Cyber Security Research Group

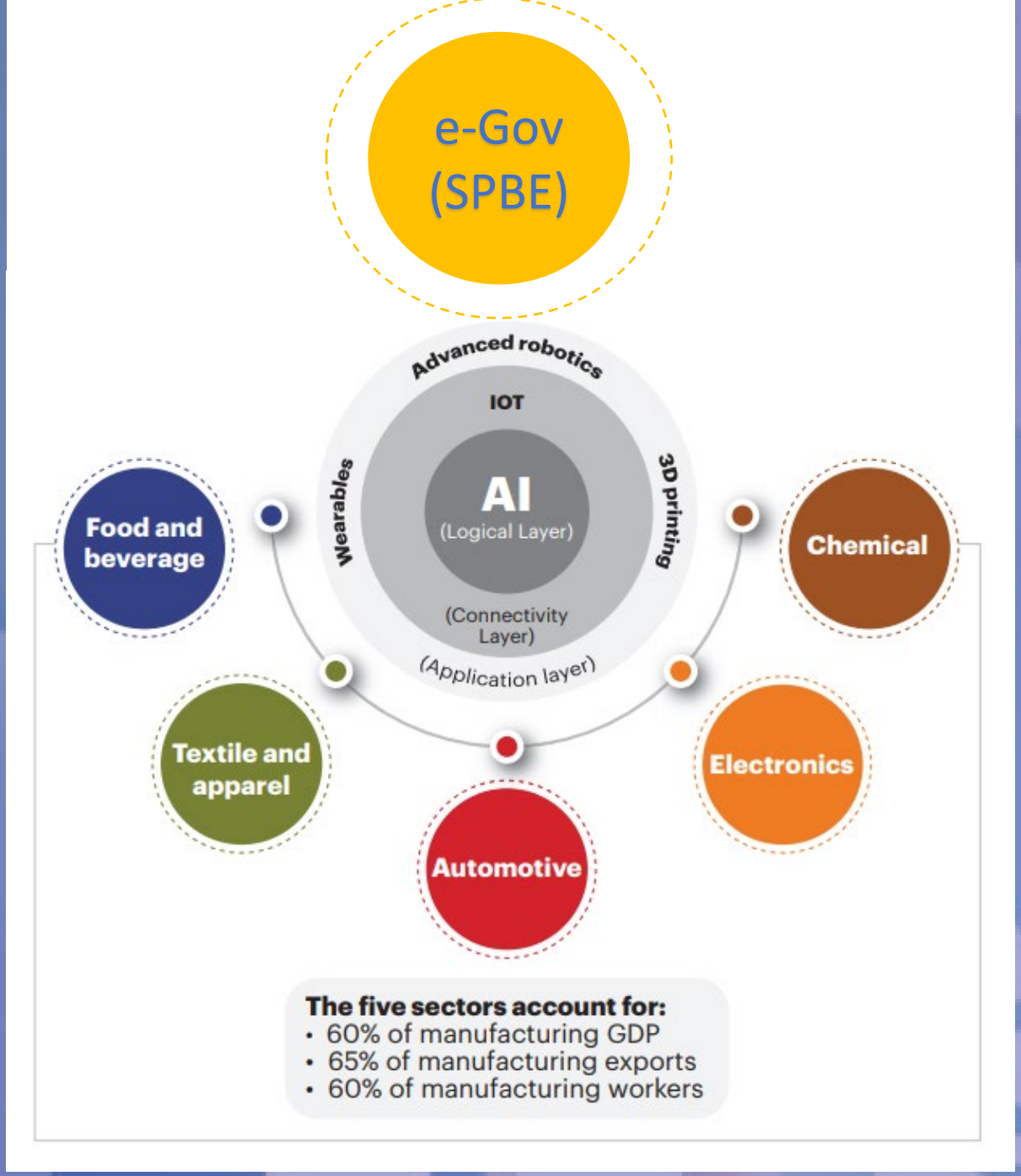
Ferry Astika Saputra

Outlines

1. Introduction: **“Making Indonesia 4.0”** as a National Industry 4.0 Strategy
2. Indonesia and Global **Threat Landscape**
3. **Cyber Security Research Group**
    1. **Description**
    2. **Four Pillars**
    3. **Our Goals**
    4. **Our Research Focus : IT-OT Security**
    5. **Roadmap**

