of personnel are prominent issues, and there is a strong demand for ASM to provide "visualization of external attack surfaces," "immediacy of threat notifications," and "provision of standardized operational guidelines."

In Organization B, given the maturity of the existing SOC structure, expectations for Macnica ASM include "enhanced automation," "API integration with SIEMand SOAR," and "reduction of report creation workload."

In the overall assessment, Macnica ASM demonstrated a certain degree of compatibility with local needs in terms of "threat intelligence provision," "accuracy of asset detection," and "risk notifications," but was found lacking in real-time responsiveness, automated integration capabilities, and report quality. By addressing these areas for improvement, ASM can achieve higher adaptability to local threat environments and regulatory requirements, thereby establishing a competitive advantage in overseas markets.

（８） Evaluation of Data Protection and Privacy Measures in the Targeted Country and at the PoC Site

Macnica ASM is a solution for managing external attack surfaces that collects and analyzes open-source information. In this proof-of-concept, only report submission was conducted.

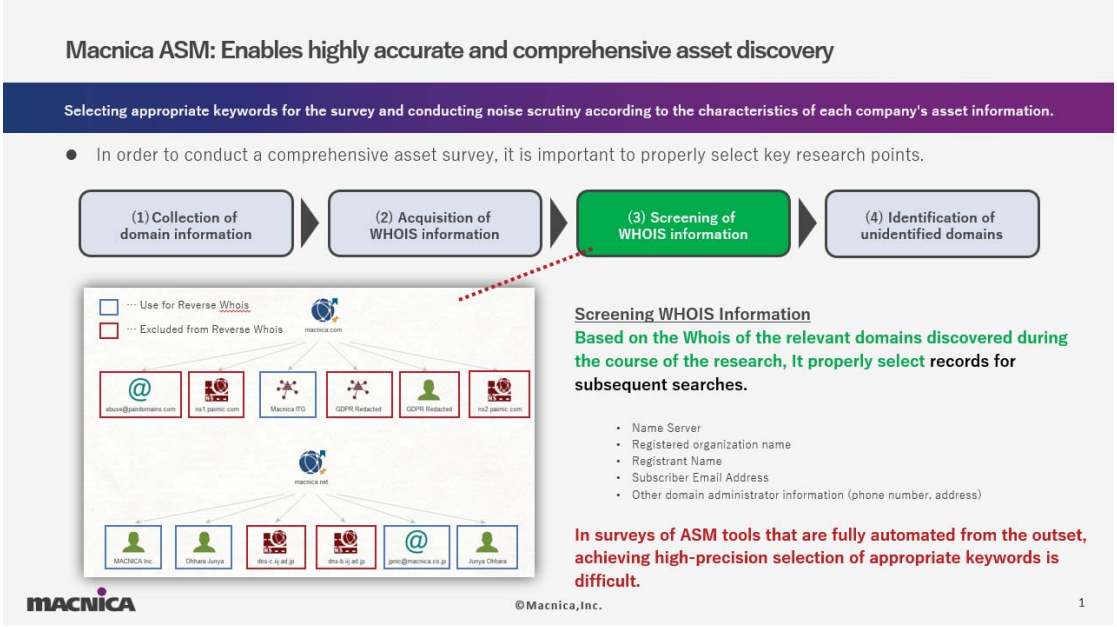
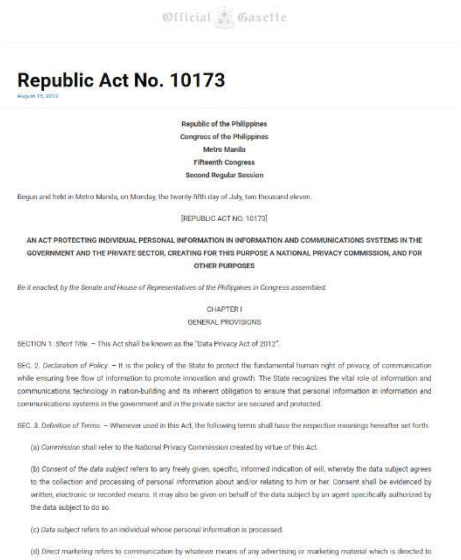


Figure 21 Diagram of Reverse Whois Investigation Using OSINT by Macnica

Under the Philippine National Cybersecurity Plan and Data Privacy Act, the information collected by ASM is limited to publicly available assets, resulting in a low risk of handling personal information and no legal concerns. The terms of use also apply only to public information, ensuring alignment with local laws. On the other hand, Organization A has expressed a preference for a data retention period of around one year, so it will be necessary to allow flexible retention period settings after implementation. Additionally, in both organizations, if internal assets or authentication information are handled in the future, enhanced encryption and access controls may be required. Overall, Macnica ASM is generally compliant with data protection and privacy requirements in the target countries; however, the lack of retention period settings and encryption features could pose future risks, and the following improvements may be necessary.

- Addition of a data retention period setting function: Enable selection of a retention period of around one year to meet local requirements.
- Provision of encryption options: Strengthen data encryption features in anticipation of future handling of internal assets.
- Enhancement of audit logs: Mandate the retention of access history and data processing records to demonstrate legal compliance.

Regarding the status of information security and compliance in Organization A, they are in compliance with the National Cybersecurity Plan (NCSP 2023–2028) and the Data Privacy Act, and the conformity with each requirement under consideration is being verified.



Official Gazette

Republic Act No. 10173

August 15, 2012

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to

Figure 22　The Data Privacy Act of 2012 (Republic Act No. 10173)

Furthermore, regarding information security and compliance in Organization B, it was confirmed that their systems are established based on adherence to international standards and industry best practices. According to the interview results, Organization B has built a management framework compliant with ISO 27001 and ISMS (Information Security Management System), and conducts regular audits based on its own policies aligned with SWIFT. For payment-related operations, compliance with PCI DSS is required, and some subsidiaries have implemented measures for specific brands and channels.

When introducing security products, Organization B requires vendors to sign non-disclosure agreements, undergo vendor risk assessments, and obtain third-party certifications such as SOC2. They also verify system integration requirements, and adoption decisions are made comprehensively, including input from legal and compliance departments. For Japanese vendors entering the Philippine market, meeting local requirements and obtaining relevant certifications are important criteria for selection.

（9） Evaluation of Integration with local infrasutrucuture

Through the proof-of-concept, it was confirmed that Macnica ASM meets the basic functional requirements from risk notification to asset identification, administrator identification, and corrective action. However, there is significant room for improvement in operational process integration and scalability for overseas markets. While the asset identification function is highly effective and maintains a certain level of compatibility with existing CTEM (Continuous Threat Exposure Management) related products and security devices, differences in APIs and data formats with external asset management tools pose obstacles to centralization. Additionally, integration design with widely used overseas IT asset management tool is insufficient. Furthermore, requirements for integration with authority management systems, as well as with RBAC (Role-Based Access Control) and IAM (Identity and Access Management) commonly used by global companies, have not been defined, which constitutes a risk factor for global expansion. Although there are features that automate and present the process from vulnerability detection to suggesting countermeasures for corrective actions, integration with existing incident response workflows is limited. The following issues have been identified as areas of insufficiency.

- Insufficient support for global standard APIs and data formats.
- The management model for administrator information is dependent on domestic specifications, resulting in low compatibility with overseas authority management systems.

- The workflow for corrective actions is confined within Macnica ASM, and integration design with external SIEM and ITSM systems is underdeveloped.

As directions for improvement, it is necessary to redesign the API architecture and data models in compliance with international standards, enable integration with major ITSM and SOAR products as well as RBAC and IAM systems, and adopt a modular design. In addition, differentiating vulnerability detection and assessment logic is important to reduce competitive risks. Overall, while Macnica ASM demonstrates operational suitability, strengthening integration, standardization, scalability, and prompt alignment with international standards are essential for successful global expansion.

（１０） Evaluation of Operability and Ease of Technical Acquisition

The main challenges in operational integration of Macnica ASM are as follows:

Firstly, field personnel may not fully understand the reasons or methods for corrective actions, leading to delays in response. In Organization A, it was pointed out that ICT staff in various ministries lack security expertise, and email notifications alone are insufficient to prompt action. As a corrective measure, it is necessary to standardize actionable guidelines that clearly indicate the background of the risk, scope of impact, priority, and recommended response procedures, in addition to technical instructions. Furthermore, it is essential to add concise elements that communicate the business impact for decision makers and to design information so that field personnel can respond immediately.

