

REPUBLIC OF INDONESIA

UNIVERSITY OF INDONESIA

REPUBLIC OF INDONESIA
PROJECT FOR HUMAN RESOURCES
DEVELOPMENT FOR CYBER
SECURITY PROFESSIONALS
(OSS DEVELOPMENT /
CYBERSECURITY)
WORK COMPLETION REPORT

MAY 2023

JAPAN INTERNATIONAL COOPERATION AGENCY

TOKYO CO., Ltd.

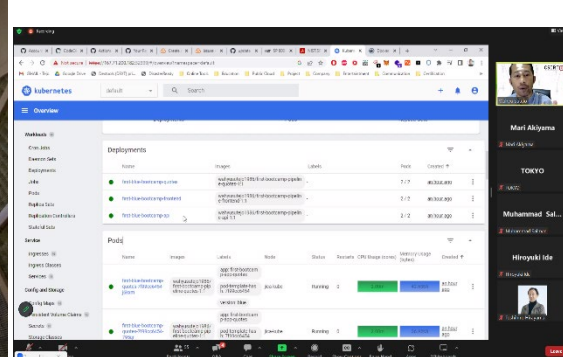
GP
JR
23-015

Photos

Material development and seminar/workshop delivery



1st Cyber Security trend seminar (Depok, 18th Oct 2022)



2nd Cyber Security trend seminar (Online, 27th Feb 2023)



Curriculum development workshop (Bali, 24th -28th Oct 2022)



Briefing session on material development (Depok, 4th Nov 2022)

Policy development for the Malware Analysis Lab

OSS development

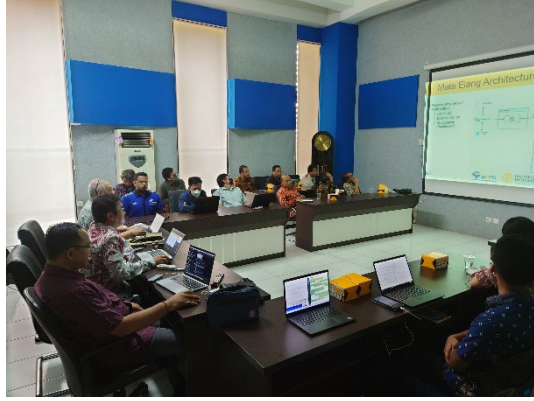


Site inspection (Jakarta, 10th Aug 2022)



UI-PENS Joint UAT (Depok, 6th Feb 2023)

OSS development



Mata Elang briefing for interested parties
(Depok, 14th Feb 2023)



Mata Elang demonstration for interested parties
(Depok, 14th Feb 2023)

Table of Contents

Photos

1. Overview of the work	1
1.1. Background	1
1.2. Purpose of the work	1
1.3. Key components	2
2. Results of the work	4
2.1. Deliverables	4
2.2. Achievement status of the technology transfer	5
3. Content of activities	17
3.1. Activity schedule	17
3.2. Consultant assignments and dispatches	19
3.3. Work contents	19
4. Special efforts and lessons learned through technology transfer	49
5. Recommendations	50

Appendices

Appendix 2-1 Topics Covered in the Common Pre-Learning Materials

Appendix 2-2 Notes on the Common Pre-Learning Materials V.1.1

Appendix 2-3 1st CS Trend Seminar Report

Appendix 2-4 2nd CS Trend Seminar Report

Appendix 2-5 Responses to the Post-Event Questionnaire After the Curriculum Development Workshop

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

Appendix 3-2 Mata Elang Community Member July 2022

Appendix 3-3 RFP on Developing Mata Elang Stable Version

Appendix 3-4 Plan of UAT

Appendix 3-5 UAT Test Cases

Appendix 3-6 Mata Elang UAT Attendees

Appendix 5-1 Specifications of Revisions

List of Tables

Table 1-1 Project Activities Related to This Work	1
Table 2-1 List of Administrative Documents and Reports	4
Table 2-2 List of Technical Outcomes.....	4
Table 2-3 List of Procured Equipment	4
Table 2-4 Common Pre-learning Materials	5
Table 2-5 Revised Subjects	6
Table 2-6 Overview of 1st CS Trend Seminar	7
Table 2-7 Overview of 2 nd CS Trend Seminar.....	9
Table 2-8 Workshop Overview.....	11
Table 3-1 Schedule of Work Actually Implemented	18
Table 3-2 Expert Dispatches	19
Table 3-3 List of Custom Subjects	20
Table 3-4 Material Development Activities	21
Table 3-5 Activities for the 1 st CS Trend Seminar.....	23
Table 3-6 Activities for the 2 nd CS Trend Seminar.....	25
Table 3-7 Activities for the Curriculum Development Workshop.....	26
Table 3-8 Policy Development Activities for the Malware Analysis Lab	29
Table 3-9 Controlled Areas and Network Segments	32
Table 3-10 Segregation of Duties.....	32
Table 3-11 Activity Indicators for the “OSS Development”	33
Table 3-12 Activity Schedule	34
Table 3-13 Teams, Roles and Persons-in-charge	39
Table 3-14 List of New Requirements for ME 1.1	39
Table 3-15 Progress Monitoring Activities	41

List of Figures

Figure 1-1 Overall Work Flow	3
Figure 2-1 Satisfaction with the 1 st CS Trend Seminar	8
Figure 2-2 Most Interesting Session in the 1 st CS Trend Seminar	8
Figure 2-3 Satisfaction with the 2 nd CS Trend Seminar	10
Figure 2-4 Most Interesting Session in the 2 nd CS Trend Seminar.....	10
Figure 2-5 Summary of the Results of Post-Event Questionnaire 1	12
Figure 2-6 Summary of the Results of Post-Event Questionnaire 2	12
Figure 2-7 Structure of the Operational Policy of the Malware Analysis Lab.....	13
Figure 2-8 Operational Policy of the Malware Analysis Lab: Table of Contents	13
Figure 3-1 Curriculum Development Flow	28
Figure 3-2 Curriculum Revision Flow	28
Figure 3-3 Strategic Roadmap for ME Development (1/5).....	36
Figure 3-4 Strategic Roadmap for ME Development (2/5).....	36
Figure 3-5 Strategic Roadmap for ME Development (3/5).....	37
Figure 3-6 Strategic Roadmap for ME Development (4/5).....	37
Figure 3-7 Strategic Roadmap for ME Development (5/5).....	38
Figure 3-8 Achievements of the ME 1.1 Development Work (1/5)	44
Figure 3-9 Achievements of the ME 1.1 Development Work (2/5)	44
Figure 3-10 Achievements of the ME 1.1 Development Work (3/5)	45
Figure 3-11 Achievements of the ME 1.1 Development Work (4/5).....	45
Figure 3-12 Achievements of the ME 1.1 Development Work (5/5)	46
Figure 3-13 Mata Elang Dashboard (1/2).....	47
Figure 3-14 Mata Elang Dashboard (2/2).....	48
Figure 5-1 Management and Implementation Structure for Mata Elang	54
Figure 5-2 Roles and Responsibilities of the Committee and Community	54
Figure 5-3 Existing and Recommended Features of Mata Elang.....	57

Figure 5-4 Kaspersky Cyberthreat Real-time Map	57
--	----

Abbreviations

Abbreviations	Definitions
ACCI	Indonesian Cloud Computing Association
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
ASIOT	Indonesian IoT Association
ASPILUKI	Indonesian Telematics Software Association
BRIN	Badan Riset dan Inovasi Nasional (National Research and Innovation Agency)
BSSN	Badan Siber dan Sandi Negara (National Cyber and Crypto Agency)
C/P	Counterpart
CAMP	Cybersecurity Academy Membership Program
CCTV	Closed-circuit Television
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
CPLMs	Common Pre-Learning Materials
CPU	Central Processing Unit
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
CSIRT.ID	Cyber Security Independent Resilience Team of Indonesia
DPO	Data Protection Officer
DSTI	Direktorat Sistem & Teknologi Informasi (Directorate of Information Systems & Technology)
DTE	Departemen Teknik Elektro (Department of Electrical Engineering)
FGD	Focus Group Discussion
FTII	Indonesian Information Technology Federation
FTUI	Fakultas Teknik Universitas Indonesia (Faculty of Engineering, University of Indonesia)
GDPR	General Data Protection Regulation
HDD	Hard Disk Drive
iCIO	Indonesian CIO community
ICION	Indonesian CIO Network
ICT	Information and Communication Technology

idCARE.UI	Indonesia Cyber Awareness and Resilience Centre
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
JICA	Japan International Cooperation Agency
JSON	JavaScript Object Notation
KSA	Knowledge, Skill, and Ability
LAN	Local Area Network
LaoCERT	National CERT in Laos
LTS	Long-term Support
MASTEL	Indonesian Telematics Society
ME	Mata Elang (Eagle Eye)
NICE	National Initiative for Cybersecurity Education
OS	Operation System
OSS	Open-Source Software
OWASP	Open Worldwide Application Security Project
PCAP	Packet Capture
PENS	Politeknik Elektronika Negeri Surabaya (Electronic Engineering Polytechnic Institute of Surabaya)
QCBS	Quality and Cost-based Selection
RFP	Request for Proposal
SecBoK	Security Body of Knowledge
SOC	Security Operation Center
SOP	Standard Operating Procedures
SSD	Solid State Drive
TTT	Train-the-Trainers
UAT	User Acceptance Testing
UI	University of Indonesia
URL	Uniform Resource Locator

1. Overview of the work

1.1. Background

The “Project for Human Resources Development for Cyber Security Professionals” (“the Project”) was launched in May 2019. The project has been developing the Cyber Security education system at the University of Indonesia (UI). Four main project outputs are expected: 1) World-class Cyber Security Professional training program is held by UI, 2) Open source Cyber Security tools required by the ICT entities are localized or developed, 3) Open courseware in Cyber Security is developed and opened to the public, and 4) A network for Cyber Security entities among the world is strengthened to increase participants and stakeholders for the course. The work covered within this Work Completion Report is expected to contribute to the achievement of the first, second, and fourth expected outputs of the Project. The table below shows the project activities related to this work.

Table 1-1 Project Activities Related to This Work

Output 1)	
Activity 1-3.	Develop syllabuses based on the curriculum
Activity 1-4.	Train university lecturers (including guest lecturers from private sector)
Output 2)	
Activity 2-3.	Select the highly demanded tools to localize or develop
Output 4)	
Activity 4-1.	Strategically conducting cyber security trainings to human resource with other countries
Activity 4-2.	Disseminating course outcomes through International/Regional organizations or any appropriate forums

1.2. Purpose of the work

The work has been conducted for the following purposes.

The work for activities 1-3, 2-3, and 4-1 is related to the results of the work done on the previous year, as reported in the previous “Work Completion Report: PROJECT FOR HUMAN RESOURCES DEVELOPMENT FOR CYBER SECURITY PROFESSIONALS (SOFTWARE QUALITY IMPROVEMENT / CS COURSE DEVELOPMENT / INSTRUCTIONAL DESIGN)” (hereinafter referred to as the “previous work”).

For Output 1 and activities 1-3 and 1-4:

Develop common pre-learning materials from the existing materials of UI's Cyber Security curriculum (also known as the idCARE.UI¹ program) as recommended in the "previous work," deliver Cyber Security (CS) trend seminars not covered by the existing program, and create a lab policy to secure the operations of the Malware Analysis Lab and make the lab available for the support of forensic subjects.

For Output 2 and activity 2-3:

Establish a project structure for the Open-Source CS tool Mata Elang and release a stable version with the requirements suggested in the "previous work."

For Output 4 and activities 4-1 and 4-2:

Deliver a CS curriculum development workshop using a curriculum revision manual developed in the "previous work" and other related materials.

1.3. Key components

The expected work has been divided into three components 1) to 3).

- 1) Material development and Seminar/Workshop delivery
 - a. Material development (related to the previous work)
 - b. Two CS trend seminars
 - c. Curriculum development workshop (related to the previous work)
- 2) Development of the Operational Policy of the Malware Analysis Lab
- 3) OSS development (related to the previous work)

Below is a flowchart for each component and administrative task.

¹ <https://idcare.ui.ac.id/>

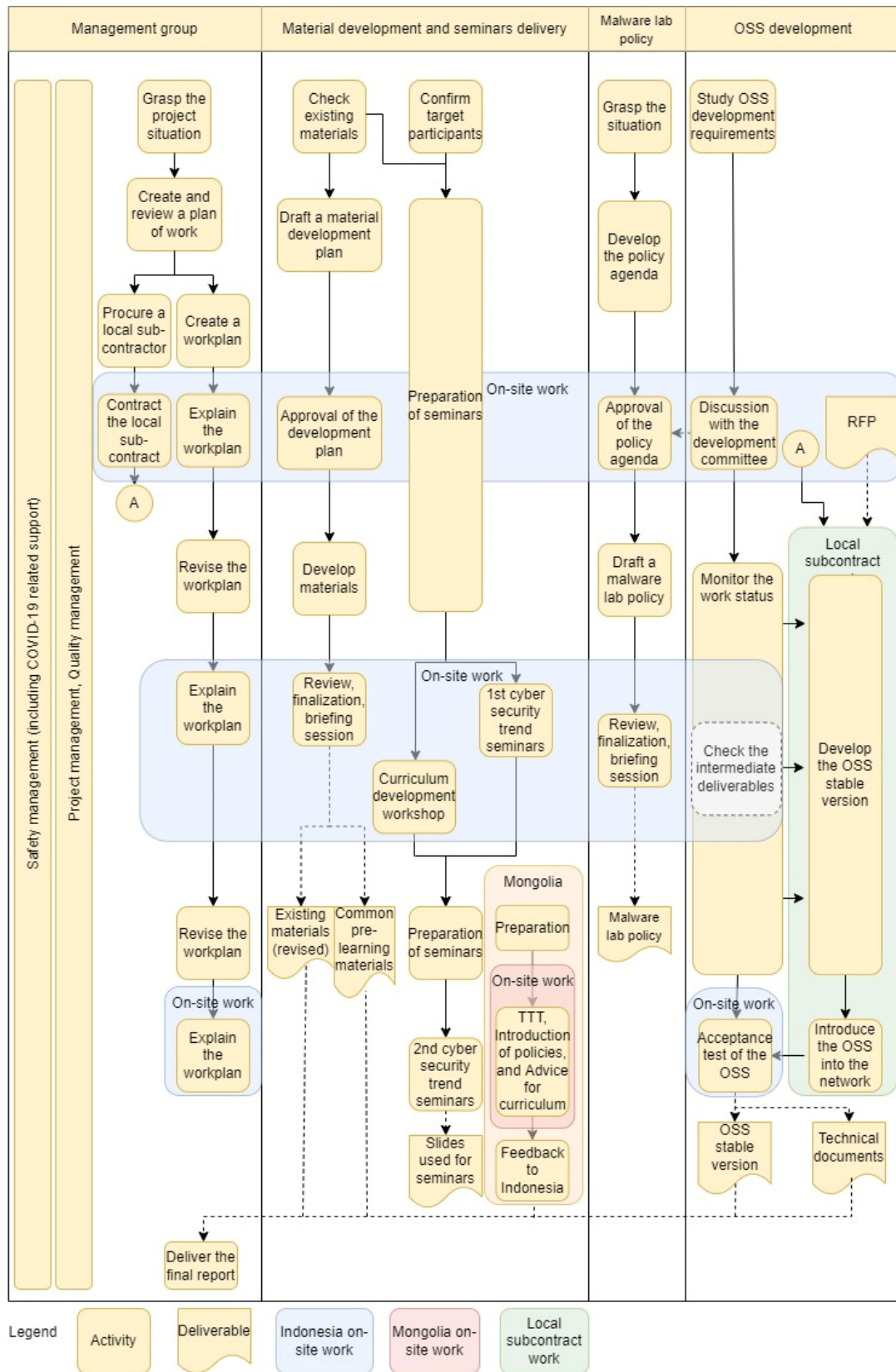


Figure 1-1 Overall Work Flow

2. Results of the work

2.1. Deliverables

1) Administrative Documents and Reports

Table 2-1 List of Administrative Documents and Reports

No	Administrative Documents and Reports
1	Work Plan
2	Work Interim Report (JP)
3	Work Completion Report (this report)
4	Progress Reports (1-11) (JP)
5	Request for Proposal (RFP) on “Developing Mata Elang Stable Version”
6	Service Contract for “Developing Mata Elang Stable Version”

2) Technical outcomes

Table 2-2 List of Technical Outcomes

No	Technical outcomes
1	Common pre-learning materials
2	Updated existing materials and syllabus of CS custom courses
3	Materials of CS trend seminars
4	Materials of the curriculum development workshop
5	Four PowerPoint slides of developed curriculums
6	Malware Analysis Laboratory Operational Policy
7	Source Code of Mata Elang Stable 1.1
8	Docker images of Mata Elang Stable 1.1
9	Updated Mata Elang Installation Manual
10	Updated Mata Elang Developers Guide
11	Complete set of Mata Elang on the purchased servers

3) Procured equipment

Table 2-3 List of Procured Equipment

No	Procured equipment	Specification	Qty
1	Server for the	Model: DELL Vostro 3888	1

	Defense Center	CPU: Intel Core i7-10700 CPU @2.90GHz – 8 Cores Memory: 32GB Storage: 512GB SSD Network: 1GbE x 2 OS: Ubuntu 20.04.4 LTS	
2	Server for Database/ Dashboard	Model: DELL Vostro 3888 CPU: Intel Core i7-10700 CPU @2.90GHz – 8 Cores Memory: 32GB Storage: 1TB HDD Network: 1GbE x 1 OS: Ubuntu 20.04.4 LTS	1

2.2. Achievement status of the technology transfer

1) Material development

The material development work consisted of three sub-activities. The following achievements have been confirmed: a. Developed Common Pre-Learning Materials (CPLMs), b. Revised existing subjects, and c. Briefed the lecturers in a briefing session. The material development work improved the effectiveness and efficiency of the existing idCARE.UI subjects. The CPLMs gave the idCARE.UI participants a firmer grasp of the CS knowledge required for the subjects. The removal of overlapping topics from the existing subjects increased the time available to cover the most important topics and exercises.

a. Developed Common Pre-Learning Materials

The Consultant developed five materials as CPLMs for the idCARE.UI participants. The participants are expected to study the materials by themselves before the classes on the existing subjects.

The CPLMs developed are summarized in the table below:

Table 2-4 Common Pre-learning Materials

Material ID	Material Name	Standard Learning Time
-------------	---------------	------------------------

PRE0010a	Common Cyber Attacks and Malwares	175 min.
PRE0020a	Basic Information Security	50 min.
PRE0030a	Basic Computer and Network Architecture	65 min.
PRE0040a	Introduction of NIST Frameworks	120 min.
PRE0050a	Introduction of NICE Framework/SecBok	70 min.

The IDs were defined according the naming rule adopted for idCARE.UI subjects. For details on the topics and time allocation for each material, see **Appendix 2-1 Topics Covered in the Common Pre-Learning Materials**.

Participants who sign up for the existing idCARE.UI subjects are required to study CPLMs corresponding to subjects defined by the Consultant. The Consultant prepared **Appendix 2-2 Notes on the Common Pre-Learning Materials V.1.1** to provide details on the administration of the CPLMs and the correspondence between the CPLMs and existing subjects.

The CPLMs were also distributed to other countries in activities related to Output 3 of the Project. Specifically, the materials were shared with institutes in Mongolia, Laos, Cambodia, and Timor-Leste that took part in the curriculum development workshop.

b. Revised the existing custom subjects

The development of the CPLMs required revisions to some of the existing subjects. The Consultant revised seven subjects whose topics had been transferred to the CPLMs:

Table 2-5 Revised Subjects

Subject ID and Subject name
COM0010a_How to make Top Management Aware of cybersecurity
COM0020a_How to make general employees aware of cybersecurity
FOR0010a_Malware Analysis
FOR0020a_How to make IT system forensic enabled
FOR0040a_Computer Forensic
GOV0010a_Cybersecurity Law and Regulation
GOV0020a_Supply Chain Risk

c. Briefed the lecturers in a briefing session

The Consultant conducted a briefing session on the outputs (CPLMs and revised existing subjects) at the completion of the material development activities. Members of the Cybersecurity Academy Membership Program (CAMP) designated as authorized lecturers in the idCARE.UI program were briefed.

Twenty-nine CAMP members participated in the session. Seventy-six percent of the participants were active members who had previously attended one or more of the project's Train-the-Trainer (TTT) training.

2) Seminar/Workshop delivery

a. Delivered the 1st CS trend seminar

Table 2-6 Overview of 1st CS Trend Seminar

Theme	Personal Data Protection
Date	18 th October 2022 (1 day)
Target participants	<ul style="list-style-type: none"> • idCARE.UI lecturers • CS-related people in Indonesia (i.e., CII operators)
Delivery method	<ul style="list-style-type: none"> • Hybrid of offline (at UI) and online (on Zoom) • In Indonesian language
Agenda	<ol style="list-style-type: none"> 0. Introduction of CS curriculum at UI (idCARE.UI program) & Mata Elang from the Project 1. Cyber security and protection of personal information under a global perspective 2. The status of laws, regulation, and standards of personal data protection in Indonesia 3. Necessary measures for daily business operation when enforcing norms of cyber security in Indonesia
Presenter	Three external presenters (one from Japan, two from Indonesia)
Number of participants	Offline: 24 Online: 172 ²

A follow-up questionnaire was conducted after the event. More than 90% of the 60 participants

² Excluding redundant participation but including participation by participants who left the seminar halfway through.

who responded felt either satisfied or very satisfied with the seminar.

1. How satisfied are you with the seminar?
60 responses

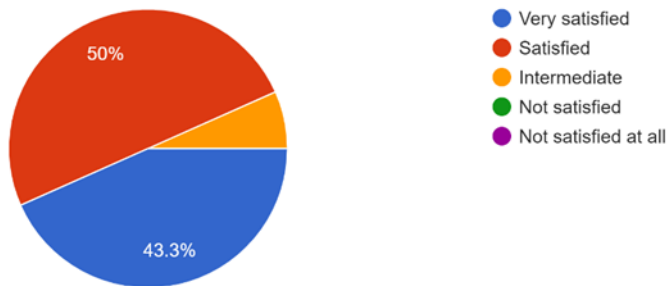


Figure 2-1 Satisfaction with the 1st CS Trend Seminar

The most interesting session for respondents was session 2. This result may be linked to the PERSONAL DATA PROTECTION BILL passed in Indonesia just before the seminar.

2. Which part of the seminar was most interesting to you?
60 responses

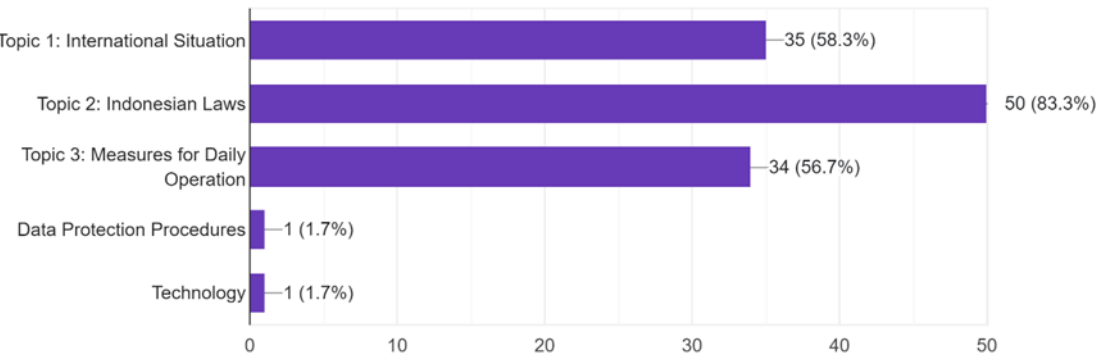


Figure 2-2 Most Interesting Session in the 1st CS Trend Seminar

Seminar participants (including UI lecturers) learned about the latest information on personal data protection in Indonesia and other countries. The offline seminar held at UI had added benefits, as the offline participants and speakers engaged in lively discussions both during and after the seminar and forged stronger networks. See **Appendix 2-3 1st CS Trend Seminar Report** for further details.

b. Delivered the 2nd CS trend seminar

Table 2-7 Overview of 2nd CS Trend Seminar

Theme	Shaping the system more secure
Date	27 th February 2023 (1 day)
Target participants	<ul style="list-style-type: none">• idCARE.UI lecturers• CS-related people (i.e., CII operators)• CISO, employees of the IT planning division, IT system managers/operators/developers• Indonesia and other countries
Delivery method	<ul style="list-style-type: none">• Online (Zoom webinar)• In English
Agenda	<ol style="list-style-type: none">0. Introduction of CS curriculum at UI (idCARE.UI program) & Mata Elang from the Project1. Trend of cloud security2. Trend of IoT security3. Human Resource for Cyber Security4. Best Practice of DevSecOps
Presenters	Four external presenters (one from Japan, three from Indonesia)
Number of participants	Approximate: 200 (Unique: 157) ³

Sixty-four respondents returned the questionnaire.

The respondents were from Indonesia (71.9%), Mongolia (14.1%), Laos (9.4%), Timor-Leste (1.6%) and Japan (1.6%). The participants from the other countries generally attended at the recommendation of persons who had attended previous curriculum development workshops.

More than 90% of the respondents were either satisfied or very satisfied with the seminar.

³ The number of participants is approximate, as some Zoom accounts were shared by several people in an organization.

1. How satisfied are you with the variety of topics presented at the seminar?

64 responses

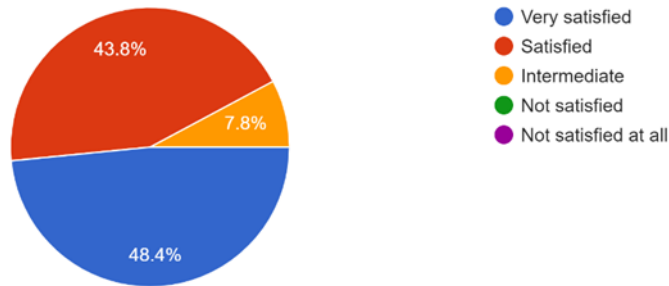


Figure 2-3 Satisfaction with the 2nd CS Trend Seminar

The most interesting session for the respondents was session 2, IoT security.

2. Which part of the seminar was most interesting to you?

64 responses

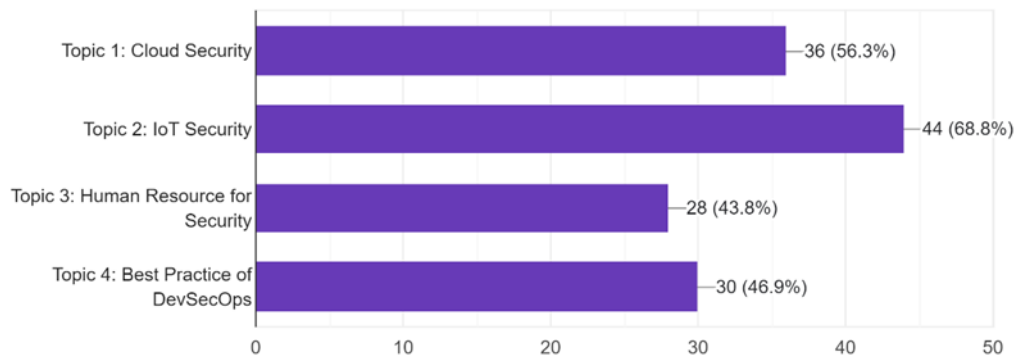


Figure 2-4 Most Interesting Session in the 2nd CS Trend Seminar

The seminar participants learned the latest detailed information on the cloud, IoT and DevSecOps. Some hoped to take part in another offline seminar to dig more deeply into specific topics. As an added benefit, this international seminar helped raise the profile of idCARE.UI in other countries. See **Appendix 2-4 2nd CS Trend Seminar Report** for more details.

c. Delivered a CS Curriculum development workshop

The Consultant conducted a five-day workshop consisting of many exercises to help the participants draft their own curriculums, based on a curriculum development method

employed at idCARE.UI.

The workshop was smoothly implemented and achieved the objectives through the drafting of curriculums (listed in the table below). The participants plan to continue updating their own curriculums with the knowledge and skills gained through the workshop.

Table 2-8 Workshop Overview

Date	24 th – 28 th October 2022 (5 days)
Venue	Prama Sanur Beach Bali
Objectives	<ul style="list-style-type: none"> • Able to analyze the latest Framework (NICE, SecBoK) for the curriculum development • Able to determine target work roles to develop a new curriculum • Able to define subjects with KSAs on SecBoK • Able to explain the curriculum revision cycle
Agenda	<ol style="list-style-type: none"> 1. Understanding SecBoK / NICE framework 2. Introduction of CS curriculum at UI -1 (including Mata Elang introduction) 3. Defining the curriculum by using the SecBoK -1 4. Introduction of CS curriculum at UI -2 5. Defining the curriculum by using the SecBoK -2 6. Method of Curriculum revision
Participants	<p>Fourteen participants from four countries in total</p> <ul style="list-style-type: none"> - 3 from Cambodia (Cambodia Digital Technology Academy, CamTech University, Ministry of Post and Telecommunications) - 4 from the National University of Laos - 4 from the Mongolian University of Science Technology - 3 from the National University of Timor Lorosa'e in Timor-Leste
Instructors	<ul style="list-style-type: none"> - 2 JICA Consultants - 4 C/Ps (for curriculum introduction and the facilitation of group exercises)

Upon learning about the project-developed curriculum, all of the country groups decided to introduce the project-developed subjects into their own curriculums.

The figures below summarize the results of the post-event questionnaire conducted after the workshop. As the charts show, the participants were satisfied with the workshop and learned the curriculum development methods well. See **Appendix 2-5 Responses to the Post-Event Questionnaire After the Curriculum Development Workshop** for details.

What is your level of satisfaction with this seminar?

14 responses

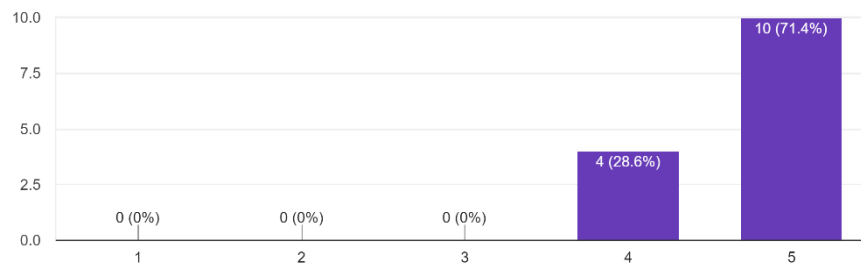


Figure 2-5 Summary of the Results of Post-Event Questionnaire 1

Which topics have you interested the most?

14 responses

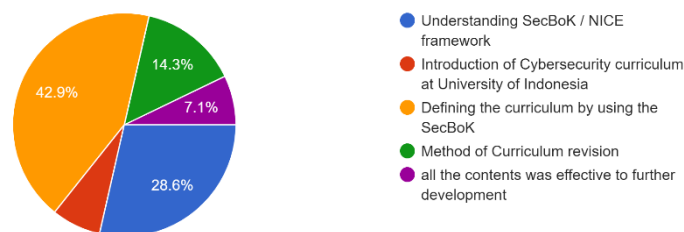


Figure 2-6 Summary of the Results of Post-Event Questionnaire 2

3) Policy development for the Malware Analysis Lab

a. Developed the Operational Policy of the Malware Analysis Lab

The Consultant successfully developed an Operational Policy of the Malware Analysis Lab with inputs from the C/Ps and the project chief advisor. The figures below show the scope of the policy and the table of contents. The policy is composed of an Operational Basic Policy and a set of Operational Standards. The C/Ps are expected to independently develop the Operational Procedures to be applied when launching the lab operations.

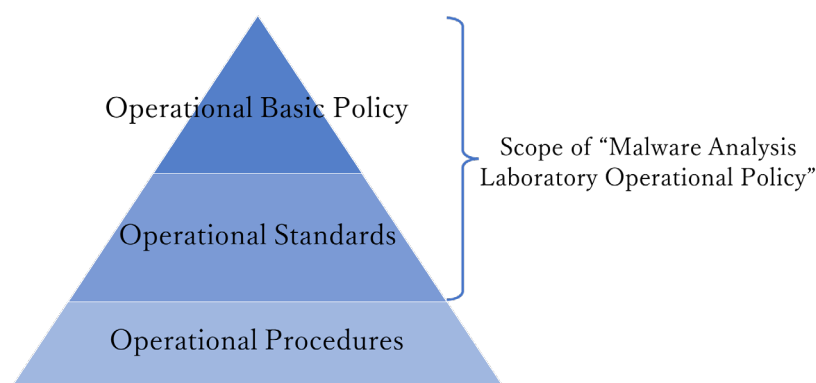


Figure 2-7 Structure of the Operational Policy of the Malware Analysis Lab

Table of Contents

1.	Malware Analysis Laboratory Operational Basic Policy.....	1
1.1.	Purpose.....	1
1.2.	Terms and Definitions.....	2
1.3.	The structure of Malware Analysis Laboratory Operational Policy	3
1.4.	Scope	3
1.5.	Compliance	4
1.6.	Policy Statements	4
1.7.	Self-Assessment.....	6
1.8.	Policy Review.....	6
1.9.	Establish the Malware Analysis Laboratory Operational Standards	6
1.10.	Establish the Malware Analysis Laboratory Operational Procedures.....	6
2.	Malware Analysis Laboratory Operational Standards	7
2.1.	Terms and Definitions.....	7
2.2.	Organizational Structure.....	8
2.3.	Asset Management	9
2.4.	Laboratory Environment	12
2.5.	Physical Security	17
2.6.	Human Resource Security	20
2.7.	Technical Security	24
2.8.	Operational Management	31
2.9.	Outsourcing and Use of External Services	35
2.10.	Compliance (with laws and ordinances).....	37
2.11.	Disciplinary Actions.....	37
2.12.	Assessment and Review.....	37

Figure 2-8 Operational Policy of the Malware Analysis Lab: Table of Contents

b. Delivered a briefing session

The C/Ps and consultant delivered a briefing session on the developed policy to 13 potential users. Potential lab services and the schedule for the launch of the services were discussed during the session. The Indonesian experts welcomed the policy developed and the potential lab services proposed as good initiatives that can be expected to benefit the public.

As a result of this activity, the C/Ps have assigned personnel to develop operational procedures under the developed policy and to operate the lab services accordingly. The C/Ps have also set up plans to hold a series of focus group discussions on the development of the procedures. The services are scheduled to start in 2023.

4) OSS development

The following advances were achieved through the OSS development work:

a. Mata Elang Steering Committee

i. The committee established a technical team and a publicity team for OSS.

Dr. Ferry (from PENS), Dr. Gde, and Mr. Elvian (from UI) joined the technical team in the committee as core members and took part in the progress meetings and user acceptance testing.

On the publicity front, articles on the Mata Elang release were published on the three news websites below (more news sites may also have covered the story).