1. Making Indonesia 4.0

Making Indonesia 4.0



Cyber Challenges of Making Indonesia 4.0

2. Indonesia and Global Threat Landscape

INDONESIA CYBER SPACE

Sektor energi dan sumber daya alam

Sektor pemerintahan (Sistem Pemerintahan Berbasis Elektronik) : 623 K/L/D

Sektor Industri

Sektor Transportasi

Sektor TIK

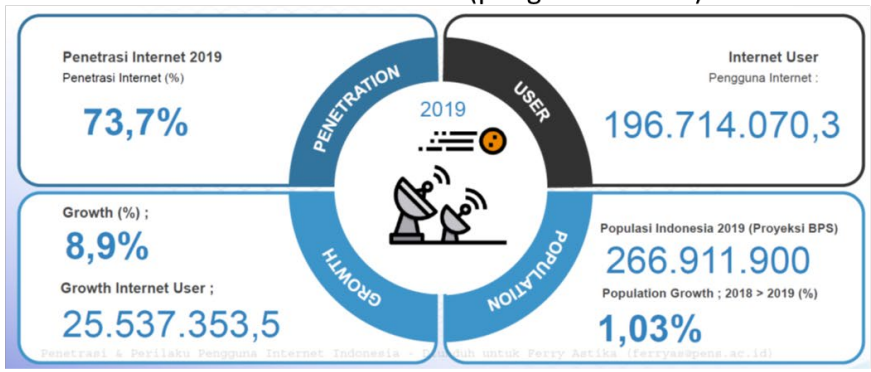
Sektor Media

Sektor perdagangan

Sektor keuangan

353 ribu domain .id

40 NAP	307 ISP	1630 ASN	18,8 juta IP
Jumlah Penyedia Gerbang Internet	Jumlah Penyedia Jasa Internet	Jumlah Autonomous System Number (pengelola blok IP)	Jumlah Alamat IP



Sumber : Laporan Tahunan APJII dan PANDI 2019

Issues & Challenges :