Secondly, there is a lack of information needed to verify the validity of corrective actions, resulting in additional investigations and manual work. While Macnica ASM detects vulnerabilities and suggests countermeasures, existing systems do not sufficiently provide data to confirm the validity of the proposed actions. In particular, if detailed information substantiating the risk cannot be obtained via API, field personnel and approvers are forced to perform additional manual verification, which risks compromising the speed and accuracy of response. In Organization A, multiple meetings and further investigations are required to confirm the validity of corrective actions, leading to delays. In Organization B, SOC staff have also confirmed that Macnica ASM's information alone is insufficient for judgment, requiring supplementary data from Splunk or other tools.

To address these issues, it is necessary to enhance ASM's API functionality and provide comprehensive data needed for validating corrective actions. Specifically, vulnerability detection evidence, details of impacted assets, and technical background of recommended measures should be obtainable via API and integrated into existing approval and verification processes to improve both the speed and accuracy of response.

Based on these challenges, key improvement measures for establishing a sustainable operational model include advanced information design and enhanced data provision through API integration. By refining information design, corrective actions can be presented in a format that enables immediate response by field personnel, while clearly conveying the significance of risks to management. Strengthening API integration enables the automatic retrieval of validation information and integration with existing approval processes, ensuring both rapid and accurate responses.

（１１） Suggestions

This section presents policy recommendations for the government to proactively consider in order to further deepen public-private collaboration and establish a foundation to enhance the international competitiveness of Japanese domestic cybersecurity vendors. These recommendations comprehensively address institutional, financial, and technical support needed to eliminate structural barriers to overseas expansion and ensure the sustained competitiveness of domestic vendors in the global market. First, as part of institutional design for compliance with global standards, it is important to develop "International Standard Compliance Guidelines" to promote product development that meets international standards such as NIST SSDF and ISO/IEC 15408 (CC). These guidelines should aim to simplify the certification process, incorporate requirements at the design stage, and streamline audit responses, directly strengthening the international competitiveness of domestic vendors. Next, to support compliance with laws and regulations in the ASEAN and Indo-

Pacific regions, it is desirable to provide a “Regulatory Compliance Handbook” summarizing the regulations of each country, as well as to establish expert consultation desks and advisory services. The handbook should comprehensively cover topics such as cross-border data regulations, privacy protection requirements, encryption mandates, and audit standards, and present them in a format that can be reflected in product design and operational models. Furthermore, to accelerate development and reduce the initial investment burden for overseas expansion, it is advisable to introduce subsidies and tax incentives, and to design support measures for local sales activities and certification acquisition costs. Finally, consideration should be given to establishing mechanisms for disseminating market information specific to the cybersecurity sector, as well as for facilitating the building of human networks, sharing best practices, and promoting business matching among companies entering new markets.

Chapter 5 Cybersecurity Measures for Industrial Systems (OT)

5.1 Overall Overview

This study aims to conduct a needs assessment for cybersecurity in industrial control systems, with a particular focus on Operational Technology (OT) used for the control and operation of facilities and systems in industrial plants and critical infrastructure. The study was executed through subcontracting agreements with specialized Japanese firms for some or all parts of the needs assessment workshops, conducted in collaboration with Japanese organizations.

- Background and Objectives of the OT Workshops

With the global advancement of digitalization, cybersecurity risks are escalating. This presents a severe challenge for developing countries, which often lack adequate security frameworks and specialized human resources. In response, the Japanese government formulated the "Basic Policy on Capacity Building Assistance for Developing Countries in the Cybersecurity Field" in 2021 to promote capacity building through international cooperation. In line with this government policy, JICA has been striving to enhance the capabilities of developing countries through technical cooperation. However, these conventional efforts have been limited in their collaboration with industry and academia. Furthermore, as many ASEAN nations have now completed the identification of their Critical Information Infrastructure (CII), securing industrial systems (OT) has become a pressing issue. Against this backdrop, these workshops were designed to ascertain the status of OT cybersecurity considerations and specific demands in ASEAN countries. The objective is to provide foundational information for exploring the potential deployment of Japan's advanced expertise, such as that held by the Information-technology Promotion Agency, Japan (IPA).

- Execution of Interviews

This study was conducted through a combination of desktop research, online interviews, and on-site interviews. Initially, domestic experts in industrial cybersecurity and relevant organizations in the target countries were identified through desktop research. Subsequently, these candidates were interviewed to confirm their willingness to cooperate with the study. For the local organizations that agreed to become cooperating partners for the workshops, further on-site interviews were conducted to gather detailed information on the current situation and challenges in each country.

- Selection of the Subcontractor

Given the highly specialized nature of this study, a subcontractor selection process was undertaken. During preliminary interviews with potential candidates, Mr. Hiroshi Sasaki of the Nagoya Institute of Technology, a leading domestic expert, expressed his interest in participating. In view of our collaboration with the IPA Industrial Cybersecurity Center of Excellence (ICSCoE) and the decision to engage members of the university's Institute for Digitalization of Manufacturing −including ICSCoE graduates−we opted to proceed via a sole-source, non-competitive contracting approach .

The Nagoya Institute of Technology possesses unparalleled expertise and a proven track record in the OT security domain. It is home to numerous experts from industry and academia, including Mr. Sasaki. The university also maintains a robust international network with critical infrastructure operators and government agencies in the Philippines, ASEAN countries, and beyond, with extensive experience in organizing international conferences and workshops.

After a comprehensive evaluation of these essential qualifications, it was determined that the Nagoya Institute of Technology was the only organization currently capable of executing the required tasks accurately and expeditiously.

- Determination of Target Countries for OT Workshops

Thailand, the Philippines, and Indonesia were selected as the target countries for the OT workshops. As detailed in Section 4.2, "Selection of Target Countries for Demonstration of Japanese Corporate Products," these countries have existing JICA cooperation records and established collaborative platforms with local governments. Conducting demonstration projects and workshops concurrently in these nations allows for efficient implementation, including the identification of local needs, verification of technology adoption effects, and sharing of on-the-ground challenges.

・ Coordination with Target Countries for Workshop Implementation

Following interviews with relevant organizations in the target countries to confirm their intent to cooperate, workshops were conducted with the following three organizations serving as national counterparts.

- Thailand: National Cyber Security Agency (NCSA)
- Philippines: Department of Information and Communications Technology (DICT)
- Indonesia: Indonesia Cyber Awareness and Resilience Center of Universitas Indonesia (idCARE.UI), a research and education institution specializing in cybersecurity established within the Universitas Indonesia

・ Implementation of OT Workshops

The on-site workshops were conducted in collaboration with local partner organizations and implemented by a team from the Manufacturing and Innovation DX Laboratory of the Nagoya Institute of Technology, led by Professor Hiroshi Sasaki. The standard workshop structure consisted of: ① Self-introductions (Lightning Talks), ② a foundational lecture on OT security, ③ group work and presentations, and ④ closing remarks, with time allocations adjusted for each country (see Table 13). Through these workshops, the study investigated "the status of deliberations on cybersecurity policies for critical infrastructure," "the status of cybersecurity measures within critical infrastructure operators," "the demand for OT training in government agencies and critical infrastructure," and "the status of cooperation from other aid agencies in OT security."

Table 10 Sample Workshop Agenda (Indonesia)

Time (PM)	Program	In charge	Contents
1:00~1:10	Opening Remarks	idCARE.UI idNSA	Opening remarks by Dr. Muhammad Salman (idCARE.UI),Dr. Rudi Lumanto (idNSA).
1:10~2:30	Lightning Talk from Participants	NITech	Self-Introduction and sharing OT Security challenges for the participants along the topic template shared in advance.
2:30~2:40	Break①	-	
2:40~3:00	OT Security Basics Lecture (First Half)	Mr.Fujihara from NITech	OT security basics lecture (about Why) by Nagoya Institute of Technology (NITech)
3:00~3:30	Break②		For prayer time and break
3:30~4:10	OT Security Basics Lecture (Second Half)	Mr.Hasegawa Mr.Nakayama From NITech	OT security basics lecture (about How) and workshop guidance by Nagoya Institute of Technology (NITech)
4:10~4:55	OT Risk Workshop Work-1 Risk Analysis	Mr.Nakayama from NITech	Group Work 35 min Group Presentation (2 groups) 10 min * Mr. Hasegawa and Mr. Fujihara will be held on the support
4:55~5:05	Break③	-	
5:05~5:50	OT Risk Workshop Work-2 Risk Response	Mr.Nakayama from NITech	Group Work 35 min Group Presentation (2 groups) 10 min * Mr. Hasegawa and Mr. Fujihara will be held on the support
5:50~6:00	Certificate Award Ceremony	idCARE.UI idNSA	
6:00~6:05	Photo Session	All	
6:05~6:20	Closing Remarks	idCARE.UI idNSA	Closing remarks by NITech, Dr. Rudi Lumanto (idNSA),Dr. Muhammad Salman (idCARE.UI)

・ Compilation of the Report

This report was compiled based on the workshop findings report received from the subcontractor, Nagoya Institute of Technology, and the results of separately conducted interview surveys. The findings from both investigations were carefully examined, and the report is structured around the key outcomes and challenges identified. During the report preparation process, we engaged in prior consultations with the subcontractor regarding the outline and direction to ensure the comprehensiveness of the information presented.