- “MATA ELANG, Official Cyber Attack Detection Application Released”
<https://lintasjatimnews.com/2023/03/03/mata-elang-aplikasi-pendeteksi-serangan-siber-resmi-dirilis/>
- “Mata Elang, PENS Innovation Cyber Attack Detection Application”
<https://www.msn.com/id-id/berita/other/mata-elang-aplikasi-pendeteksi-serangan-siber-inovasi-pens/ar-AA18cp4f>
- “PENS Releases ‘Mata Elang’ Cyber Attack Detection Application”
<https://beritajatim.com/pendidikan-kesehatan/pens-rilis-aplikasi-pendeteksi-serangan-siber-mata-elang/>

Mata Elang was also introduced in at least three CS seminar/workshop sessions.

An official website is now being built (domain: www.mataelang.net).

- ii. The committee became better able to discuss and decide the OSS requirements and the official OSS release, with help from expert advice.

Twenty-three requirements were defined through discussions held in the course of this development work, of which 18 have been implemented. After reviewing the user acceptance test report, the committee approved the official release and set the release date for 1st March 2023. The committee has already set new requirements for the next stage of Mata Elang.

- iii. The committee has begun to promote the OSS.

As of the end of February 2023, two organizations have already piloted Mata Elang in actual network environments.

- Trustmedis (e-health service company)
- City Government of Blitar, East Java

Several other organizations have also expressed interest in Mata Elang, and a committee member has already conducted briefings for at least the following organizations.

- BSSN (Badan Siber dan Sandi Negara; National Cyber and Crypto Agency)
- Government of East Java Province
- Dr. Sotomo Provincial Hospital

- iv. The committee plans to create a pilot user community group for regular discussion.

b. Mata Elang Community as the developer

- i. The community gained experience in quality management, including user acceptance testing and source code management.

The community gained experience in software development with quality management in the course of this development work by conducting unit testing, system testing, functional testing, installation testing, stability testing, performance testing, and simulated attack testing. Upon the completion of the development work, the community had experienced planning work and conducted a two-week user acceptance test regimen as part of the quality management. The community had also performed source code management and version control management. As of this writing, the community can be assumed to be capable for managing the release for the public deployment of the software, a process not executed during the project.

- ii. The community has established a new online forum for information exchange.

The community has established the “Mata Elang Open Source Community,” a new online forum for information exchange, on a messaging application. The Mata Elang Open Source Community already has 95 members.

c. Mata Elang Development

Mata Elang Stable version 1.1 is now ready to run in an actual network environment.

i. New features released

- IP v6 support.
- New visualization dashboard.
- PCAP (packet capture) file output for further event analysis.

ii. Improved performance

- Snort v3 was applied.
- Improved response time: 60 sec → 30 sec.
- Reduced Defense Center memory requirements: 64GB → 32GB.
- Performance in a real network environment: 54 million network events in three weeks.

iii. Expanded coverage

- Support for offline installation in weak Internet areas.
- ARM CPU support for sensors. The software also run on an inexpensive Raspberry Pi, although testing is required.

iv. Simplified installation

- Offline installation scripts are now available.
- Further Docker containerization.
- Simplified installation procedure.

Regarding the offline installer, technical difficulties prevented us from preparing an offline installation of Zabbix (a component of Mata Elang used for resource management). Mata Elang itself, however, works well without Zabbix.

3. Content of activities

3.1. Activity schedule

The schedule of work actually implemented is shown in the table below.

Table 3-1 Schedule of Work Actually Implemented

Work item	Period	FY2022											FY2023		
	6	7	8	9	10	11	12	1	2	3	4	5	6		
Milestone															
University semester break		June-August						January-Early February							
Events		★ Submit the plan of work	★ Issue OSS development RFP	★ Approval of draft Malware lab policy	★ Approval of draft pre-learning materials development plan	★ Cyber security trend seminar	★ Curriculum development seminar	★ Submit malware lab policy	★ Submit pre-learning materials	★ Cyber security trend seminar	★ OSS acceptance test	★ Submit OSS	★ Submit final report		
1)Management group															
Grasp the project situation															
Create and review a plan of work															
Create workplan															
Create final report															
2)Material development and seminars delivery															
Confirm target participants of seminars															
Preparation of seminars															
Deliver seminars															
Check existing materials / Draft a material development plan															
Develop materials															
Review / finalization / briefing session															
2')Mongolia															
Prepare for TTT, Introduction of CS initiatives, and Advice for curriculum revision															
conduct TTT, Introduction of CS initiatives, and Advice for curriculum revision															
Feedback to Indonesia															
3)Malware lab policy development															
Grasp the malware lab situation															
Develop the policy agenda															
Develop a malware lab policy															
Review / finalization / briefing session															
4)OSS development															
Study OSS development requirements / Discuss with the development committee															
Monitor the work status															
Introduce the OSS into the network / Acceptance test															
Legend : ———period of preparation ■ On-site work □ Off-site work △—△ Explanation of reports ----- Other tasks															

3.2. Consultant assignments and dispatches

Table 3-2 Expert Dispatches

Name	Assignments	Dispatch period
Mari Akiyama TOKYO Co., Ltd.	<ul style="list-style-type: none">• Chief Consultant• Material development and seminar/workshop delivery• OSS development (deputy)• Policy development for the Malware Analysis Lab (deputy)	3 rd Aug – 20 th Aug 2022 19 ^h Oct – 9 th Nov 2022
Hitohiro Sakurai TOKYO Co., Ltd.	<ul style="list-style-type: none">• Deputy Chief Consultant• OSS development	22 nd Nov – 10 th Dec 2022 29 th Jan – 18 th Feb 2023
Kohei Ogura TOKYO Co., Ltd.	<ul style="list-style-type: none">• Material development and seminar/workshop delivery (deputy)	7 th Aug – 20 th Aug 2022 16 th Oct – 9 th Nov 2022
Takumi Uchiyama Densan Co., Ltd.	<ul style="list-style-type: none">• Policy development for the Malware Analysis Lab	-
Yuji Komazawa Densan Co., Ltd.	<ul style="list-style-type: none">• Policy development for the Malware Analysis Lab	7 th Aug – 20 th Aug 2022

3.3. Work contents

1) Material development

a. About materials

The target material to be developed through the development activity is a CS curriculum for professionals to be provided by the idCARE.UI program. idCARE.UI was established under the Faculty of Engineering at UI (Fakultas Teknik Universitas Indonesia, FTUI) in the course of project implementation in 2020. The program covers two subject categories: 1. “Custom Subjects” developed by the Project with reference to the NICE framework and SecBok framework; 2. “Commercial Subjects” provided by commercial partners such as the EC

Council and CompTIA. The report on the completion of “previous work” stated that common topics and prerequisite knowledge were found in multiple custom subjects, and proposed that they be extracted. CPLM development on that basis was expected in this activity.

The custom subjects are summarized in the table below (CPLM targets written in bold):

Table 3-3 List of Custom Subjects

Subject ID	Subject Name	Status
COM0010a	How to make top managements aware of CS	Developed
COM0020a	How to make general employees aware of CS	Developed
GOV0010a	Cybersecurity law and regulation	Developed
GOV0020a	Case Study & Practice: Supply-chain risk	Developed
GOV0030a	Desktop exercise for managers	Not Available
FOR0010a	Case Study & Practice: Malware analysis	Developed
FOR0020a	Case Study & Practice: How to make IT system forensic-enabled	Developed
FOR0030a	Case Study & Practice: Cyber criminal investigation	Not Available
FOR0040a	Computer Forensic	Developed
FOR0050a	Mobile device forensic	Developed
CMP0010a	Comprehensive exercise: CSIRT	Developed
CMP0020a	Comprehensive exercise: SOC	Not Available
CMP0030a	Cyber range	Not Available

b. Implemented Activities

The Consultant developed the five CPLMs shown in **Table 2-4 Common Pre-learning**. The topics are selected according to the following policy:

- Extract topics that overlap with topics from the existing subjects.

- The topics extracted from the existing subjects should be fundamental topics appropriate for self-study.
- Add topics that are not covered in the existing subjects but are important for CS personnel.
- Cover the international CS frameworks suggested in the previous work.

Seven existing subjects were revised in conjunction with the CPLM development work. The specific revisions are summarized below:

- Slide materials: Instructor guide and Student guide
 - Some pages were altered or removed in line with the topic extraction to the CPLMs.
 - A slide about prerequisite CPLM self-study was added for each subject.
- Test
 - Some questions were altered to reflect the slide modifications. The number of questions remains unchanged.
- Syllabus, Time-mapping Table
 - The syllabi were altered to reflect the slide modifications.
 - The time saved through the topic extraction was reallocated to the exercises. The number of class sessions remains unchanged.

The following material development activities were performed:

Table 3-4 Material Development Activities

Activity	Main points
Approval of the activity plan 9 th Aug 2022 (On-Site)	<p>A material development plan was approved by the various persons concerned, including the project manager and project chief advisor.</p> <p>The plan included:</p> <ul style="list-style-type: none"> • Expected outputs; slides, tests, supplemental documents • The existing subjects that need to be revised • Work schedule for the activities • Consideration of the CPLMs <p>➤ The participants in idCARE.UI are mainly professionals who work in enterprises or government agencies. Because</p>

	<p>of their professional commitments, they have limited time for self-study. Each CPLM should consist of small modules that can be studied within a short span of time.</p> <p>➤ To achieve the best effect for self-study, the CPLMs should have sufficient opportunities for self-assessment, such as recaps and tests, built in. They should also incorporate an exercise to collect information from publicly available sources such as the OWASP Top 10.</p>
<p>Material development</p> <p>Aug – Oct 2022</p> <p>(On-Site, Off-Site)</p>	<p>The consultant and a local consultant worked together to develop the CPLMs and revise the existing subjects.</p> <p>The materials were reviewed multiple times by the lecturers involved and the leaders of the following subject clusters⁴:</p> <ul style="list-style-type: none"> • Common subject cluster • Governance subject cluster • Cyber Forensic subject cluster <p>As a result of the review, several fundamental but important topics remained in the existing materials. Those topics are also covered in the CPLMs.</p>
<p>Approval of outputs</p> <p>20th Oct 2022</p> <p>(On-Site)</p>	<p>The project manager and project chief advisor performed the final review. The outputs were approved pursuant to the completion of several very minor revisions concerning the addition of topics to the CPLMs.</p>
<p>Briefing session</p> <p>4th Nov 2022</p> <p>(On-Site)</p>	<p>The Consultant held a briefing session covering the following content for the CAMP members:</p> <ul style="list-style-type: none"> • Overview of the material development work • What the CPLMs are and how they are used • The several revisions made to the existing subjects

⁴ idCARE.UI categorizes subjects into the following five groups (“Clusters”) based on their content: Common, Governance, Cyber Forensic, Vulnerability Assessment & Pentest, and Comprehensive Exercise.

	The briefing materials and recorded videos were shared online for the CAMP members who were unable to attend the briefing session in person.
--	--

2) Seminar/Workshop delivery

a. 1st CS trend seminar

The Consultant held the 1st CS trend seminar on 18th Oct 2022. This seminar covered CS trends in Indonesia, focusing closely on the laws and regulations on Personal Data Protection being deliberated in the Indonesian parliament. The main target participants were lecturers at idCARE.UI and the C/Ps of the Project. Several other people involved in CS from external organizations in Indonesia, including Critical Information Infrastructure (CII) operators, were invited to take part to boost the effectiveness of the seminar.

Three main seminar sessions were held. In the first, a Japanese speaker introduced the “global situation surrounding personal data protection.” In the second, an Indonesian expert who had engaged in the development of the personal data protection law explained the “unique situation in Indonesia.” In the third, an Indonesian practitioner presented a talk on “practices in daily business operation from a personal data protection viewpoint.” Separately from the main theme, a C/P also introduced idCARE.UI and an OSS (Mata Elang) developed in the Project.

Online participants were invited to participate in a publicly open call, and the Project asked several offline participants to visit the venue, as well. The Consultant advertised the seminar using an online registration form.

Table 3-5 Activities for the 1st CS Trend Seminar

Activity	Main points
Approval of the seminar plan 11 th Jul 2022 (On-Site)	The seminar plan was approved in conjunction with an overall work plan. The seminar plan included: <ul style="list-style-type: none"> • Theme, topics, and speakers • Target participants • Delivery method
Preparation	The Consultant worked on the following preparations:

Aug – Oct 2022 (On-Site, Off-Site)	<ul style="list-style-type: none"> • Making contracts and discussing the details of the event with three presenters from external organizations • Advertising through the following organizations: <ul style="list-style-type: none"> ➤ Indonesian Cloud Computing Association (ACCI) ➤ Indonesian CIO Network (ICION) ➤ Indonesian CIO community (iCIO) ➤ Indonesian IoT Association (ASIOT) ➤ Faculty of Engineering, University of Indonesia (FTUI) • Arranging a simultaneous interpretation service (Indonesian <-> Japanese) for a Japanese presenter
Delivery of the seminar 18 th Oct 2022 (On-Site)	<p>The Consultant managed the seminar offline and online.</p> <ul style="list-style-type: none"> • Offline (a meeting room in UI) <ul style="list-style-type: none"> ➤ Presenters: 2 Indonesian speakers ➤ Participants: 24 invited participants • Online (by Zoom) <ul style="list-style-type: none"> ➤ Presenters: 1 Japanese speaker, 2 simultaneous interpreters ➤ Participants: 172 participants
Sharing of seminar materials with the Project Oct 2022 (On-Site)	<p>After confirming that there were no intellectual property conflicts, the Consultant shared the presentation slides for the talks and video recordings of the sessions with the Project.</p>

b. 2nd CS trend seminar

The Consultant held the 2nd CS trend seminar on 27th Feb 2023. Compared to the 1st seminar, which had focused mainly on laws and regulations on personal data protection, the 2nd seminar provided more detailed technical information. To provide information useful for secure system development and strategies for system operations in organizations, the seminar also invited

personnel engaged in IT system development/operation. To take advantage of the online seminar format, the Consultant advertised the seminar to potential participants in other countries, including attendees of the CS curriculum development workshop in October 2022 in Bali (from Mongolia, Laos, Cambodia, and Timor-Leste).

The seminar consisted of four sessions. Sessions 1 and 2 focused on CS threats and countermeasures in trending technologies such as cloud and IoT. Sessions 3 and 4 were related to each other, as both covered the topic of DevSecOps⁵. The presenter in session 3 explained the importance of having CS human resources within organizations for DevSecOps. The presenter in session 4 explained the DevSecOps best practices and demonstrated the actual tools used for DevSecOps.

Table 3-6 Activities for the 2nd CS Trend Seminar

Activity	Main points
Approval of the seminar plan 21 st Oct – 2 nd Dec 2022 (On-Site, Off-Site)	The project manager and project chief advisor discussed content of the seminar and approved the overall seminar plan. The seminar plan included: <ul style="list-style-type: none"> • Theme, topics, and speakers • Target participants • Delivery method
Preparation Nov 2022 – Feb 2023 (Off-Site)	The Consultant worked on the following preparations: <ul style="list-style-type: none"> • Making contracts and discussing the details of the event with four presenters from external organizations • Advertising through the following organizations: <ul style="list-style-type: none"> ➤ Indonesian Cloud Computing Association (ACCI) ➤ Indonesian CIO Network (ICION) ➤ Indonesian CIO community (iCIO) ➤ Indonesian IoT Association (ASIOT) ➤ Faculty of Engineering, University of Indonesia (FTUI)

⁵ DevSecOps is a practical method for system development and system operation integrated with CS.

	<ul style="list-style-type: none"> ➤ Indonesian Telematics Society (MASTEL) ➤ Indonesian Information Technology Federation (FTII) ➤ Indonesian Telematics Software Association (ASPILUKI) ➤ National CERT in Laos (LaoCERT) <ul style="list-style-type: none"> • Arranging a simultaneous interpretation service (English <-> Japanese) for the Japanese presenter
Delivery of the seminar 27 th Feb 2023 (Off-Site)	The Consultant managed the seminar online. <ul style="list-style-type: none"> • Online (by Zoom) <ul style="list-style-type: none"> ➤ Presenters: 3 Indonesian speakers, 1 Japanese speaker, 2 simultaneous interpreters ➤ Participants: about 200
Sharing of the materials with the Project Feb 2023 (Off-site)	The Consultant shared the presentation slides for the talks and video recordings of the sessions with the Project. To avoid potential intellectual property conflicts, the consultant requested that the video of session 3 be kept private.

c. Curriculum development workshop

Workshop participants from educational institutes from third countries were expected to obtain knowledge from idCARE.UI's experience with curriculum development work, as well as from their own experience at the workshop. A curriculum revision manual developed earlier was also used.

The Consultant delivered a five-day intensive curriculum development workshop focused on Output 4 of this Project. The Project invited 14 participants from four countries (Cambodia, Laos, Mongolia, Timor-Leste).

The seminar activities are summarized in the table below.

Table 3-7 Activities for the Curriculum Development Workshop

Activity	Main points
Preliminary	The workshop participants completed a preliminary survey to assess

<p>survey</p> <p>Aug – Oct 2022</p> <p>(Off-Site)</p>	<p>their awareness of the education target. The survey results were used in the workshop to analyze the gap between the targets/supplies in their organization's and the market demands in their regions or countries.</p> <p>For details, see Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis.</p>
<p>Preparations</p> <p>Aug – Oct 2022</p> <p>(Off-Site)</p>	<p>The participants were expected to:</p> <ul style="list-style-type: none"> • Understand the methodology used for CS curriculum development • Understand the curriculum revision cycle <p>The Consultant prepared the following content to achieve these goals: an introduction to the SecBoK and NICE framework as foundational CS curriculum at idCARE.UI; an introduction to UI's curriculum/subjects, including commercial courses such as EC-Council and CompTIA.</p> <p>The Consultant prepared the two workflows described just below this table, along with various types of exercises for gap analysis, Excel work with the SecBoK framework, a training plan, a feedback evaluation using Google Data Studio, and curriculum revisions with ADDIE Instructional Design⁶.</p>
<p>Delivery</p> <p>24th – 28th Oct 2022</p> <p>(On-Site)</p>	<p>The Consultant brought UI lecturers and country managers from the EC-Council (Ms. Tin Tin Hadijanto) and CompTIA (Mr. Hairil Izwan Isamuddin) into the workshop to help participants understand the curriculums/subjects developed at idCARE.UI and their adaptability to participant institutions.</p> <p>Three countries out of four signed a Letter of Intent to obtain further assistance from UI. The participants also showed an interest in joining the Mata Elang community. Further collaboration can be expected in the OSS development.</p>

The diagram below shows the curriculum development flow.

⁶ The ADDIE Instructional Design method is a framework for designing and developing educational and training programs. "ADDIE" stands for Analyze, Design, Develop, Implement, and Evaluate.

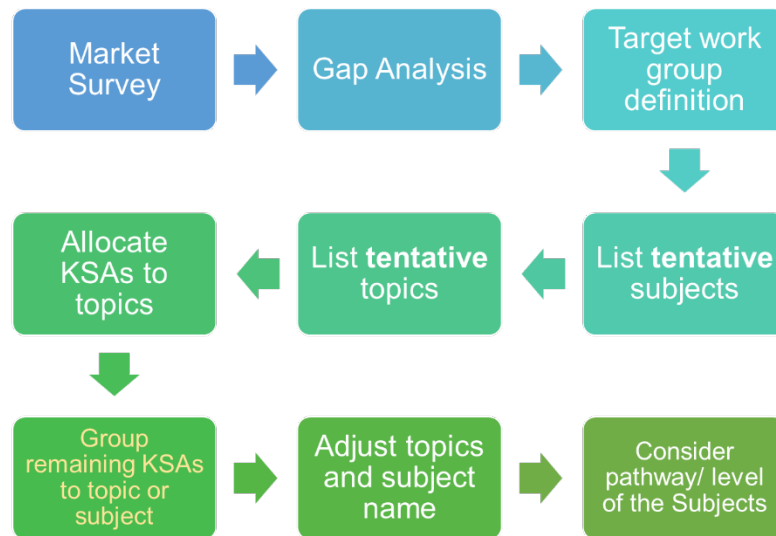


Figure 3-1 Curriculum Development Flow

The diagram below shows the curriculum revision cycle.

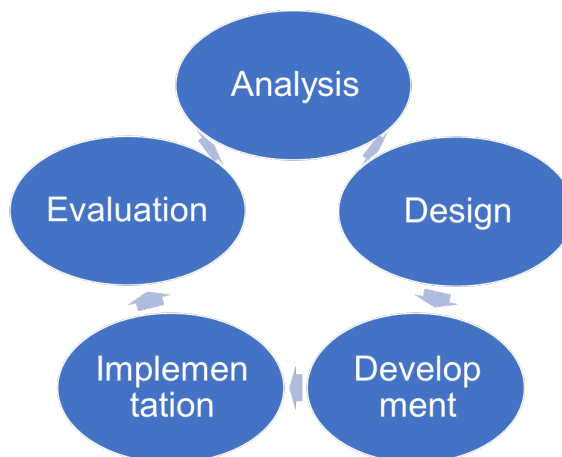


Figure 3-2 Curriculum Revision Flow

3) Policy development for the Malware Analysis Lab

The Consultant and C/Ps conducted a site inspection and interviews to develop the policy. In the process, the Consultant shared knowledge on cases of policy development and implementation in Japan.

The following activities were conducted.

Table 3-8 Policy Development Activities for the Malware Analysis Lab

Activity	Main points
Site inspection 10 th Aug 2022 (On-Site)	<p>The Consultant raised the following issues and suggestions after completing the inspection:</p> <p>Policy related</p> <ul style="list-style-type: none"> • Define the personnel allocation in order to better manage physical access control. • Decide which roles have the authority to reset environments. • Allocate an administrator to be stationed in the lab. If allocating an administrator is difficult, consider setting limitations on use. • Authentication is required (by a system or by an access management book). • Develop a password management procedure according to the policy. • Clarify the incident response processes. • Define the process for acquiring malware specimens. One possible procedure would be the following: User acquires a specimen > User uploads a password protected zip (zipped more than three times) file > Administrator downloads the zipped specimen to the download environment <p>Facility related</p> <ul style="list-style-type: none"> • A new connection from an ISP should be prepared. The network needs to be separated from the existing network in the event incidents occur. • The storage of evidence is required during analysis to securely store malware specimens in physical devices. • A power supply should be prepared for the server rack. (Consider redundant supplies, if required.) • Specify the location of the malware analysis room for renovation according to the policy requirements for compartmentalization and access restrictions.

	<p>Other points</p> <ul style="list-style-type: none"> • Recommendation: For smooth operation, have an internal discussion on the software installation order on the host OS and virtual machines.
<p>Interviews</p> <p>9th Aug – 15th Sep 2022</p> <p>(On-Site)</p>	<p>Interviewees:</p> <ul style="list-style-type: none"> • DSTI (Dr. Gde) • DTE (Dr. Salman and Mr. Yan) <p>For reference, information on the treatment of intellectual property at Shinshu University, Japan was shared on 15th Sep.</p>
<p>Policy development</p> <p>Aug – Nov 2022</p> <p>(Off-Site)</p>	<p>The Consultant worked on policy development.</p> <ul style="list-style-type: none"> • To reduce the operational difficulties with human resources and budget in UI, the Consultant introduced an “Information Security Policy Guideline for Local Government Authorities, Ministry of Internal Affairs and Communications, Japan” as an input for the Operational Policy. • To avoid security incidents during the operation, the network separation and the incident report line were defined. • While the network segments are not normally mentioned in a policy document, they are stated in the Operational Policy in this case to ease the development of procedures (shown in Table 3-9 Controlled Areas and Network).
<p>Briefing session</p> <p>16th Nov 2022</p> <p>(On-Site)</p>	<p>The Consultant explained the developed policy and facilitated discussions on the policy and lab operations. The participants were potential users such as lecturers and master students from UI and experts from external organizations.</p> <p>The participants in the discussion offered several suggestions and comments. The Project made plans for further activities as a result.</p> <p>Plan:</p> <ul style="list-style-type: none"> • Procedure development: 2022- before Aug 2023 • FGDs: Two discussions before March 2023

	<ul style="list-style-type: none"> • License procurement: Earlier than August 2023 • Renovation of the lab: Start in December 2022 <p>Suggestions:</p> <ul style="list-style-type: none"> • Impose strict permissions to keep the networks for analysis (malware) and daily operations separate and avoid malware leakages. • Recommend the creation of a malware database open to the public. • Announce the analysis findings/research to the public, including instructions on how to remove certain types of malware. • Recommend the opening of a sandbox to the public. (This has been declined, as it is not aligned with the developed policy.) • Start the service as a static analysis first and evolve to a dynamic analysis later. • Strengthen the internal infrastructure by deploying sensors to guard against malware. <p>Concerns:</p> <ul style="list-style-type: none"> • Make sure everyone follows the SOP. • Monitoring is needed with regard to forensic events. • The usage of the UI network for the Malware Analysis Lab is a concern. • Strengthen internal affairs first, offer services to the public later. Time will be required for this. <p>Other remarks:</p> <ul style="list-style-type: none"> • The opening of the Malware Analysis Lab to the public is a good initiative. • Help mitigate malware in the UI network. • There has been no major malware attack on the UI network so far.
--	--

The site survey revealed that the plan for the lab services had not been discussed and that the information assets were not well managed in the Project. This was not ideal, as the project members had to reach a mutual understanding on the objectives and prerequisites before policy development. The Consultant and C/Ps therefore discussed the objectives (potential services) and

necessary preparations, then shared them with the long-term experts to guide and incite further actions while developing the policy, including activities to prepare the physical environments and the human resources for lab operations (shown in **Table 3-10 Segregation of Duties**).

Table 3-9 Controlled Areas and Network Segments

Controlled Areas	Network segments for environments
Server Control room	Malware download environments
	System management server environments (Optional)
	Software repository environments
Malware Analysis room	Malware analysis environments
	Sandbox analysis environments
	Anti-malware test environments
Storage cabinet for electronic media	(In the Server Control room)

Table 3-10 Segregation of Duties

Roles	Description	Personnel
Head of Malware Analysis Laboratory	The decision-maker responsible for everything in the Lab.	Dr. Muhanmmad Salman
Malware Analysis Laboratory Administrator	Handle incidents at the instruction of the Head of the Lab. Create and maintain the Procedures. Educate Lab-Users.	Dr. Yohan Suryanto Mr. Yan Maraden Mrs. Diyanatul Husna
Malware Analysis Laboratory Operator	Follow the instructions of the Administrators. Carry out practical tasks.	Master's students from UI Mr. Didit Hari Kuncoro, Mr. Elfrin Erawan, Mr. Permata Putra Satria

		Sinurat, Mr. Elieser Mangara Hutapea, Mr. Ali Akbar Khatami
Registered Users of Malware Analysis Laboratory	Normal Lab-Users other than the Operators, Administrators, and Head of Lab.	Experts from organizations such as CSIRT.ID, the Indonesian Honeynet Project, and DSTI

4) OSS development

a. About Mata Elang, Committee and Community

“Mata Elang” (“ME”) is an OSS IDS (Intrusion Detection System) being developed in this activity. For more details, please visit the Mata Elang project site (<https://github.com/mata-elang-stable/mataelang-platform/wiki>).

“Mata Elang version 1.0” (“ME 1.0”) was released in March 2022. Not long after, Mata Elang version 1.1” (“ME 1.1”) was developed as a revised version to further improve the functionality and performance of the system, make the system practical in actual network environments, and simplify its operation.

The “Mata Elang Steering Committee” (the “Committee”) was organized in 2021 to release a stable version for target users such as government, CII operators, and educational entities. The steering committee is also the primary decision-maker guiding the strategy, release plans, and specifications of ME.

The “Mata Elang Community” (the “Community”) was established in 2021 as a platform for announcements and information exchange. The Community now serves as a contact point for everyone interested in ME.

b. Objectives, critical points, issues, and countermeasures

The table below summarizes the overall status and issues of the Project, along with the objectives, critical points, issues, and “OSS Development” countermeasures, as of the beginning of this work.

Table 3-11 Activity Indicators for the “OSS Development”

Item	Description
Objectives	Establish the system necessary to continuously release stable versions of the OSS tools being developed in the Project
Critical points	Developing the OSS at an operational level in a real environment and enhancing the OSS community through the development of ME.
Issues	<ul style="list-style-type: none"> • ME is not yet operational in a real environment. • Additional components such as IPv6 support will have to be developed to make ME operational. • ME installation is very difficult in low-speed Internet countries.
Countermeasures	<ul style="list-style-type: none"> • Develop additional installations to run ME in a real network environment. • Develop an ME offline installer.

c. Activity Schedule

The following table summarizes the schedule for the “OSS Development” activities performed.

Table 3-12 Activity Schedule

Period	Location	Main Activity
4 th July - 8 th Aug 2022	Online	<ul style="list-style-type: none"> • Consideration and Preliminary Estimation of New Requirements • Discussion of New Requirements with the Committee
3 rd Aug - 19 th Aug 2022 (plan)	On-Site: Jakarta / Surabaya	• (Cancelled; Replaced with the online activity below)
10 th Aug - 23 rd Sep 2022	Online	• Procurement and Contracting for ME Development
23 rd Sep 2022 - 5 th Feb 2023	Online	• ME 1.1 Development and Monitoring of Progress
23 rd Nov - 3 rd Dec 2022 (11 days)	On-Site: PENS, Surabaya	• On-site Progress Inspection
4 th Dec –	On-Site:	• Preparations for User Acceptance Testing

Period	Location	Main Activity
9 th Dec 2022 (7 days)	UI, Depok	
10 th Dec 2022 – 5 th Feb 2023	Online	<ul style="list-style-type: none"> • Testing of Interim Deliverables
29 th Jan – 18 th Feb 2023	On-Site: UI, Depok	<ul style="list-style-type: none"> • User Acceptance Testing
19 th Feb – 1 st Mar 2023	Online	<ul style="list-style-type: none"> • Release of Mata Elang 1.1

d. Activity Report

i. Consideration and Preliminary Estimation of New Requirements

The new development requirements for ME 1.1 were based on the remaining requirements left over from the ME 1.0 development in the previous work. Preliminary estimates have been received from the three software development companies in Indonesia, according to the requirements at that point.

ii. Discussion of New Requirements with the Committee

The first committee meeting for the project year 2022-2023 was held on 13th July 2022. The Consultant provided an overview of this development project and presented a draft of the requirements for the ME 1.1 development. Additionally, the strategic plan for the ME development created in the previous work was reviewed once more. The figures below summarize the strategic roadmap for ME development.

Strategy Roadmap – Basics (1/2)

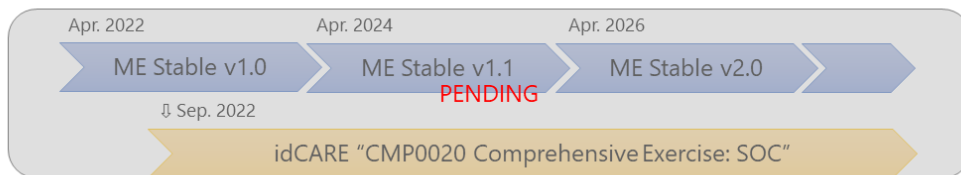
This section describes the development strategy of ME Stable for next 5 years.

Three versions of ME stable are proposed here.

1. ME Stable v1.0 : Initial release of ME Stable with JICA support
- » 2. ME Stable v1.1 : New features release & performance improvement with JICA support
3. ME Stable v2.0 : Comprehensive update of ME Stable

	ME R&D	ME Stable v1.0	ME Stable v1.1	ME Stable v2.0 (Draft)
Release	Released	April 2022	April 2024	April 2026
Lifetime	(n/a)	At least 2 years	At least 2 years	At least 2 years
JICA Support	NO	YES	Possibly, YES	NO

ME Stable will be used by idCARE "SOC exercise" from September 2022.



Copyright Mata Elang Committee

Figure 3-3 Strategic Roadmap for ME Development (1/5)

Strategy Roadmap – Basics (2/2)

(cont.)

	ME R&D	ME Stable v1.0	ME Stable v1.1	ME Stable v2.0 (Draft)
Release	Released	April 2022	April 2024	April 2026
Lifetime	(n/a)	At least 2 years	At least 2 years	At least 2 years
JICA Support	NO	YES	Possibly, YES	NO

Requirements of ME Stable v1.0

- ME Stable will be used by idCARE
- ME Stable must be well-tested and well-documented
- Bug fix activities must be continued for at least 24 months

Development Policy of ME Stable v1.1

- No architecture changes
- Adding new features to improve practicality
- Additional 2-year support

Possible Strategic Direction of ME Stable v2.0

- Improvement of practicality
- Reducing the use of system resources
- Multi-tenant system
- Cloud IDS etc.



Copyright Mata Elang Committee

Figure 3-4 Strategic Roadmap for ME Development (2/5)

Strategy Roadmap – Functions (1/2)

The following table shows the strategy roadmap from the perspective of ME functionality.

	ME R&D	ME Stable v1.0	ME Stable v2.0 or later (Draft)
IDS	Network IDS	Network IDS	Cloud IDS?
Data Collecting	MQTT	MQTT	Optimized MQTT?
Data Processing	Streaming Data Processing - Realtime Processing - Batch Data Aggregation	Streaming Data Processing - Realtime Processing	Distributed Streaming Data Processing?
Data Storage	Big Data Storage	Big Data Storage	Distributed Big Data Storage?
Search Engine	(n/a)	Data Aggregation	Data Aggregation
Dashboard	Simple Dashboard - Signature-base and protocol-base analysis - Time-series analysis	Customizable Dashboard - Signature-base and protocol-base analysis - Time-series analysis - Geographical analysis	Multi-Tenant Dashboard? Risk-Threat Analysis?

✓ ME 2.0 roadmap will be revised at future re-planning.



Copyright Mata Elang Committee

Figure 3-5 Strategic Roadmap for ME Development (3/5)

Strategy Roadmap – Functions (2/2)

(cont.)

	ME R&D	ME Stable v1.0	ME Stable v2.0 or later (Draft)
Operation & Management	(n/a)	[Operation] ✓ Server Resource Monitoring ✓ Log Rotation <div>ME Stable v1.1</div> <div>✓ IPv6 Support</div> <div>✓ Offline installer</div>	Functions of ME Stable v1.0 + [Management] ✓ Sensor Management ✓ User Management ✓ Rule Management [Notification] ✓ Incident Notification - e.g. High Severity Incident ✓ Anomaly Detection Alert - e.g. Change-point Detection [Data Analysis] ✓ Enrich Query for detail analysis ✓ Threat-intelligent for detail analysis and risk analysis [Visualization] ✓ Enrich Visualization [Inter-organizational Cooperation] ✓ STIX Format Support

✓ Some of these functions come from the ME documents.
 ✓ Some others are for improvement of practicality.
 ✓ ME 2.0 roadmap will be revised at future re-planning.