Top Vectors of Indonesia Cybersecurity Incidents

ID-SIRTII/CC Traffic Monitoring & Attack Detection

2018

205.502.159
Attacks Detected

36.423.773
Malware Activities

98.787
Vulnerabilities Detected

2.260
Incident Reports

2017

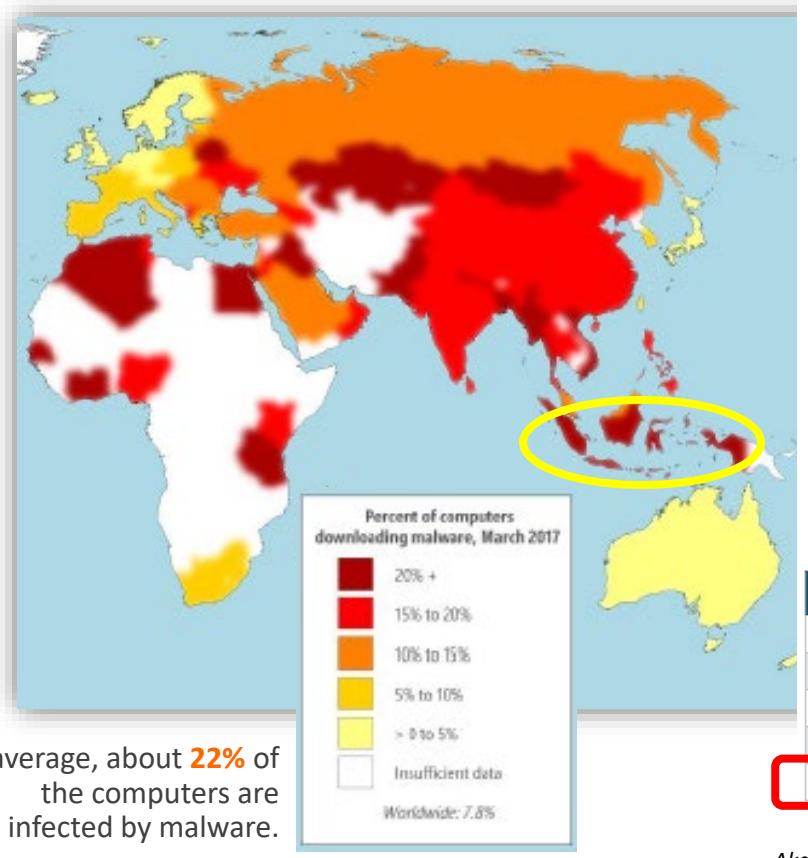
135.672.984
Attacks Detected

63.766.303
Malware Activities

37.124
Vulnerabilities Detected

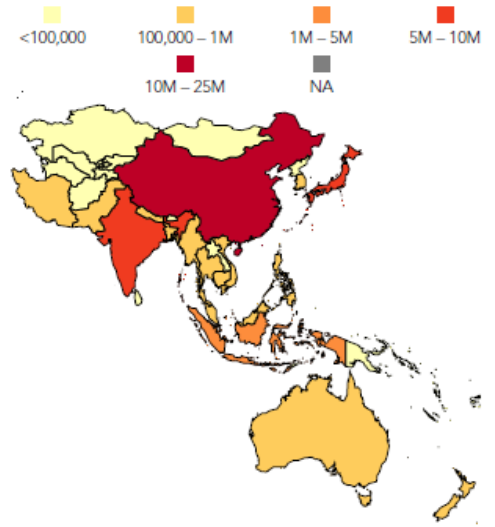
2.260
Incident Reports

Percentage of Computers Downloading Malware



At average, about **22%** of the computers are infected by malware.

Web Application Attack
Source Countries—Asia Pacific, Q1 2017



Country	Attacks Sourced	Global Rank
China	18,963,654	4
India	6,150,881	12
Japan	5,839,869	13
Singapore	4,285,527	15
Indonesia	3,248,604	17

Image Source :
Akamai's [State Of The Internet]/Security Q1 2017 Report

Incident in Indonesia:

CNN Indonesia — Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan

Home > Teknologi > Berita Teknologi Informasi

Malindo Air Selidiki Dugaan Pembocoran 21 J

Senin, 18 Mar 2019 09:20 WIB

Hacker Klaim Curi dan Jual 13 Juta A Bukalapak

Adi Fida Rahman - detikInet

CNN Indonesia — Home Nasional Internasional Ekonomi Olahraga Teknologi Hiburan Gaya H

Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry

Lesthia Kertopati, CNN Indonesia | Sabtu, 13/05/2017 19:40 WIB

Bagikan :

LAPORAN KASUS

Kebocoran Data di Indonesia Sejak 2020

Tokopedia
Mei 2020
91 juta data pengguna dan 7 juta merchant
Dijual di EmpireMarket dengan harga **US$5.000**

Bhineka.com
Mei 2020
1,2 juta data pengguna
Dijual di darkweb dengan harga **US$1.200**

Komisi Pemilihan Umum
Mei 2020
2,3 juta pemilih Indonesia pada pemilu 2014
Dijual di Raid Forums. **Harga tidak diketahui**

Bukalapak
Juni 2020
13 juta data pengguna
Dijual di Raid Forums bersama dengan data dari platform lain seharga **US$5.000**

Data Covid-19
Juni 2020
230 ribu data pasien Covid-19
Dijual di Raid Forums. **Harga tidak diketahui**

Cermati
November 2020
2,9 juta data pengguna
Dijual di dark web seharga **US$2.200**

Kreditplus
Agustus 2020
819.976 data nasabah
Dijual di Raid Forums. **Harga tidak diketahui**

BPJS Kesehatan
12 Mei 2021
100.002 data peserta dari 279 juta data (masih investigasi)
Dijual di Raid Forums seharga **0,15 Bitcoin atau sekitar Rp87,1 juta (kurs Rp580.914.000)**

Infografis dan ilustrasi: Fajrian | Naskah: Joko Panji Sasongko | Sumber diolah

CNN Indonesia

Issues & Challenges :
Cybersecurity Cases in Indonesia

- **70**/165 in Global Cybersecurity Index.
- **12**/25 based on Cybersecurity Maturity in Asia Pacific Region.
- **17th** in Akamai Web Application Attack Source Countries, 2017.
- **10th** of the biggest consumer loss of through cyber crime worldwide in 2017, by victim country (in billion U.S. dollars) – Statista.