5.2 Information on Cybersecurity Measures for Critical Information Infrastructure in ASEAN

5.2.1 Overview of OT Security across ASEAN

According to the 2023 report "Operational Technology Security in ASEAN[80]," published by the Association of Southeast Asian Nations (ASEAN) and the Economic Research Institute for ASEAN and East Asia (ERIA) awareness of information and communications technology (ICT) security has been

[80] Economic Research Institute Operational Technology Security in ASEAN

improving across the ASEAN region; however, awareness of—and preparedness for—operational technology (OT) security remain insufficient.

At the national level, Singapore and Malaysia are at the forefront of these efforts. Singapore has undertaken advanced initiatives, such as adopting the international standard IEC 62443 as a national standard and establishing a product certification scheme linked to government procurement requirements. Malaysia also adopted IEC 62443[81] as a national standard in 2023 and has begun developing guidelines for OT security. However, in many other ASEAN countries, concrete national-level initiatives for OT security have yet to emerge.

At the corporate level, the state of implementation is also inconsistent. Global corporations and some local companies—particularly those in critical infrastructure or those that have previously experienced OT-related incidents—tend to proactively implement measures by referencing global standards, regardless of the existence of domestic regulations. On the other hand, many ASEAN-based local firms, even if they recognize the importance of OT security, have not been able to undertake systematic countermeasures due to factors such as high costs, a shortage of specialized personnel, or the absence of clear government guidelines. Furthermore, there is a significant number of companies that assign a low priority to OT security due to a lack of understanding of its importance, as well as those that perceive a lower need for such measures because their factory automation is not advanced.

Thus, the current landscape of OT security in the ASEAN region is characterized by its reliance on the voluntary efforts of individual nations and companies. However, with the expansion of global supply chains, the importance of enhancing cyber resilience through coordinated regional efforts is growing. It has been noted that continuing with fragmented, individually optimized approaches poses a risk of losing global business opportunities. Furthermore, ERIA concludes that a coordinated, consensus-based regional approach is preferable－whereby national governments establish regulations grounded in regional agreement, and, within that framework, enterprises progressively mature their OT security measures.

5.2.2 Policy and Institutional Frameworks in Each Country

(1) Comparative Analysis of Cybersecurity-Related Policies and Strategies

All three countries—Thailand, the Philippines, and Indonesia—are actively working to strengthen the cybersecurity of their national critical infrastructure. They share a common approach in that central regulatory bodies lead these efforts: the National Cyber Security Agency (NCSA) in Thailand, the Department of Information and Communications Technology (DICT) in the Philippines, and the National Cyber and Crypto Agency (BSSN) in Indonesia. However, there are notable differences in the maturity of their institutional frameworks and the specific application of these frameworks to OT/ICS environments.

Table 11 Overview of Critical Infrastructure Security Policies by Country

Comparison Item	Thailans	Philippines	Indonesia
Lead Agency	NCSA	DICT	BSSN
CII Designation/Framework	Cybersecurity Act（2019）[82] established a framework for CII, defining CII and mandating risk assessments.	Institutional framework for mandating CII protection is under development（including legislative review[83]）	Presidential Regulation 82/2022 establishes a framework for IIV (Vital Information Infrastructure)[84]
Applicability to OT/ICS	Obligations for CII are being clarified (e.g., risk assessments).	National plans are in place, but implementation	National plans are in place, but implementation is still

[81] The international cybersecurity standards for OT (control systems) in factories and infrastructure, issued by the International Electrotechnical Commission (IEC)

[82] Government Gazette cybersecrutiy-act-2019-en.pdf

[83] Senate of the Philippines 19th Congress - Senate Bill No. 1365 - Senate of the Philippines

[84] Indonesian Audit Board (BPK) PERPRES No. 82 Tahun 2022

Comparison Item	Thailans	Philippines	Indonesia
		is still in the developmental stage.	in the developmental stage.
Standards Referenced by Participants	NIST CSF[85], NERC CIP[86]	None mentioned	IEC 62443[87]、NIST CSF

As shown in the table above, Thailand is relatively advanced in its institutional development, having formalized its Critical Information Infrastructure (CII) framework based on the Cybersecurity Act of 2019 and clarifying obligations such as risk assessments. In contrast, while the Philippines has articulated its direction at the national planning level, implementation in the OT domain remains in a developmental phase. Indonesia has established multiple regulations under the leadership of BSSN and made references to international standards like IEC 62443, but faces challenges related to varying levels of maturity among different organizations in practical application.

(2) Status and Challenges of Legal Systems and Guidelines for CII/IIV Protection

While all three countries are developing legal systems and guidelines for the protection of CII/IIV, a common challenge has emerged: frameworks designed primarily for IT environments often conflict with the unique constraints of OT. In OT environments, safety and availability are paramount, and legacy systems with long operational lifecycles are common. This makes it difficult to apply standard IT security measures, such as frequent patching or system reboots. As a result, even where policies and guidelines exist, they often fail to provide concrete solutions to practical questions on the ground, such as "How can we implement these measures without halting operations?" This "implementation gap" is a fundamental issue that undermines the effectiveness of regulations at the operational level.

5.2.3 Status and Challenges of Countermeasures by Critical Infrastructure Operators (from Pre-Workshop Surveys)

(1) Execution of the Pre-Workshop Survey

A pre-workshop survey was administered to all individuals registered for the OT Risk Workshop. The objective of this survey was to gain an understanding of the status of cybersecurity initiatives at the national level and the specific OT security measures within each participant's organization. This preliminary data collection was intended to ensure that the workshop discussions would be both effective and targeted. For detailed information on the survey respondents, please refer to Section 5.4.1 (Table 14).

The survey gathered participants' names and company affiliations and inquired about national-level cybersecurity frameworks, including relevant laws, regulations, and policies; the competent authorities for critical infrastructure; and the existence of information-sharing platforms or Information Sharing and Analysis Centers (ISACs). Furthermore, to assess the state of OT security within each organization, the survey investigated several key areas: perceived maturity levels across different sectors, the adoption status of formal policies and risk management frameworks, the locus of decision-making authority, the frequency of audits and inspections, and any prior experience with security incidents. These questions were designed to ascertain the current conditions and challenges at both the national and organizational levels, thereby enhancing the quality and substance of the workshop discussions.

(2) Current State of Organizational Structure and Governance for OT Security

The pre-workshop surveys revealed disparities in the development of OT security policies and frameworks among the countries. While Thailand showed progress in policy formulation, nearly half of the respondents in Indonesia reported having no such policies. A common trend was the involvement of executive

[85] An abbreviation for the NIST Cybersecurity Framework, which is a security framework designed for critical infrastructure in the United States.

[86] An abbreviation for North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), a set of standards to secure the North American bulk power system.

[87] An international standard for the cybersecurity of Industrial Automation and Control Systems (IACS).

management or IT/CISO[88] roles in final decision-making. However, the specific locus of authority varied, reflecting national policy influences on corporate governance structures: IT/CISO in Thailand, management committees in the Philippines, and the CISO in Indonesia. Despite the establishment of these governance structures, their effectiveness at the operational level is a separate issue, suggesting a potential disconnect between policy and practice.