Copyright Mata Elang Committee

Figure 3-6 Strategic Roadmap for ME Development (4/5)

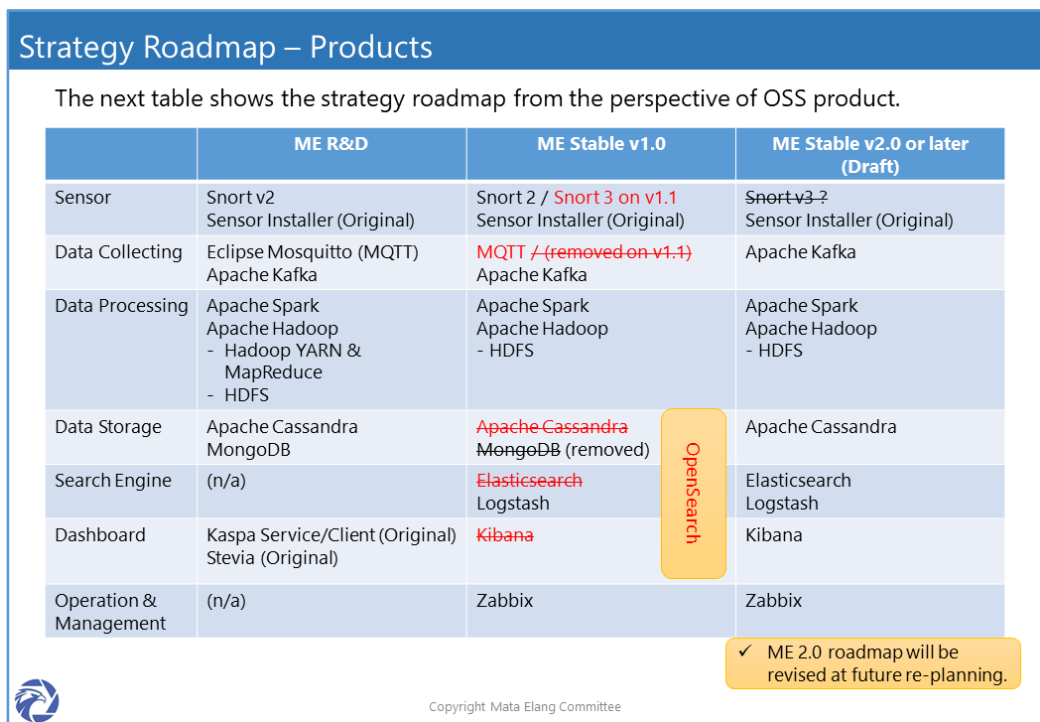


Figure 3-7 Strategic Roadmap for ME Development (5/5)

The objectives of this OSS development project and the agenda of the first committee meeting are summarized below.

<p>[Objectives]</p> <ol style="list-style-type: none"> Enhancement of the Mata Elang Committee and Community <ul style="list-style-type: none"> Establishment of a Mata Elang technical team Acceptance testing and release management Launch of publicity on the Mata Elang Stable Version Development of Mata Elang Stable 1.1 <ul style="list-style-type: none"> New feature releases and performance improvements Offline installer development
<p>[Agenda]</p> <ul style="list-style-type: none"> Establishment of an ME Technical Team Explanations on Acceptance Testing Launch of Publicity on the ME Stable Version

The agenda above was developed based on suggestions from the previous work. The committee membership roster and roles were updated during the committee meeting, as shown in **Appendix 3-2 Mata Elang Community Member July 2022**.

New working teams were established for the Project in 2022-2023, as listed in the table

below.

Table 3-13 Teams, Roles and Persons-in-charge

Working Team	Roles and Persons-in-charge
ME Technical Team	Manager: Dr. Ferry Astika Saputra, PENS (for 2022-2023) Dr. I Gde Dharma Nugraha, UI (for the Next Term) Core-Engineer: Mr. Elvian Syahrurizal, UI
Publicity on ME	Building the ME Website: Dr. Ferry Astika Saputra, PENS *IdCARE.UI can also be linked from the main site. Preparing Contact Email Address: Dr. Ferry Astika Saputra, PENS ME Introduction at Seminars in 2022-2023 Dr. I Gde Dharma Nugraha, UI

Due to the delay in determining the requirements, the first on-site activity by the Consultant scheduled for August 3-19 had to be cancelled and replaced with an online activity. The new requirements were finally determined on August 8.

Some but not all of the new requirements were to be implemented in the ME 1.1 development work, as permitted by the available development period and budget.

Table 3-14 List of New Requirements for ME 1.1

No	Requirement	Activity	Level, Priority
1	Offline Installation	<ul style="list-style-type: none"> Develop an offline installer. Create an easy installation manual. 	Mandatory
2	Performance Improvement	<ul style="list-style-type: none"> Update Snort to version 3. Add Ipv6 compatibility. 	Mandatory
3	Update of Dashboard	<ul style="list-style-type: none"> Make the dashboard compatible with ipv6. 	Mandatory
4	Elimination of Unnecessary Processes	<ul style="list-style-type: none"> Put the parameters into external files and avoid unnecessary builds. 	Mandatory
5	Testing	<ul style="list-style-type: none"> Unit test, system test, stability test, simulator attack test. 	Mandatory

No	Requirement	Activity	Level, Priority
6	Documentation	<ul style="list-style-type: none"> Update the installation manual, developer's guide, and other technical documents. 	Mandatory
7	Log Rotation	<ul style="list-style-type: none"> Snort Log 	Mandatory
8	Packet Logger	<ul style="list-style-type: none"> Output a packet dump in PCAP format. 	Mandatory
9	Signature	[Non-functional operational requirement] <ul style="list-style-type: none"> Describe how to update the Snort signature file in a Wiki. 	Mandatory
10	Backup Log	[Non-functional operational requirement] <ul style="list-style-type: none"> Describe how to back up in a Wiki. Prepare a backup file in JSON format for further analysis. 	Mandatory
11	OSS Component updates	<ul style="list-style-type: none"> Update the OSS components of ME. 	Optional (High Priority)
12	Version fixes	<ul style="list-style-type: none"> Specify versions at installation. 	Optional (High Priority)
13	System Monitoring	<ul style="list-style-type: none"> Monitor services. 	Optional (Middle Priority)
14	Docker Containerization	<ul style="list-style-type: none"> Make Docker images of Spark. 	Optional (Middle Priority)
15	User Account Management	<ul style="list-style-type: none"> Make a procedure to change account settings. 	Optional (Middle Priority)
16	Implementation of Resource Updates	<ul style="list-style-type: none"> Make a procedure to download frequent update files. 	Optional (Middle Priority)
17	Explanations on Security Issues	<ul style="list-style-type: none"> Add explanations to avoid the known security issues. 	Optional (Low Priority)
18	ARM CPU Support	<ul style="list-style-type: none"> Provide support for ARM CPUs. 	Optional (Low Priority)
19	Threat Classification	<ul style="list-style-type: none"> Add information on severity. 	Optional (Low Priority)
20	Asset Management	<ul style="list-style-type: none"> Add asset management processes to identify the impacts on assets (i.e., criticality, risk level, target attack). 	Optional (Low Priority)
21	Sensor	<ul style="list-style-type: none"> Add a sensor registration scheme 	Optional (Low Priority)

No	Requirement	Activity	Level, Priority
	Registration	(provided by the users, i.e., subnet, asset classification, criticality level)	Priority)
22	Threat Intelligence Feed	<ul style="list-style-type: none"> Add a threat intelligence feed (from any free source of data feed intelligence, such as Talos). 	Optional (Low Priority)
23	Ticketing System	<ul style="list-style-type: none"> Add a ticketing system for incident management. 	Optional (Low Priority)

iii. Procurement and Contracting for Mata Elang Development

After the requirements were determined on August 8, an RFP (Request for Proposal) was sent to four interested entities on August 10. For details, please see **Appendix 3-3 RFP on Developing Mata Elang Stable Version**.

The deadline for proposal submissions was August 24.

Proposals were evaluated based on a Quality- and Cost-based Selection (QCBS) process. CV. Pratama Teknologi Nusantara (the "Developer") was selected as the developer for ME 1.1.

The Consultant and the Developer signed the contract on September 23.

iv. Mata Elang 1.1 Development and Monitoring of Progress

The ME 1.1 development work began immediately after the contract was signed. The software development was carried out under a lump-sum contract agreement.

The Consultant and Developer held an online progress meetings every two weeks to monitor the progress of the development work. The members of the ME technical team participated as observers.

The Consultant visited Surabaya and Jakarta from November 22 to December 9 to inspect the progress on-site and software quality and prepare for the next round of user acceptance testing.

Table 3-15 Progress Monitoring Activities

Date, Period	Activities
10 th October	1st online progress meeting
21 st October	2nd online progress meeting
4 th November	3rd online progress meeting

23 rd November – 3 rd December	<ul style="list-style-type: none"> • On-site progress meeting in PENS, Surabaya • On-site inspection of progress
4 th December – 9 th December	<ul style="list-style-type: none"> • Software quality inspection • Preparations for user acceptance testing at the next visit

At the progress monitoring meeting between the Developer and consultant in Surabaya, the Developer reported on a number of difficulties faced with the Zabbix Offline Installer. The Consultant reviewed the issue and came to agree with the Developer's claim regarding Zabbix, as expressed below. Consequently, the installation of Zabbix in the offline installer was dropped from the requirements.

The difficulties including this installation procedure into Mata Elang installer is the difference in service context. Zabbix server must be run on a different server other than Mata Elang Defense Center to optimize the resources. Therefore, the integrated offline installer is not possible.

Another reason is, Zabbix dependencies are too many to handle comprehensively. On the other hand, Zabbix is managed by their company, and that company should prepare the offline installer, not external body.

Zabbix usage should be limited to monitor resources for our testing purpose, for example when UAT. Mata Elang users may have preferences for their own monitoring platform.

For Docker perspective, the offline installer is possible but strongly not recommended for production use. This could be a threat for Mata Elang services itself and causing concern for users.

From a networking perspective, an offline installer shouldn't be offline after all. Users should prepare their environment using certain security standards. These security standards include operating system updates, software updates and security updates for patching bugs or security issues. It will be the user's awareness to keep their system up-to-date.

Mata Elang should be used to monitor external sourced attacks. For that purpose, the monitored infrastructure must be connected to the internet. The components of Mata Elang are also recommended to be kept updated to detect the newest attack possible.

Therefore, Zabbix and Mata Elang are better to use online installers.

Resource monitoring for the Mata Elang will be prepared separately, and will be carried out in the next version, as an additional component for the Mata Elang, so that it can also be used to monitor all the Mata Elang component, thereby making installation easier, more efficient and lighter.

(From Zabbix Offline Installer Difficulties)

On December 25, the Developer delivered the interim deliverables as per the contract.

The Consultant began testing the deliverables and provided feedback to the Developer up to the end of January 2023.

v. User Acceptance Testing

From January 29 to February 18, the Consultant visited Jakarta to prepare for and conduct the User Acceptance Testing (UAT).

The UAT preparation meeting was held on January 30. The Consultant presented the plan for the preparation and implementation of the UAT, and the plan was finalized after several modifications (see **Appendix 3-4 Plan of UAT**).

The Developer delivered the final deliverables on February 6, and the Consultant thereupon began the UAT with full on-site support from the Developer. The UAT test cases examined are summarized in **Appendix 3-5 UAT Test Cases**.

The persons and organizations present at the UAT are listed in **Appendix 3-6 Mata Elang UAT Attendees**.

The UAT was successfully completed, and the final source code, compiled objects, and Docker images were submitted on February 14. At the request of the JICA Project, the ME system environment used in the UAT was provided on February 15 for evaluation and testing.

A committee meeting was held on February 14. The Consultant presented the current progress of the UAT and the achievements of this development work. The committee approved the release of ME 1.1 and set the release date for March 1.

Requirements (1/2)			
The targets of this development			
No	Requirement	Activity	Level, Priority
1	Offline Installation	Develop offline installer Create easy installation manual	Mandatory
2	Performance Improvement	Update Snort to version 3 Add Ipv6 compatibility	Mandatory
3	Update of Dashboard	Making the dashboard compatible with ipv6	Mandatory
4	Elimination of Unnecessary Processes	Put parameters into external files and avoid unnecessary build	Mandatory
5	Testing	Unit test, System test, Stability test, Simulator Attack test	Mandatory
6	Documentation	Update installation manual, developer's guide and other technical documents	Mandatory
7	Log Rotation	Snort Log	Mandatory
8	Packet Logger	Output packet dump in PCAP format	Mandatory
9	Signature	[Non-functional operational requirement] - Describe how to update Snort signature file on Wiki	Mandatory
10	Backup Log	[Non-functional operational requirement] - Describe how to back up on Wiki - Backup file is in JSON format for further analysis	Mandatory
11	Update of OSS Components	Update OSS components of Mata Elang	Optional Priority High
12	Fixing the Version	Specifying versions at installation	Optional, Priority High

Figure 3-8 Achievements of the ME 1.1 Development Work (1/5)

Requirements (2/2)			
The targets of this development			
No	Requirement	Activity	Level, Priority
13	System Monitoring	Services Monitoring	Optional, Priority Mid
14	Docker Containerization	Making of Docker images of Spark	Optional, Priority Mid
15	User Account Management	[Non-functional operational requirement] Making of a procedure to change account settings	Optional, Priority Mid
16	Implementation of Resource Update	[Non-functional operational requirement] Making of a procedure to download frequent update files	Optional, Priority Mid
17	Explanation for Security Issues	[Non-functional operational requirement] Adding explanation to avoid the known security issues	Optional, Priority Low
18	ARM CPU Support	Support for ARM CPU	Optional, Priority Low
The requirements below will be the subjects at next development.			
19	Threat Classification	Adding severity information	Optional, Priority Low
20	Asset Management	Adding asset management to identify the impact on asset (i.e: criticality, risk level, target attack)	Optional, Priority Low
21	Sensor Registration	Adding sensor registration scheme (provided by the users, i.e: subnet, asset classification, criticality level, etc)	Optional, Priority Low
22	Threat Intelligence Feed	Adding threat intelligence feed (from any free data feed intelligence such as Talos)	Optional, Priority Low
23	Ticketing System	Adding ticketing system for incident management	Optional, Priority Low

Figure 3-9 Achievements of the ME 1.1 Development Work (2/5)

Achievements (1/3)

Performance Improvement

- Snort v3 Applied
- Response Time: 60 sec -> 30 sec
- Defense Center Memory Requirement: 64 GB -> 32 GB
- Performance under actual network environment:
54 million network events in 3 weeks



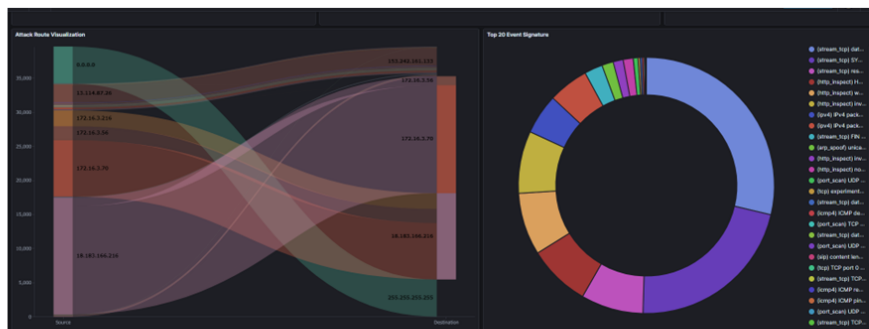
Copyright Mata Elang Committee

Figure 3-10 Achievements of the ME 1.1 Development Work (3/5)

Achievements (2/3)

Functional Improvement

- IPv6 Support
- New visualization on Dashboard
- PCAP (Packet Capture) File Output



Copyright Mata Elang Committee

Figure 3-11 Achievements of the ME 1.1 Development Work (4/5)

Achievements (3/3)

Expansion of Coverage

- Offline Installation Support for Weak Internet Area
- ARM CPU Support for Sensors:
Runs on inexpensive Raspberry Pi

Easy Installation

- Offline install scripts are now available.
- More Docker containerization.
- Simplified Installation Procedure.



Copyright Mata Elang Committee

Figure 3-12 Achievements of the ME 1.1 Development Work (5/5)

On the same day (February 14), the committee invited potential ME 1.1 pilot users such as DSTI (Direktorat Sistem & Teknologi Informasi; Directorate of Information Systems & Technology), BRIN (Badan Riset dan Inovasi Nasional, National Research and Innovation Agency), BSSN (Badan Siber dan Sandi Negara; National Cyber and Crypto Agency), and CBN (Internet Service Provider, <https://cbn.id/>) to attend an explanation and demonstration of the features of ME 1.1. The participants evaluated ME 1.1 positively in the runup to the software implementation.

vi. Release of Mata Elang 1.1

The remaining UAT on the documentation was completed on February 28.

ME 1.1 was released on GitHub on March 1 and is now available at the URL <https://github.com/mata-elang-stable/MataElang-Platform/wiki>.

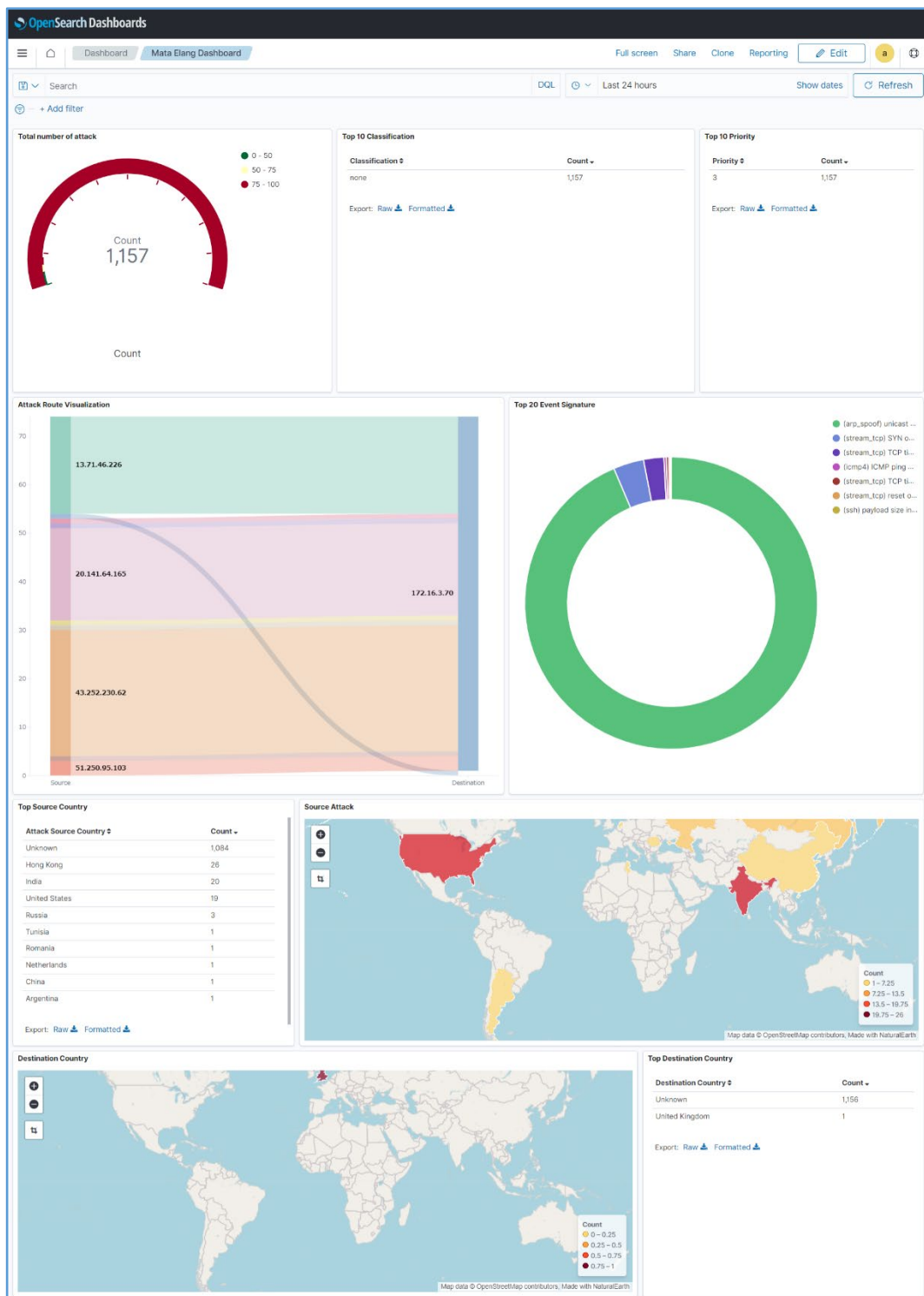


Figure 3-13 Mata Elang Dashboard (1/2)

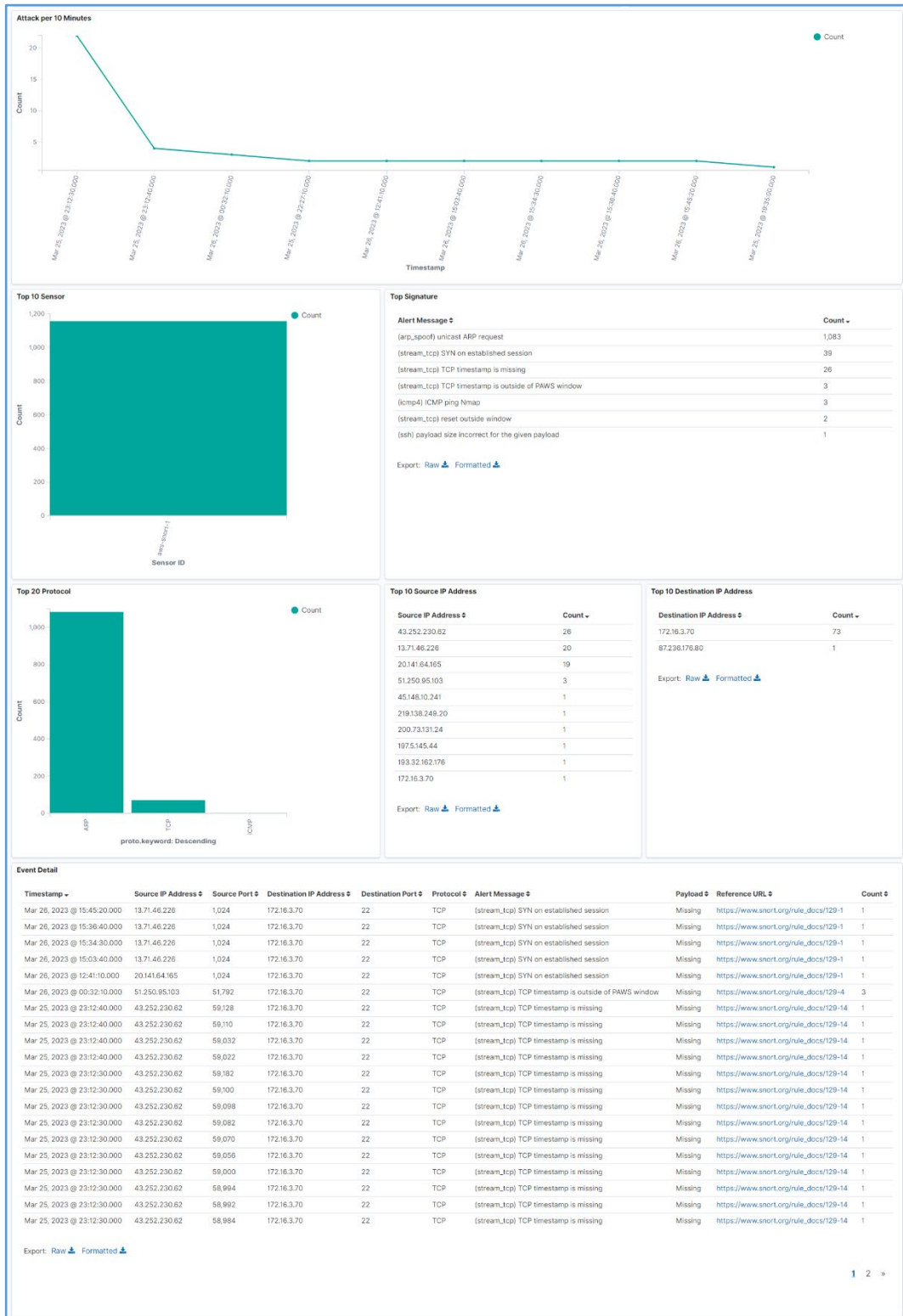


Figure 3-14 Mata Elang Dashboard (2/2)

4. Special efforts and lessons learned through technology transfer

1) Material development

a. Work flow for compiling and reviewing materials

The materials review process was conducted asynchronously to improve work efficiency. The Consultant clarified the viewpoints shaping the review and compiled a check-sheet to simplify and speed up the review process. The approach taken for the review reduced the work burden of the reviewers during the busy academic semester, which ran from September to December.

2) Seminar/Workshop delivery

a. CS trend seminars

The results of post-event questionnaire indicated that the seminar/workshop topics related to law tended to attract more people from the government sector, while technology-related topics tended to attract people from the education sector. This information could be useful when selecting advertising targets in preparation for the upcoming seminars.

b. CS Curriculum development workshop

A preliminary survey was conducted to help participants understand the differences between the current education supply and the potential market demands. The survey gave the participants an opportunity to discuss the supply and demand balance in their institutions and the relevance of their target human resources.

The assignment of the C/Ps as facilitators contributed to the curriculum development exercises. The C/Ps assisted the participants in applying the UI method to the needs of their own organizations. The ideas and examples from the Indonesian lecturers enlivened the discussions and made them more effective.

In a workaround session, the participants visited other groups and asked questions about the drafted curriculum in front of a flipchart. This session tightened the connections between the participants and improved their understanding of the methodology and the educational systems in other countries.

3) Policy development for the Malware Analysis Lab

Developing and implementing an effective policy requires a coordinated effort across all levels of the university. In order to achieve this, the Consultant brought the university-level directorate,

DSTI, into the process. This ensured a common understanding of the status of the Malware Analysis Lab and its lines of communication for further discussions and incident reports. This approach increased the effectiveness of the policy development activity.

4) OSS development

The recommendations from the previous OSS development were implemented. The Committee has become more deeply involved as a result.

5) Overall management

The allocation of deputy consultants on each work component streamlined the implementation of the work. The deputy consultants worked alongside the well-experienced main consultants to provide technical support and work on coordination and communications. The chief consultant brought in years of local experience as an effective manager of the on-site work.

5. Recommendations

1) Material development

a. Opening the Common Pre-Learning Materials to the public

The CPLMs are also useful for open education. The materials can be studied over the course of a few hours and cover a wide range of fundamental CS knowledge. Making the CPLMs publicly available through idCARE.UI (i.e., on the Internet) opens up various other types of prospective uses. Other universities, for example, can use them as pre-requisite studying materials for their CS courses, or government agencies can use them to improve CS awareness within their organizations.

When the Project opens a CPLM to the public, the Consultant recommends the adoption of an “Attribution-NonCommercial-ShareAlike” (CC BY-NC-SA) license, a Creative Commons license often used for open courseware. A “BY-NC-SA”-licensed user can share, copy, or modify the materials on the condition that the content creator is appropriately credited and all uses are non-commercial. When licensed users reproduce the modified materials, they need to inherit the same license from the original. As a side note, the Open Education Global organization also encourages the use of Creative Commons licenses for open educational resources.

b. Policy on Updating Common Pre-Learning Materials

CPLMs include topics on framework, CS incident cases, and threats such as OWASP Top 10. Given the rapid and steady changes taking place in the cyber-environment, the learning materials on these topics need to keep up with the latest trends. Regular CPLM updates are therefore key, along with the curriculum revisions scheduled to take place every two years. For details on the required updates, see **Appendix 2-2 Notes on the Common Pre-Learning Materials V.1.1**.

2) Seminar/Workshop delivery

a. Topics for future CS trend seminars

The 1st CS trend seminar focused on the circumstances surrounding the personal data protection law in Indonesia. The law is based on the GDPR and requires organizations to assign data protection officers (DPOs). As the demand for DPOs increases in Indonesia, seminars and workshops to make people aware of the importance of DPOs are expected.

In giving feedback, the participants in the 2nd CS trend seminar mentioned that they expected more detailed technical topics to be covered. The range of topics may have been limited for the following reasons:

- The seminar covered independent topics, and the time for each topic was limited.
- With a one-way format such as that used in an online seminar, the speakers can only explain and demonstrate in a fairly simple way.

The future seminars and workshops can cover topics such as:

- The importance of DPOs as personal data management professionals
- The skills and experience required of a DPO (i.e., knowledge of the law and skills in data analysis, IT system operation, and organizing stakeholders)
- Case studies to discuss how DPOs are to act in different cases
- Interactive technical workshops; e.g., a workshop on DevSecOps tools (i.e., Github Secret Scanning, SonarCloud/SonarQube, Snyk Vulnerability Scanner)

b. Delivering a CS Curriculum revision workshop

To maintain the curriculum continuously, some have suggested that a series of curriculum revision workshops be delivered for organizations that have implemented the developed curriculum for more than two years. Evaluation and analysis exercises using Google Data

Studio or similar business intelligence tools with automated dashboards would attract participants.

3) Policy development for the Malware Analysis Lab

a. Updating the Compliance section (2.10)

The compliance section on the Operational Policy should be updated when relevant policies and regulations are clarified. Two policies were omitted from the section due to insufficient information and a lack of formal documents: “Safety & Health Working Environment Policy” and “Internet Access Policy.” A conflict has been observed between the Operational Policy of the Malware Analysis Lab and the Internet Access Policy. The Internet Access Policy restricts all of the connections passing through the university proxy, whereas the Operational Policy requires an independent line connected to the Internet. This conflict will need to be addressed among the stakeholders. Some have suggested that it be treated as an exceptional measure under the Internet Access Policy.

b. Coordinating an organizational structure / emergency response structure

The details of the organizational structure, including the emergency response structure, are to be well coordinated. Two factors need to be considered: the location and the resources. The lab is located in the center of Jakarta, while the C/Ps are stationed in the Depok campus. The distance between them makes it more difficult to station an administrator in the lab. One solution would be to assign appropriate operators who can assist the administrators remotely. We noticed a project plan to restrict the operators from directly accessing the server rack. One possible way to implement the plan would be to set up Wake On LAN on the server and allow operators to send magic packets to boot up the server without opening the server rack.

c. Developing operational procedures and conducting operational training

If possible, experienced malware analysis experts who participated in the briefing session should take part in the development of the procedures and environment. The Head of the Malware Analysis Lab should conduct operational training after the procedures are developed and the environment is prepared.

As stated in the policy, we recommend that the following environment be prepared.

- A network separates from other existing networks
- Safe storage for electronic mediums that contain malware specimens
- A large-capacity power supply for the server rack

- Renovation of the controlled area in accordance with the policy
- Optionally, air conditioners in the controlled area and CCTVs for monitoring

We also recommend that the following operations be discussed.

- The method for managing entries and exits
- Mutual understanding of software installation orders on both the host OS and guest OS
- The collection of official documents on relative policies and regulations
- Operational procedures for the change work, incident response, analysis environment reset, usage of the download environment, and identity management (including passwords).

The operational training may include the following simulations.

- Incident escalation
- The Operational Policy and the implementation of the operational procedures (from the point artifacts are received to the point they are discarded)

4) OSS development

a. Strengthening the committee and community for the next phase

Now that the stable version of ME has been developed, the next goal as a committee and community is to promote its deployment. Given the “difficulty of maintaining an OSS community without users,” we need to focus on promoting the spread of ME in general. While we have already defined the management and implementation structure for ME (see below), we believe that we need to review and strengthen the committee and community for the next phase.

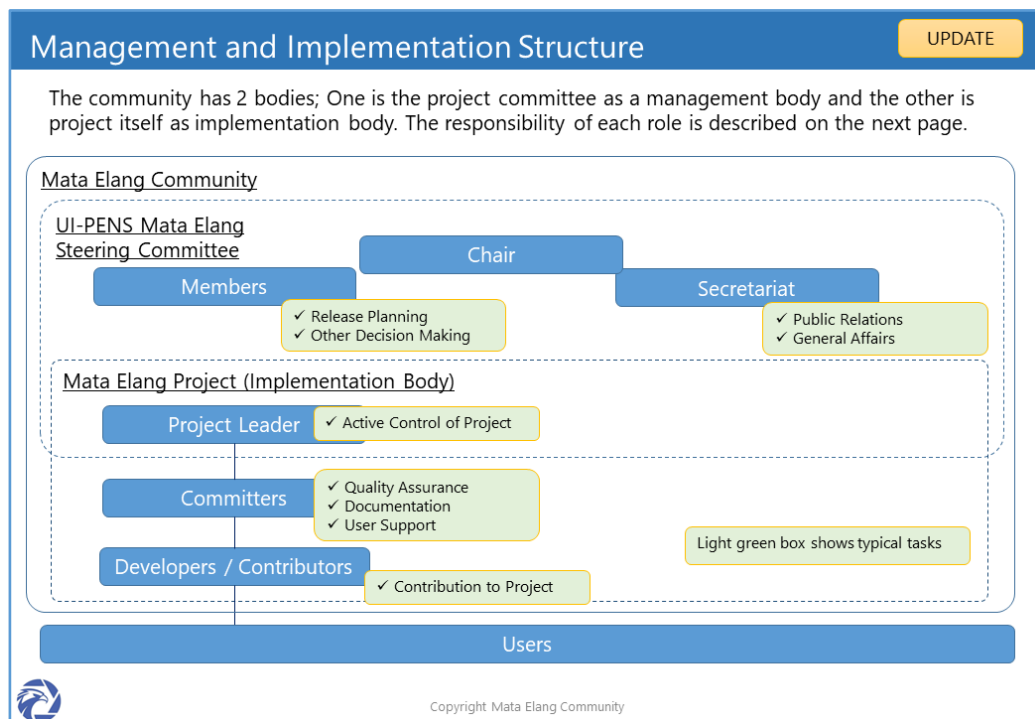


Figure 5-1 Management and Implementation Structure for Mata Elang

Role and Responsibility

Committee Chair	✓ The head of the committee
Committee Member	✓ The owner of the project ✓ Responsible for active management and decision-making of the project
Committee Secretariat	✓ Responsible for the day-to-day affairs of the committee such as public relations and general affairs
Project Leader	✓ Responsible for active control of the project ✓ Interface between the committee and the project, and has the accountability of the project
Committer	✓ Has write access to the code repository ✓ Responsible for the quality assurance, documentation and user support ✓ Has a signed agreement regarding intellectual property
Developer / Contributor	✓ Contributes to the project in the form of code or documentation

Copyright Mata Elang Community

Figure 5-2 Roles and Responsibilities of the Committee and Community

To strengthen the ME committee, we recommend the following:

- i. Define clear goals and objectives: Establish a clear mission statement and set objectives for the committee for the next phase.
- ii. Enhance communication: Establish regular communication channels and encourage all members to participate in discussions. Building a secretariat may be one solution to facilitate communication.