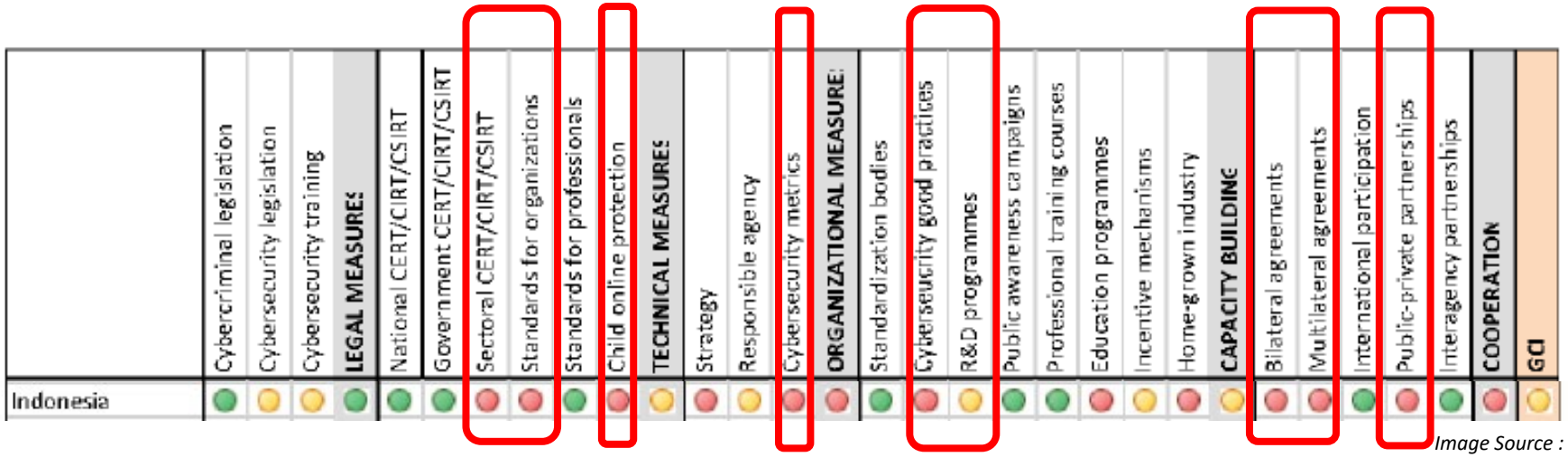


Image Source : ITU Global Cybersecurity Index 2017.

Impact of Cybersecurity Threats in Indonesia :

- The **potential economic losses** in Indonesia resulting from cyber security incidents can reach **US $ 34.2 billion** (equivalent to 3.7 per cent of Indonesia's total GDP of US $ 932 billion).

- 22% of the companies had experienced **cyber security incidents**.
- 3 out of 5 (61%) of respondents stated that their company has **delayed digital transformation efforts** because of concerns about cyber risks.

Source : Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World – Frost & Sullivan (Initiated by Microsoft)

Cyber Security Research Group (CSRG)

Why do we exist ?

- Threats to the integrity and functionality of systems in connected systems in cyberspace are numerous, varied and dynamic, as well as the ways in which they can be compromised or exploited by adversaries, criminal or political. The Cyber Security Research Group (CSRG) studies the nature and character of these threats and formulates the right way of thinking to implement cybersecurity in the service of society.

- CSRG is an intellectual center for studying various issues in cybersecurity and related fields, including cyber warfare and cyber warfare, national and military cyber strategy, protection of critical infrastructure, information security, information warfare, digital surveillance, cyber crime and solutions security in OT (Operation Technology) systems in industrial automation connected to the Internet.