(3) Status of Technical Measure Implementation and the "Partially Implemented" Challenge
Regarding technical measures, many organizations have implemented network segmentation (e.g., firewalls at the IT/OT boundary), basic monitoring, and access controls. However, the adoption of more advanced measures, such as comprehensive OT asset visibility, OT-specific threat detection and analysis (e.g., OT-IDS), and SIEM integration with OT environment logs, is lagging. A significant issue is that many measures are only "partially implemented." This does not indicate a disregard for security on the part of operators; rather, it reflects an inability to determine "what and how much is sufficient" within the unique constraints of their OT environments. This results in fragmented measures that fail to achieve comprehensive risk reduction.

(4) Status of Incident Response (IR) Readiness and On-the-Ground Anxiety
The results of the pre-workshop survey on incident response planning are as follows:

Table 12 Incident Response Planning

Aspect	Thailand	Philippines	Indonesia	Common Implication
Incident Experience (last 3 yrs)	14% (2/14)	7% (1/13)	11% (2/19)	Low level of practical experience.
IR Plan Covering OT	57% (8/14)	54% (7/13)	32% (6/19)	Lack of plans and drills is a significant weakness.
Confidence in Response	Medium to Low	Medium to Low	Low to Medium	Reflects insufficient training.

In all three countries, a low percentage of organizations (7% to 14%) reported experiencing an incident in the past three years, suggesting limited practical experience. The rate of having an Incident Response (IR) plan that includes OT is notably lower in Indonesia (32%) compared to Thailand (57%) and the Philippines (54%), indicating that a lack of comprehensive planning and training is a systemic weakness across the region. Correspondingly, confidence in their ability to respond to an incident remains at a "Medium to Low" level. Personnel on the ground commonly expressed anxieties such as, "We don't know how to respond if an incident occurs," and "Our IR plan doesn't cover OT, or it's just a theoretical exercise." This makes it evident that the absence of practical plans and sufficient drills is a major source of concern at the operational level.

5.2.4 Demand for OT Training and the Current State/Challenges of Support from Other Donors

(1) Analysis of OT Training Needs Based on Pre-Workshop Surveys
The pre-workshop surveys confirmed a strong demand for OT training, which can be categorized into three main areas. First, there is a demand for "training to make technology actionable," focusing on how to apply technical solutions like network segmentation and monitoring to their specific OT environments. Second, there is a "demand for human resource development for governance and operations," aimed at cultivating personnel who can manage the division of roles between IT and OT departments and oversee the development and execution of incident response plans. Third, there is a "clear need for hands-on, participatory training," with a preference for case studies, risk analysis, and incident response exercises

[88] An abbreviation for Chief Information Security Officer, a C-level executive responsible for an organization's information and data security.

over purely theoretical lectures, as these are directly applicable to solving organizational challenges.

(2) Current State and Limitations of Support from Other Institutions

In the ASEAN and Indo-Pacific region, various international organizations, national governments, and private entities, including JICA, provide cybersecurity training and capacity-building support. These efforts have achieved some success in promoting institutional understanding and disseminating foundational knowledge. However, limitations have also been identified. Common issues include training being delivered as one-off events that do not support long-term operational integration within organizations; a focus on IT security that fails to adequately address the unique availability and safety constraints of OT; and program designs that do not integrate technology, human resources, and operations holistically. As a result, existing support does not always translate into solutions for the concrete challenges faced on the ground.

5.2.5 Willingness of Relevant Organizations to Cooperate, Identified Challenges, etc.

This section describes the results of interviews conducted by the study team with potential counterpart organizations in each country prior to the workshops.

(1) ASEAN Japan Cybersecurity Community Alliance

- Organizational Overview

The ASEAN Japan Cybersecurity Community Alliance [89] (hereinafter "AJCCA") is an international collaborative organization composed of cybersecurity-related groups from Japan and ASEAN countries. Its primary objective is to deepen mutual understanding, exchange, and cooperation regarding cybersecurity governance and operations in the Japan-ASEAN region, aiming to enhance cyber resilience and build capacity. Its activities include information sharing on cyber threats, promoting industry-government-academia collaboration, and fostering sustainable cybersecurity capabilities. Its members include the Japan Network Security Association (JNSA) and eight other cybersecurity industry associations from ASEAN countries (at the time of its establishment).

- Interview Summary

An interview was conducted with AJCCA to ascertain its organizational overview, strengths, and the collaborative value it could bring to this project. Specifically, it was determined that because cybersecurity matters often involve sensitive national information, the alliance's intermediation would provide access to substantive, on-the-ground information held by local government agencies and critical infrastructure operators—information that is typically difficult to obtain. This access is rooted in the strong, trust-based relationships that AJCCA has cultivated with these national bodies. The understanding was reached that this capability represents an indispensable asset for the project's success, one that would be nearly impossible for a Japanese company to secure independently.

(2) Indonesia

- Badan Siber dan Sandi Negara (National Cyber and Crypto Agency, Indonesia)
  - Organizational Overview

Established on January 3, 2018, the Badan Siber dan Sandi Negara (hereinafter "BSSN") is Indonesia's primary government agency for cybersecurity. It has comprehensive jurisdiction over cybersecurity, cyber intelligence, cryptography, and information security. In coordination with the police and the national intelligence agency, BSSN is responsible for ensuring the security of Indonesia's digital space by combating cybercrime, preventing the spread of disinformation (fake news) and hate speech, and countering the online proliferation of extremist ideologies.

  - Interview Summary

BSSN expressed its willingness to cooperate in hosting the OT workshop in Indonesia. For the workshop's execution, they requested a demonstration of a fully automated OT cybersecurity product that is currently in practical use within Japanese private-sector companies. They also

[89] SEAN Japan Cybersecurity Community Alliance (AJCCA) Landing - ASEAN Japan Cybersecurity Community Alliance (AJCCA)

requested that the workshop's content be sharply focused on the OT domain. Furthermore, as a means of differentiating the workshop, they proposed including a presentation on the cybersecurity strategies employed by Japanese corporations. To ensure the workshop's success, BSSN raised specific points for consideration aimed at enhancing its effectiveness, such as "clarifying the requirements for issuing training certificates" and "differentiating the initiative from similar programs to heighten interest among potential participating companies." A constructive dialogue was conducted, and BSSN committed to introducing the project to relevant agencies and critical infrastructure operators, on the understanding that these considerations would be addressed.

- Indonesia Network Security Association
  - ➢ Organizational Overview

The Indonesia Network Security Association (hereinafter "idNSA") is an industry association dedicated to enhancing cybersecurity and network security within Indonesia. Its vision and mission are to foster security professionals, share knowledge, and promote standardization. Its main activities include hosting seminars, providing training and certification programs, and community-building. Governed by a board of directors, idNSA is a leading entity in Indonesia's cybersecurity field. As a key member of the ASEAN-Japan Cybersecurity Community Alliance (AJCCA), it actively engages in strengthening regional collaboration and cooperating with Japan (JNSA).

  - ➢ Interview Summary

idNSA showed a positive attitude towards conducting an OT-related workshop and confirmed its capacity to facilitate discussions with partners such as the Universitas Indonesia. They advised that AI-based products are a current trend in the cybersecurity field and that a Memorandum of Understanding (MOU) or Non-Disclosure Agreement (NDA) might be required when conducting a Proof of Concept (PoC). It was also shared that a key characteristic of the Indonesian market is the high demand for cybersecurity professionals—with an estimated shortfall of 1.5 million—coupled with significant room for improvement in corporate awareness. This indicates a substantial opportunity for the project's capacity-building and awareness-raising activities to effectively address these pressing local needs. Furthermore, it was pointed out that the budgets of critical infrastructure companies currently tend to be prioritized for other areas, which led to the conclusion that a strategy focused on introducing cost-effective solutions and clearly articulating the importance of OT security investment would be effective.

(3) Philippines

- Department of Information and Communications Technology (Cybersecurity Bureau)
  - ➢ Organizational Overview

The Department of Information and Communications Technology[90] (hereinafter "DICT") is the primary executive agency in the Philippines responsible for ICT policy-making and promotion. It contributes to improving citizens' lives and economic development by formulating ICT development strategies, improving public access, developing communications infrastructure, implementing cybersecurity measures, promoting the digitalization of government agencies and industrial growth, and engaging in international cooperation.

  - ➢ Interview Summary

DICT expressed its willingness to cooperate in conducting an OT-related workshop. It confirmed its intention to assist with all necessary preparations, from inviting participants to managing the workshop on the day of the event.