To strengthen the ME community, we recommend the following:

- i. Create a website: Create a website that showcases the features and benefits of ME. Blog and presentation postings are also useful ways to increase awareness and understanding on ME.
- ii. Educate users: Provide documentation and tutorials to help users understand how to use ME. This can include getting started guides, installation instructions, and FAQs.
- iii. Offer support channels: Provide support channels, such as a helpdesk or support forum, to help users troubleshoot issues and provide feedback. This can help to lower the barriers to deployment and encourage more people to get involved.
- iv. Collaborate with others: Collaborate with other organizations or communities that use cybersecurity tools to create new opportunities for ME. This can include joint events or partnerships to promote each other's projects.
- v. Demonstrate real-world use cases: Share success stories and case studies to demonstrate real-world use cases of ME. This can help potential users understand how ME can benefit their organizations and encourage them to adopt it.
- vi. Organize events and activities: Organize events and activities that bring community members together and provide opportunities for them to collaborate.
- vii. Recognize and reward contributions: Recognize and reward members for their contributions to the community. This can include giving credit in the software's documentation, providing awards or certificates, or highlighting contributors on the community's website.

Overall, promoting ME in public requires a combination of outreach, education, and engagement. The Project can increase the visibility and deployment of ME by reaching out to and engaging with potential users, providing educational resources, and collaborating with others.

- b. Building UI-SOC and training a technical team

ME has already been implemented in several companies and governments. As a result of committee and community efforts, several organizations have expressed positive attitudes toward deploying ME. We believe, however, that UI needs to implement ME within its network at the research and operational level so as to gain knowledge and experience through the building and operation of a Security Operation Center (SOC), and to train a technical team to guide the ME users.

Establishing the SOC will require the planning and execution of several steps. The following steps can help guide UI through the process:

- i. Define the scope and objectives of the SOC: Determine the specific goals and scope of the SOC based on the organization's risk profile and objectives.
 - ii. Define the SOC team: Identify the roles and responsibilities needed to build the UI-SOC team.
 - iii. Select SOC tools and technologies: ME would be the core tool.
 - iv. Establish policies and procedures: Develop policies and procedures that outline the processes for threat detection, incident response, and security monitoring.
 - v. Implement the SOC infrastructure: Build and deploy ME for the UI-SOC.
 - vi. Train the SOC team: Provide comprehensive training for the UI-SOC team on the tools.
 - vii. Test and refine SOC operations: Conduct regular testing of the UI-SOC operations to identify areas for improvement and refine UI's incident response plans.
 - viii. Establish reporting: Develop rules and content for regular reporting to the committee.
- c. Enhancement of Mata Elang

As the IDS is the only data source available for the system at present, ME has a limited ability to collect CS events across the organization. Detecting login events, for example, requires server authentication logs, while firewall attacks require information from the firewall. ME needs to have multiple data sources as observation points for CS events in the future, including logs from servers, firewalls, network equipment, and other security tools.

ME also needs to have an alerting capability to notify the security team of potential threats and enable them to take action.

We recommend continuing the UI-, PENS-, and community-led development of ME.

We also recommend developing a real-time cyberthreat map that can effectively convince

decision-makers to deploy ME.

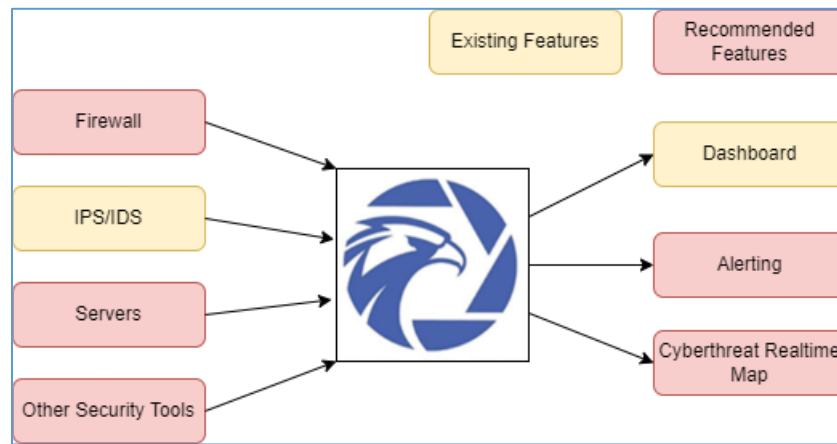


Figure 5-3 Existing and Recommended Features of Mata Elang

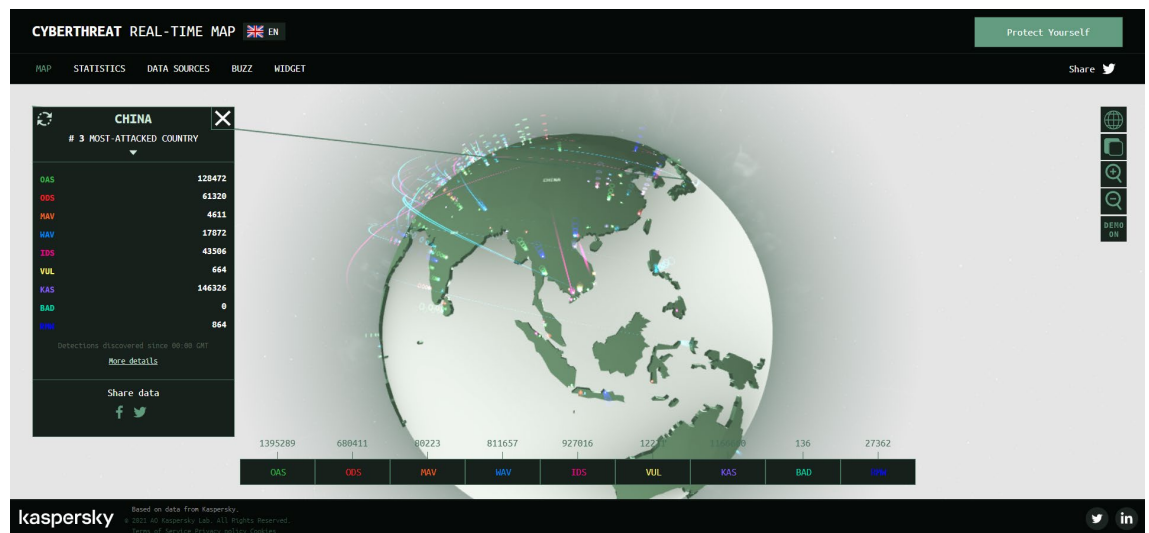


Figure 5-4 Kaspersky Cyberthreat Real-time Map

5) Feedback from the Project for the Development of Human Resources in CS in Mongolia

Three subjects developed in idCARE.UI, namely, “COM0010a How to make top management Aware of cybersecurity,” “COM0020a How to Make General Employees Aware of Cyber Security”, and “FOR0040a Computer Forensic,” were introduced through Train-the-Trainer (TTT) training in Mongolia. Update requirements were found and proposed to the cluster leaders during the preparation and implementation of the TTT. The Project should hold internal discussions on which proposals to accept and make plans for implementation.

Below is the summary of the feedback. See **Appendix 5-1 Specifications of Revisions** for details.

(A template for “Specifications for Revisions from the Curriculum Revision Manual developed in the previous work” was used.)

a. Slides

- When converting these three subjects to Open Courseware, the content will have to be localized or generalized in consideration of the local cases and laws in Indonesia. The following modifications were made during the TTT in Mongolia.
 - COM0010a: A discussion on the ID-SIRTII annual report was replaced with a discussion on “APAC-STATE-OF-INCIDENT-RESPONSE-2022.”
 - COM0020a: The case studies on local cases in Indonesia were translated into English.
 - FOR0040a: The section introducing Indonesian laws was changed to a set of questions on similar laws in Mongolia.
- The test links on the slides were extracted for easy maintenance.

b. Hands-on Guide / Data

- Templates for discussions on COM0010a and COM0020a were introduced.
- The hands-on guide and virtual machine data on FOR0040a were updated to streamline and facilitate the instructions and exercises. Virtual machine prepared by the Consultant supports Windows 11 and the VMware Workstation 17.0.0 player ,which supports the Windows 64-bit Operating System. The updated hands-on guide and data are suitable mostly for 3rd-country training and training for less experienced participants.
- Tools and data should be checked and updated frequently to support the latest OS and compatible version of the virtualization software.

c. Tests (Google forms)

- Some questions were revised to make them clearer. The test forms were reconfigured to better ensure that the responders could properly get their results. The revised test forms were shared.
- Revisions to the questions were proposed to make the test more relevant to the objectives and to make the questions less similar to the online quizlets. We suggest that a call for test question submissions be sent out to CAMP members and that a question bank be developed for more frequent test updates.

d. Mapping table

The time allocated to each topic needs to be revised based on the actual time used. We believe that too little time was allocated to some of the topics, though we understand that the TTT in Mongolia had been performed in a hybrid manner with both an online lecturer and on-site tutors, and that the allocated time cannot be the same as that for the on-site training.

Appendices

PRE0010a_Common Cyber Attacks and Malwares

Topic	Standard learning time (min)	Slides page
Title		1
Objectives and Goals		2
Outline		3
1. Background of Cyber Attacks	20	4
1-1. Trend technologies in Cyber Space Today		5
1-2. Chance for attackers		9
1-3. What is Cyber Attack?		11
1-4. Who are the attackers?		12
1-5. Reflection		18
2. Common Cyber Attacks and Threats	60	19
2-1. Common types of cyber attacks		20
2-2. Cyber Threats Top 10		33
2-2-1. Social Engineering		34
2-2-2. Third Party Exposure		36
2-2-3. Configuration Mistakes		37
2-2-4. Poor Cybersecurity Hygiene		38
2-2-5. Cloud Vulnerability		39
2-2-6. Ransomware Attack		40
2-2-7. Mobile Device Vulnerability		41
2-2-8. Internet of Things		42
2-2-9. Poor Data Management		43
2-2-10. Inadequate Post-Attack Procedures		44
2-2-11. Other threats to cyber security		45
2-3. Cases of cyber attacks		46
2-4. Reflection		61
3. Understanding of Malware	15	62
3-1. What is Malware		63
3-2. Common types of malware		64
3-3. Malware Infection Channels		67
3-4. Malware Behavior		68
3-5. Reflection		69
4. Knowledge base of threats and vulnerabilities		70
4-1. Vulnerability database	5	71
4-2. MITRE ATT&CK and Owasp Top10	5	74
4-3. Excercise : With Owasp Top10, Look for some latest threats, report about what those threats are and how to prevent those.	60	77
Post test	10	78
Total	175	78

PRE0020a_Basic Information security

Topic	Standard learning time (min)	Slides page
Title		1
Objectives and Goals		2
Outline		3
1. What is Information security?	20	4
1-1. Definition of Information		5
1-2. Risk in Information Lifecycle		10
1-3. Concept of Information Security		12
1-4. Importance of Information Security		16
1-5. Information security vs. Cyber Security		17
1-6. Reflection		18
2. Introduction to ISO/IEC 27001:2013	20	19
2-1. What is ISO/IEC 27001:2013?		20
2-2. Contents of ISO/IEC 27001:2013		26
2-3. Reflection		34
Post test	10	35
Total	50	35

PRE0030a Basic Computer and Network Architecture

Topic	Standard learning time (min)	Slides page
Title		1
Objectives and Goals		2
Outline		3
1. Basic Computer Architecture	25	4
1-1. Computer Architecture		5
1-2. File management system		10
1-3. File System Data Structure		12
1-4. Boot Process		15
1-5. Reflection		18
2. Network and protocols	30	19
2-1. Network basics		20
2-2. OSI & TCP/IP		22
2-3. Transmission Control Protocol		30
2-4. Internet Protocols		32
2-5. E-mail Protocols		36
2-6. Reflection		37
Post test	10	38
Total	65	38

PRE0040a Introduction of NIST Frameworks

Topic	Standard learning time (min)	Slides page
Title		1
Objectives and Goals		2
Outline		3
1. Overview NIST publications	15	4
1-1. What is NIST		5
1-2. Publications from NIST		6
1-3. Privacy Framework(PF) vs. CSF		7
1-4. NIST SP 800-53 vs. SP 800-171		8
1-5. Introduction of another SP		9
1-6. Reflection		13
2. NIST Cyber Security Framework (CSF)	25	14
2-1. What is CSF		15
2-2. CSF elements : Core		19
2-3. CSF elements : Tiers		26
2-4. CSF elements : Profile		28
2-5. Usage of CSF		30
2-6. Reflection		31
3. NIST SP 800-37 Rev.2 as Risk Management Framework (RMF)	10	32
3-1. What is NIST SP 800-37		33
3-2. Introduction of RMF concept		35
3-3. Related publications with RMF		36
3-4. Reflection		37
4. NIST SP 800-171 Rev.2 as requirements for protecting unclassified information	30	38
4-1. What is NIST SP 800-171 Rev.2		39
4-2. Security requirements		41
4-3. Reflection		57
5. NIST SP 800-61 Rev.2 as Cyber Security Incident Handling Guide	20	58
5-1. What is NIST SP 800-61 Rev.2		59
5-2. Step1:Preparation		62
5-3. Step2: Detection & Analysis		68
5-4. Step3: Containment Eradication & Recovery		69
5-5. Step4: Post Incident Activity		70
5-6. Reflection		71
6. Other frameworks for cyber security	10	72
6-1. Cyber/Physical Security Framework (CPSF)		73
6-2. Cybersecurity Maturity Model Certification (CMMC)		75
6-3. Security Incident Management Maturity Model (SIM3)		76
Post test	10	77
Total	120	77

Introduction of NICE Framework / SecBoK

Topic	Standard learning time (min)	Slides page
Title		1
Objectives and Goals		2
Outline		3
1. What is the NICE Framework?	15	4
1-1. What is the NICE Framework?		5
1-2. Goals of the NICE Framework		6
1-3. Components of the NICE Framework		7
1-4. Definitions of Tasks and KSAs		9
1-5. Reflection		10
2. How is the NICE Framework used in U.S?	10	12
2-1. Who are using it?		13
2-2. Affiliated Programs		14
2-3. Reflection		16
3. What is the SecBoK?	10	17
3-1. What is the SecBoK?		18
3-2. Relation with the NICE Framework		19
3-3. Reflection		23
4. How is the SecBoK used in Japan?	5	24
4.1. Affiliated program		25
5. Usage of NICE Framework and SecBoK in the idCARE Curriculum	5	27
5.1. Usage of NICE Framework and SecBoK in the project		28
5-2. Reflection		29
6. Revision of NICE and SecBoK	15	30
6-1. Revision of NICE and SecBoK		31
6-2. Gap :NICE and NICE rev1		32
6-3. Definitions of TKSs		34
6-4. Use case of NICE rev1		35
6-5. Gap :SecBoK 2019 and 2021		36
6-6. Use case of SecBoK 2021		37
Post test	10	38
Total	70	38

Notes on the

Common Pre-learning Materials

1. Background

Under the material development activity in 2022, “Common Pre-learning Materials” are developed for 2 purposes below:

- There are some overlapped topics among several existing materials of course subjects. By extracting the overlapped topics to the Common Pre-learning Materials, the efficiency of lectures would be improved.
- Make sure learners to have basic knowledge of cybersecurity by pre-learning.

2. Structure of Materials

2.1. Materials

In 2022, 5 Common Pre-learning Materials below are developed. Each material has slides with notes and is identified by code such as PRExxxxx.

- PRE0010a_Common Cyber Attacks and Malwares
- PRE0020a_Basic Information Security
- PRE0030a_Basic Computer and Network Architecture
- PRE0040a_Introduction of NIST Frameworks
- PRE0050a_Introduction of NICE Framework/SecBok

2.2. Post-test and exercise

Each Common Pre-learning Material has a post-test. Some material(s) also has exercises.

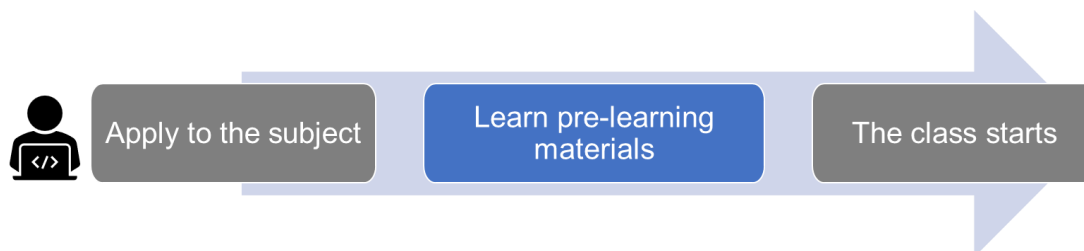
3. Guidance for learning

3.1. Learning form

The Common Pre-learning Materials are the materials for **self-study**.

3.2. Learning flow

At first, learners apply to the subjects, then study Common Pre-learning Materials by themselves **before the class starts**.



3.3. Correspondence of common pre-learning materials for subjects

Learners can access all the common pre-learning materials; however, some materials are prerequisite to specific subjects.

Requirements for prerequisite:

- Self-study the materials
- Take the post-test with a target score 70/100 (can try multiple times)

The correspondence of subjects and Common Pre-learning Materials as prerequisites is shown in the table below and is indicated on each subject's syllabus.

Subject		Prerequisite
Code	Name	Code
COM0010a	How to make top management Aware of cybersecurity	PRE0010a
COM0020a	How to make general employees aware of cybersecurity	PRE0010a
		PRE0020a
		PRE0040a
FOR0010a	Malware Analysis	PRE0010a
FOR0020a	How to make IT system forensic enabled	PRE0010a
		PRE0040a
FOR0040a	Computer Forensic	PRE0030a
GOV0010a	Cybersecurity Law and Regulation	PRE0010a
GOV0020a	Supply Chain Risk	PRE0010a
		PRE0040a

e.g.) If a learner applies for COM0020, he/she needs to study PRE0010a, PRE0020a and PRE0040a and get a score above 70 on the post-tests respectively, before the class starts.

Note) “PRE0050a_Introduction of NICE Framework_SecBok” is recommended to study for all learners but not compulsory.

3.4. Learning duration

Although learning time depends on each learner, there is a standard learning time. Refer to “Standard learning time allocation.xlsx” for details.

3.5. Self-assessment

- Post-tests or exercises are NOT evaluated by lecturers, and also it does NOT affect the grades of subjects.
- Even if learners haven't reach on the target score(70/100) on post-tests of prerequisites, the learners wouldn't be refused to take the subjects.
- On the other hand, lecturers can refer the results of post-tests.

4. Management

- Common Pre-learning Materials are managed by COMMON cluster leader.
- Major revision of Common Pre-learning Materials shall follow the curriculum revision cycle. On the other hand, minor revisions are encouraged under the COMMON cluster leader's responsibility.

The table below shows sections that may require frequent revisions:

Every year	
PRE0010a	2. Common Cyber Attacks and Threats - Cyber Threats Top 10 4. Knowledge base of threats and vulnerabilities - OWASP Top10
Under the curriculum revision cycle (every 2 years)	
PRE0010a	2. Common Cyber Attacks and Threats - Cases of cyber attacks
With the revision of reference publications	
PRE0020a	2. Introduction to ISO/IEC 27001
PRE0040a	2. NIST Cyber Security Framework (CSF) 3. NIST SP 800-37 as Risk Management Framework (RMF) 4. NIST SP 800-171 as requirements for protecting unclassified information 5. NIST SP 800-61 as Cyber Security Incident Handling Guide 6. Other cyber security frameworks - Cyber/Physical Security Framework (CPSF) - Cybersecurity Maturity Model Certification (CMMC) - Security Incident Management Maturity Model (SIM3)

PRE0050a	- NICE - SecBoK
----------	--------------------

Note) If materials are updated, post-test and exercises shall be revised too.

5. Conditions using the materials outside idCARE

5.1. License

When using Common Pre-learning Materials outside idCARE, it's recommended to adopt Creative Commons' license of Attribution-NonCommercial-ShareAlike.

5.2. Links to post-tests and exercises

Post-tests and exercises are delivered with Google Form. Therefore, when idCARE provides materials with post-tests and exercises outside, the segregation shall be considered. Depending on the scope of using, prepare 2 types below:

5.2.1. Type A (Original)

➤ Scope

For learners who take idCARE subjects.

➤ Procedure

Provide the original materials as it is.

5.2.2. Type B

➤ Scope

For Open Course Ware (OCW).

✓ Outside users can study and take post-tests and exercises as it is.

✓ Besides, materials (slides) and forms (post-tests/exercises) can be duplicated and modified by outside users.

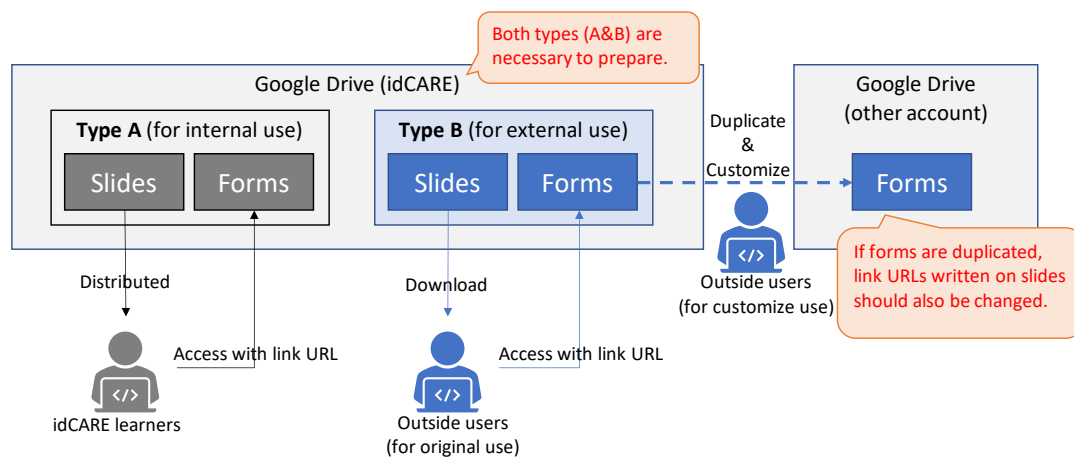
➤ Procedure

✓ Materials (slides): Make it can be downloaded by everyone.

✓ Forms (post-tests/exercises): On google form, share the folder as "Anyone with the link" and "Viewer". Then, inform the link URL of the folder.

Note) If users duplicate the forms, they should change the link URL written on slides as well.

Appendix 2-2 Notes on the Common Pre-Learning Materials V.1.1



1st CS trend seminar report

1st Nov 2022

1. Objective

The main objective of the seminar is that lecturers of idCARE.UI get latest information of cyber security. Besides, to make the seminar more effective, external CS related people in Indonesia are targeted, including Critical Information Infrastructure (CII) operators.

2. Theme

This seminar focused on CS trend in Indonesia, especially the law and regulation of Personal Data Protection which the bill has been deliberated in the Indonesian parliament.

3. Date

18th October 2022 (1 day)

4. Delivery method

- Hybrid of offline (at University of Indonesia) and online (Zoom)
- In Indonesian language

5. Agenda

1	Introduction of CS course in UI & Mata-Elang from the project)	Dr. Muhammad Salman, Project manager
2	Cyber security and protection of personal information under global perspective	Prof. Yuasa Harumichi, Graduate School of Governance Studies -Public Policy School-, Meiji university
3	The status of laws, regulation, and standards of personal data protection in Indonesia	Mr. Satriyo Wibowo, Chair of national standard for competency in personal data protection
4	Necessary measures for daily business operation when enforcing norms of cyber security in Indonesia	Mr. Rusdi Rachim, Vice president for ISC2 Jakarta chapter

6. Participants

Offline participants at the venue were invited by the project, the number was 24. Online participants were called publicly. The consultant advertised the seminar with an online registration form. The number of online participants was 172¹.

7. Post-event questionnaire

The number of answers of post-event questionnaire was 60.

a. Respondents attribute

¹ The number is exclusive of overlap, and inclusive of leaving in the middle.

Organizations of participants can be categorized into three, Ministry/Municipality (45%), Education institute (32%), and Private company (22%). The Indonesian parliament passed the PERSONAL DATA PROTECTION BILL on September 20, right before the seminar. That had a huge impact to the department of information and communication of each Ministry/Municipality, therefore the seminar was attractive for them to get detail information about it.

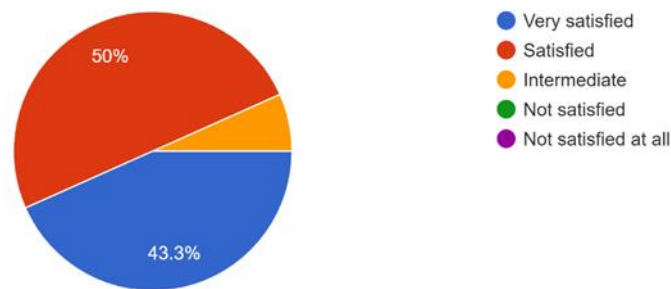
More than half of participants are related with CS/IT/telecom field. On the other hand, CII operators are few as long as confirmed, even though they were one of the targets.

b. Satisfaction

More than 90% respondents felt very satisfied/satisfied with the seminar.

1. How satisfied are you with the seminar?

60 responses

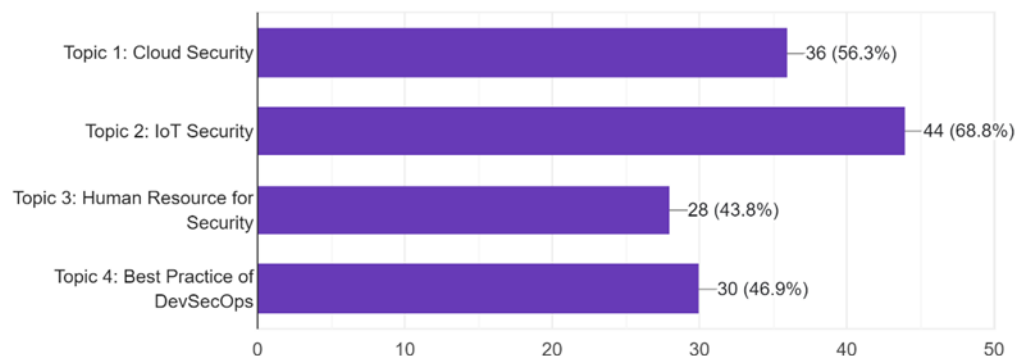


c. Most interesting session

Most interesting session for respondents was the session 2. This result came from the situation in Indonesia that the PERSONAL DATA PROTECTION BILL was passed right before the seminar.

2. Which part of the seminar was most interesting to you?

64 responses

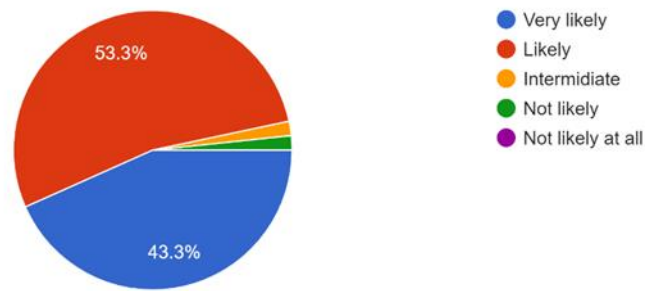


d. Recommendation to others

More than 90 % respondents were very likely/likely to recommend the seminar to others.

3. How likely would you recommend the seminar to a friend or colleague?

60 responses

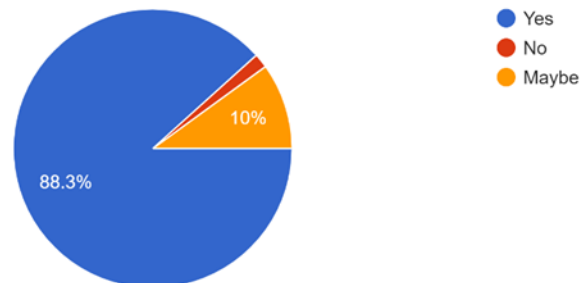


e. Expectation for next seminar

Near 90 % respondents are planning to return to next event held by idCARE.UI.

4. Are you planning to return to next event held by idCARE.UI?

60 responses

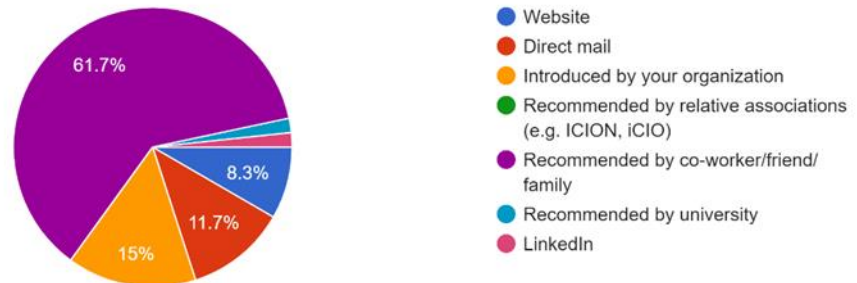


f. Source of information

Looking at the source of advertisements, nearly 90% of respondents are passively aware of the seminar; recommended by co-worker/friend/family (61.7%), introduced by their organization (15%) or direct mail (11.7%), recommended by university (8.3%). The most effective way of advertisement was word of mouth by influencers such as speakers.

5. How did you get to know about this seminar?

60 responses



g. Suggestion for next seminar

- If possible, provide cases from industry players.
- Prefer technical discussion.
- Full offline.
- Want to know about cyber criminals law.

8. Lesson learned

- This time, the seminar focused on law and regulation. As a result, participants got theoretical knowledge about personal data protection. It is expected to focus on more practical aspects such as real cases in CII, next time.
- Having started advertisements to the public one month before the seminar, the number of registrations in advance was 173 in total. Among them, 84 people registered within 7 days before the seminar. Based on that result, for more effectiveness, advertisements should be boosted few days before the seminar. Besides, registration should be accepted as closed to the start of the seminar as possible.
- Participants from private companies including CII operators were fewer than expected. To get more participants from private companies, special efforts such as holding a seminar without working hours or issuing official invitations are necessary.
- Certificates of participation were automatically distributed to respondents of post-questionnaire by using a free tool and e-mail. It improved the efficiency of operational duties.

END

2nd CS trend seminar report

1st Mar 2023

1. Objective

The main objective of the seminar is that lecturers of idCARE.UI get latest information of cyber security. Besides, to make the seminar more effective, external CS related people in Indonesia are also targeted, including Critical Information Infrastructure (CII) operators.

Taking advantage of online seminar, participants from other countries were welcomed including the attendees of the CS Curriculum development workshop in October 2022 in Bali (Mongolia, Laos, Cambodia and Timor-Leste).

2. Theme

Comparing to the 1st seminar which was mainly about personal data protection law and regulation, the 2nd seminar provided more detailed technical information. It was useful for the secure system development and its operation in organizations.

3. Date

27th February 2023 (1 day)

4. Delivery method

- Online (Zoom)
- In English

5. Agenda

1	Introduction of CS course in UI & Mata-Elang from the project)	Dr. Muhammad Salman, Project manager
2	Trend of cloud security	Mr. Muhammad Salahuddien Manggalanny, Deputy Director of Operations, CSIRT.ID
3	Trend of IoT security	Mr. Teguh Prasetya, Chairman of Indonesian IoT Association
4	Human Resource for Cyber Security	Prof. Toshihiro Hirayama, Professional University of Information and Management for Innovation (i-university), Japan
5	Best Practice of DevSecOps	Mr. Wahyu Sutejo, CSIRT.ID

6. Participants

The approximate number of participants was 200. The number of unique participants was 157, exclusive of overlap, and inclusive of leaving in the middle. However, there are some cases that several people shared a zoom account in an organization. Therefore, exact number of participants could not be counted.

7. Post-event questionnaire

The number of answers of post-event questionnaire was 64.

a. Respondents attribute

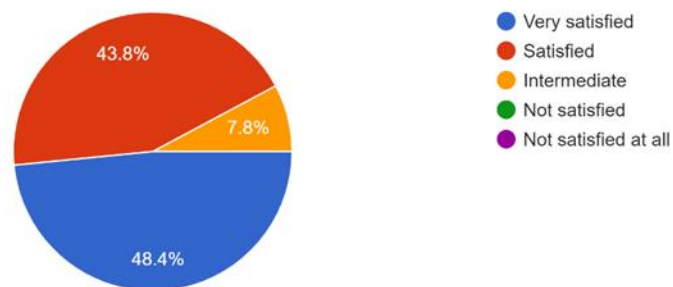
Countries of respondents were Indonesia (71.9%), Mongolia (14.1%), Laos (9.4%), Timor-Leste (1.6%) and Japan (1.6%). It is natural to have Indonesian participants the most, as the host of seminar, the project, is in Indonesia. It can be considered that participants from other countries, Mongolia, Laos, Timor-Leste and Cambodia were recommended from those who had attended the CS Curriculum development workshop held by the project in October 2022 in Bali. (It was confirmed that some participants came from Cambodia although it cannot be found in the result of questionnaire.) Organizations of respondents were Education institute (64.1%), Ministry/Municipality (21.9%), and Private company (9.4%). Comparing to the result of 1st seminar, the rate of Education institute much increased and half of them were students.

b. Satisfaction

More than 90% of respondents felt very satisfied/satisfied with the seminar.

1. How satisfied are you with the variety of topics presented at the seminar?

64 responses

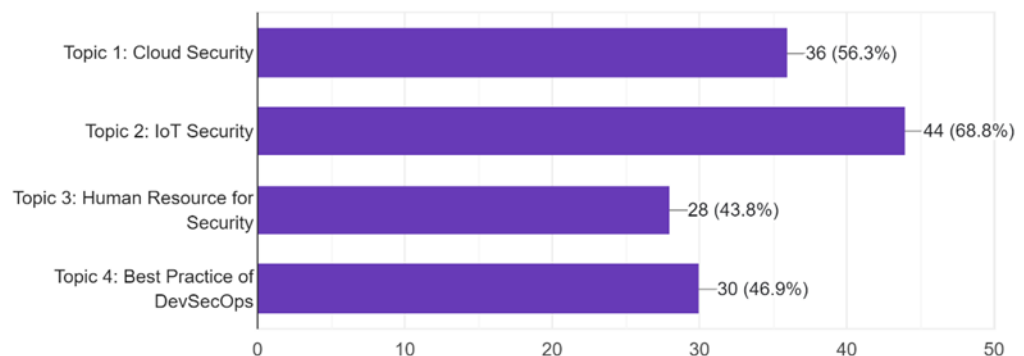


c. Most interesting session

Most interesting session for respondents was the session 2, IoT security.