- We encourage innovation, in theory, concepts and methods, and provide solutions to cybersecurity problems, while encouraging discussion and engagement across academia, governments, companies, defense and security agencies, the media and the general public.

Mengapa CSRG ada?

- Ancaman terhadap integritas dan fungsionalitas sistem pada sistem yang terkoneksi dalam ruang siber sangat banyak, beragam dan dinamis, demikian pula cara mereka dapat dikompromikan atau dimanfaatkan oleh musuh, kriminal atau politik. Cyber Security Research Group (CSRG) mempelajari sifat dan karakter dari ancaman ini dan merumuskan cara berpikir yang tepat untuk menerapkan keamanan siber dalam melayani masyarakat.
- CSRG adalah pusat intelektual untuk mempelajari berbagai masalah dalam keamanan dunia maya dan bidang terkait, termasuk perang dunia maya dan perang dunia maya, strategi dunia maya nasional dan militer, perlindungan infrastruktur kritis, keamanan informasi, perang informasi, pengawasan digital, kejahatan dunia maya dan solusi keamanan pada sistem OT (Operation Technology) pada otomasi industri yang tehubung di Internet.
- Kami mendorong inovasi, dalam teori, konsep, dan metode, serta memberikan solusi terhadap masalah keamanan dunia maya, sambil mendorong diskusi dan keterlibatan lintas akademisi, pemerintah, perusahaan, lembaga pertahanan dan keamanan, media, dan masyarakat umum.

Keselarasan RG dengan RIRN

TEMA RISET	TOPIK RISET	DUKUNGAN ANGGARAN	INSTITUSI TERKAIT	TARGET	LINK RIPIN 2015-2035
Pengembangan Infrastruktur TIK	Teknologi 5G (broadband)	Kominfo	Kominfo Kemenristekdikti Kemenperin PPN/Bappenas PUPR LIPI BPPT	Prototipe teknologi 5G	Peralatan komunikasi
	Telekomunikasi berbasis internet protocol (IP)	Kominfo	Kominfo Kemenperin PPN/Bappenas PUPR LIPI BPPT	Integrasi teknologi *Dense Wavelenght Division Multiplexing* (DWDM)	Peralatan Komunikasi
	Penyiaran multimedia berbasis digital	Kominfo	Kominfo BPPT	Teknologi penyiaran multimedia berbasis digital	Peralatan Komunikasi
	IT security	Kominfo	Kominfo PUPR Kemenhan BPPT	Teknologi digital security untuk akses digital, transakasi pembayaran, *smart-card* Teknologi *cyber defence*	Peralatan Komunikasi Komputer

RIRN 2017-2014

	5.4 Teknologi Informasi dan Komunikasi serta Kebijakan untuk Mendukung Industri 4.0	5.4.1 Big Data dan Komputasi Awan, Internet untuk Segala, Kecerdasan Buatan (RTT)	Koordinator: Badan Penelitian dan Pengembangan Kementerian Komunikasi dan Informatika	Sistem Big Data untuk Kepentingan Nasional dan Aplikasi yang Aman dan Komprehensif	Sistem Big Data Nasional	500

Permenristekdikti No. 39/2019 tentang Prioritas Riset Nasional 2020 - 2024

Four Pilars of CSRG

- Government Agency
- Research Institution
- Business Sector
- International Collaboration

- Cyber Security Tools
- Security Critical Infrastructure Security on Industrial IoT
- Security on Control System

- Whitepaper
- Policy
- Technology Proof of Concept

- Incident Handling
- Real world simulation Attack and Defense
- Incident analysis and forensic