- Philippine Computer Emergency Response Team
  - ➢ Organizational Overview

The Philippine Computer Emergency Response Team[91] (hereinafter "PH-CERT") is the highest

[90] Department of Information and Communications Technology https://dict.gov.ph/our-mandate
[91] NCERT About Us | NCERT

body for cybersecurity activities in the Philippines. Its primary roles include responding to cybersecurity incidents, coordinating with and receiving reports from various domestic CERTs, and conducting network monitoring, security testing, and vulnerability assessments. PH-CERT is the common name for the National Computer Emergency Response Team (NCERT), a subordinate unit of the Cybersecurity Bureau of the DICT, and was also established as the Philippines' first non-profit cybersecurity organization.

- Interview Summary

PH-CERT indicated its willingness to cooperate in organizing an OT-focused workshop, offering to introduce relevant contacts and arrange for speakers. They expressed a cooperative stance towards the project and anticipation for its future development.

(4) Thailand

- National Cyber Security Agency
  - Organizational Overview

The National Cyber Security Agency (hereinafter "NCSA") is the central government body overseeing Thailand's cybersecurity measures. The NCSA is responsible for formulating national cybersecurity policies and strategies, defending critical information infrastructure, responding to cyberattacks, raising cybersecurity awareness, developing human resources, and promoting international cooperation with ASEAN nations and others. Established under the *Cybersecurity Act of 2019*, it plays a vital role in ensuring the safety and resilience of Thailand's digital environment.

  - Interview Summary

The NCSA expressed its willingness to cooperate in hosting the OT workshop for this project, including introducing the project to critical infrastructure operators. Regarding cybersecurity challenges in Thailand, the NCSA acknowledged the slow response speed to domestic cybersecurity incidents. It was noted that strengthening measures is particularly necessary in the healthcare sector, which handles sensitive information, and in the "Energy and Public Utilities" and "Transportation and Logistics" sectors with respect to OT.

- Thailand Information Security Association
  - Organizational Overview

The Thailand Information Security Association (hereinafter "TISA") is a leading non-profit association composed of information security professionals, researchers, and related industry groups in Thailand. TISA's main activities include promoting cybersecurity domestically and internationally, fostering human resources and standardization, collaborating with domestic and international industry groups, and sharing information. It contributes to the advancement of the cybersecurity field by organizing seminars and workshops, developing best practices and ethical codes, and participating in international cooperative activities such as the Japan-ASEAN Cybersecurity Public-Private Joint Forum. TISA is a key private-sector partner organization that works in conjunction with the NCSA, which was established in 2019.

  - Interview Summary

TISA shared insights into the current situation in Thailand, explaining the de facto division of roles wherein government-led workshops are primarily handled by the NCSA. Consequently, they advised that the most effective structure for this workshop would be to designate NCSA as the primary collaborating partner, with TISA contributing in its capacity as a representative of the private sector by providing specialized expertise and facilitating industry outreach. Additionally, a common understanding was reached that OT security constitutes the primary cybersecurity challenge within Thailand's critical infrastructure. Given that investments are presently focused on the IT sector, enhancing OT security has been identified as a key priority moving forward. A view was expressed that there is particularly significant potential demand for OT security measures in sectors such as electricity, water, and transportation, indicating considerable scope for this project to make a meaningful contribution. Furthermore, they observed a market trend shifting away from the traditional model of equipment procurement and installation towards

consulting, offensive cybersecurity services for infrastructure testing, and the utilization of Managed Service Providers.

5.3 Status of Deliberation and Needs Regarding OT Cybersecurity

5.3.1 Current Status of Deliberation and Recognized Challenges in OT Security

As analyzed in section 5.2, while national governments are promoting the strengthening of OT security, the policies they have formulated are often IT-centric, leading to a common "implementation gap" at the operational level. Against this backdrop, critical infrastructure operators recognize that the increasing integration of IT and OT networks, driven by digital transformation (DX) initiatives and the introduction of remote maintenance, is creating new attack vectors. The common challenges faced by these operators can be summarized into the following four points:

1. Emergence of risks associated with IT-OT convergence.
2. Constraints imposed by long-running legacy equipment, such as systems with end-of-support OS, and the paramount need for availability.
3. A shortage of security personnel who understand the unique characteristics of OT.
4. Anxiety regarding response capabilities in the event of an incident.

These challenges have resulted in a situation where many operators have only implemented technical measures partially, failing to achieve systematic risk reduction.

5.3.2Needs Related to OT Security

(1) Needs for Technology Implementation and Consulting

Given that many operators have only "partially implemented" technical measures and are struggling with the question of "what to do and to what extent is sufficient," there is a strong demand for consulting services related to technology implementation prioritization and overall architectural design. What is required is not merely support for product installation, but a partnership to collaboratively develop a risk-based approach. This partnership would presuppose the unique constraints of OT, such as availability and safety requirements and the presence of legacy equipment, to assess risks and devise a phased implementation plan, starting with low-impact measures like asset visibility and network segmentation.

(2) Needs for Human Resource Development and Training

Regarding human resource development, there is a high demand for cross-organizational training that includes not only technical staff but also executive management and operational departments. Specifically, there is a need to foster capabilities in designing and operating technology within OT-specific constraints, bridging the gap between IT and OT, and developing and operationalizing incident response plans. Furthermore, there is a very high expectation for hands-on, participatory training programs that encourage participants to think and discuss solutions tailored to their own organization's challenges, rather than passively receiving knowledge. On a country-specific basis, Thailand shows a high demand for implementation- and exercise-focused training, the Philippines for support in investment decision-making, and Indonesia for systematic, foundational training.

(3) Needs for Participation in Domestic and International Information Sharing and Exercises

Many organizations feel limited in their ability to handle incident response and advanced threat analysis on their own and are seeking opportunities to learn from the experiences and knowledge of other organizations. Since threats to critical infrastructure can affect an entire sector, there is a high demand for initiatives that enhance the collective response capability of the industry through sector-wide information sharing and joint drills. In particular, many organizations lack formal incident response plans or have low confidence in their response capabilities, creating a clear demand for participation in practical exercises to improve the effectiveness of their plans and enhance their response skills.

5.3.3Presenting a Japan-led Approach to Address Challenges and Needs

To address the challenges and needs identified in this study, particularly the issue of "IT-centric security concepts not being translated for the OT environment," the workshops presented an approach based on Japan's advanced expertise.

(1) Design Philosophy of the Foundational Lecture in the Workshops

The foundational lecture on OT security was designed not merely to provide knowledge, but to equip participants with a "common language" and a "framework for thinking" to connect policy, on-the-ground challenges, and implementable measures. The intention was to foster a shared understanding among participants from diverse backgrounds and thereby enhance the quality of the subsequent group work.

(2) Deploying Japanese Expertise: Utilization of METI Guidelines

The lecture covered an explanation of the checklist based on METI's "Guidelines for Cyber-Physical Security Measures in Factory Systems (Ver. 1.0)," issued on November 16, 2022, and its mapping to solutions in the operational technology (OT) domain (Figure 32).

Sub Cat.	Item	OT security solutions for each term	
Asset management	2-6 2-7	Communication terminal visibility and control in the network	OT-IDS, Asset Management tool, NAC
Endpoint Protection	3-1 3-2 3-3	• Client protection and centralized management • Apply virtual patches • Application whitelist or blocking of designated communications	AV,EDR,. Whitelist (WL),. USB-Type AV
Network	3-5 3-6 3-7	• Segmentation and security measures with VLANs • Secure remote maintenance • Communication terminal visibility and control in the network	UTM,SW/AP FW, SRA,. Decoys, OT-IDS
Log	3-8	Communication log storage and reporting	Syslog Server SIEM, etc.

Figure 23 Checklist based on METI's "Cyber/Physical Security Guidelines for Factory Systems"and Its Correspondence with Security Products

This checklist served as a practical tool for many operators facing the challenge of "not knowing where to start," enabling them to visualize their current status and prioritize countermeasures. A key feature was its positioning not as an audit checklist, but as a dialogue tool to help determine the best starting point for action.

(3) Presentation of a Risk-Based Approach and Phased Implementation

A core element of the lecture was the presentation of a "risk-based approach" (Figure 32), which starts from business risks (safety, quality, business continuity, etc.) rather than treating technical measures as an end in themselves.