2. Which part of the seminar was most interesting to you?

64 responses

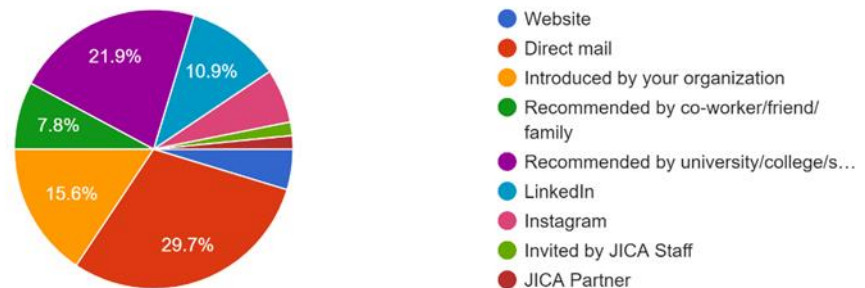


d. Source of information

Looking at the source of advertisements, same as the 1st seminar, most participants (more than 70%) got the information passively; direct mail (29.7%), Introduced by organization (15.6%), recommended by co-worker/friend/family (7.8%), recommended by university/college/school (21.9%). However, for this seminar, strengthened advertisements on SNS such as LinkedIn of JICA CS network (10.9%) and Instagram of FTUI (6.3%), achieved some degree of success.

3. How did you get to know about this seminar?

64 responses



e. Suggestion for next seminar

- The seminar was very interesting, with more practical demonstration will more interesting.
- Maybe next, we can hold seminar or workshop offline.
- Continue provide to us the seminar.
- Can provide material related to cyber security at a higher level.

8. Lesson learned

- This seminar delivered more technical topics than the 1st CS trend seminar. We can consider that such topics were attractive especially for students because much more students attended at this time comparing to the 1st seminar.
- There were several feedbacks expecting to continue such seminars, more frequently.

END

Appendix 2-5 Responses to the Post-Event Questionnaire After the Curriculum Development Workshop

Post-event questionnaire

Event: **Workshop for Cybersecurity Curriculum Development**

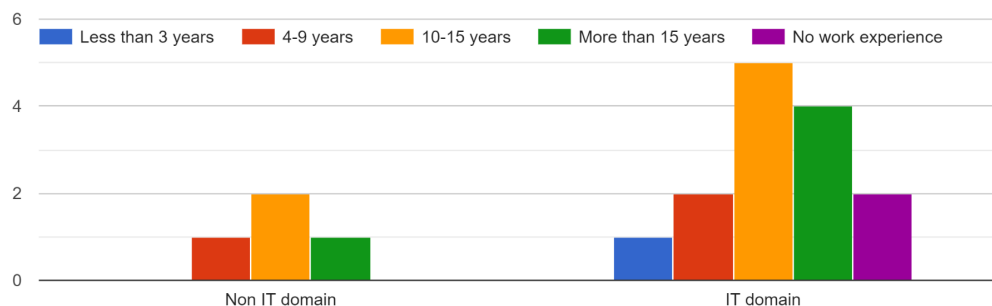
Date: 24th Oct to 28th Oct 2022 (5 days)

Respondents: 14 (fourteen)

1. Respondents attribute

Most of the participants have experience in IT domain more than 10 years.

Please select your work experience.



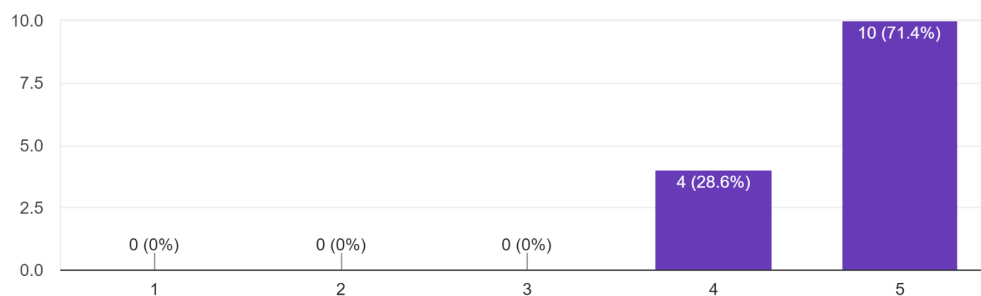
2. Satisfaction

All the participants satisfied or very satisfied with the seminar.

The contents are aligned with their expectation.

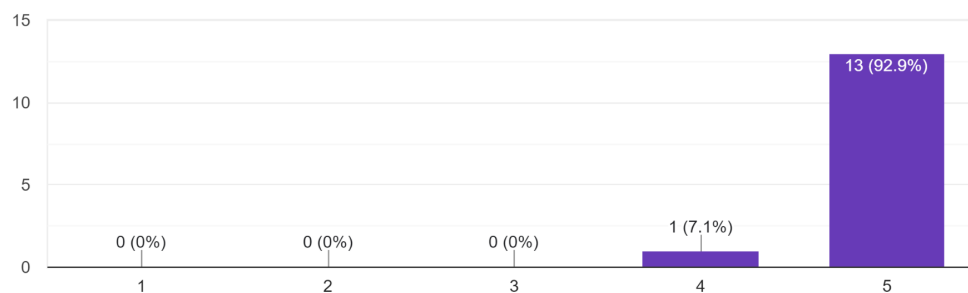
What is your level of satisfaction with this seminar?

14 responses



The seminar contents are aligned to your expectation.

14 responses



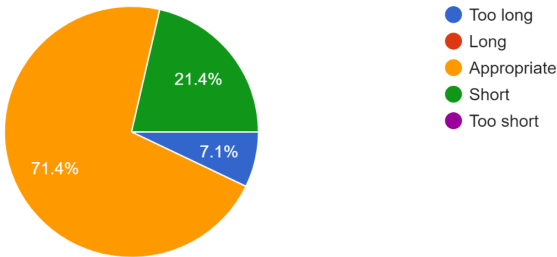
Appendix 2-5 Responses to the Post-Event Questionnaire After the Curriculum Development Workshop

3. Appropriateness

The length and difficulties of the workshop were appropriate for 70% of the participants.

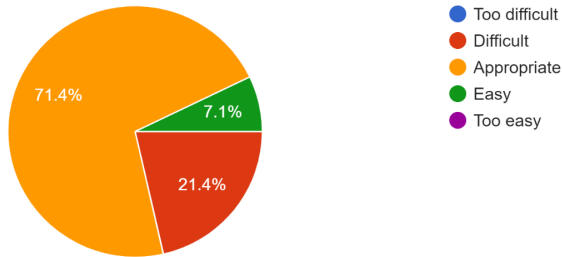
The seminar length are appropriate.

14 responses



How do you find the difficulties of topics presented today?

14 responses

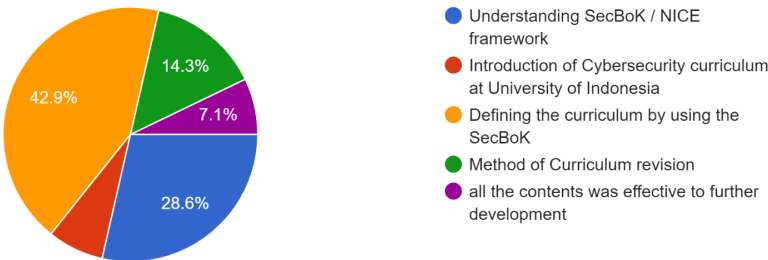


4. Most interesting topic

The most interesting topic was curriculum development and the second was framework introduction.

Which topics have you interested the most?

14 responses

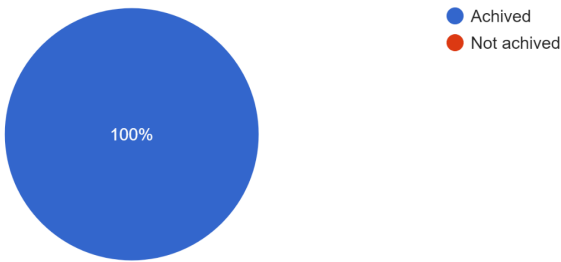


Appendix 2-5 Responses to the Post-Event Questionnaire After the Curriculum Development Workshop

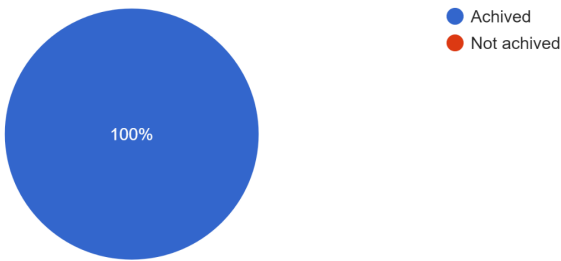
5. Achievement of each topic

It is noticed that the curriculum revision topic needs more exercises.

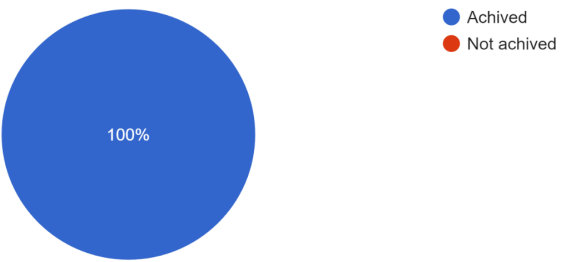
•Able to analyze the latest Framework(NICE, SecBoK) for the curriculum development
14 responses



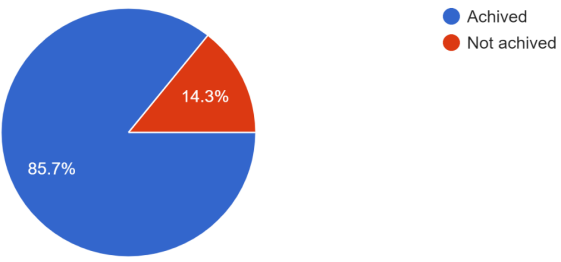
•Able to determine target work roles to develop a new curriculum
14 responses



•Able to define subjects with KSAs on SecBoK
14 responses



•Able to explain the cycle of curriculum revision
14 responses



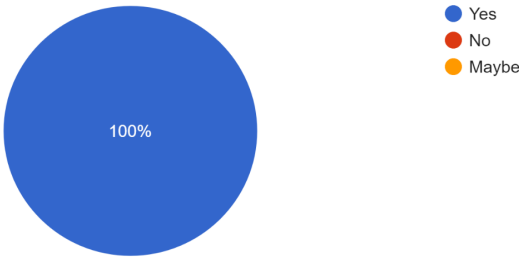
6. Comments and suggestions

Tell us your favorite part of the seminar and suggestions for the next seminar.

Please more detailed explain to evolution method
Defining Curriculum using SecBoK, UI Curriculum of Cybersecurity ,
I like how the instructor is easy to engage with participants, and participant are actively discussing on topic and sharing their country information.
Should provide the documents and guidelines for self study before training
Defining work roles and pathways for cybersecurity curriculum. It would be great to have more examples which is filled already in revision section so that it can be more easier to follow the tasks in revision session
cyber security Syllabus development and training to trainer in CS
Defining the curriculum by using the SecBoK
Most parts are interesting, this workshop is my new experience on creating new course. I would like to attend more deeper cybersecurity course.
Very clear , thank you very much

Will you recommend the seminar to your friends or colleagues?

14 responses



Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

Survey result analysis



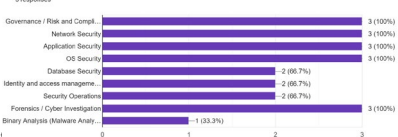
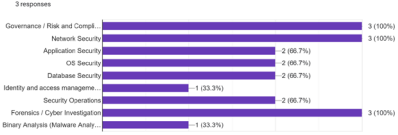

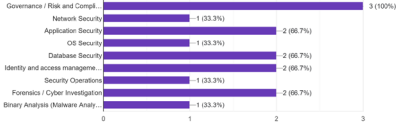
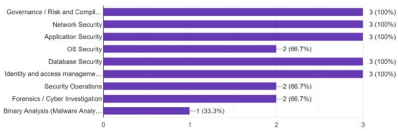
Objective: Analyze the gap between supply and demand, then define your group target.

◆Procedure

1. Decide your group target program
2. Analyze your answers to questions at Items 2 to 4, both in the column of Supply and the column of Demand
Discuss whether the result of the survey is proper or not. Decide your group target for this workshop.

Start from the questions of Supply.

- Consider the "Demands" as good input to define what you would supply
3. Compare the analysis result of supply and demand on each item
4. Choose the target work roles that suit your group's target education program

Item	Your organization(Supply)	Compare Supply and Demand	Private sector(Demand)
1	<p>Q1 shows your target education program Decide your group target xxx degree adding cs subjects? Developing new cs program?</p> <p>1-1. Select the main target of curriculum that your organization plans to develop. 3 responses</p>  <p>1-2. Select the main target of curriculum that your organization plans to develop. 3 responses</p> 		
2	<p>Q2 and 3 show what you should supply Select the top 3 areas that your students should learn but lack in your program. 1 xxx 2 xxx 3 xxx</p> <p>figure 2</p> <p>2. Select technical areas of cybersecurity that your students supposed to have. (Select all that apply.) 3 responses</p>  <p>3. Select technical areas that you think is lacking in cybersecurity education at your organization. (Select all that apply.) 3 responses</p>  <p>you should think whether to upgrade the existing subjects or add new subjects</p> <p>no figure <i>Network security, Information Security, Introductions to cybersecurity</i></p>	<p>Analyze each result of questions Discuss the gap of supply and demand. (Objective: Examine the relevance between supply and demand. Determine which technical areas should be supplied in your program. Determine the treatment of existing subjects.)</p>	<p>Q8 shows what kind of education is lacking or what kind of engineer is needed in your region xxx incident means a lack of security awareness? governanmce? Network security? OS security? Xxx? To respond xxx attacks, Network engineer?, Incident responder?, SOC analysts? are needed</p> <p>8. What are the top 3 security risks / incidents in your country or region? 3 responses</p>  <p>Q10 and 11 show the potential demand in the human resource market. In other words, it shows what you should supply. for students willing to work in IT vendors: xxx, OS security?, Application security? for students willing to work in IT user companies: xxx, xxx (Does this match with the result of Q8?) (On Q9, which company is the potential employer for your students?)</p> <p>10. Select technical areas that you think is lacking in cybersecurity workforce in IT vendors. (Select all that apply.) 3 responses</p>  <p>11. Select technical areas that you think is lacking in cybersecurity workforce in IT user companies. (Select all that apply.) 3 responses</p> 

Page 2 of 8

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

Survey result analysis

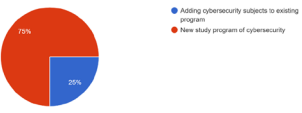

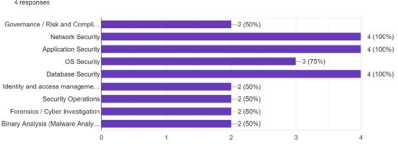
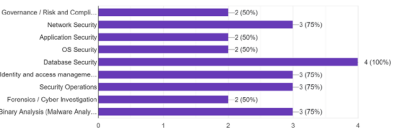
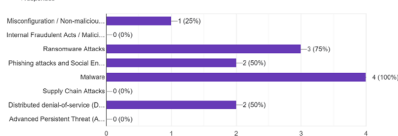
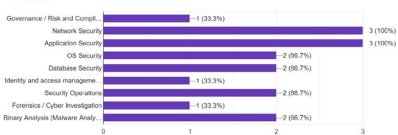
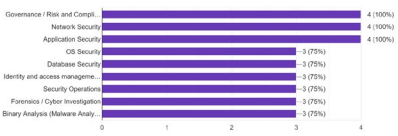
Objective: Analyze the gap between supply and demand, then define your group target.

◆Procedure

1. Decide your group target program
2. Analyze your answers to questions at Items 2 to 4, both in the column of Supply and the column of Demand
Discuss whether the result of the survey is proper or not. Decide your group target for this workshop.

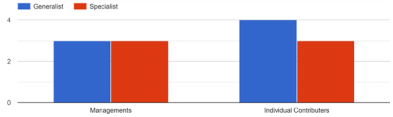
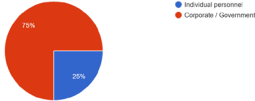
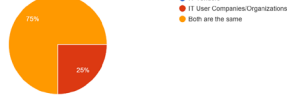


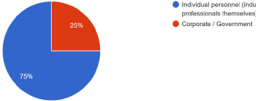
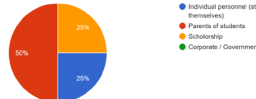
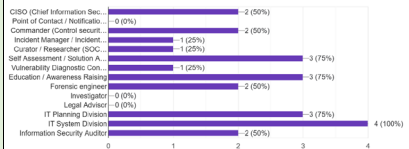
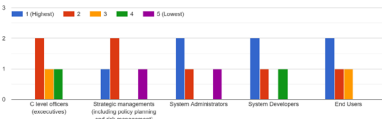

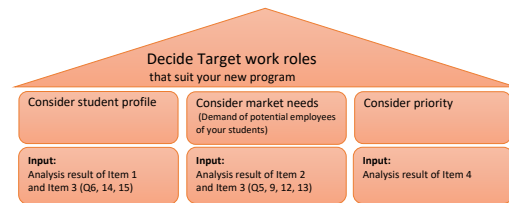
Start from the questions of Supply.

- Consider the "Demands" as good input to define what you would supply
3. Compare the analysis result of supply and demand on each item
4. Choose the target work roles that suit your group's target education program

Item	Your organization(Supply)	Compare Supply and Demand	Private sector(Demand)
1	<p>Q1 shows your target education program Decide your group target xxx degree adding cs subjects? Developing new cs program?</p> <p>1-1. Select the main target of curriculum that your organization plans to develop. 4 responses</p>  <p>1-2. Select the main target of curriculum that your organization plans to develop. 4 responses</p> 		
2	<p>Q2 and 3 show what you should supply Select the top 3 areas that your students should learn but lack in your program.</p> <ol style="list-style-type: none"> 1 xxx 2 xxx 3 xxx <p>2. Select technical areas of cybersecurity that your students supposed to have. (Select all that apply.) 4 responses</p>  <p>3. Select technical areas that you think is lacking in cybersecurity education at your organization. (Select all that apply.) 4 responses</p>  <p>Q4 shows existing subjects you should think whether to upgrade the existing subjects or add new subjects</p> <p>no figure</p>	<p>Analyze each result of questions Discuss the gap of supply and demand. (Objective: Examine the relevance between supply and demand. Determine which technical areas should be supplied in your program. Determine the treatment of existing subjects.)</p>	<p>Q8 shows what kind of education is lacking or what kind of engineer is needed in your region xxx incident means a lack of security awareness? governanmce? Network security? OS security? Xxx? To respond xxx attacks, Network engineer?, Incident responder?, SOC analysts? are needed</p> <p>f 8. What are the top 3 security risks / incidents in your country or region? 4 responses</p>  <p>Q10 and 11 show the potential demand in the human resource market. In other words, it shows what you should supply. for students willing to work in IT vendors: xxx, OS security?, Application security? for students willing to work in IT user companies: xxx, xxx (Does this match with the result of Q8?) (On Q9, which company is the potential employer for your students?)</p> <p>10. Select technical areas that you think is lacking in cybersecurity workforce in IT vendors. (Select all that apply.) 3 responses</p>  <p>11. Select technical areas that you think is lacking in cybersecurity workforce in IT user companies. (Select all that apply.) 4 responses</p> 

Information Security, Network security (Cisco network security), Computer Network, Database Administration, System Administration
Network security, Cyberlaw and policy, safe online, cyber threats, attack and vulnerabilities
Network security, Digital Forensics, how organizations can protect their operations against these attacks, cyber threats analysis

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

3	<p>Q5,6 show your target customer(student)</p> <p>According to the target degree and students profile</p> <ul style="list-style-type: none"> -will your students be individual contributors or managements? -will your students be generalists or specialists? <p>Whose needs should you know, individuals or market needs?</p> <p>5. Mark target image of human resources that your organization is trying to develop through cybersecurity education. (Select all that apply.)</p>  <p>6. Select a customer(student) profile that your organization targets mainly.</p> <p>4 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine the type of human resources that your group should educate.</p> <p>Determine the balance of demands from your marketing target and potential employers of your students</p> <p>)</p>	<p>Q9,12,13,14,15 shows your potential customer profile</p> <p>Who are the potential employers of your students?</p> <ul style="list-style-type: none"> -Consider plus CS human resources(non-security specialist but required security skills) for bachelor students for IT vendors, your students could be generalists? specialists? as individual contributors? managements? for IT user companies, your students could be generalists? specialists? as individual contributors? managements? <p>the interests of your professional students might be similar to the above result</p> <p>how about the interests of your usual students?</p> <p>9. Which type of corporate is more struggling with a shortage of cybersecurity human resources?</p> <p>4 responses</p>  <p>12. Mark target image of human resources in IT vendors. (Select all that apply.)</p>  <p>13. Mark target image of human resources in IT user companies. (Select all that apply.)</p>  <p>14. Who pays for industry professionals to study at university?</p> <p>4 responses</p>  <p>15. Who pays for usual students to study at university?</p> <p>4 responses</p> 
4	<p>Q7 shows your tentative target work role for the curriculum</p> <p>What is your tentative target in this workshop?</p> <p>If you are adding subjects to the existing program, consider work roles covered by the program.</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>(Does this match with the result of Q2 and Q3?)</p> <p>7. Select work roles that your organization try to develop through cybersecurity education. (Select all that apply)</p> <p>4 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine priority of target work roles in your program</p> <p>)</p>	<p>Q16 shows the layer of workforce that you should target in your curriculum</p> <p>1st priority : xxxx *Decide all levels</p> <p>2nd: *System administrators includes security operators</p> <p>3rd:</p> <p>4th:</p> <p>5th:</p> <p>16. Based on the above answers, which layer of workforce do you think should be trained in prior to others in your country or region? Choose different priority in each row to make the workforce in order.</p>  <p>Q17 shows your target work role for the curriculum</p> <p>see the difference between this and the result of Q7, Q10 and Q11</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>17. Based on the above answers, which work roles (human resources) do you think should be trained in your country or region? (Select all that apply)</p> <p>4 responses</p> 
5		<p>Make a comprehensive conclusion</p> <p>1.Copy your analysis result here for getting an overview.</p> <ul style="list-style-type: none"> •Target degree and program: •Marketing target(Student profiles): •Who needs the human resource?: •Target image of human resources: •Training priority of workforce layer: <p>2.List up your target work roles for your new program</p> <p>XXXX</p> <p>XXXX</p> <p>XXXX</p>	<p><<<< The figure below could assist you in deciding target work roles</p> 

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

Survey result analysis

Objective: Analyze the gap between supply and demand, then define your group target.

◆Procedure



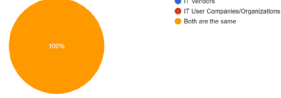


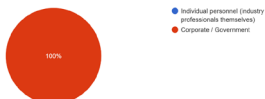


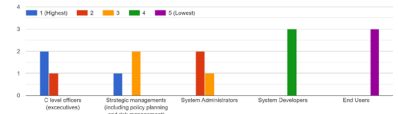
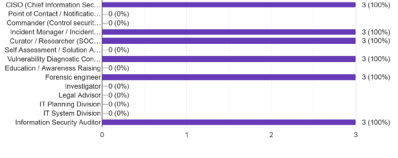
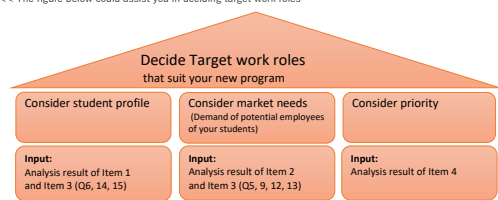
1. Decide your group target program
2. Analyze your answers to questions at Items 2 to 4, both in the column of Supply and the column of Demand
Discuss whether the result of the survey is proper or not. Decide your group target for this workshop.

Start from the questions of Supply.

- Consider the "Demands" as good input to define what you would supply
- Compare the analysis result of supply and demand on each item
- Choose the target work roles that suit your group's target education program

Item	Your organization(Supply)	Compare Supply and Demand	Private sector(Demand)
1	<p>Q1 shows your target education program Decide your group target</p> <p>xxx degree adding cs subjects? Developing new cs program?</p> <p>1-1. Select the main target of curriculum that your organization plans to develop. 3 responses</p> <p>1-2. Select the main target of curriculum that your organization plans to develop. 3 responses</p>		
2	<p>Q2 and 3 show what you should supply Select the top 3 areas that your students should learn but lack in your program.</p> <p>1 xxx 2 xxx 3 xxx</p> <p>2. Select technical areas of cybersecurity that your students supposed to have. (Select all that apply) 3 responses</p> <p>3. Select technical areas that you think is lacking in cybersecurity education at your organization. (Select all that apply) 3 responses</p> <p>Q4 shows existing subjects you should think whether to upgrade the existing subjects or add new subjects</p> <p>no figure</p> <p>Cyber security, Introduction to Programming, Object-Oriented Programming, Data Structures and Algorithms, Computer Network I, Network security, Application Security, Introduction to Information Security, System Security Project I, OS security, Cyberlaw and P Malware Analysis, Network defense, Attack detection, Firewall and Intrusion Detection Systems, Web Security, Ethical Hacking, N Mobile Systems Security, Information Security Laws and Ethics, Computer Forensics, Management of Information Security Assessment, Advanced Topics in System Security, Digital forensics, Pen testing, network defence, Information security Auditing</p>	<p>Analyze each result of questions Discuss the gap of supply and demand. (Objective: Examine the relevance between supply and demand. Determine which technical areas should be supplied in your program. Determine the treatment of existing subjects.)</p>	<p>Q8 shows what kind of education is lacking or what kind of engineer is needed in your region xxx incident means a lack of security awareness? governanmce? Network security? OS security? Xxx? To respond xxx attacks, Network engineer?, Incident responder?, SOC analysts? are needed</p> <p>8. What are the top 3 security risks / incidents in your country or region? 3 responses</p> <p>Company Answer A Ransom, Phish, Malware B Misconfig, Phish, APT C Internal Fraud, Phish D Ransom, Phish, Malware</p> <p>Q10 and 11 show the potential demand in the human resource market. In other words, it shows what you should supply. for students willing to work in IT vendors: xxx, OS security?, Application security? for students willing to work in IT user companies: xxx, xxx (Does this match with the result of Q8?) (On Q9, which company is the potential employer for your students?)</p> <p>10. Select technical areas that you think is lacking in cybersecurity workforce in IT vendors. (Select all that apply) 3 responses</p> <p>Company A, C, D B, C B, C B, D A, D D D</p> <p>11. Select technical areas that you think is lacking in cybersecurity workforce in IT user companies. (Select all that apply) 3 responses</p> <p>B, C, D A A, D A A, C, D A, B, C, D A A, D A, D B: HR</p>

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

3	<p>Q5,6 show your target customer(student)</p> <p>According to the target degree and students profile</p> <ul style="list-style-type: none"> -will your students be individual contributors or managements? -will your students be generalists or specialist? <p>Whose needs should you know, individuals or market needs?</p> <p>f</p> <p>5. Mark target image of human resources that your organization is trying to develop through cybersecurity education. (Select all that apply.)</p>  <p>6. Select a customer(student) profile that your organization targets mainly</p> <p>2 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine the type of human resources that your group should educate.</p> <p>Determine the balance of demands from your marketing target and potential employers of your students</p> <p>)</p>	<p>Q9, 12,13,14,15 shows your potential customer profile</p> <p>Who are the potential employers of your students?</p> <p>-Consider plus CS human resources(non-security specialist but required security skills) for bachelor students for IT vendors, your students could be generalists? specialists? as individual contributors? managements? for IT user companies, your students could be generalists? specialists? as individual contributors? managements? the interests of your professional students might be similar to the above result</p> <p>how about the interests of your usual students?</p> <p>fi</p> <p>9. Which type of corporate is more struggling with a shortage of cybersecurity human resources?</p> <p>3 responses</p>  <p>fi</p> <p>12. Mark target image of human resources in IT vendors. (Select all that apply.)</p>  <p>f</p> <p>13. Mark target image of human resources in IT user companies. (Select all that apply.)</p>  <p>f</p> <p>14. Who pays for industry professionals to study at university?</p> <p>3 responses</p>  <p>f</p> <p>15. Who pays for usual students to study at university?</p> <p>3 responses</p> 
4	<p>Q7 shows your tentative target work role for the curriculum</p> <p>What is your tentative target in this workshop?</p> <p>If you are adding subjects to the existing program, consider work roles covered by the program.</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>(Does this match with the result of Q2 and Q3?)</p> <p>f</p> <p>7. Select work roles that your organization try to develop through cybersecurity education. (Select all that apply)</p> <p>3 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine priority of target work roles in your program</p> <p>)</p>	<p>Q16 shows the layer of workforce that you should target in your curriculum</p> <p>1st priority : xxxx</p> <p>2nd: *Decide all levels</p> <p>3rd: *System administrators includes security operators</p> <p>4th:</p> <p>5th:</p> <p>16. Based on the above answers, which layer of workforce do you think should be trained in prior to others in your country or region? Choose different priority in each row to make the workforce in order.</p>  <p>Q17 shows your target work role for the curriculum</p> <p>see the difference between this and the result of Q7, Q10 and Q11</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>f</p> <p>17. Based on the above answers, which work roles (human resources) do you think should be trained in your country or region? (Select all that apply)</p> <p>3 responses</p> 
5	<p>Make a comprehensive conclusion</p> <p>1.Copy your analysis result here for getting an overview.</p> <ul style="list-style-type: none"> •Target degree and program: •Marketing target(Student profiles): •Who needs the human resource?: •Target image of human resources: •Training priority of workforce layer: <p>2.List up your target work roles for your new program</p> <p>xxxx</p> <p>xxxx</p> <p>xxxx</p>		<p><<<< The figure below could assist you in deciding target work roles</p> 

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

Survey result analysis



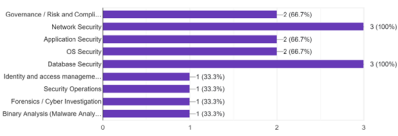
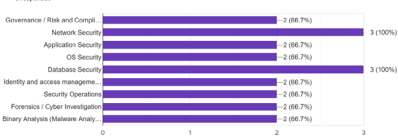
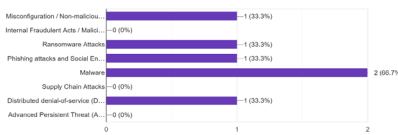


Objective: Analyze the gap between supply and demand, then define your group target.

◆Procedure

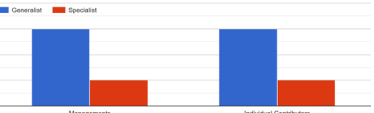

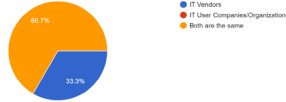
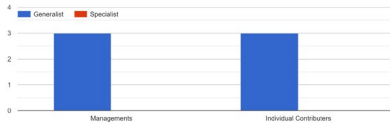
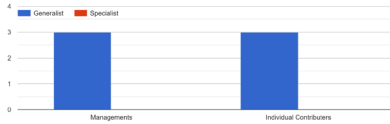



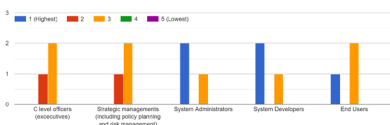
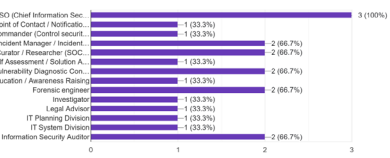
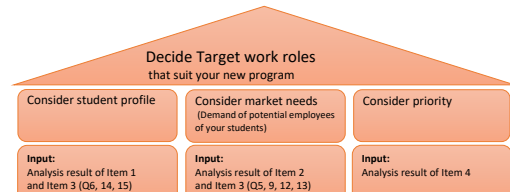
1. Decide your group target program
2. Analyze your answers to questions at Items 2 to 4, both in the column of Supply and the column of Demand
Discuss whether the result of the survey is proper or not. Decide your group target for this workshop.

Start from the questions of Supply.