Our Goals

Cyber Security Research Group

Postgraduate Program in Cyber Security

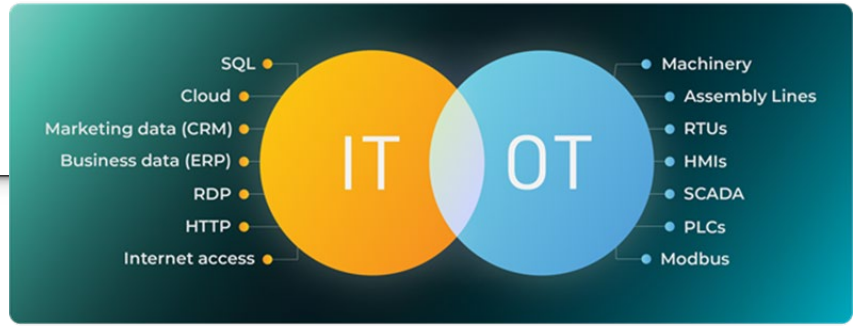
Cyber Security related Research

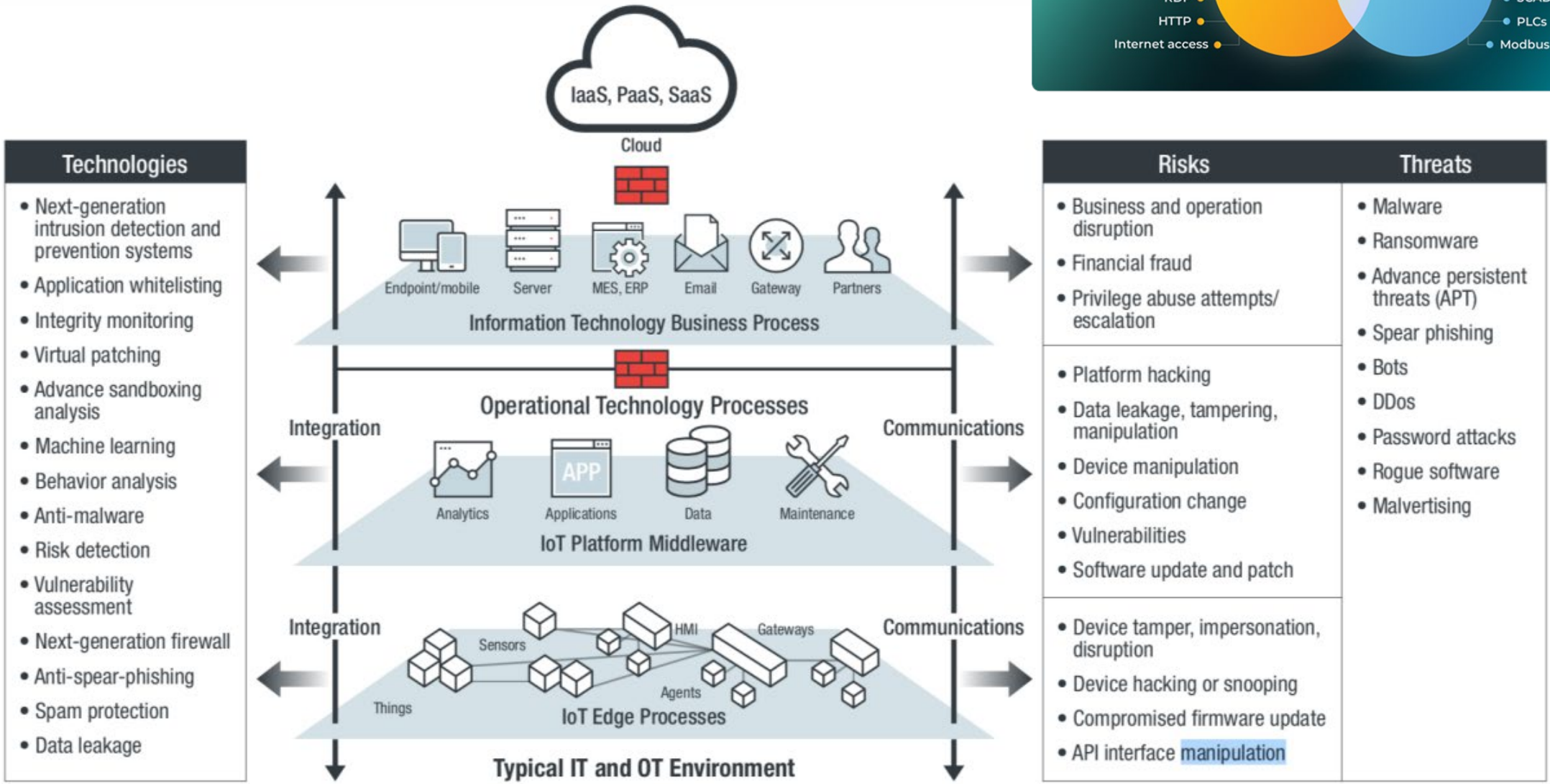
Collaboration and Partnership

Capacity Building & Certification

ENHANCING CYBER SECURITY CAPACITY OF HUMAN RESOURCES

We focus on IT-OT Security





Technologies

- Next-generation intrusion detection and prevention systems
- Application whitelisting
- Integrity monitoring
- Virtual patching
- Advance sandboxing analysis
- Machine learning
- Behavior analysis
- Anti-malware
- Risk detection
- Vulnerability assessment
- Next-generation firewall
- Anti-spear-phishing
- Spam protection
- Data leakage

Risks

- Business and operation disruption
- Financial fraud
- Privilege abuse attempts/ escalation
- Platform hacking
- Data leakage, tampering, manipulation
- Device manipulation
- Configuration change
- Vulnerabilities
- Software update and patch
- Device tamper, impersonation, disruption
- Device hacking or snooping
- Compromised firmware update
- API interface manipulation

Threats

- Malware
- Ransomware
- Advance persistent threats (APT)
- Spear phishing
- Bots
- DDos
- Password attacks
- Rogue software
- Malvertising

http://dx.doi.org/10.13140/RG.2.2.28293.29920

Roadmap

Capaian

1. pembangunan aplikasi keamanan siber