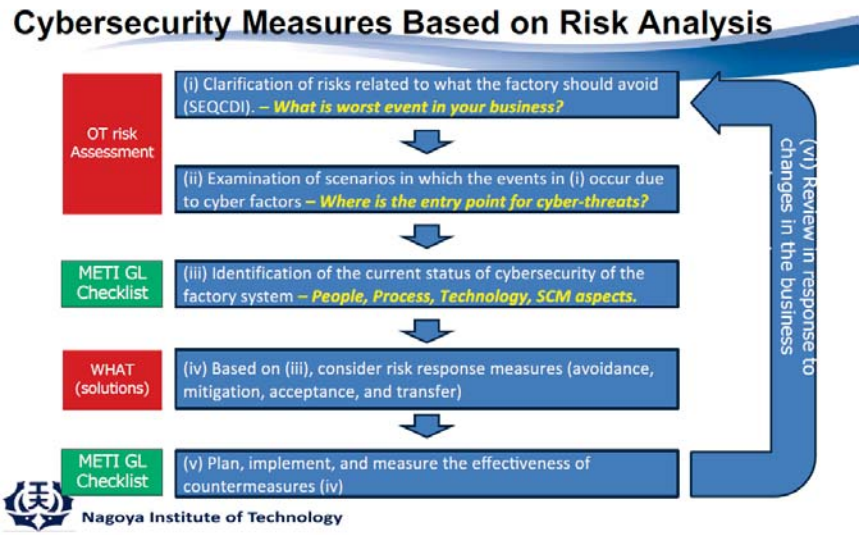


Figure 24 A Field-Risk-Based Approach to OT Security

This methodology involves first articulating "undesirable events" from the perspectives of Safety, Environment, Quality, Cost, Delivery, and Information (SEQCDI), and then linking these to cyber factors and considering appropriate countermeasures. Furthermore, for technology implementation, a model (Model X/Y/X+/Y+) was presented, categorizing solutions based on the scope of threat detection and the level of response automation. This model conveyed the concept of phased maturity, showing that it is possible to "build up from what is currently achievable" rather than feeling that "nothing can be done without advanced products." This proved to be a realistic and effective approach for operators constrained by legacy systems and budgets.

5.4 Information Gathered from Workshop Implementation

5.4.1Workshop Implementation Overview

The workshops were held in three countries—Thailand, the Philippines, and Indonesia—with the objectives of assessing the current state of OT cybersecurity measures, clarifying training needs and policy challenges, and enhancing the awareness and capabilities of the participants. The implementation details are as follows.

Table 13 Workshop Implementation Overview

Item	Thailand	Philippines	Indonesia
Country/City	Thailand, Bangkok	Philippines, Manila	Indonesia, Jakarta
Venue	TK Palace Hotel & Convention	The B Hotel	Universitas Indonesia
Date	November 2, 2025	November 24, 2025	December 22, 2025
Valid Survey Responses	14	12	19
Main Participant Sectors	Electricity, Transportation, Government, Telecom, Water, Oil & Gas	Electricity (Generation), Government, Water	Telecom, Manufacturing, Energy, Finance, Government
Local Partner(s)	NCSA	DICT	idNSA[92]、idCARE.UI[93]
Format	In-person	In-person	In-person

[92] Indonesia Network Security Association (an industry association)
[93] Indonesia Cyber Awareness and Resilience Center, Universitas Indonesia

Participants were IT and OT security personnel invited from critical infrastructure operators and relevant government agencies in each country, representing a wide range of sectors. The program consisted of ① self-introductions, ② a foundational lecture on OT security, ③ group work and presentations, and ④ closing remarks, designed to foster a common understanding and stimulate concrete discussions among participants.

5.4.2Key Discussions and Implications from Each Country's Workshop

・ Thailand: "Policy-led, but challenges in operationalization and talent retention"

The workshop in Thailand suggested a structure where, despite relatively well-developed national policies and guidelines, the on-the-ground operationalization—including incident response planning and training—is lagging due to a limited number of personnel who understand OT. This points to a challenge of being "policy-led, but with issues in operationalization and talent retention." Although there was a knowledge and experience gap among participants, the objective of understanding the basic framework for risk assessment through group work was achieved. Future cooperation would be effective if it focused on enhancing practical application through exercises and operational templates, building upon the existing frameworks.

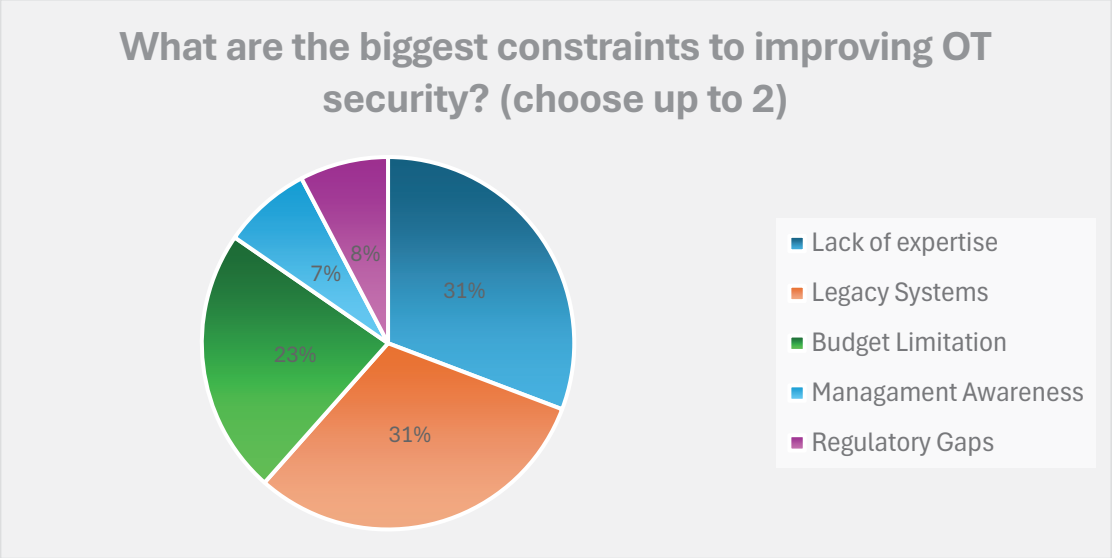


Figure 25　Responses on the Biggest Challenge in Improving OT Security (Thailand)

・ Philippines: "High management engagement, but budget and legacy constraints are barriers"

In the Philippines, discussions reflected a high level of management engagement and awareness of business impacts. However, the situation was characterized as "high management engagement, but with budget and legacy constraints acting as barriers" to the implementation of technical measures. The overall skill level of participants was high, leading to sophisticated discussions that clearly identified assets to be protected and priorities. Future cooperation should focus on providing support that clarifies the rationale for investment decisions through risk prioritization and visualization.

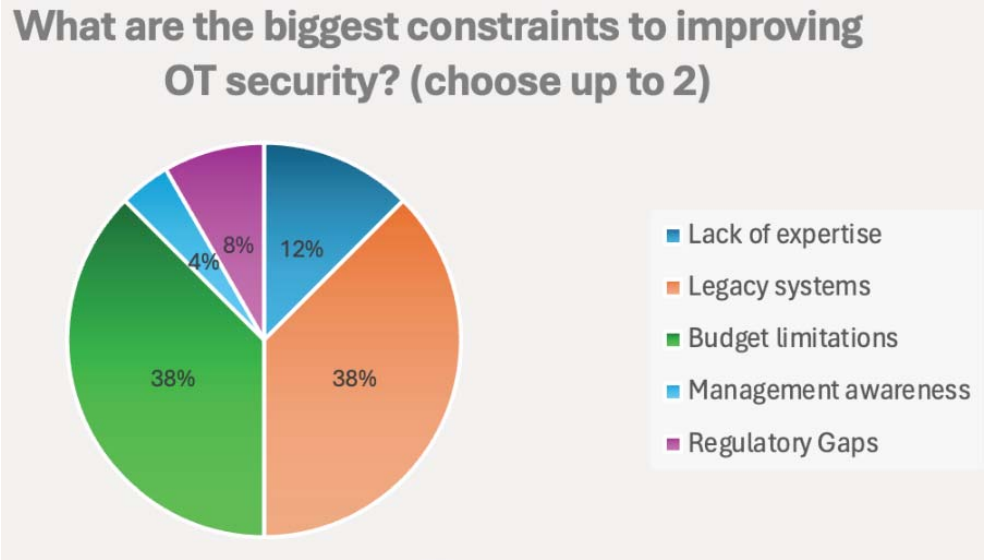


Figure 26　Responses on the Biggest Challenge in Improving OT Security (Philippines)

・ Indonesia: "Numerous regulations, but a lack of personnel and planning is the greatest challenge"

In Indonesia, while multiple regulations and international standards are referenced, the rate of formal incident response planning that includes OT is low (31.6%), indicating a failure to transition to an organized operational framework. This suggests a situation of "numerous regulations, but a lack of personnel and planning is the greatest challenge." High-quality discussions were led by participants well-versed in both IT and OT. Future cooperation must prioritize foundational templates (e.g., IR Playbooks) and exercises to provide phased support that builds up the organization's overall response capability from the ground up.