- Consider the "Demands" as good input to define what you would supply
3. Compare the analysis result of supply and demand on each item
4. Choose the target work roles that suit your group's target education program

Item	Your organization(Supply)	Compare Supply and Demand	Private sector(Demand)
1	<p>Q1 shows your target education program Decide your group target xxx degree adding cs subjects? Developing new cs program?</p> <p>1-1. Select the main target of curriculum that your organization plans to develop. 3 responses</p>  <p>1-2. Select the main target of curriculum that your organization plans to develop. 3 responses</p> 		
2	<p>Q2 and 3 show what you should supply Select the top 3 areas that your students should learn but lack in your program.</p> <p>1 xxx 2 xxx 3 xxx</p> <p>2. Select technical areas of cybersecurity that your students supposed to have. (Select all that apply) 3 responses</p>  <p>3. Select technical areas that you think is lacking in cybersecurity education at your organization. (Select all that apply) 3 responses</p>  <p>Q4 shows existing subjects you should think whether to upgrade the existing subjects or add new subjects</p> <p>no figure</p> <p><i>Cryptography, Computer security Application Security and Network security Network defense</i></p>	<p>Analyze each result of questions Discuss the gap of supply and demand. (Objective: Examine the relevance between supply and demand. Determine which technical areas should be supplied in your program. Determine the treatment of existing subjects.)</p>	<p>Q8 shows what kind of education is lacking or what kind of engineer is needed in your region xxx incident means a lack of security awareness? governance? Network security? OS security? Xxx? To respond xxx attacks, Network engineer?, Incident responder?, SOC analysts? are needed</p> <p>8. What are the top 3 security risks / Incidents in your country or region? 3 responses</p>  <p>Q10 and 11 show the potential demand in the human resource market. In other words, it shows what you should supply. for students willing to work in IT vendors: xxx, OS security?, Application security? for students willing to work in IT user companies: xxx, xxx (Does this match with the result of Q8?) (On Q9, which company is the potential employer for your students?)</p> <p>10. Select technical areas that you think is lacking in cybersecurity workforce in IT vendors. (Select all that apply) 3 responses</p>  <p>11. Select technical areas that you think is lacking in cybersecurity workforce in IT user companies. (Select all that apply) 3 responses</p> 

Appendix 3-1 Survey Responses Used for the Curriculum Development Gap Analysis

3	<p>Q5,6 show your target customer(student)</p> <p>According to the target degree and students profile</p> <ul style="list-style-type: none"> -will your students be individual contributors or managements? -will your students be generalists or specialists? <p>Whose needs should you know, individuals or market needs?</p> <p>5. Mark target image of human resources that your organization is trying to develop through cybersecurity education. (Select all that apply.)</p>  <p>6. Select a customer(student) profile that your organization targets mainly.</p> <p>3 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine the type of human resources that your group should educate.</p> <p>Determine the balance of demands from your marketing target and potential employers of your students</p> <p>)</p>	<p>Q9,12,13,14,15 shows your potential customer profile</p> <p>Who are the potential employers of your students?</p> <ul style="list-style-type: none"> -Consider plus CS human resources(non-security specialist but required security skills) for bachelor students for IT vendors, your students could be generalists? specialists? as individual contributors? managements? for IT user companies, your students could be generalists? specialists? as individual contributors? managements? <p>the interests of your professional students might be similar to the above result</p> <p>how about the interests of your usual students?</p> <p>9. Which type of corporate is more struggling with a shortage of cybersecurity human resources?</p> <p>3 responses</p>  <p>12. Mark target image of human resources in IT vendors. (Select all that apply.)</p>  <p>13. Mark target image of human resources in IT user companies. (Select all that apply.)</p>  <p>14. Who pays for industry professionals to study at university?</p> <p>3 responses</p>  <p>15. Who pays for usual students to study at university?</p> <p>3 responses</p> 
4	<p>Q7 shows your tentative target work role for the curriculum</p> <p>What is your tentative target in this workshop?</p> <p>If you are adding subjects to the existing program, consider work roles covered by the program.</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>(Does this match with the result of Q2 and Q3?)</p> <p>7. Select work roles that your organization try to develop through cybersecurity education. (Select all that apply.)</p> <p>3 responses</p> 	<p>Analyze each result of questions</p> <p>Discuss the gap of supply and demand.</p> <p>(Objective:</p> <p>Determine priority of target work roles in your program</p> <p>)</p>	<p>Q16 shows the layer of workforce that you should target in your curriculum</p> <p>1st priority : xxxx *Decide all levels</p> <p>2nd: *System administrators includes security operators</p> <p>3rd:</p> <p>4th:</p> <p>5th:</p> <p>16. Based on the above answers, which layer of workforce do you think should be trained prior to others in your country or region? Choose different priority in each row to make the workforce in order.</p>  <p>Q17 shows your target work role for the curriculum</p> <p>see the difference between this and the result of Q7, Q10 and Q11</p> <p>1 xxx</p> <p>2 xxx</p> <p>3 xxx</p> <p>figure 17</p> <p>17. Based on the above answers, which work roles (human resources) do you think should be trained in your country or region? (Select all that apply.)</p> <p>3 responses</p> 
5		<p>Make a comprehensive conclusion</p> <p>1.Copy your analysis result here for getting an overview.</p> <ul style="list-style-type: none"> •Target degree and program: •Marketing target(Student profiles): •Who needs the human resource?: •Target image of human resources: •Training priority of workforce layer: <p>2.List up your target work roles for your new program</p> <p>XXXX</p> <p>XXXX</p> <p>XXXX</p>	<p><<<< The figure below could assist you in deciding target work roles</p> 

Appendix 3-2 Mata Elang Community Member July 2022

Mata Elang Community (as of July 2022)

UI-PENS Mata Elang Steering Committee		
Chair	Prof. Dr-ing. Kalamullah Ramli (EE-UI)	
Co-Chair	Dr. Rudi Lumanto (CSIRT.ID)	
Member	Dr. Udin Harun Al Rasyid (PENS)	
	* Dr. Ferry Astika Saputra (PENS)	Project Leader for Stable Version 1.1
	Dr. Muhammad Salman (EE-UI)	
	* Dr. I Gde Dharma Nugraha (EE-UI)	(Next Project Leader for Stable Version)
	* Dr. Bisyrn Wahyudi (CSIRT.ID)	
	(* Person who is assigned both committee)	

Techial Team under Committee	
Core-Engineer	Mr. Elvian Syahrurizal (EE-UI)

Project (Implementation Body) List		
Project Name	Project Leader	
Mata Elang Stable Version 1.1	Dr. Ferry Astika Saputra (PENS)	

Mata Elang Core Project for Research Committee		
Chair	* Dr. Ferry Astika Saputra (PENS)	
Co-Chair	* Dr. I Gde Dharma Nugraha (EE-UI)	
Member	Dr. Ruki Harwahyu (EE-UI)	
	Dr. Yohan Suryanto (EE-UI)	
	Mr. F. Astha Ekadiyanto (EE-UI)	
	Dr. Iwan Syarif (PENS)	
	Mr. Jauhari (PENS)	
	Mr. Isbat Uzzin (PENS)	Project Leader of Mata Elang IoT Malware
	* Dr. Bisyrn Wahyudi (CSIRT.ID)	
	Mr. Taufik (BPPT)	
	Mr. Andi Saputra(BPPT)	
	Mr. Cahyono (BPPT)	
	Mr. Ahmada Yusril (PANDI)	Project Leader of Mata Elang Stevia
	Mr. Alfiyan Syamsuddin (Independent)	Project Leader of Mata Elang Sensor (Snort3 Based)
		Project Leader of Mata Elang Lab for Researchers
		Project Leader of Mata Elang Sensor(Flow Based IDS- Zeek)
	Mr. Fadhil Yori (Independent)	Project Leader of Mata Elang ELK Integration
	Mr. Ikbar Maulana (Independent)	
	Mr. Aditya (IDNSA/independent)	
	Mr. Haidir (IDNSA/independent)	
	(* Person who is assigned both committee)	

Project (Implementation Body) List		
Project Name	Project Leader	
Mata Elang Sensor (Snort3 Based)	Mr. Alfiyan Syamsuddin	
Mata Elang Stevia	Mr. Ahmada Yusril	
Mata Elang Lab for Researchers	Mr. Alfiyan	
Mata Elang IoT Malware	Mr. Isbat Uzzin	
Mata Elang ELK Integration	Mr. Fadhil Yori	
Mata Elang Sensor (Flow Based IDS-Zeek)	Mr. Alfiyan Syamsuddin	
Plan	Mata Elang Sensor (Suricata based)	EE UI Lecturer ??

REQUEST FOR PROPOSALS

Title of Outsourcing Services:
Developing Mata Elang Stable Version

Date: 10 August 2022

TOKYO Co., Ltd.

Section 1. Letter of Invitation

Subject: Request for Proposal

Reference Title: Developing Mata Elang Stable Version

The TOKYO Co., Ltd. (hereinafter referred to as TOKYO) now invites proposals to provide the following outsourcing services: Developing Mata Elang Stable Version for the Project for Human Resources Development for Cyber Security Professionals under the Japan International Cooperation Agency (JICA). More details of the services are provided in the Terms of Reference.

It is not permissible to transfer this invitation to any other firm.

The RFP includes the following documents

- Section 1 - Letter of Invitation (LOI)
- Section 2 - Summary Sheet of the Instruction to Developers
- Section 3 - Instruction to Developers (ITD)
- Section 4 - Technical Proposal Forms
- Section 5 - Financial Proposal Forms
- Section 6 - Terms of Reference (TOR)
- Section 7 - Form of Contract (FOC) (*[Lump-Sum]*)

Sincerely,

Hitohiro Sakurai
Chief Executive Officer
TOKYO Co., Ltd.

1. Name of the assignment	Developing Mata Elang Stable Version
2. Method of selection	QCBS (Quality and Cost Based Selection)
3. Officer in charge	Hitohiro SAKURAI Address: <u>BIZMARKS Nihonbashi-Kayabacho, 8-2,</u> <u>Nihonbashi-Koamicho, Chuo-Ku, Tokyo, 103-0016, JAPAN</u> Telephone: +81-3-6403-3750 E-mail: [REDACTED]
4. Pre-proposal conference	A pre-proposal conference will be held: Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Shall arrange in the week of (n/a)
5. Type of contract	Lump-sum
6. Deadline of request for clarification	5 calendar days before the Proposals' submission deadline
7. Proposal submission deadline	Date: 24th August 2022 Time: 16:00 WIB
8. Proposal submission address	Hitohiro SAKURAI Address: <u>BIZMARKS Nihonbashi-Kayabacho, 8-2,</u> <u>Nihonbashi-Koamicho, Chuo-Ku, Tokyo, 103-0016, JAPAN</u> Telephone: +81-3-6403-3750 E-mail: [REDACTED]
9. Expected date for the negotiations	31st August 2022
10. Expected date for the commencement of the Services	7th September 2022

Section 3. Instructions to Developers

A. General Provisions

1. **Introduction**
 - 1.1 Developers are invited to submit a Technical Proposal together with a Financial Proposal for outsourcing services required for the assignment (hereinafter called the “Proposal”). The Proposal will be the basis for negotiating and ultimately signing the Contract with the selected Developer.
 - 1.2 TOKYO will timely provide, at no cost to the Developers, the inputs, relevant project data, and reports required for the preparation of the Developer’s Proposal as specified below:
 1. Subject materials
 -
 -
 -
 -

B. Preparation of Proposals

2. **General Considerations** In preparing the Proposal, the Developer is expected to examine the Request for Proposal (hereinafter called the “RFP”) in detail. Material deficiencies in providing the information requested in the RFP may result in rejection of the Proposal.
3. **Cost of Preparation of Proposal** The Developer shall bear all costs associated with the preparation and submission of its Proposal, and TOKYO shall not be responsible or liable for those costs, regardless of the conduct or outcome of the selection process. TOKYO is not bound to accept any proposal, and reserves the right to annul the selection process at any time prior to Contract award, without thereby incurring any liability to the Developer.
4. **Language** The Proposal, as well as all correspondence and documents relating to the Proposal exchanged between the Developer and TOKYO, shall be written in **English**.
5. **Documents Comprising the Proposal** The Proposal shall comprise the documents and forms listed below;
 - (1) TECH-1 Technical Proposal Submission Form
 - (2) TECH-2 Developer’s Organization and Experience
 - (3) TECH-3 Description of Approach, Methodology, and Work Plan for Performing the Assignment
 - (4) TECH-4 Work Schedule and Planning for Deliverables
 - (5) ~~TECH-5~~ (Not required)
 - (6) TECH-6 Curriculum Vitae (Any format is acceptable)
 - (7) FIN-1 Financial Proposal Submission Form
 - (8) FIN-2 Breakdown of Remuneration, Expenses and Indirect Local Tax Estimates (Any format is acceptable)
 - (9) FIN-3 Breakdown of Remuneration, Expenses based on

additional proposal by the Developer (Any format is acceptable)

- | | |
|---|--|
| 6. Only One Proposal | N/A |
| 7. Proposal Validity | Proposal must remain valid for 30 calendar days after the Proposal submission deadline. |
| 8. Clarification and Amendment of RFP | <p>The Developer may request a clarification of any part of the RFP no later than 5 calendar days before the Proposals' submission deadline. Any request for clarification must be sent by email, to TOKYO's address indicated in Section 2. Summary Sheet of the Instruction to Developers. TOKYO will respond in writing, or by standard electronic means (including an explanation of the query but without identifying its source) to all shortlisted Developers. Should TOKYO deem it necessary to amend the RFP as a result of a clarification, it shall do so following the procedure described below;</p> <p>(1) At any time before the proposal submission deadline, TOKYO may amend the RFP by issuing an amendment in writing or by standard electronic means. The amendment shall be sent to all shortlisted Developers and will be binding on them. The shortlisted Developers shall acknowledge receipt of all amendments in writing.</p> <p>(2) If the amendment is substantial, TOKYO may extend the proposal submission deadline to give the shortlisted Developers reasonable time to take an amendment into account in their Proposals.</p> |
| 9. Technical Proposal Format and Content | <p>9.1 The Technical Proposal shall not include any financial information. A Technical Proposal containing financial details shall be declared non-responsive.</p> <p>9.2 The Developer is required to submit a Technical Proposal using the standard forms provided in Section 4. Technical Proposal Forms.</p> |
| 10. Financial Proposal | <p>10.1 The Financial Proposal shall be prepared using the provided in Section 5. Financial Proposal Forms. It shall list all costs associated with the assignment, including (a) remuneration, (b) expenses indicated in the Financial Proposal Forms.</p> <p>10.2 The Developer is responsible for meeting all tax liabilities arising out of the Contract.</p> <p>10.3 The Developer shall express the price for its Services in Indonesian Rupiah.</p> |

C. Submission, Opening and Evaluation

11. Submission and Marking of Proposals

- 11.1 The Developer shall submit a complete Proposal comprising the documents and forms in accordance with Clause 5 (Documents Comprising Proposal). The submission can be done by email.
- 11.2 The Proposal must be sent to the email and received by TOKYO no later than the deadline indicated in **Section 2. Summary Sheet of the Instruction to Developers**, or any extension to this deadline. Any Proposal received by TOKYO after the deadline may be declared late and rejected, and promptly returned unopened.

12. Confidentiality

From the time the Proposals are opened to the time the Contract is awarded, the Developer should not contact TOKYO on any matter related to its Technical and/or Financial Proposal. Information relating to the evaluation of Proposals and award recommendations shall not be disclosed to the Developers who submitted the Proposals or to any other party not officially concerned with the process, until the publication of the Contract award information.

13. Proposals Evaluation

- 13.1 The evaluators of the Technical Proposals shall have no access to the Financial Proposals until the technical evaluation is concluded.
- 13.2 The Developer is not permitted to alter or modify its Proposal in any way after the proposal submission deadline. While evaluating the Proposals, TOKYO will conduct the evaluation solely on the basis of the submitted Technical and Financial Proposals.

14. Evaluation of Technical Proposals

- 14.1 TOKYO shall evaluate the Technical Proposals on the basis of their responsiveness to the TOR and the RFP, applying the evaluation criteria, sub-criteria, and point system described below;

Criteria / Sub-criteria	Point	Point*
I. Developer's general experience and competence in the field covered by the TOR	25	25
II. Adequacy of the proposed approach, methodology and work plan in responding to the TOR	25	25
III. Experience and records of the staff members to be assigned to the work	(45)	(45)
a) Position 1 Project Manager	25	30
b) Position 2 Quality Assurance Manager	10	-
c) Position 3 Full-time Chief Engineer	10	15
IV. Additional suggestions	5	5
Total Points for Four Criteria	100	100

* In case the quality assurance manager is concurrent assignment.

- 14.2 Each responsive Proposal will be given a technical score (St). A Proposal shall be rejected at this stage if it does not respond to important aspects of the RFP or if it fails to achieve the minimum technical score required to pass: 70
- 15. Correction of Errors**
- Activities and items described in the Technical Proposal but not priced in the Financial Proposal, shall be assumed to be included in the prices of other activities or items, and no corrections are made to the Financial Proposal.
- a. Time-Based Contracts**
- 15.1 If a Time-based Contract form is included in the RFP, TOKYO will (a) correct any computational or arithmetical errors, and (b) adjust the prices if they fail to reflect all inputs included for the respective activities or items in the Technical Proposal. In case of discrepancy between (i) a partial amount (sub-total) and the total amount, or (ii) between the amount derived by multiplication of unit price with quantity and the total price, or (iii) between words and figures, the former will prevail. In case of discrepancy between the Technical and Financial Proposals in indicating quantities of input, the Technical Proposal prevails and TOKYO shall correct the quantification indicated in the Financial Proposal so as to make it consistent with that indicated in the Technical Proposal, apply the relevant unit price included in the Financial Proposal to the corrected quantity, and correct the total Proposal cost.
- b. Lump-Sum Contracts**
- 15.2 If a Lump-sum Contract form is included in the RFP, the Developer is deemed to have included all prices in the Financial Proposal, so neither arithmetical corrections nor price adjustments shall be made.
- 16. Taxes**
- The TOKYO's evaluation of the Developer's Financial Proposal shall include taxes and duties in Indonesia.
- 17. Combined Quality and Cost Evaluation**
- 17.1 The total score is calculated by weighting the technical and financial scores and adding them as per the formula and instructions stated below.
- [Financial Score]**
- The lowest evaluated Financial Proposal (Fm) is given the maximum financial score (Sf) of 100.
- The formula for determining the financial scores (Sf) of all other Proposals is calculated as following:
- $$Sf = 100 \times Fm / F$$
- in which "Sf" is the financial score, "Fm" is the lowest price, and "F" the price of the proposal under consideration.
- [Combined Score]**
- The weights given to the Technical (T) and Financial (F) Proposals are:
- W1 (T) = 70%, and**
- W2 (F) = 30%**
- Proposals are ranked according to their combined technical (St)
- (In case of Quality- and Cost-Based Selection (QCBS))

and financial (Sf) scores using the weights (W1 = the weight given to the Technical Proposal; W2 = the weight given to the Financial Proposal; $W1 + W2 = 100(\%)$) as following: $S = St \times T\% + Sf \times F\%$

- 17.2 The Developer achieving the highest combined technical and financial score will be invited for negotiations.

D. Negotiations and Award

18. Negotiations

The negotiations will be held shortly after notification to successful/unsuccessful Developer(s) with the successful Developer's representative(s).

[Technical negotiations]

- 18.1 The negotiations include discussions of the Terms of Reference (TOR), the proposed methodology, TOKYO's inputs, the Conditions of the Contract, and finalizing the "Description of Services" part of the Contract. These discussions shall not substantially alter the original scope of services under the TOR or the terms of the contract, in order that the quality of the final product, its price, or the relevance of the initial evaluation may not be affected.

[Financial negotiations]

- 18.2 The financial negotiations will reflect the agreed technical modifications in the cost of the services.
- 18.3 The financial negotiations will, as necessary, include remuneration rate and quantities of items of expenses that may be increased or decreased from the relevant amounts shown in the Financial Proposal but without significant alterations.

19. Conclusion of Negotiations

- 19.1 The negotiations are concluded with a review of the finalized draft Contract, which then shall be initialled by TOKYO and the Developer's authorized representative.
- 19.2 If the negotiations fail, TOKYO shall terminate the negotiations informing the Developer of the reasons for doing so and will invite the next-ranked Developer to negotiate a Contract.

20. Award of Contract

- 20.1 After completing the negotiations TOKYO shall award the Contract to the selected Developer and promptly notify the other shortlisted Developers. Technical Proposals of those Developers who were unsuccessful shall be disposed or returned.
- 20.2 The Developer is expected to commence the assignment on the date specified in **Section 2. Summary Sheet of the Instruction to Developers**.

Section 4. Technical Proposal Forms

{Notes to Developer shown in brackets { } throughout Section 4 provide guidance to the Developer to prepare the Technical Proposal; they should not appear on the Proposals to be submitted.}

Checklist of Required Forms

Form	Description	Page Limit
TECH-1	Technical Proposal Submission Form	2
TECH-2	Developer's Organization and Experience A. Developer's Organization B. Developer's Experience	5
TECH-3	Description of the Approach, Methodology, and Work Plan for Performing the Assignment	5
TECH-4	Work Schedule and Planning for Deliverables	2
TECH-5	Personnel Schedule	N/A
TECH-6	Curriculum Vitae (CV) for the following Key Experts - Project Manager - Quality Assurance Manager - Full-time Chief Engineer	3 persons/ 6 pages per person

Form TECH-1**TECHNICAL PROPOSAL SUBMISSION FORM**

{Location, Date}

To: Chief Executive Officer
TOKYO Co., Ltd.

Dear Sirs:

We, the undersigned, offer to provide the outsourcing services for Developing Mata Elang Stable Version in accordance with your Request for Proposals dated 10th August 2022 and our Proposal. We are hereby submitting our Proposal, which includes this Technical Proposal and a Financial Proposal.

We hereby declare that:

- (a) All the information and statements made in this Proposal are true and we accept that any misinterpretation or misrepresentation contained in this Proposal may lead to our disqualification by TOKYO.
- (b) Our Proposal shall be valid and remain binding upon us for the period of time specified in the Instructions.
- (c) Our Proposal is binding upon us and subject to any modifications resulting from the Contract negotiations.

We undertake, if our Proposal is accepted and the Contract is signed, to initiate the Services related to the assignment no later than the expected date for the commencement of the Services indicated in **Section 2. Summary Sheet of the Instruction to Developers**.

We understand that you are not bound to accept any Proposal that you receive.

We remain,

Yours sincerely,

Authorized Signature {In full and initials}: _____

Name and Title of Signatory: _____

Name of Firm: _____

Address: _____

Contact information (phone and e-mail): _____

Form TECH-2

DEVELOPER'S ORGANIZATION AND EXPERIENCE

{Form TECH-2: a brief description of the Developer's organization and an outline of the recent experience of the Developer that is most relevant to the assignment. In the case of a joint venture, information on similar assignments shall be provided for each partner. For each assignment, the outline should indicate the duration of the assignment, the contract amount (total and, if it was done in a form of a joint venture or a sub-consultancy, the amount paid to the Developer), and the Developer's role/involvement.}

A - Developer's Organization

{Provide here a brief description of the background and organization of your company, and - in case of a joint venture - of each member for this assignment, including organizational chart, a list of Board of Directors, and beneficial ownership.}

B - Developer's Experience

{1. List only previous similar assignments successfully completed in the last 10 years.}

Duration	Assignment name & brief description of main deliverables/outputs	Name of Client & Country of Assignment	Approx. Contract value (in Rupiah) / Amount paid to your firm	Role on the Assignment
{e.g., Jan.2009–Apr.2010}	{e.g., “Improvement quality of.....”: designed master plan for rationalization of; }	{e.g., Ministry of, country}	{e.g., Rp.100 mill/Rp.50 mill}	{e.g., Lead partner in a JV A&B&C}
{e.g., Jan-May 2008}	{e.g., “Support to sub-national government.....”: drafted secondary level regulations on.....}	{e.g., municipality of....., country}	{e.g., Rp.20 mil/Rp.20 mil}	{e.g., sole Developer}

Form TECH-3

DESCRIPTION OF APPROACH, METHODOLOGY, AND WORK PLAN FOR PERFORMING THE ASSIGNMENT

{Form TECH-3: a description of the approach, methodology, and work plan for performing the assignment}

{Suggested structure of your Technical Proposal}

a) **Technical Approach, Methodology, and Organization of the Developer's team.**

{Please explain your understanding of the objectives of the assignment as outlined in the Terms of Reference (TOR), the technical approach, and the methodology you would adopt for implementing the tasks to deliver the expected output(s); the degree of detail of such output; and describe the structure and composition of your team. Please do not repeat/copy the TOR in here.}

b) **Work Plan and Staffing.**

{Please outline the plan for the implementation of the main activities/tasks of the assignment, their content and duration, phasing and interrelations, milestones (including interim approvals by TOKYO), and tentative delivery dates of the reports. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the TOR and ability to translate them into a feasible working plan and work schedule showing the assigned tasks for each expert. A list of the final documents (including reports) to be delivered as final output(s) should be included here. The work plan should be consistent with the FORM Tech-4 (Work Schedule).}

c) **Comments (on the TOR and on counterpart staff and facilities)**

{Your suggestions should be concise and to the point, and incorporated in your Proposal. Please also include comments, if any, on counterpart staff and facilities to be provided by TOKYO. For example, administrative support, office space, local transportation, equipment, data, background reports, etc.}

Form TECH-4: WORK SCHEDULE AND PLANNING FOR DELIVERABLES

N°	Activity	Months										
		1	2	3	4	5	6	7	8	9	n

1. List the deliverables with the breakdown for activities required to produce them and other benchmarks such as TOKYO's approvals. For phased assignments, indicate the activities, delivery of reports, and benchmarks separately for each phase.
2. Duration of activities shall be indicated in a form of a bar chart.
3. Include a legend, if necessary, to help read the chart.



FORM TECH-6**CURRICULUM VITAE (CV) FOR EXPERTS**

Position Title	{e.g., TEAM LEADER}
Name of Expert:	{Insert full name}
Date of Birth:	{day/month/year}
Country of Citizenship / Residence	

Education: {List college/university or other specialized education, giving names of educational institutions, dates attended, degree(s)/diploma(s) obtained}

Employment record relevant to the assignment:

{Starting with present position, list in reverse order. Please provide dates, name of employing organization, titles of positions held, types of activities performed and location of the assignment, and contact information of previous clients and employing organization(s) who can be contacted for references. Past employment that is not relevant to the assignment does not need to be included.}

Period	Employing organization and your title/position. Contact info for references	Country	Summary of activities performed relevant to the Assignment
[e.g., May 2005-present]	[e.g., Ministry of, advisor/Developer to... For references: Tel...../e-mail.....; Mr. Hbbbb, deputy minister]		

Membership in Professional Associations and Publications:

Language Skills (indicate only languages in which you can work):

Expert's contact information: (e-mail, phone)

Certification:

I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes myself, my qualifications, and my experience, and I am available to undertake the assignment in case of an award. I understand that any misstatement or misrepresentation described herein may lead to my disqualification or dismissal by TOKYO.

Name of Expert	Signature	Date {day/month/year}
----------------	-----------	-----------------------

Name of authorized Representative of the Developer (The same who signs the Proposal)	Signature	Date {day/month/year}
--	-----------	-----------------------

Section 5. Financial Proposal Forms

{*Notes to Developer* shown in brackets { } provide guidance to the Developer to prepare the Financial Proposals; they should not appear on the Financial Proposals to be submitted.}

Financial Proposal Forms shall be used for the preparation of the Financial Proposal according to the instructions provided in Section 2 and 3.

FIN-1 Financial Proposal Submission Form

FIN-2 Breakdown of Remuneration, Expenses and Indirect Local Tax Estimates

- 1) Server procurement cost with delivery fee to the University of Indonesia
- 2) Development cost for offline installation
- 3) Development cost for Mata Elang Enhancement
- 4) Other costs necessary for project implementation

FIN-3 Breakdown of Remuneration, Expenses based on additional proposal by the Developer

- 1) Development cost for other requirements proposed by the Developer.

The estimates of FIN-3 are exempt from cost evaluation.

FORM FIN-1

FINANCIAL PROPOSAL SUBMISSION FORM

{Location, Date}

To: Chief Executive Officer
TOKYO Co., Ltd.

Dear Sirs:

We, the undersigned, offer to provide the outsourcing services for Developing Mata Elang Stable Version in accordance with your Request for Proposal dated 10th August 2022 and our Technical Proposal.

Our attached Financial Proposal is for the amount of {indicate the corresponding to the amount(s) currency} {Insert amount(s) in words and figures}, including of all indirect local taxes.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.

We understand that you are not bound to accept any Proposal that you receive.

We remain,

Yours sincerely,

Authorized Signature {In full and initials}: _____

Name and Title of Signatory: _____

Name of Firm: _____

Address: _____

Contact information (phone and e-mail): _____

FORM FIN-2**BREAKDOWN OF REMUNERATION, EXPENSES AND INDIRECT LOCAL TAX ESTIMATES****TOTAL COSTS OF (1), (2), (3), (4) AND (5) : *{insert: total estimate cost}***

Server Procurement Cost with Delivery Fee to UI					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total of (1)					

Development Cost for Offline Installation					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total of (2)					

Development Cost for Mata Elang Enhancement					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total of (3)					

Other Costs Necessary for Project Implementation					
	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total of (4)					

Total Costs of (1)+(2)+(3)+(4)	
---------------------------------------	--

Indirect Local Tax Estimates		
1	{insert type of tax. e.g., VAT or sales tax}	
2	{e.g., income tax on non-resident experts}	
3		
4		
Total Estimate for Indirect Local Tax (5)		

FORM FIN-3**BREAKDOWN OF REMUNERATION, EXPENSES
BASED ON ADDITIONAL PROPOSAL BY THE DEVELOPER**

(The estimates are exempt from cost evaluation)

Development Cost for {other requirements proposed by the Developer}					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total					

Development Cost for {other requirements proposed by the Developer}					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total					

Development Cost for {other requirements proposed by the Developer}					
<i>No.</i>	<i>Description</i>	<i>Unit</i>	<i>Unit Cost</i>	<i>Quantity</i>	<i>Cost</i>
1					
2					
3					
4					
5					
6					
Total					

Section 6. TERMS OF REFERENCE

Project for Human Resources Development for Cyber Security Professionals

Title of Service : Developing Mata Elang Stable Version
Client : TOKYO Co., Ltd.
Duration : From August 2022 to February 2023

Objective :

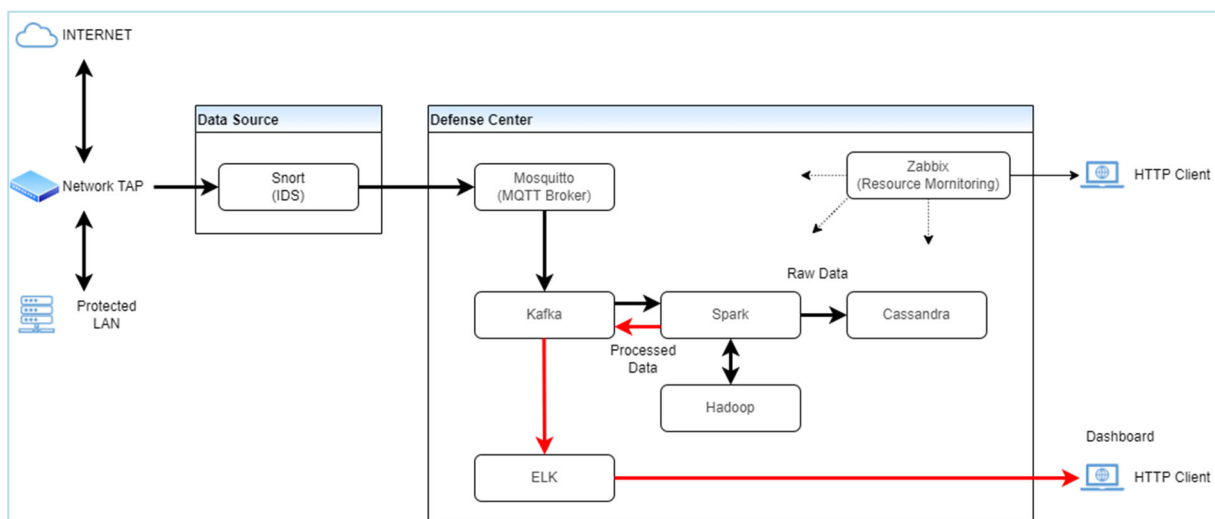
Mata Elang is an Open-Source Security Tool to monitor network intrusions. The Client (Japanese consultants) plans to enhance Mata Elang Stable version for actual use in target organizations. This development is the 2nd development following the 1st development in 2021.

For more information regarding 1st development, please see the attached references.

Mata Elang Overview:

Mata Elang codes and documentations are published via GitHub¹ and Docker Hub. The Mata Elang Stable version project is managed and controlled by the steering committee (the Committee). Its development strategy, plan and product specifications are decided by the Committee as well.

Mata Elang stable version consists of two sections: Data Source and Defense Center. **Data Source** section has IDS (Intrusion Detection System) sensors which use Snort version 2 as the core IDS engine. The output of the sensors sent to the Defense Center. **Defense Center** (included Database and Dashboard) section has seven components: Mosquitto, Kafka, Spark, Hadoop, Cassandra, ELK and Zabbix.



¹ <https://github.com/Mata-Elang-Stable>

Section	Components	Explanation
Data Source	Snort	In this version of Mata Elang, the sensor uses Snort™ as the core IDS engine.
Defense Center	Mosquitto	In the process of Kafka, the data will be received and processed by the MQTT server. In MQTT the data will be processed by coding and simplification using Kafka Avro. Then it will be connected to the confluent so that the data is ready to proceed to spark via Apache Kafka.
	Kafka	The data collection process is a continuation stage after the sensor receives data attacks that occur on a network. In conducting data collection, the system uses Apache Kafka. Kafka here is a bridge between the sensor and spark as the primary data processors.
	Spark	Data processing in the Mata Elang system uses Apache Spark. The Apache Spark feature used in data processing is a streaming feature that can record and process data in live time. In streaming processing, a Spark will stream brokers to Kafka.
	Hadoop	Hadoop Distributed File System is used in Mata Elang. A large amount of data received from Spark that does not fit in the storage of one server is divided into several servers and managed.
Database / Dashboard	Cassandra	Cassandra is a database. The batch job process saves analytical data in Cassandra.
	ELK	A system for displaying the data stored in Cassandra as a time-series graph.
	Zabbix	A system for monitoring system resource and sending alerts to administrators.

For more details, please refer the followings:

- ✓ Installation Guide - <https://github.com/Mata-Elang-Stable/MataElang-Platform/wiki>
- ✓ Developer's Guide - <https://github.com/Mata-Elang-Stable/DevelopersGuide>

Scope of services :

The Consultant shall enhance and test functions and deploy new version of Mata Elang Stable to a certain environment under the Project for Human Resources Development for Cyber Security Professionals at Depok Campus, University of Indonesia.

The requirements are described below with request level and priority. The Consultant can select and propose feasible requirements among optional requirements by considering the various constraints.

No	Requirement	Activity	Level, Priority
1	Offline Installation	Develop offline installer Create easy installation manual	Mandatory
2	Performance Improvement	Update Snort to version 3 Add Ipv6 compatibility	Mandatory
3	Update of Dashboard	Making the dashboard compatible with ipv6	Mandatory
4	Elimination of Unnecessary Processes	Put parameters into external files and avoid unnecessary build	Mandatory
5	Testing	Unit test, System test, Stability test, Simulator Attack test	Mandatory
6	Documentation	Update installation manual, developer's guide and other technical documents	Mandatory
7	Log Rotation	Snort Log	Mandatory
8	Packet Logger	Output packet dump in PCAP format	Mandatory
9	Signature	[Non-functional operational requirement] - Describe how to update Snort signature file on Wiki	Mandatory
10	Backup Log	[Non-functional operational requirement] - Describe how to back up on Wiki - Backup file is in JSON format for further analysis	Mandatory
11	Update of OSS Components	Update OSS components of Mata Elang	Optional Priority High
12	Fixing the Version	Specifying versions at installation	Optional, Priority High
13	System Monitoring	Services Monitoring	Optional, Priority Mid
14	Docker Containerization	Making of Docker images of Spark	Optional, Priority Mid
15	User Account Management	Making of a procedure to change account settings	Optional, Priority Mid
16	Implementation of Resource Update	Making of a procedure to download frequent update files	Optional, Priority Mid
17	Explanation for Security Issues	Adding explanation to avoid the known security issues	Optional, Priority Low
18	ARM CPU Support	Support for ARM CPU	Optional, Priority Low
19	Threat Classification	Adding severity information	Optional, Priority Low
20	Asset Management	Adding asset management to identify the impact on asset (i.e: criticality, risk level, target attack)	Optional, Priority Low

No	Requirement	Activity	Level, Priority
21	Sensor Registration	Adding sensor registration scheme (provided by the users, i.e: subnet, asset classification, criticality level, etc)	Optional, Priority Low
22	Threat Intelligence Feed	Adding threat intelligence feed (from any free data feed intelligence such as Talos)	Optional, Priority Low
23	Ticketing System	Adding ticketing system for incident management	Optional, Priority Low

a) Development of the Offline Installer (relevant to Requirement No 1)

To deploy Mata Elang in countries with weak Internet bandwidth, an offline installer must be prepared.

Requirements:

- ✓ The installation media shall be a USB memory stick or DVD, and all components of Mata Elang can be installed from the installation media.
- ✓ Mata Elang and all of the necessary modules can be installed without the Internet access.

Target components for offline Installation:

- ✓ Ubuntu Server 20.04 LTS
- ✓ OpenSSH
- ✓ Docker Engine
- ✓ Snort v3
- ✓ Mosquitto or alternatives
- ✓ Kafka
- ✓ Spark
- ✓ Hadoop
- ✓ Cassandra
- ✓ ELK
- ✓ Zabbix
- ✓ And all necessary libraries and software to meet with a new installation manual on GitHub. (Reference: <https://github.com/Mata-Elang-Stable/MataElang-Platform/wiki>).