2. Kerjasama mandiri dengan PT, instansi pemerintah dan instansi non pemerintah
3. Gabung ke dalam Jatim Gov-CSIRT dan ACAD CSIRT
4. Pendanaan Mandiri : JICA

2014-2109 — MATA GARUDA
THE INDONESIA INTERNET TRAFFIC MONITORING PROJECT https://www.youtube.com/watch?v=bJziWfHJYrU
https://github.com/mata-elang-stable/MataElang-Platform/wiki

2019-now — Mata Elang Cloud IDS : Research Community
1. PENS Chapter
2. UI Chapter
3. BRIN Chapter
https://github.com/Mata-Elang-Stable/MataElang-Platform

2019-now — Mata Elang Cloud IDS : Stable version
1. Board of Director : PENS dan DTE FT-UI
2. Managed from 2019-now
3. ME v1.0 and 1.1 were funded by JICA-UI Project

Dalam Proses

1. Lanjutan pengembangan cyber security tools lainnya
2. Kerjasama implementasi ME di IPPD, Acad CSIRT, sector Swasta, bahkan lintas negara (Timor Leste, Laos, OIC-Cert)
3. Membangun bisnis model Platform Security as a Service
4. Kerjasama denga BSSN melalui Politeknik SSN
5. Pembangunan simulator IT-OT Cyber Range Mandiri
6. Penguatan riset

FASE TRANSFORMASI

1. Kerjasama dengan pihak ketiga: CSRG sebagai Product Development dan Pihak ketiga sebagi Business Development
2. Menjadi salah satu pusat unggulan keamanan siber di Indonesia → training center, auditor keamanan SPBE, masuk
3. IT-OT simulator mejadi pusat training keamanan IT-OT