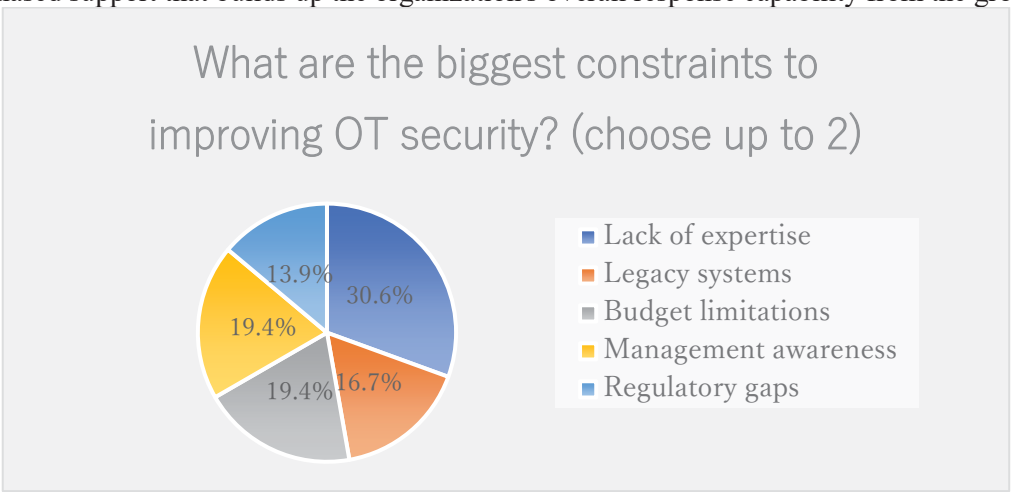


Figure 27　Responses on the Biggest Challenge in Improving OT Security (Indonesia)

5.4.3Overall Observations

・ Common Challenges and Needs Across the Three Countries

A structural issue common to all three countries was the "implementation gap between policy and practice," where national-level policy development is progressing, but a concrete vision for implementation that considers OT-specific constraints has not reached the operational level. This has led operators to face common challenges, including "risks from IT-OT convergence," "legacy systems," "personnel shortages," and "anxiety about incident response." Against this backdrop, there was a strong, shared demand for training to make technology practical, for developing personnel to lead governance, and for hands-on, exercise-based training.

・ Recommendations for the Direction of Future Cooperation

Based on the findings of this study, future cooperation should leverage Japan's unique strengths, such as

the philosophy of "securing operations without disruption" embedded in its manufacturing industry and its risk-based approach that starts from on-the-ground realities. We propose the following three directions. First, to "evolve from one-off workshops to continuous programs" with phased stages for foundational knowledge, application, and institutionalization. Second, to bridge the gap between policy and practice by placing "templates and exercises, such as IR Playbooks and exercise scenarios, at the core" of the support. Third, to "provide support premised on a phased technology adoption" that progresses from "visualization" to "monitoring" and "control," in line with the realities of OT environments.

Chapter 6 Recommendations and Summary

(1) Implementation of the Reporting Session

A) Overall Summary

In order to summarize the outcomes of this project and obtain concrete insights for future project formulation by JICA, the final reporting session was held in Japan on Wednesday, January 28, 2026. The session took place at the Marunouchi Nijubashi office of Deloitte Tohmatsu LLC. The program consisted of two parts: Part 1 (9:30–11:00), where the three companies that conducted PoCs shared their results regarding Japanese cybersecurity products; and Part 2 (11:00–12:00), where the results of the OT workshop were presented, focusing on cybersecurity measures for industrial systems (OT). Participants included representatives from the STI&DX Office, Governance and Peacebuilding Department, JICA, Deloitte Tohmatsu LLC, the three companies that conducted PoCs (Amiya, Macnica, IIJ) in Part 1, and representatives from Nagoya Institute of Technology in Part 2. Active discussions were held among all parties.

The aim of this reporting session was to understand the current state of Japanese private sector and academic knowledge and technology in the cybersecurity field, and to consider the potential for deployment to ASEAN countries. Given the limited utilization and knowledge of Japanese companies and research institutions, as well as the insufficient progress in capturing on-site needs and overseas expansion of products, the session aimed to share the achievements and challenges obtained during the project period with JICA, and to facilitate multifaceted discussion for future project formulation. The agenda included reports from the three PoC-implementing companies and Nagoya Institute of Technology on their results, identified challenges, and recommendations for future JICA project development. Lively discussions involving JICA followed each report.

B) Information on Japanese Cybersecurity Products

During the exchange of opinions with the three PoC companies, proposals for strengthening event support to accelerate Japanese companies' local deployment were presented to JICA. Specific suggestions included providing opportunities for business matching, holding security conferences, and organizing workshops inviting government officials. There were also expectations for JICA-hosted events in the "Japan Pavilion" format. The importance of supporting the discovery and development of local partners through collaboration with local IT associations and industry was emphasized.

Regarding field deployment, adaptation to local regulations and the costs of implementation and maintenance were identified as barriers. Environmental improvements in terms of systems and costs were cited as challenges. Specific proposals included support for developing guidelines to comply with regulations, subsidies for local implementation costs as incentives, and assistance for compliance with international standards. In particular, it was reported that local government agencies requested subsidies for implementation costs. Additionally, there were expectations for support in securing budgets and streamlining contract procedures for full-scale implementation after the PoC phase.

For the sustainable operation of cybersecurity measures, the development of local human resources and the establishment of continuous support systems after implementation were deemed essential. Given the shortage of local personnel and resources, proposals included subscription-based ongoing support and technology transfer-type assistance to enable local staff to become self-reliant. JICA introduced examples of cybersecurity human resource development across ASEAN, expressing the view that practical training for field staff and community formation through collaboration with major universities and national institutions would be effective.

Furthermore, the importance of promoting public relations and awareness activities to highlight the strengths of Japanese products and enhance brand recognition in local markets was stressed by the PoC companies. Japan's strengths were identified not only as technological capability but also in design, including operation and governance, as well as a commitment to accountability. The importance of building trust based on the local culture of valuing face-to-face relationships was pointed out. Flexible

reporting and operational support tailored to the varying levels of maturity and culture in each country and sector, as well as the sharing of patterns and knowledge for execution support to compensate for workforce shortages, were also considered meaningful initiatives for future efforts.

Figure 28 PoC Reporting Session: company reports and discussion

C) Status of Cybersecurity Measures for Industrial Systems (OT)

In the exchange with Nagoya Institute of Technology, which conducted the OT workshop, it was pointed out that OT cybersecurity measures should not be seen merely as technology adoption but as tools for reducing business risk. The top priority is to protect field operations and safety, with cyberattacks being one of many threats. This change in perspective is believed to facilitate understanding and acceptance on the ground and prevent institutional hollowing. Concerns were also raised about measures becoming ends in themselves. If measures are implemented for their own sake, there is a risk that patches may be applied

in accordance with guidelines even if there is a risk of system downtime. Instead, it is necessary to determine whether the measures are appropriate from the perspective of reducing business risk.

The importance of providing support tailored to the level of maturity in each country was also highlighted. In Thailand, the Philippines, and Indonesia, there are different challenges such as human resource development, equipment renewal, and planning. Therefore, rather than uniform support, implementation support that fits the situation on the ground is preferable. Concrete support for improving the effectiveness of incident response plans and initial implementation support using checklists based on the Ministry of Economy, Trade and Industry (METI) guidelines were considered effective. The METI checklist has fewer items than frameworks such as NIST and starts from the "People" perspective, making it easier to assess the current situation even if the organizational structure is not fully established.