The versions of the above components shall be in accordance with "Mata Elang Component Version List".

Expected Deliverables:

No	Deliverable	Format
1	Installation media	USB memory stick or DVD
2		ISO file
3	Offline installation manual	Microsoft Word format
4	How to create installation media	Microsoft Word format
5	Offline installation Script (*1)	GitHub Repository

*1 Offline installation Script is not mandatory, but is desirable.

b) Mata Elang Enhancement (relevant to Requirement No 2 - 4, 6 - 10)

We plan to update Snort from version 2 to 3 to improve the performance of IDS (Snort) and to introduce new features in Snort v3. We also plan to solve the issue that the current Mata Elang does not support IP v6.

Requirements:

- ✓ Update Snort to version 3
- ✓ Support of IP v6
 - Mata Elang Stable v1.1 should analyze IPv6 packets and display the analysis results on the dashboard.
- ✓ Update the Installation manual and Developer's Guide if necessary.
- ✓ Describe how to update Snort signature file on Wiki.
- ✓ Describe how to back up on Wiki, Backup file is in JSON format for further analysis

Target components for Mata Elang Enhancement:

Component	Enhancement Point	Execution Type
Snort	Update Snort from version 2 to 3. JSON output is preferred.	Docker container
Mosquitto or alternatives	Connect between Snort and Kafka. Filebeat and Logstash can be alternatives to Mosquitto. If using the alternative components, the performance test "Sensor detects simultaneous attacks from two sources and displays them on the dashboard within one minute" must be passed.	Native or Docker container
Kafka	Kafka is a bridge between the sensor and spark as the primary data processors. IP v6 support is required.	Docker container
Spark	Put environmental parameters into external files or environmental variables so as to avoid unnecessary build process. IP v6 support is required.	Native or Docker container
Hadoop	IP v6 support is required.	Native
Cassandra	IP v6 support is required.	Native
ELK	IP v6 support is required.	Docker container
Zabbix	None	Native

Expected Deliverables:

No	Deliverable	Format
1	Source Code	GitHub Repository
2	Docker Images	Docker Hub Repository
3	Installation Manual (Updated)	GitHub Repository
4	Developer's Guide (Updated)	GitHub Repository
5	Complete Set of Mata Elang	On the Purchased Servers (mentioned below)

c) Update of Mata Elang Components (relevant to Requirement No 9 - 10)

This requirement is optional.

Several of Mata Elang's OSS components have already reached or will soon reach EOS (End of Support). Therefore, the components must be updated.

Version List of Mata Elang Components:

Product	ME1.0		ME1.1 planned		Reason of Update
	Version	Release EOS/EOL	Version	Release EOS/EOL	
Ubuntu	18.04.6 LTS	2021/09 2023/04	20.04.4 LTS	2020/04 2025/04	EOS coming soon
Docker Engine	2.10.11 or later	2021/11 n/a	20.10.12	2022/06 n/a	Apply new ubuntu packages
Docker Compose	1.17.1	2017/11 n/a	1.25.0	2020/04 n/a	Apply new ubuntu packages
	1.29.2	2021/05 n/a			
Java / OpenJDK	1.8.0_312 LTS	2021/10 2026/05	1.8.0_312 LTS	2021/10 2026/05	No change
Snort	2.9.19	2021/12 n/a	3.1.36 (or later)	2021/01 n/a	Enhance IDS
pulledpork	0.7.3	2017/12 2020/09	0.7.4	2020/09 n/a	EOS
Mosquitto	1.4.15	2018/05 n/a	n/a		Replace to Beats & Logstash
Confluent / Kafka	6.2.2 / 2.8.x	2021/07 2023/07	7.2.0 / 3.2.0	2022/07 2024/07	EOS coming soon
Spark	2.4.8	2021/05 2021/05	3.2.2	2022/07 n/a	EOS
Scala	2.11.12	2017/11 n/a	2.12.16	2022/06 n/a	No change
Hadoop	3.2.2	2021/01 n/a	3.3.3	2022/05 n/a	ARM Support
Cassandra	3.11.11 or later	2021/06 2023/07	4.0.5	2022/02 2024/07	EOS coming soon
ELK - Elasticsearch	8.0.0	2020/02 2023/08	8.3.2	2022/07 2023/12	EOL coming soon

Product	ME1.0		ME1.1 planned		Reason of Update
	Version	Release EOS/EOL	Version	Release EOS/EOL	
- Logstash - Kibana - Beats					
Zabbix	6.0.1 LTS	2022/03 2027/02	6.0.1 LTS	2022/03 2027/02	No change
MariaDB	10.6.7 LTS	2022/02 2026/07	10.6.8 LTS	2022/05 2026/07	Security update
Apache HTTP Server	2.4.29	2017/10 n/a	2.4.54	2022/06 n/a	Security update

d) Procurement of Servers

Purchase and delivery of two (2) Mata Elang development servers. The developer may use the purchased servers for its development. The servers must be delivered with Mata Elang installed at the time of acceptance testing scheduled for February 2023.

Minimum Requirements of Servers:

No	Product	Specification	Qty
1	Defense Center	CPU: Intel Xeon / Core i7 - 8 Cores Memory: 32GB Storage: 500GB <u>SSD</u> SATA LAN: 1GbE x 1 OS: Ubuntu Server 20.04 LTS	1
2	Database / Dashboard	CPU: Intel Xeon / Core i7 - 8 Cores Memory: 32GB Storage: 500GB HDD SATA LAN: 1GbE x 1 OS: Ubuntu Server 20.04 LTS	1

Notes:

- ✓ The developer can develop Mata Elang using AWS for up to 3 months before purchasing a server; AWS is provided by a Japanese consultant.
- ✓ Up to 2 network taps and 2 laptops as data sources (sensors) can be borrowed upon developer's request.

e) Software Testing (relevant to Requirement No 5)

The developer shall keep records of both unit and system testing as evidence of software testing and submit software test report.

Expected Deliverables:

No	Deliverable	Format
1	Software Test Report	PDF or Microsoft Office format
2	List of Found Bugs	PDF or Microsoft Office format
3	Software Test Evidence	Any. Only if the client requests to submit.

f) Support of User Acceptance Testing

The developer shall provide two-week on-site support for user acceptance testing at the University of Indonesia scheduled for February 2023. Refreshments and lunches (for 5 people for 2 weeks at maximum) during the user acceptance testing shall be included in the quotation.

g) Team Composition

The Developer shall compose a team which can work on Documentation, Network, Application, and Docker. The team shall also include the following position.

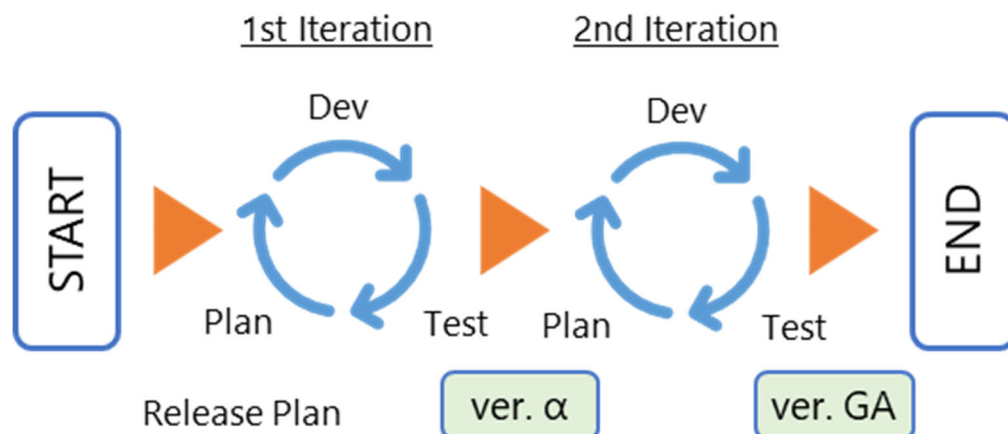
Position	Explanation
Project Manager	Required.
Quality Assurance Manager	Required. Concurrent assignment is available.
Full-time Chief Engineer	Required.
Technical Advisor of Mata Elang	Assignments from the Mata Elang team at PENS are recommended to ensure that the development is completed on time.

h) Progress Meeting

The developer shall hold the bi-weekly progress meeting.

Conditions:

- ✓ Intermediate delivery must be done by November 2022.
- ✓ The target for the interim delivery is expected to be the deliverables of 'b) Mata Elang Enhancement', but the target is negotiable.
- ✓ Mata Elang in November 2022 after the first iteration development will be released as an alpha version.
- ✓ Mata Elang in February 2023 after the second iteration development shall be released as a GA (general available) version.
- ✓ The developed Mata Elang shall be installed on the purchased servers and bringing it to the University of Indonesia.
- ✓ Acceptance test will be done by Mata Elang Committee at the University of Indonesia.

**Acceptance test:**

Acceptance test shall be conducted by a team assigned by the Committee. Expected duration of the acceptance test is two weeks. Below are the possible testing types and cases.

No	Testing Types	Description
1	Document check	Check if documentation is appropriate and correct.
2	Smoke Testing	Preliminary testing to reveal simple failures before further testing.
3	Installation Testing	Check if the specified installation procedures succeed.
4	Functional Testing	Check the system meets the functional requirement.
5	Performance Testing	Assess the system performance in terms of responsiveness and stability under a particular workload.
6	Usability Testing	Assess if the user interface is easy to use and understand.
7	Stability Testing	Assess the efficiency and ability of the system to run continuously over a long period of time.
8	Concurrent Testing	Assess the behavior and performance of the system during concurrency.
9	Simulator Attack Testing	Check the system behavior using simulator attack tools.

[Financial estimation]

Financial estimation shall include 3 sections.

- 1) Server procurement cost with delivery fee to the University of Indonesia
- 2) Development cost for offline installation
- 3) Development cost for Mata Elang Enhancement
- 4) Development cost for other requirements proposed by the Developer.
- 5) Other costs necessary for project implementation

[Milestones]

Aug 2022: Development commencement

Nov 2022: Intermediate delivery of Mata Elang

Feb 2023: Final delivery of Mata Elang with purchased servers and Acceptance testing

Note: There is a possibility that the Japanese consultants will not be able to visit Indonesia due to COVID-19. In such case, the review will be remotely conducted by Japanese consultants, and the local consultants will be expected to communicate frequently.

[Important Notices]

- ✓ The requirements in this RFP contain uncertain and unclear factors, and some changes to the requirements are expected during the development.
- ✓ If these change orders can be acceptable within the scope of the contract in terms of cost, time, and quality assurance, then the Developer should address them in a positive and productive manner. If not, the change order can be withdrawn or the contract may be amended.
- ✓ There is a plan to revise requirements in November 2022. After the revision, the amendment of the contract may be made.

[Attached References]

- ✓ Previous RFP of Development for Mata Elang Stable Version
- ✓ Test cases of previous acceptance testing

Form of Contract

CONTRACT FOR OUTSOURCING SERVICES (Lump-Sum)

Project Name: Developing Mata Elang Stable Version

between

TOKYO Co., Ltd.

and

[insert: name of the Developer PT XXX]

Dated: 7th September 2022

This CONTRACT (hereinafter called the “Contract”) is made the *[insert: number]* day of the month of *[month]*, *[year]*, between, on the one hand, **TOKYO Co., Ltd.** (hereinafter called the “Client”) and, on the other hand, *[PT XXX]* (hereinafter called the “Developer”).

WHEREAS

- (a) the Client has requested the Developer to provide certain outsourcing services as defined in this Contract (hereinafter called the “Services”);
- (b) the Developer, having represented to the Client that it has the required professional skills, expertise and technical resources, has agreed to provide the Services on the terms and conditions set forth in this Contract;

NOW THEREFORE the Parties hereto hereby agree as follows:

1. The following documents attached hereto shall be deemed to form an integral part of this Contract:

- (a) The Conditions of Contract;
- (b) Appendices:
 - Appendix A: Terms of Reference
 - Appendix B: Breakdown of Contract Price
 - Appendix C: List of Key Experts
 - Appendix D: Technical Proposals

For the purpose of interpretation, the priority of the listed documents shall be in accordance with the above listed order.

2. The mutual rights and obligations of the Client and the Developer shall be as set forth in the Contract, in particular:
 - (a) The Developer shall carry out the Services in accordance with the provisions of the Contract; and
 - (b) The Client shall make payments to the Developer in accordance with the provisions of the Contract.

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names as of the day and year first above written.

For and on behalf of TOKYO Co., Ltd.

Hitohiro Sakurai
Chief Executive Officer
TOKYO Co., Ltd.

For and on behalf of *[insert: name of the Developer PT XXX]*

[insert: Authorized Representative of the Developer – name and signature]

PT XXX

DRAFT

Conditions of Contract

A. General Provisions

1. **Law Governing Contract** The law that applies to the Contract is the law of **Indonesia**.
2. **Language** This Contract has been executed in **English**, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.
3. **Communications** Any communication required or permitted to be given or made pursuant to this Contract shall be in writing in **Clause 2** above. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the address specified as follows;
A Party may change its address for notice hereunder by giving the other Party any communication of such change.

For the Client

Address: BIZMARKS Nihonbashi-Kayabacho.8-2, Nihonbashi-Koamicho,
Chuo-Ku,Tokyo, 103-0016, JAPAN

Attention: Mr. Hitohiro SAKURAI

Telephone: +81-3-6403-3750

Facsimile: _____

E-mail: _____

For the Developer

Address: _____

Attention: _____

Telephone: _____

Facsimile: _____

E-mail: _____

4. **Authorized Representatives** Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the Client or the Developer may be taken or executed by the officials specified as follows;

For the Client: **Hitohiro Sakurai, Chief Executive Officer**

For the Developer: *[insert: name, title]*

B. Modification and Termination of Contract

5. **Entire Agreement** This Contract contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.
6. **Modifications or Variations** Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. However, each Party shall

give due consideration to any proposals for modification or variation made by the other Party.

7. Force Majeure

- 7.1 For the purposes of this Contract, “Force Majeure” means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable, and makes a Party’s performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible under the circumstances, and subject to those requirements, includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other adverse weather conditions, strikes, lockouts or other industrial action, confiscation or any other action by Government agencies.
- 7.2 The failure of a Party to fulfill any of its obligations hereunder shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure.
- 7.3 A Party affected by an event of Force Majeure shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall take all reasonable measures to minimize the consequences of any event of Force Majeure.
- 7.4 A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) calendar days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible.
- 7.5 Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.
- 7.6 During the period of their inability to perform the Services as a result of an event of Force Majeure, the Developer, upon instructions by the Client, shall either:
 - (a) demobilize, in which case the Developer shall be reimbursed for additional costs they reasonably and necessarily incurred, and, if required by the Client, in reactivating the Services; or
 - (b) continue with the Services to the extent reasonably possible, in which case the Developer shall continue to be paid under the terms of this Contract and be reimbursed for additional costs reasonably and necessarily incurred.

8. Suspension

The Client may, by written notice of suspension to the Developer, suspend all payments to the Developer hereunder if the Developer fails to perform any of its obligations under this Contract, including the carrying out of the Services.

9. Termination

This Contract may be terminated by either Party as per provisions set up below:

- 9.1 The Client may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause. In such an occurrence the Client shall give at least thirty (30) calendar days’ written notice of termination to the Developer:
 - (a) If the Developer fails to remedy a failure in the performance of its obligations hereunder;
 - (b) If the Developer becomes insolvent or bankrupt;
 - (c) If, as the result of Force Majeure, the Developer is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;
 - (d) If the Client, in its sole discretion and for any reason whatsoever, decides to terminate this Contract;

- (e) If the Client determines that the Developer has engaged in corrupt, fraudulent, collusive, coercive or obstructive practices, in competing for or in executing the Contract.
- 9.2 The Developer may terminate this Contract, by not less than thirty (30) calendar days' written notice to the Client, in case of the occurrence of any of the events specified in paragraphs (a) through (b) of this Clause.
 - (a) If the Client fails to pay any money due to the Developer pursuant to this Contract within forty-five (45) calendar days after receiving written notice from the Developer that such payment is overdue.
 - (b) If, as the result of Force Majeure, the Developer is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days.
- 9.3 Upon termination of this Contract, the Client shall make the following payments to the Developer:
 - (a) Payment for Services satisfactorily performed prior to the effective date of termination;
 - (b) If the advance payment had already paid to the Developer, the amount of the advance payment shall be reduced from the amount defined in paragraph (a) above.
 - (c) In the case of the paragraph (b) above, if there is still a balance of the advance payment, the Developer shall refund the balance to the Client.

C. Obligations of the Developer

10. General

10.1 The Developer shall perform the Services and carry out the Services with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods.

10.2 The Expert(s) of the Developer means an individual professional whose skills, qualifications, knowledge and experience are critical to the performance of the Services under the Contract.

11. Confidential Information and Obligation of the Developer

The Developer shall maintain in confidence all information disclosed by the Client ("Confidential Information") and shall not disclose or divulge Confidential Information to a third party without the prior written consent of the Client, provided that the Developer may disclose Confidential Information to its officers and employees and attorneys, certified public accountants, licensed tax accountants and other professionals whom the Developer retains in connection with this Contract to that extent necessary for the purposes of this Contract.

12. Reporting Obligations

The Developer shall submit to the Client all of the reports, documents, and data *on or before the* *[insert date]*, *[insert month]*, *[insert year]* in the form, in the numbers specified in **Appendix A (Terms of Reference)**. Such reports, documents, and data shall become and remain the property of the Client or Japan International Cooperation Agency (JICA), including its copyrights and intellectual property rights, upon delivery thereof.

13. Inspection

13.1 The Client shall inspect the Services (or a part of the Services, in such case), based on the said reports, documents, and data within 30 days after receiving them.

- 13.2 If the Client cannot approve any part of the Service, the Developer shall submit such further information and make such change in the said reports, documents, and data as the Client may reasonably require.
- 13.3 Promptly after the approval of the Services (or a part of the Services, in such case) by the Client, the reports, documents, and data said above shall be delivered to the Client.

- 14. Liability of the Developer** The Developer shall be responsible for, and shall indemnify the Client from and against any and all claims, losses and damages incurred by the Developer during or in connection with the Services, caused by intentional or negligent act of the Developer.
- 15. No Replacement of Experts** Except as the Client may otherwise agree in writing, no changes shall be made in the Experts.

D. Payment to the Developer

- 16. Contract Price** 16.1 The total amount of the Contract price is *[insert amount in numbers and in words] [Rupiah]* as fixed and set forth in **Appendix B** (Breakdown of Contract Price).
- 16.2 Any change to the Contract price can be made only if the Parties have agreed to the revised scope of the Services and have amended in writing the Terms of References in **Appendix A**.
- 17. Currency of Payment** Any payment under this Contract shall be made in **Rupiah**.
- 18. Terms and Conditions of Payment** 18.1 The total payments under this Contract shall not exceed the Contract prices set forth in **Appendix B**.
Lump-sum installment Payment(s)
The Lump-sum installment Payment(s) shall be made only after each deliverable specified below and an invoice have been submitted and approved as satisfactory by the Client.
(a) 1st payment of *[insert: amount and currency (cannot exceed 40% of the Contract price)]* shall be made for the deliverables of intermediate delivery.
Final Payment
The final payment of *[insert: amount]* under this Clause shall be made only after the final report, all of deliveries and a final invoice have been submitted by the Developer and approved as satisfactory by the Client.
- 18.2 All payments under this Contract shall be made to the accounts of the Developer specified as follows:
[insert: account].

E. Fairness and Good Faith

- 19. Good Faith** The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

F. Settlement of Disputes

20. Amicable Settlement

The Parties shall seek to resolve any dispute amicably by mutual consultation. If either Party may file a written Notice of Dispute to the other Party providing in detail the basis of the dispute. The Party receiving the Notice of Dispute will consider it and respond in writing within fourteen (14) days after receipt. If that Party fails to respond within fourteen (14) days, or the dispute cannot be amicably settled within fourteen (14) days following the response of that Party, Clause 21 shall apply.

21. Dispute Resolution

Any dispute between the Parties as to matters arising pursuant to this Contract that cannot be settled amicably according to the Clause 20 shall be submitted to settlement proceedings under the laws of the Client's country.

DRAFT

Appendices

Appendix A – Terms of Reference

[This Appendix shall include the final Terms of Reference (TORs) worked out by the Client and the Developer during the negotiations; dates for completion of various tasks; location of performance for different tasks; detailed reporting requirements; Client's input, including counterpart personnel assigned by the Client to work on the Developer's team; specific tasks that require prior approval by the Client.]

[Insert the text based on the Section 6 (Terms of Reference) of the ITC in the RFP and modified based on the Forms TECH-1 through TECH-4 in the Developer's Proposal.]

Appendix B – Breakdown of Contract Price

[Insert a table based on Form FIN-2- of the Developer's Technical Proposal and finalize at the Contract's negotiations.]

Appendix C – List of Experts

[Insert: a table based on Form TECH-3 of the Developer's Technical Proposal and finalized at the Contract's negotiations.]

Appendix D – Technical Proposal

[Attach Technical Proposal submitted by the Developer.]

User Acceptance Test (UAT) of Mata Elang 1.1 (Final Draft)

Date & Time: February 6 (Mon) – 17 (Fri) 10:00 – 17:00

Venue: Cisco room, MRPQ Building 3F, DTE, UI, Depok

Expected Participants:

- Gde san, Elvian san and other members from UI side (*1) with 5 or 6 students and staff
- Fahrizal san from JICA project (*1)
- Members of PTNu and Surabaya development team. Five persons including Ferry san.
- Sakurai from TOKYO Co., Ltd.

(*1) They do not need to attend all of UAT, but please join as much as possible.

Maximum 15 members will attend the UAT.

Objectives:

- Verifying that ME functions as expected and meets the needs of the users.
- Identifying any issues or defects that need to be addressed before ME is deployed.
- Ensuring that ME is user-friendly and easy to navigate.
- Evaluating ME's overall performance.
- Determining that ME is ready for release and deployment.
- Learning how to install and manage Mata Elang.

Program:

Date	Activities (DRAFT)
Feb 6 (Mon)	Preparation of UAT
Feb 7 (Tue)	Preparation of UAT
Feb 8 (Wed)	Installation Testing, Smoke Testing
Feb 9 (Thu)	Installation Testing, Smoke Testing
Feb 10 (Fri)	Offline Installation Testing, Smoke Testing
Feb 11 (Sat)	(Day off)
Feb 12 (Sun)	(Day off)
Feb 13 (Mon)	Performance Testing, Concurrent Testing, Usability Testing
Feb 14 (Tue)	Functional Testing
Feb 15 (Wed)	Simulator Attack Testing, Functional Testing
Feb 16 (Thu)	AM: Demonstration for committee PM: Demonstration for potential uses Handover of servers to UI & Cleanup
Feb 17 (Fri)	(Optional extra day)

Later	Make minor corrections and adjustments for public release. Public Release of Mata Elang 1.1 on March

Equipment and facilities:

- A room with good internet access. Direct internet connection is desirable. (UI)
- Two (and two, for extra) switching hubs and several LAN cables. Ten physical cables or over is desirable. (UI)
- Two development servers (PTNu)
- Two network taps (JICA)
- Two laptop PCs (JICA)
- Portable Wi-Fi router (JICA)
- Projector (UI)
- Four power extension cables (UI)
- Wi-Fi AP (UI)

Demonstration:

- If possible, I would like to do a one-hour demonstration for committee members on Thursday 16th AM.
- PM session of demonstration if for potential users. DSTI, BRIN, BSSN, CBN

Topology of UAT environment:

- See attached diagram.

Test Case:

1) Installation Testing:

UAT001: Successful installation using online installation manual.

2) Offline Installation Testing:

UAT002: Successful installation using offline installation media and offline installation manual.

3) Smoke Testing

UATxxx: Attacks are detected by sensors and displayed on the dashboard.

4) Stability Testing (COMPLETED)

UAT901: The system runs continuously over ten(10) days without any termination.

UAT902: No severe failures and issues for the operation are found during the above stability testing

5) Performance Testing

UAT903: Concurrent attacks from two(2) sources are detected by sensors and displayed them on the dashboard within one(1) minute.

6) Usability Testing

UAT904: The user interface is easy to use and understand.

7) Concurrent Testing

UAT905: Concurrent attacks from two(2) sources are detected by sensors and displayed every attacks on the dashboard without data loss.

8) Simulator Attack Testing

UAT906: Attacks are detected by sensors and displayed it consistently on the dashboard.

9) Functional Testing

IPv6 Compatibility/Dashboard

UAT022: Attacks from/to IPv6 are detected by sensors and correctly displayed on the dashboard.

Remarks:

- Lunch and drinks during UAT will be prepared by PTNu.
- Public Release of Mata Elang 1.1 is scheduled on March.

Acceptance Criteria

C1	Pass user acceptance test and evaluations.
C2	Submitted documents, source code and docker images are approved.
C3	Submitted test result is approved.
C4	Support of UAT is completed and approved.
C5	Completion report is submitted.

Deliverables

D01	Installation Media	ISO file or USB memory stick
D02	Offline Installation Manual	MS Word or others
D02a	Documentation on the difficulties of offline installation of Zabbix.	MS Word or others
D03	Manual for How to Create Installation Media	MS Word or others
D04	Offline Installation Script	GitHub Repository
D05	Source Code	GitHub Repository
D06	Docker Images	Docker Hub Repository
D07	Installation Manual (Online)	GitHub Repository
D08	Developer's Guide	GitHub Repository
D09	Complete Set of Mata Elang	On the Purchased Servers
D10	Two Development Servers	Hardware
D11	Software Test Report	MS Word or others
D12	List of Found Bugs	MS Word or others
D13	Software Test Evidence	Any
D14	Operations Manual	MS Word or others
D15	Completion Report	MS Word or others

Requirements

R01	Offline Installation
R02	Performance Improvement
R03	Update of Dashboard
R04	Elimination of Unnecessary Processes
R05	Testing
R06	Documentation
R07	Log Rotation
R08	Packet Logger
R09	Signature
R10	Backup Log
R11	Update of OSS Components
R12	Fixing the Version
R13	System Monitoring
R14	Docker Containerization
R15	User Account Management
R16	Implementation of Resource Update
R17	Explanation for Security Issues
R18	ARM CPU Support

Format**Test Type**

Installation Testing	Smoke Testing
Installation Testing	
Installation Testing	Smoke Testing
Installation Testing	Smoke Testing
Installation Testing	Smoke Testing
Installation Testing	Smoke Testing
Installation Testing	
	Smoke Testing
HW Inspection	
Document Check	
Document Check	
Document Check	
Document Check	
Document Check	

Test Type

Installation Testing	Smoke Testing
Functional Testing	
Functional Testing	
Functional Testing	Installation Testing
Document Check	
Document Check	Installation Testing
Functional Testing	
Functional Testing	
Functional Testing	
Functional Testing	
	Installation Testing
Code Review	
Functional Testing	
	Installation Testing
Functional Testing	Smoke Testing
Functional Testing	
Document Check	
	Installation Testing
	Smoke Testing

Deliverables		Testing Type	Test Cases					
D01	Installation Media	Installation Testing	UAT002	Successful installation using offline installation media and offline installation manual.				
		Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT002)				
D02	Offline Installation Manual	Document Check	UAT901	Document was reveiewd and approved by the the client.				
		Installation Testing	UAT002	Successful installation using offline installation media and offline installation manual.				
D02a	Documentation on the difficulties of offline installation of Zabbix.	Document Check	UAT901	Document was reveiewd and approved by the the client.				
D03	Manual for How to Create Installation Media	Document Check	UAT901	Document was reveiewd and approved by the the client.				
		Installation Testing	UAT009	Successful installation using selfmade offline installation media.				
		Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT009)				
D04	Offline Installation Script	Code Review	UAT900	Code was reveiewd and approved by the the client. - Offline Installation(me-ansible-playbook) - Snort (sensor-snort) - Snort3 Parser (snort3-parser) - Snort3 Docker Image for Mata Elang (snort3-docker-image) - Mosquitto (mosquitto-asset) - Kafka (kafka-asset)				
			Installation Testing	UAT002	Successful installation using offline installation media and offline installation manual.			
			Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT002)			
			D05	Source Code	Code Review	UAT900	Code was reveiewd and approved by the the client. - Snort (sensor-snort) - Snort3 Parser (snort3-parser) - Snort3 Docker Image for Mata Elang (snort3-docker-image) - Mosquitto (mosquitto-asset) - Kafka (kafka-asset) - Kafka MQTT Source (kafka-mqtt-source) - Spark (spark-asset) - Kaspacore Java (kaspacore-java) - OpenSearch (opensearch-asset) - Zabbix (zabbix-asset)	
						Installation Testing	UAT001	Successful installation using online installation manual.
							UAT003	Successful installation using online installation manual. (ARM)
							UAT005	Successful Build of modules.
		UAT006					Successful installation with build module. (Build by UAT005)	
		UAT007					Successful installation with Docker Container.	
		Smoke Testing				UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT001)	
UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT003)							
UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT006)							
D06	Docker Images	Installation Testing	UAT001	Successful installation using online installation manual.				
			UAT003	Successful installation using online installation manual. (ARM)				
			UAT007	Successful installation with Docker Container.				
			- Snort (mataelang/snort-base)					

			<ul style="list-style-type: none"> - Snort3 Parser (mataelang/snort3-parser) - Spark (mataelang/spark) - Kafka MQTT Source(mataelang/kafka-mqtt-source)
	Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT001)
		UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT003)
D07 Installation Manual (Online)	Document Check	UAT901	Document was reveiewd and approved by the the client.
	Installation Testing	UAT001	Successful installation using online installation manual.
		UAT005	Successful Build of modules.
D08 Developer's Guide	Document Check	UAT901	Document was reveiewd and approved by the the client.
D09 Complete Set of Mata Elang	Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard.
D10 Two Development Servers	HW Inspection	UAT102	Satisfied minimum server requirements.
D11 Software Test Report	Document Check	UAT901	Document was reveiewd and approved by the the client.
D12 List of Found Bugs	Document Check	UAT901	Document was reveiewd and approved by the the client.
D13 Software Test Evidence	Document Check	UAT901	Document was reveiewd and approved by the the client.
D14 Operations Manual	Document Check	UAT901	Document was reveiewd and approved by the the client.
			How to Get PCAP Files
			- How to Update Community Snort Rules
			- How to Update Local Snort Rules
			- Backup Documentation
			- Document for User Account Management
			- Document of How to Update GeoLite2
			- Explanation for Security Issues
D15 Completion Report	Document Check		Submitted.
Requirements / Functional Testing	Testing Type	Test Cases	
R01 Offline Installation	Installation Testing	UAT002	Successful installation using offline installation media and offline installation manual.
		UAT009	Successful installation using selfmade offline installation media.
	Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT002)
		UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT009)
R02 Performance Improvement Update to Snort v3	Functional Testing	UAT300	Snort v3 is installed.
		UAT200	Attacks are detected by sensors and displayed on the dashboard.
IPv6 Compatibility		UAT301	Attacks from/to IPv6 are detected by sensors and correctly displayed on the dashboard.
R03 Update of Dashboard IPv6 Compatibility	Functional Testing		
		UAT301	Attacks from/to IPv6 are detected by sensors and correctly displayed on the dashboard.
R04 Elimination of Unnecessary Processes	Installation Testing	UAT008	Installation is completed without compilation.
	Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT008)
	Functional Testing	UAT302	All mandatory settings can be set in the files.
R05 Testing	Document Check	UAT901	Document was reveiewd and approved by the the client.
			- Software Test Report
			- List of Found Bugs
			- Software Test Evidence
R06 Documentation	Document Check	UAT901	Document was reveiewd and approved by the the client.

			<ul style="list-style-type: none"> - Offline Installation Manual - Documentation on the difficulties of offline installation of Zabbix. - Manual for How to Create Installation Media - Installation Manual (Online) - Developer's Guide - Operations Manual <ul style="list-style-type: none"> - How to Get PCAP Files - How to Update Community Snort Rules - How to Update Local Snort Rules - Backup Documentation - Document for User Account Management - Document of How to Update GeoLite2 - Explanation for Security Issues
		Installation Testing	UAT001 Successful installation using online installation manual. UAT002 Successful installation using offline installation media and offline installation manual.
R07	Log Rotation Snort Mosquitto Kakka Spark & Hadoop OpenSearch Zabbix	Functional Testing	UAT303 alert_json.txt and log.pcap are rotated according to snort.lua UAT304 Disk usage does not increase rapidly and log rotation is properly managed. UAT304 Disk usage does not increase rapidly and log rotation is properly managed. UAT304 Disk usage does not increase rapidly and log rotation is properly managed. UAT304 Disk usage does not increase rapidly and log rotation is properly managed. N/A UAT304 Disk usage does not increase rapidly and log rotation is properly managed.
R08	Packet Logger Logger Data Extraction	Functional Testing	UAT305 All packets are logged to the log.pcap file. UAT306 The log.pcap file can be retrieved according to the operation manual.
R09	Signature Registered Rule Update Local Rule Update	Functional Testing	UAT307 Registered rules successfully updated. UAT308 Local rules successfully updated.
R10	Backup Log Export Import	Functional Testing	UAT309 Export OpenSearch data of a specified date. UAT310 Import OpenSearch data.
R11	Update of OSS Components	Installation Testing	UAT100 OSS components are up-to-date.
R12	Fixing the Version	Code Review	UAT101 The version to be installed is specified.
R13	System Monitoring	Installation Testing Functional Testing	UAT010 Successful installation of Zabbix UAT312 Zabbix can monitor system resources. UAT313 Zabbix can send alerts about system resources.
R14	Docker Containerization	Installation Testing Smoke Testing	UAT007 Successful installation with Docker Container. UAT200 Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT007)
R15	User Account Management	Document Check	UAT901 Document was reviewed and approved by the client.
R16	Implementation of Resource Update Snort Rules GeoLite2	Functional Testing	UAT307 Registered rules successfully updated. UAT311 The GeoLite2 database can be updated.