In IT-centric systems, "confidentiality" tends to be prioritized, but in OT environments, "safety" and "availability" are the top priorities. To bridge this gap, it is necessary to adopt a risk-based approach specialized for OT and to consider feasible measures from a field perspective that do not halt operations. Due to the historical background of IT security, there is a tendency to focus on confidentiality; however, in OT, service disruption from cyberattacks poses a major risk, so it is important to proceed in ways that the field can understand "why this measure is necessary."

Support that integrates not only technology but also organizations ("People") and processes ("Process") could lead to differentiation unique to Japan. Providing practical mechanisms that connect systems and the field could be a strength of JICA's international cooperation. For example, there was a case where a factory, after a cyberattack, resumed production by manually retrieving shipping information instead of restoring the IT system. Such responses are only possible through prior planning and organizational/system preparedness, showing that support for organizations and processes, not just technology, is effective.

Based on the above, proposals for JICA's future initiatives included on-site, hands-on support focused on field implementation, introducing a business risk reduction perspective, promoting OT-specific risk-based approaches, and providing comprehensive support for organizations and processes.

Figure 29 OT Workshop Reporting Session: Presentation and Discussion

(2) Recommendations & Summary

A) Information on Japanese Cybersecurity Products

The initiatives of the three companies in this PoC project concretely demonstrate the conditions and issues for Japanese cybersecurity products to be competitive in the global market.

Macnica, in the competitive Philippine market where high technical capability and compliance with global standards from US and Israeli vendors are required, is advancing product design and rapid market entry based on local laws and regulations. It leverages trust and networks with local partners and takes into account the unique culture and business practices of the Philippines. Challenges remain in local language

support, human resource development, and brand recognition, requiring the establishment of a local sales structure, agile product development, and strengthened marketing. Going forward, Macnica will continue to focus on providing solutions and strengthening its system to meet local needs for sustainable market development.

Amiya Corporation's ALog SIEM proposes a product design and operational model tailored to the constraints of the Thai market (cost-consciousness, shortage of personnel, compliance with personal data protection laws, etc.). For mid-sized companies where the introduction of advanced SIEMs is difficult, features such as no need for specialized knowledge, patented compression technology, local storage, and automation help lower realistic barriers to implementation and operation. High compatibility with PDPA (Thailand's Personal Data Protection Act) and easy management of audit trails and cause identification are highly valued locally. Partnerships with local companies and educational institutions are already in place, forming a foundation for future horizontal expansion. ALog is positioned not as an "automatic decision-making SIEM" but as a "SIEM that makes human decision-making easier," and its operational design matches local needs.

IIJ is advancing the standardization of access control and audit trail models using Safous in the maritime sector, a critical infrastructure area. In environments where IT and OT coexist, IIJ achieves visibility, accountability, and operational efficiency simultaneously. The phased introduction and common model proposals serve as leading examples for the advancement of OT security and compliance with global regulations. Safous has been recognized for its effectiveness in addressing existing challenges such as lack of access control, unclear responsibilities, and absence of audit systems. The platform also provides a foundation for expansion into maritime information platforms, aligning with the trend toward strengthened regulations and incident responses in critical infrastructure both domestically and internationally.

From these cases, the key factors for successful overseas expansion are thorough compliance with local laws and regulations, UX and operational design calculated from on-site issues, collaboration with local personnel and partners, and building common platforms with an eye to phased expansion. Going forward, it is necessary to develop institutional, financial, and technical foundations to support ecosystem-type growth, including government-private sector cooperation for global certification and regulatory support, the rapid establishment of local sales structures, and the design of incentives for local companies.

B) Status of Cybersecurity Measures for Industrial Systems (OT)

Based on the results of cybersecurity workshops for industrial systems conducted in Thailand, the Philippines, and Indonesia, it was found that while national-level policies and frameworks are steadily advancing in all three countries, significant challenges remain in implementing these measures on the ground. The main factors behind this so-called "implementation gap" include the fact that, at industrial sites such as factories, safety and operational continuity are the highest priorities. Because many legacy systems remain in operation for long periods, it is difficult to directly apply measures and regulations that have been primarily designed for the IT sector.

As a result, common issues have emerged such as the lack of comprehensive incident response plans, shortages of specialized personnel, and only partial adoption of technical countermeasures. To address these challenges effectively, it is important to standardize risk-based checklists and incident response plans, conduct onsite exercises and training, and promote information sharing and joint exercises within the industry. Additionally, gradually and systematically introducing technical measures such as asset visibility, network segmentation, and monitoring is essential.

As for priorities by country: in Thailand, the urgent issues are ensuring the proper integration of measures into daily operations and enhancing practical exercises; in the Philippines, prioritizing risks and clarifying the basis for investment decisions are key; and in Indonesia, building a foundation for human resource development and plan formulation is a pressing need. Going forward, it is expected that cooperation will evolve into continuous support programs that connect policy with field operations, leveraging Japan's philosophy of "protecting without halting operations" and approaches that start from onsite risks.

C) Overall Summary

While policy and institutional development are progressing in each country, there is still a gap in actual implementation at OT sites, and it is necessary to address this gap while simultaneously strengthening the global competitiveness of Japanese cybersecurity products. The background to the implementation gap includes operational cultures that prioritize safety and availability, the existence of legacy equipment, and shortages of personnel and budgets, resulting in only partial implementation of measures. On the product side, challenges include compliance with local laws, UX design based on field operations, language and personnel support, brand recognition, and lack of common platforms. To address these issues, ongoing implementation support that bridges policy and practice and support for ecosystem-type market development are considered effective.

For example, in technical cooperation, it is effective to jointly develop, with Japanese companies, cybersecurity product implementation packages that can be immediately utilized at system user sites in developing countries, while also providing guidance on operational methods to promote the establishment of "protect without halting operation" measures. It is expected that risk-based checklist and incident response plan templates will be customized according to the maturity level of the site, and step-by-step introduction mechanisms will be built. In addition, establishing regular tabletop exercises, sharing evaluation indicators, and institutionalizing cross-sector joint exercises are meaningful. Providing integrated IT/OT operational models and guides for phased implementation of asset visualization, segmentation, and monitoring will also enhance effectiveness on the ground. Furthermore, it is important to develop frameworks for public-private consortia to formulate procedures for compliance with local laws and division of responsibilities, and to promote the establishment of regulatory operations in cooperation with relevant authorities. For local human resource development and community formation, promoting technology transfer in collaboration with major universities and national institutions is expected.

Regarding grant aid, it is effective to supplement initial equipment shortages and create environments where countermeasures can be quickly started on site. Efforts to maximize impact while minimizing costs include the provision of equipment with basic monitoring and visualization functions, establishment of logical separation and gateways, installation of training labs and regional training centers, and initial support for network-centric measures that can be introduced without halting operations. In addition, as part of partial subsidies for local implementation costs and sustained operational support, measures such as subsidizing operating expenses related to local support for a certain period, providing phased assistance for maintenance costs, and funding the development and dissemination of guidelines for compliance with local laws and regulations are considered effective.Financial support is also needed for securing budgets and streamlining contract procedures for full-scale implementation.

Japanese cybersecurity companies may consider leveraging JICA's SDGs Business Supporting Survey (JICA Biz) as one option to advance, in an integrated manner, the local deployment of Japan-origin products and services, the establishment of operational frameworks, and the building of trust with stakeholders. The program provides hands-on, side-by-side support for local regulatory compliance of products and services, the acquisition of international certifications, and the development of local business partners and business models, while also conducting small-scale pilot demonstrations in specific sectors of critical information infrastructure to make the effectiveness visible. Furthermore, based on the operational, technical, and commercial insights (including distribution flows) gained from these pilots, further demonstrations in other sectors are expected, aiming for horizontal rollout. In addition, because it is desirable to promote the discovery and development of local partners through collaboration with local IT associations and industry, it may also be considered, as part of validating customer needs, to raise the brand awareness of Japanese cybersecurity companies (JICA Biz-selected companies) by participating in various local events and conferences and by hosting workshops.

Overall, an approach that simultaneously enhances the resilience of critical infrastructure and the competitiveness of Japanese solutions by integrating institutional, financial, and technological measures,

centered on Japan's philosophy of "protect without halting operation", is considered effective. Sustained achievement is expected through continuous support for field-based implementation and the gradual resolution of gaps between policy and operation.


ジャイカ
JICA