R17	Explanation for Security Issues	Document Check	UAT901	Document was reviewed and approved by the client.
R18	ARM CPU Support	Installation Testing	UAT003	Successful installation using online installation manual. (ARM)
		Smoke Testing	UAT200	Attacks are detected by sensors and displayed on the dashboard. (Installed by UAT003)
Non-Functional Testing		Testing Type	Test Cases	
		Stability Testing	UAT901	The system runs continuously over ten(10) days without any termination.
		Stability Testing	UAT902	No severe failures and issues for the operation are found during the above stability testing
		Stability Testing	UAT907	The usage of system resource does not monotonically increase and is properly managed.
				CPU
				- Memory
				- Storage
		Performance Testing	UAT903	Concurrent attacks from two(2) sources are detected by sensors and displayed them on the dashboard within one(1) minute .
		Usability Testing	UAT904	The user interface is easy to use and understand.
		Concurrent Testing	UAT905	Concurrent attacks from two(2) sources are detected by sensors and displayed every attacks on the dashboard without data loss .
		Simulator Attack Testing	UAT906	Attacks are detected by sensors and displayed it consistently on the dashboard.
				- DoS Attack / hammer by IPv4
				- DoS Attack / hammer by IPv6
				- Directory Listing nikto
				- SYN Denial of Service hping3
				- Port Scanning nmap
				- SSH Bruteforce hydra
				- Slowloris Slowloris
				- SQL Injection sqlmap
				- RCE Remote Code Execution File Upload

Installation Testing

UAT001	Successful installation using online installation manual.
UAT002	Successful installation using offline installation media and offline installation manual.
UAT003	Successful installation using online installation manual. (ARM)
UAT004	CANCELLED
UAT005	Successful Build of modules.
UAT006	Successful installation with build module.
UAT007	Successful installation with Docker Container.
UAT008	Installation is completed without compilation.
UAT009	Successful installation using selfmade offline installation media.
UAT010	Successful installation of Zabbix

Target	Check Date	Test No	Result
Online Installtion			
Sensor x86	2023/01/19	UAT001	Successful installation using online installation manual.
Sensor arm	2023/01/30	UAT003	Successful installation using online installation manual. (ARM)
Defence Center	2023/01/19	UAT001	Successful installation using online installation manual.
Offline Installtion			
Sensor x86	2023/01/24	UAT002	Successful installation using offline installation media and offline installation manual.
Sensor arm		UAT004	CANCELLED
Defence Center	2023/01/24	UAT002	Successful installation using offline installation media and offline installation manual.
Build			
kaspacore.jar	2023/01/05	UAT005	Successful Build of modules.
mataelang/snort-base:3.1.47.0 / amd	2023/01/29	UAT005	Successful Build of modules.
mataelang/snort-base:3.1.47.0 / arm	2023/01/29	UAT005	Successful Build of modules.
mataelang/snort3-parser:1.1 / amd	2023/01/29	UAT005	Successful Build of modules.
mataelang/snort3-parser:1.1 / arm	2023/01/29	UAT005	Successful Build of modules.
mataelang/kafka-mqtt-source:1.1	2023/01/28	UAT005	Successful Build of modules.
mataelang/spark:3.3.1-scala2.13	2023/01/12	UAT005	Successful Build of modules.
Installation with built module			
kaspacore.jar	2023/01/19	UAT006	Successful installation with build module.
mataelang/snort-base:3.1.47.0 / amd	2023/01/30	UAT006	Successful installation with build module.
mataelang/snort-base:3.1.47.0 / arm	2023/01/30	UAT006	Successful installation with build module.

mataelang/snort3-parser:1.1 / amd	2023/01/30	UAT006	Successful installation with build module.
mataelang/snort3-parser:1.1 / arm	2023/01/30	UAT006	Successful installation with build module.
mataelang/kafka-mqtt-source:1.1	2023/02/01	UAT006	Successful installation with build module.
mataelang/spark:3.3.1-scala2.13	2023/02/01	UAT006	Successful installation with build module.
Docker Containerization			
Sensor	2023/01/19	UAT007	Successful installation with Docker Container.
Mosquitto	2023/01/19	UAT007	Successful installation with Docker Container.
Kafka	2023/01/19	UAT007	Successful installation with Docker Container.
Hadoop	N/A		
Spark	2023/01/19	UAT007	Successful installation with Docker Container.
OpenSearch	2023/01/19	UAT007	Successful installation with Docker Container.
Zabbix Server	2023/01/19	UAT007	Successful installation with Docker Container.
Zabbix Agent	N/A		
Installation Process			
Elimination of Compile Process	2023/01/19	UAT008	Installation is completed without compilation.
Offline Installtion Media			
Offline Installtion Media	2023/02/05	UAT009	Successful installation using selfmade offline installation media.
System Monitoring			
Zabbix Installation	2023/01/19	UAT010	Successful installation of Zabbix

R11 Update of OSS Components

R12 Fixing the Version

Check Date: 2023/02/06

Check Date: 2023/02/06

UAT100

UAT101

OSS components are up-to-date.

The version to be installed is specified.

1) Online installation

Service	Version	Update	Fixed	Source	Check Command
Ubuntu	20.04.5 LTS or later	x	x	Specified in installation instructions	\$ cat /etc/os-release
Docker	20.10.12 or later	x	x	Specified in installation instructions	\$ sudo docker version
Docker Compose	2.13.0	x	x	Specified in installation instructions	\$ docker-compose version
Snort	3.1.47	x	x	FROM mataelang/snort-base:3.1.47.0	\$ sudo docker-compose -f ~/sensor/docker-compose.yaml exec snort snort --version
PulledPork	3.0.0.4 or later	x	x	FROM mataelang/snort-base:3.1.47.0	\$ sudo docker-compose -f ~/sensor/docker-compose.yaml exec snort pulledpork.py --version
snort-parser	Dec 26, 2022	x	x	image: mataelang/snort3-parser:1.1	\$sudo docker history 0ea32dffc084 --human=false
Mosquitto	2.0.15	x	x	image: eclipse-mosquitto:2.0.15	\$ sudo docker-compose -f ~/mosquitto/docker-compose.yaml exec mosquitto mosquitto -h
Kafka	7.3.0	x	x	image: confluentinc/cp-kafka:7.3.0	\$ sudo docker-compose -f ~/kafka/docker-compose.yaml exec kafka /bin/kafka-configs --version
Kafka UI	0.4.0 or later	x	x	image: provectuslabs/kafka-ui	(Displayed on dashboard)
kafka-mqtt-source	Dec 10, 2022	x	x	image: mataelang/kafka-mqtt-source:1.1	\$ sudo docker history 27f0838d2cdf --human=false
Java/openjdk	11.0.17 LTS or later	x	x	Specified in installation instructions	\$ java --version
Hadoop	3.3.3 or later	x	x	Specified in installation instructions	\$ hadoop version
Spark	3.3.1	x	x	image: mataelang/spark:3.3.1-scala2.13	\$ sudo docker-compose -f ~/spark/docker-compose.yaml exec spark-master /opt/spark/bin/spark-shell --version
Kaspacore	Jan 5, 2023	x	x		
GeoLite2	Redistribution Prohibited	-	-		
OpenSearch	2.4.0	x	x	image: opensearchproject/opensearch:2.4.0	\$ curl -ku admin:admin https://localhost:9200/
OpenSearch Dashboard	2.4.0	x	x	image: opensearchproject/opensearch-dashboards:2.4.0	(Displayed on dashboard)
Logstash	8.4.0	x	x	image: opensearchproject/logstash-oss-with-opensearch-output-plugin:8.4.0	\$ sudo docker-compose -f ~/opensearch/docker-compose.yaml exec opensearch-logstash logstash --version
Zabbix Server	6.2.6 or later	x	x	image: zabbix/zabbix-server-mysql:ubuntu-6.2-latest	\$ sudo docker-compose -f ~/zabbix/docker-compose.yaml exec zabbix-server zabbix_server -V
Zabbix / nginx	1.22.1 or later	x	x	image: zabbix/zabbix-web-nginx-mysql:ubuntu-6.2-latest	\$ sudo docker-compose -f ~/zabbix/docker-compose.yaml exec zabbix-web-nginx-mysql nginx -v
Zabbix / MySQL	8.0.31 or later	x	x	image: mysql:8.0-oracle	\$ sudo docker-compose -f ~/zabbix/docker-compose.yaml exec mysql-server mysql --version
Zabbix Agent	6.2.6	x	x	Specified in installation instructions	\$ zabbix_agentd --version

2) Offline installation

Service	Version		Fixed	Source	Check Command
Ubuntu	20.04.5 LTS	x	x	Specified in installation instructions	\$ cat /etc/os-release
Docker	20.10.12	x	x	https://download.docker.com/linux/static/stable/x86_64/docker-20.10.12.tgz	\$ sudo docker version
Docker Compose	1.29.2	x	x	https://files.pythonhosted.org/packages/f3/3e/ca05e486d44e38eb495ca60b8ca521	\$ docker-compose version
	2.14.2	x	x	https://github.com/docker/compose/releases/download/v2.14.2/docker-compose-L	\$ /usr/local/lib/docker/cli-plugins/docker-compose version
Snort	3.1.47	x	x	FROM mataelang/snort-base:3.1.47.0	\$ sudo docker-compose -f ~/sensor/docker-compose.yml exec snort snort --version
PulledPork	3.0.0.4	x	x	FROM mataelang/snort-base:3.1.47.0	\$ sudo docker-compose -f ~/sensor/docker-compose.yml exec snort pulledpork.py --version
snort-parser	Dec 26, 2022	x	x	image: mataelang/snort3-parser:1.1	\$sudo docker history 0ea32dffc084 --human=false
mosquitto	2.0.15	x	x	image: eclipse-mosquitto:2.0.15	\$ sudo docker-compose -f ~/mosquitto/docker-compose.yml exec mosquitto mosquitto -h
kafka	7.3.0	x	x	image: confluentinc/cp-kafka:7.3.0	\$ sudo docker-compose -f ~/kafka/docker-compose.yml exec kafka /bin/kafka-configs --version
Kafka UI	0.5.0	x	x	image: provectuslabs/kafka-ui	(Displayed on dashboard)
kafka-mqtt-source	Dec 10, 2022	x	x	image: mataelang/kafka-mqtt-source:1.1	\$ sudo docker history 27f0838d2cdf --human=false
Java/openjdk	11.0.18 LTS	x	x	https://corretto.aws/downloads/latest/amazon-corretto-11-x64-linux-jdk.tar.gz	\$ jdk/bin/java --version
Hadoop	3.3.4	x	x	https://dlcdn.apache.org/hadoop/common/hadoop-3.3.4/hadoop-3.3.4.tar.gz	\$ hadoop/bin/hadoop version
Spark	3.3.1	x	x	image: mataelang/spark:3.3.1-scala2.13	\$ sudo docker-compose -f ~/spark/docker-compose.yml exec spark-master /opt/spark/bin/spark-shell --version
Kaspacore	Jan 5, 2023	x	x		
GeoLite2	Redistribution Prohibited	-	-		
OpenSearch	2.4.0	x	x	image: opensearchproject/opensearch:2.4.0	\$ curl -ku admin:admin https://localhost:9200/
OpenSearch Dashboard	2.4.0	x	x	image: opensearchproject/opensearch-dashboards:2.4.0	(Displayed on dashboard)
Logstash	8.4.0	x	x	image: opensearchproject/logstash-oss-with-opensearch-output-plugin:8.4.0	\$ sudo docker-compose -f ~/opensearch/docker-compose.yaml exec opensearch-logstash logstash --version
Zabbix Server	N/A	-	-		
Zabbix / nginx	N/A	-	-		
Zabbix / MySQL	N/A	-	-		
Zabbix Agent	N/A	-	-		

Minimum Requirements of Servers**Check Date: 2023/02/06**

UAT102 Satisfied minimum server requirements.

1. Defense Center

Category	Minimum Requirement	Actual Specification	Check Date
CPU:	Intel Xeon / Core i7 - 8 Cores	Intel Core i7-10700 CPU @2.90GHz - 8 Cores	2023/02/06
Memory:	32GB	32GB	2023/02/06
Storage:	500GB SSD SATA	512GB SSD	2023/02/06
LAN:	1GbE x 1	1GbE x 2	2023/02/06
OS:	Ubunutu Server 20.04 LTS	Ubuntu 20.04.4 LTS	2023/02/06

2. Database / Dashboard

Category	Minimum Requirement	Actual Specification	Check Date
CPU:	Intel Xeon / Core i7 - 8 Cores	Intel Core i7-10700 CPU @2.90GHz - 8 Cores	2023/02/06
Memory:	32GB	32GB	2023/02/06
Storage:	500GB HDD SATA	1TB HDD	2023/02/06
LAN:	1GbE x 1	1GbE x 1	2023/02/06
OS:	Ubunutu Server 20.04 LTS	Ubuntu 20.04.4 LTS	2023/02/06

<Check Command>

CPU: \$ lscpu
 Memory: \$ free -m
 Storage: \$ sudo lshw -c disk
 \$ cat /sys/block/nvme0n1/queue/rotational (0:SSD, 1:HDD)
 LAN: \$ sudo lshw -c network
 OS: \$ cat /etc/os-release

User Acceptance Testing of Mata Elang 1.1

Cisco room, MRPQ Building 3F, DTE, UI, 6th – 17th February, 2023

UI-JACA Project for Human Resources Development for Cybersecurity Professionals

List of Attendees

No.	Name
1	Dr. Gde Dharma, Lecturer of Dept. of Electrical Engineering, UI
2	Mr. Elvian Syahrurizal, Lecturer of Dept. of Electrical Engineering, UI
3	Mr. Fahrizal Nugraha JICA Project
4	Dr. Ferry Astika Saputra, ST. M.Sc., Project leader of Mata-Elang committee, PENS
5	Mr. Mohamad Iman Prajitno Project Manager, CV.PTNu
6	Mr. Fadhil Yori Hibatullah Chief Engineer, Mata Elang Project
7	Mr. Muhammad Izzat Engineer, Mata Elang Project
8	Mr. Muhammad Rifki Yuda Pratama Engineer, Mata Elang Project
9	Mr. Yan Maraden
10	Mr. Tedi Setiawan Student of UI
11	Mr. Muhammad Wafiyulloh Student of UI
12	Mr. Faldy Syofra Martinus Student of UI
13	Mr. Seno Aji Wicaksono Student of UI
14	Mr. Yovan Yudhistira Student of UI
15	SAKURAI Hitohiro JICA Consultant

Appendix 5-1 Specifications of Revisions

How to make top managements aware of CS

No	Revision status	Priorities (High-Low)	Type of actions	Materials	Topics / Modules	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of issue	Received by	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Accepted	High	Modify	Mapping Table COM0010a	All modules		Modified time allocation from 2days to 3days.	Too short duration for the subject.	-	Ogura	01-Mar-23			Expand time allocation especially for exercise and discussion.	01-Mar-23	02-Apr-23
2	Accepted	High	Modify	Instructor guide, Student guide	Module2		Practical test could be a proposal of an appropriate response to a certain cyber incident.	Not clear direction for discussion.	-	Ogura	01-Mar-23			Added explanation for discussion on instructor guide p.24.	01-Mar-23	02-Apr-23
3	Accepted	High	Modify	Instructor guide, Student guide	Module2		Statement on slide p.16 are not correct. - "CIO got angry" should be "CEO got angry" - "CIO doesn't calm" should be "CEO doesn't calm"	For consistency between video and slides.	-	Ogura	01-Mar-23			Revised p.16	01-Mar-23	02-Apr-23
4	Accepted	High	Modify	Instructor guide, Student guide	Module3		"Explain by ID-SIRT report" (p.36); Due to ID-SIRT report only in Bahasa, prepared an alternative report in English for Mongolia TTT. "apac-state-of-incident-response-2022.pdf" in https://drive.google.com/drive/folders/1WmnxT4hQoBtYcDQ8QQ3r5MUI3ysY48-s?usp=sharing	For other language than Bahasa	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
5	Accepted	High	Modify	Instructor guide, Student guide	Module3		Change "Group discussion" to "Exercise with Statistic Report" (p.37) and add detail instructions	For help on instruction	-	Ogura	01-Mar-23			Revised p.37	01-Mar-23	02-Apr-23
6	Accepted	High	Modify	Mapping Table COM0010a	Module3		"Exercise with Statistic Report" (instructor guide p.37); On mapping table, no time is allocated for discussion.	For availability of subject	-	Ogura	01-Mar-23			Allocated 65min for this exercise	01-Mar-23	02-Apr-23
7	Accepted	High	Modify	Instructor guide, Student guide	Module3		Hide slide p.38, instead of the exercise on p.37.	The exercise on p.38 is very similar to an exercise at the end of Module 2.	-	Ogura	01-Mar-23			Hidden p.38	01-Mar-23	02-Apr-23
8	Accepted	High	Modify	Module 3 test	Module3		Module3 test Question5: the answer seems not correct, should be "All of the above statements."	For correct answer	-	Ogura	01-Mar-23			Changed the answer	01-Mar-23	02-Apr-23
9	Accepted	High	Modify	Instructor guide, Student guide	Module4		"Exercise and Discussion" (p.32); No direction for discussion was showed.	For help on instruction	-	Ogura	01-Mar-23			Added instructions on note area. - Please identify and discuss the challenges in your organization to implement cybersecurity risk assessment. - Give short analysis what are things to be improved to tackle those challenges.	01-Mar-23	02-Apr-23
10	Accepted	High	Modify	Instructor guide, Student guide	Module4		"Exercise and Discussion" (p.54); Recommended to provide a template file. Sample in Mongolia TTT is "ASSET RISK IDENTIFICATION.docx" in https://drive.google.com/drive/folders/16oUSYkRZh9PpW0t1goBHSY8A22rHSv6z7usp=sharing	For help on understanding	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
11	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Exercise: Quantitative Risk Assessment" (p.21); To clarify the question, revised the slide and note.	For help on understanding	-	Ogura	01-Mar-23			Revised p.21. (Words are added, "weekly" to slide and "700%" to note.)	01-Mar-23	02-Apr-23
12	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Sample Scenario on Profit/Loss" (p.23); There was an incorrect number on the table. The cost -60 of "COGS: labor / manufacturing" on the column "Indirect 5% future loss" is not correct, -75 is correct.	For help on instruction	-	Ogura	01-Mar-23			Changed the number "-60" to "-75"	01-Mar-23	02-Apr-23
13	Accepted	High	Modify	Instructor guide, Student guide	Module5		"Exercise1" (p.40); Recommended to provide a template file. Sample in Mongolia TTT is "Exercise Impact calculation.xlsx" in https://drive.google.com/drive/folders/1WmnxT4hQoBtYcDQ8QQ3r5MUI3ysY48-s?usp=sharing	For help on understanding	-	Ogura	01-Mar-23			The template file has already been located in "Hands on Data"	01-Mar-23	02-Apr-23
14	Accepted	High	Modify	Module 5 test	Module5		Module5 test Question3: the answer seems not correct, should be "Qualitative Risk Assessment"	For correct answer	-	Ogura	01-Mar-23			Changed the answer	01-Mar-23	02-Apr-23
15	Accepted	High	Modify	Instructor guide, Student guide	Module6		Change the title "6.2 Exercise and discussion" to "Appendix: Guideline for Exercises"	The title "6.2 Exercise and discussion" is not appropriate with its contents.	-	Ogura	01-Mar-23			Changed the title	01-Mar-23	02-Apr-23
16	Accepted	High	Modify	Module 6 test	Module6		Module6 test Question3; The allocated score was incorrectly "0", should be "10".	For correct scoring	-	Ogura	01-Mar-23			Changed the score	01-Mar-23	02-Apr-23
17	Accepted	High	Modify	Mapping Table	Module1~7		Time allocation needs to be revised based on actual time used in the TTT in Replace following questions with other questions.	For appropriate time allocation	-	Ogura	01-Mar-23			Changed time allocation	01-Mar-23	02-Apr-23
18	Accepted	Middle	Modify	Post test	Post test		2. Investments in cyber security technologies should be based on: 9. A successful cyber security management program should use which of the following to determine the amount of resources devoted to mitigating exposures? 10. Which of the following will BEST protect an organization from internal security attacks? 14. When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify: 17. A common concern with poorly written web applications is that they can allow an attacker to:	The questions are less relative to the material content, too technical or too similar to other questions.	-	Akiyama	21-Mar-23			Replaced with following questions. Module1 related: 1 What is not the benefit of adopting a risk management approach to cybersecurity? a. Corporate decision making is improved through the high visibility of risk exposure b. Reduced of losses and improved "Value for Money" potential (correct). Employees are not leaving the organizations d. Being assured of adequate contingency plans Module 2 related: 2 Which response activity is NOT appropriate when an incident happens and grows bigger ? a. Identify the attack and understand the severity	21-Mar-23	02-Apr-23
19	Issued	Low	Modify	(Hands on Data) Cyber Security Awareness Movie.mp4	Module2		According to ending credit of video material, COO doesn't appear in the video. The credit on video should be changed.	For consistency between video and slides.	-	Ogura	01-Mar-23					
20	Issued	Low	Modify	(Hands on Data) Cyber Security Awareness Movie.mp4	Module2		Caption on video scene 5 (9:00) is not correct. - "CIO got angry on IT team" should be "CEO got angry on IT team"	For consistency between video and slides.	-	Ogura	01-Mar-23					
21	Issued	Low	Modify	Instructor guide, Student guide	Module3		Needs detail direction or sample of "Show some leaked data" (p.16) and "Dark web" (p.23) for instructors. Example in Mongolia TTT is "sample of 'Show some leaked data' and 'Dark web'.mp4" in https://drive.google.com/drive/folders/1umDqghw9MuQwE4W0McjR2UFGVXQu9Yw?usp=sharing	For help on instruction	-	Ogura	01-Mar-23					
22	Issued	Low	Modify	Instructor guide, Student guide	Module5		"Exercise: How to prioritize actions" (p.25); There's the same slide on p.55. Thus, just provide introduction on p.25, do exercise on p.55.	For correct information	-	Ogura	01-Mar-23					
23	Issued	Low	Modify	Instructor guide, Student guide	Module5		In COM0010a Module5 "THREAT * VULNERABILITY = RISK" should be explicitly explained in earlier stage. At least early in Module4	For help on understanding	-	Ogura	01-Mar-23					

Appendix 5-1 Specifications of Revisions

24	Issued	Low	Modify	Post test	Post test	Modify following questions. 5. Which of the following would be MOST effective in successfully implementing restrictive password policies? 7. The MOST important characteristic of good security policies is that they: 8. A risk management program should reduce risk to: 11. Which of the following risks would BEST be assessed using qualitative risk assessment techniques? 12. Quantitative risk analysis is MOST appropriate when assessment data: 13. A successful risk management program should lead to: 15. Which of the following attacks is BEST mitigated by utilizing strong passwords? 20. Senior management commitment and support for cyber security can BEST be obtained through presentations that:	The questions are copies of CISM online quizlet.		Akiyama	21-Mar-23						
25																
26																
27																
28																
29																
30																

Appendix 5-1 Specifications of Revisions

How to make general employees aware of CS

No	Revision status	Priorities (High-Low)	Type of actions	Materials	Topics / Modules	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of Iss	Received by	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Accepted	High	Modify	(Hands on data) Studi Kasus Ilham Bintang.docx, Studi Kasus Tokopedia.docx	Module4		Input files for discussion were only in Bahasa.	For using in other countries	-	Ogura	01-Mar-23			Added description in English to the end of files.	01-Mar-23	02-Apr-23
2	Accepted	High	Modify	Module test	Module5		Module5 test Question4; invalid question, there were several correct answers.	For correct answer	-	Ogura	01-Mar-23			Changed options of the question.	01-Mar-23	02-Apr-23
3	Accepted	High	Modify	Instructor guide, Student guide, (Hands on data) template for designing and evaluating awareness program.xlsx	Module6		Instructor guide p.43: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	For help on instruction	-	Ogura	01-Mar-23			Instructor guide p.43: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	01-Mar-23	02-Apr-23
4	Accepted	High	Modify	Instructor guide, Student guide	Module7		"Discussion" (Instructor guide p.20); To clarify what to discuss, use the template file same as module6 ("template for designing and evaluating awareness program.xlsx"). Participants update the "Programs" sheet based on module7 lesson.	For help on instruction	-	Ogura	01-Mar-23			"Discussion" (Instructor guide p.20); Changed the instruction sentence.	01-Mar-23	02-Apr-23
5	Accepted	High	Modify	Instructor guide, Student guide	Module8		Instructor guide p.25: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	For help on instruction	-	Ogura	01-Mar-23			Instructor guide p.25: Added a page that instructs to fill in "template for designing and evaluating awareness program.xlsx"	01-Mar-23	02-Apr-23
6	Accepted	High	Modify	Mapping Table COM0020a	Module1-8		Time allocation needs to be revised based on actual time used in the TTT in Mongolia.	For appropriate time allocation	-	Ogura	01-Mar-23			Changed time allocation	01-Mar-23	02-Apr-23
7	Accepted	Middle	Modify	Post test	Post test		<p>Replace following questions with other questions:</p> <p>2. Who has the primary responsibility of determining the classification level for information?</p> <p>3. Which of the following is not addressed by the data retention policy?</p> <p>4. A preferred technique of attackers is to become "normal" privileged users of the systems they compromise as soon as possible. This can normally be accomplished in all the following ways except which one?</p> <p>5. It is important that organizations ensure that their security efforts are effective and measurable. Which of the following is not a common method used to track the effectiveness of security efforts?</p> <p>6. What is the main concern with single sign-on?</p> <p>7. When is it acceptable to not take action on an identified risk?</p> <p>12. What is called an event or activity that has the potential to cause harm to the information systems or networks?</p> <p>13. What is called the probability that a threat to an information system will materialize?</p> <p>18. Which of the following is the most effective, positive method to promote security awareness?</p> <p>19. Security awareness training includes:</p> <p>8. How do you calculate residual risk?</p> <p>17. Which of the following is considered the weakest link in a security system?</p> <p>20. When speaking to an organization's human resources department</p>	<p>The questions are less relative to the material content, too technical or too similar to other questions.</p>		Akiyama	21-Mar-23		<p>Module 1:</p> <p>1. As an information security measure, Information on computers can only be accessed by authorized persons. This is an example of:</p> <p>a.Integrity (correct)b.Confidentiality</p> <p>c.Availability</p> <p>d.Traceability</p> <p>2. Classify confidentiality of company regulations.</p> <p>a.Public (correct)b.Internal</p> <p>d.White</p> <p>Module 2:</p> <p>3. What are the differences between information security and cybersecurity?</p> <p>a.Cybersecurity is a broader term that encompasses all data, both physical and digital. (correct)b. Information security is a broader term that encompasses all data, both physical and digital.</p> <p>c. Common attacks in cybersecurity include illegal access, modification disclosure, alteration, and disruption.</p> <p>d. There are no differences</p> <p>4. Basic principles of cybersecurity consist of the following except:</p> <p>(correct)a. Removing all threats</p> <p>b. Protecting information</p> <p>c. Enabling risk management</p>	21-Mar-23	02-Apr-23	
8	Issued	Low	Modify	Post test	Post test		<p>Modify following questions.</p> <p>1. Information classification is most closely related to which of the following?</p> <p>9. The term used to denote a potential cause of an unwanted incident, which may result in harm to a system or organization is?</p> <p>10. Which of the following term best describes a weakness that could potentially be exploited?</p> <p>11. Which answer best describes a computer software attack that takes advantage of a previously unpublished vulnerability?</p> <p>14. In terms of Risk Analysis and dealing with risk, which of the four common ways listed below seek to eliminate involvement with the risk being evaluated?</p> <p>15. Another example of Computer Incident Response Team (CIRT) activities is:</p>	<p>The questions are copies of CISSP or CISM online quizlet.</p>		Akiyama	21-Mar-23					
9																
10																
11																
12																
13																
14																
15																
16																
17																
18																
19																
20																

Appendix 5-1 Specifications of Revisions

Computer Forensic

No	Revision status	Priorities (High-Low)	Type of actions	Materials	Topics / Modules	Modification ID	Directions of Revision	Reason of the Revision	Applied framework/theories	Issued by	Date of issue	Received by	Date of received	Actions taken	Date of Submission	Date of Acceptance
1	Submitted	High	Modify	Module1 test	Module1		Module1 test Q2, the question and answer don't match. The question should be changed as: From: "The following are Processes of Digital Evidence, Except." To: "Which of the following is types of Digital Evidence?"	To make questions clear	-	Ogura	04-Mar-23			Changed the question sentence	04-Mar-23	
2	Submitted	High	Modify	Hands On Guide	Module1~3		Add a document that describes facilities to be prepared for training.	For proper preparation of exercises	-	Ogura	04-Mar-23			Added a document "Preparation for FOR0040a exercises.docx".	04-Mar-23	
3	Submitted	High	Modify	Hands On Guide	Module1~3		Change using software-tools to the updated version which is compatible with Windows11.	For feasibility of exercises	-	Ogura	04-Mar-23			Updated software-tools	04-Mar-23	
4	Submitted	High	Modify	Hands On Guide	Module1~3		Prepare data which are required for practices.	For feasibility of exercises	-	Ogura	04-Mar-23			Prepared data which are required for practices.	04-Mar-23	
5	Submitted	High	Modify	All of tests	Module1~4		Add an item of "Name" into the test form to identify who responder is.	For proper management of test results	-	Ogura	04-Mar-23			Added an item of "Name" into the test form to identify who responder is.	04-Mar-23	
6	Submitted	High	Modify	All of tests	Module1~4		Change the setting of test form "Send responders a copy of their response" From: "Off" To: "Always" "Missed questions" From: "Off" To: "On" (Exclude of post-test) "Correct answers" From: "Off" To: "On" (Exclude of post-test) "Point values" From: "Off" To: "On"	For responders checking their answers	-	Ogura	04-Mar-23			Changed the setting of test form	04-Mar-23	
7	Submitted	High	Modify	Practical Test Module 1, Practical Test Module 3, WU-practical test.docx, Assessment of practical skill.xlsx	Module1, 3		Add sample image to Module1 Q1 Module3 Q1	To make questions clear	-	Ogura	04-Mar-23			Added sample image to Module1 Q1 Module3 Q1	04-Mar-23	
8	Submitted	High	Modify	Instructor guide, Student guide	Module2		Slide p.35, there's a typo. "Reconstruct fragments of deleted f" should be "Reconstruct fragments of deleted file" Slide p.39, there's a typo. "e tool dependencies" should be "The tool dependencies". Slide p.84. On the slide, there are words in Bahasa, "layanana yang berfungsi untuk menerima e-mail". It should be in English to keep consistency. Slide p.85. Bubbles for the previous updating work are remaining on the slide p.85. The bubbles should be removed.	To correct mistakes	-	Ogura	04-Mar-23			Revised as pointed	04-Mar-23	
9	Submitted	High	Modify	Hands On Module 2.docx	Module2		2.2. Image Mounting For Windows11, FTK imager 4.7 is available, but FTK imager 4.7 shows an error when mounting image. Alternatively, using OSFMount is available.	For feasibility of exercises	-	Ogura	04-Mar-23			Added an option to use OSFMount instead of FTK imager.	04-Mar-23	
10	Submitted	High	Modify	Practical Test Module 2, WU-practical test.docx, Assessment of practical skill.xlsx	Module2		Questions and answers of practical test need to be changed as below. Question1-3 From:./test/photo.jpg To:tes.jpg Answer1 From:Bogor To:Bogor or West Java or Indonesia Question4 Change source: From:tes.html To:File Signature.rar Question5 From:recovery.dd To:ez-recovery	For feasibility of practical test	-	Ogura	04-Mar-23			Changed questions	04-Mar-23	
11	Submitted	High	Modify	Module2 test	Module2		Module2 test Question4 seems invalid. Question: Which of the following is a form of attack via email? Answer: Brute Force password and Social Engineering	To make questions clear	-	Ogura	04-Mar-23			Changed question as "Which of the following is a form of attack on an email?"	04-Mar-23	
12	Submitted	High	Modify	Instructor guide, Student guide, mapping table, Syllabus FOR0040a Computer Forensic V1.2.docx	Module2, 3		On module2 and 3, module tests are placed before practices. Module tests should be at the end of each module.	For proper evaluation	-	Ogura	04-Mar-23			Changed the order of contents so that module tests are placed in the end of each module.	04-Mar-23	
13	Submitted	High	Modify	Hands On Module 3.docx	Module3		For case study 2, there were unclear questions and answers. Especially step6 (finding pdf and office files in a .mp4 file as steganography), a correct procedure is missing.	For feasibility of exercises	-	Ogura	04-Mar-23			Revised sentences to be clear and skipped some steps.	04-Mar-23	

Appendix 5-1 Specifications of Revisions

14	Submitted	High	Modify	WU-practical test.docx, Assessment of practical skill.xlsx	Module3	<p>Practical test module 3 question 4 The answer seems not correct.</p> <p>From: "[66.68.99.53], [198.82.59.65], [65.14.7.224]; Alternative :[213.66.32.81], [65.34.1.56]"</p> <p>To: "[213.66.32.81], [65.34.1.56]"</p> <p>On FOR0040a WU-practical test.docx, added a procedure to get the answer.</p>	For feasibility of exercises	-	Ogura	04-Mar-23			Revised answers to be correct.	04-Mar-23	
15	Submitted	High	Modify	Hands On Module 3.docx	Module3	<p>Module3 Case study2, there's a question that participants submit a report of case study2, but no format for the report.</p>	For feasibility of exercises	-	Ogura	04-Mar-23			Provided a format of report, that is "blank-chain-of-custody-form.pdf", in Hands on Data > USB-FOR0040 > Data for Case Study > module3 > case study	04-Mar-23	
16	Submitted	High	Modify	Instructor guide, Student guide	Module3	<p>Slide p.47, there's a typo. "TCP/OP Model" should be "TCP/IP Model"</p>	To correct mistakes	-	Ogura	04-Mar-23			Revised as pointed	04-Mar-23	
17	Submitted	High	Modify	Module4 test	Module4	<p>For questions which need multiple choices (Q3, Q9), put a note of "select all of correct options" explicitly.</p>	To make questions clear	-	Ogura	04-Mar-23			Put a note of "Select all of correct options." to each question.	04-Mar-23	
18	Submitted	High	Modify	Post test	Module4	<p>Change the title on the top of Post test form. From: POST TEST digital forensic - JICA To: FOR0040a POST TEST</p>	For consistency	-	Ogura	04-Mar-23			Changed the title on the top of Post test form.	04-Mar-23	
19	Submitted	High	Modify	Post test	Module4	<p>Post test Q18, the answer is not correct. It should be changed as From: Physical To: Data Link</p>	To correct mistakes	-	Ogura	04-Mar-23			Changed the answer.	04-Mar-23	
20	Submitted	High	Modify	Hands on Guide	Module4	<p>P.4 Mbox viewer to EML viewer</p>	For the feasibility of exercises. MBox viewer is old version of viewer and it doesn't work with Catalina	-	Akiyama	21-Mar-23			Changed the text and link for MBox viewer to EML viewer.	21-Mar-23	
21	Issued	Low	Modify	Instructor guide, Student guide	Module1	<p>Slides p.74-81, 85. These slides are discussing cyber law in Indonesia. When the material is used in other countries, it's recommended to adjust contents with the country.</p>	For open courseware	-	Ogura	04-Mar-23					
22	Issued	Low	Modify	Module1 test	Module1	<p>Module1 test Q4, the question is about Indonesian local law. When using materials in other countries, it should be changed.</p>	For open courseware	-	Ogura	04-Mar-23					
23	Issued	Low	Modify	Practical Test Module 2, Hands On Module 3	Module2, 3	<p>Module2 practical test Q3 is the exactly same activity with Case study on Module3. Used file is same jpg file. At least, the jpg file should be changed on Module2 practical test.</p>	For effectiveness of practice	-	Ogura	04-Mar-23					