PENGUATAN RISET MANDIRI — **2014-2022**

EKSPANSI KOLABORASI DAN INISIASI BISNIS MODEL — **2022-2024**

MENJADI PUSAT UNGGULAN KEAMANAN SIBER — **2024-2027**

CONTINOUS CYCLE — **2027-???**

TERIMA KASIH
THANK YOU
ARIGATOU

Attachments

PENELITIAN & PUBLIKASI JURNAL

PENELITIAN DAN PENDANAAN

2013	Community Driven Search Engine Based on Community's Proxy Server Log, Case Study on EEPIS network	UPPM-PENS
2014	Indonesia Internet Monitoring Project : Mata Garuda	IDSIRTII/CC
2016	Pengembangan sistem monitoring daya dan suhu guna mendukung operasi yang adil dalam sistem monitoring daya di pusat data.	P3M-PENS
2017-2018	Pengembangan Sistem Monitoring dan Deteksi Intrusi Keamanan Internet terinegrasi berbasis Cyber Situational Awareness Framework (Tahun 1)	DRPM-UI PUPT Universitas Indonesia
2018-2019	Pengembangan Sistem Monitoring dan Deteksi Intrusi Keamanan Internet terinegrasi berbasis Cyber Situational Awareness Framework (Tahun 2)	DRPM-UI PUPT Universitas Indonesia
2020-2021	A new approach for improving the effectiveness of distributed IDS sensor over big data environment	DRPM-UI (PUTI-Q2)
2021	Mata Elang versi 1.0	JICA
2022	Mata Elang versi 1.1	JICA

JURNAL

Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor/Tahun
The Critical Needed of IPv6 Development in Indonesia	EMITTER	Volume 1 No. 1 2008
The Internet as Complex Networks: Understanding Its Structure and Its Dynamical Properties	NATURAL-A – Journal of Scientific Modeling & Computation	Volume 1 No.1 – 2013
Performance Evaluation of Beacon-Enabled Mode for IEEE 802.15.4 Wireless Sensor Network	EMITTER International Journal of Engineering Technology	Volume 2 No.1 – 2013
Distribution system for urban agricultural products using genetic algorithms based on Android	International Journal of Engineering and Technology(UAE)	Volume 7,2018
Spatio Temporal with Scalable Automatic Bisecting-Kmeans for Network Security Analysis in Matagaruda Project	EMITTER International Journal of Engineering Technology	Volume 7 (1), 83-104, 2019
The Next-Generation NIDS Platform: Cloud-Based Snort NIDS Using Containers and Big Data	MDPI Big Data and Cognitive Computing (special Issue: Big Data for Cyber Security)	Volume 6, no 1, February 2022

PUBLIKASI SEMINAR

Thirteenth International Conference on Digital Information Management (ICDIM 2018)	Botnet Detection in Network System Through Hybrid Low Variance Filter, Correlation Filter and Supervised Mining Process	Berlin, 2018
FIRST TC (FIRST Technical Colloquium) 2018	Designing Distributed Honeypot Network Based on Linux Container Using Docker	Bali,2018
International Electronics Symposium on Knowledge Creation and Intelligent Computing 2018	Big data analysis architecture for multi IDS sensors using memory based processor	Surabaya, 2018
International Conference on Applied Science and Technology (iCAST)	I-on smart controller: Portable smart home solution based on arduino and raspberry pi	Jakarta,2018
International Electronics Symposium on Knowledge Creation and Intelligent Computing 2019	Smart Home System for Fire Detection Monitoring Based on Wireless Sensor Network	Surabaya,2019
International Electronics Symposium on Knowledge Creation and Intelligent Computing 2019	Feature Selection Algorithm For Intrusion Detection Using Cuckoo Search Algorithm	Surabaya,2019
5th International Conference on Science in Information Technology (ICSITech), 2019	Implementation MQTT-SN Protocol on Smart City Application based Wireless Sensor Network	Yogyakarta, 2019
International Electronics Symposium on Knowledge Creation and Intelligent Computing 2020	Surveillance Monitoring System based on Internet of Things	Surabaya,2020

Pelatihan Mata Garuda untuk 3 Negara Asean (November 2016) bekerja sama dengan JICA

Past and Current Research Activities

Technologies

- Next-generation intrusion detection and prevention systems
- Application whitelisting
- Integrity monitoring
- Virtual patching
- Advance sandboxing analysis
- Machine learning
- Behavior analysis
- Anti-malware
- Risk detection
- Vulnerability assessment
- Next-generation firewall
- Anti-spear-phishing
- Spam protection
- Data leakage

2014-2109

MATA GARUDA
THE INDONESIA INTERNET TRAFFIC MONITORING PROJECT https://www.youtube.com/watch?v=bJziWfHJYrU

https://github.com/mata-elang-stable/MataElang-Platform/wiki

2019-now

Mata Elang Cloud IDS : Research Community

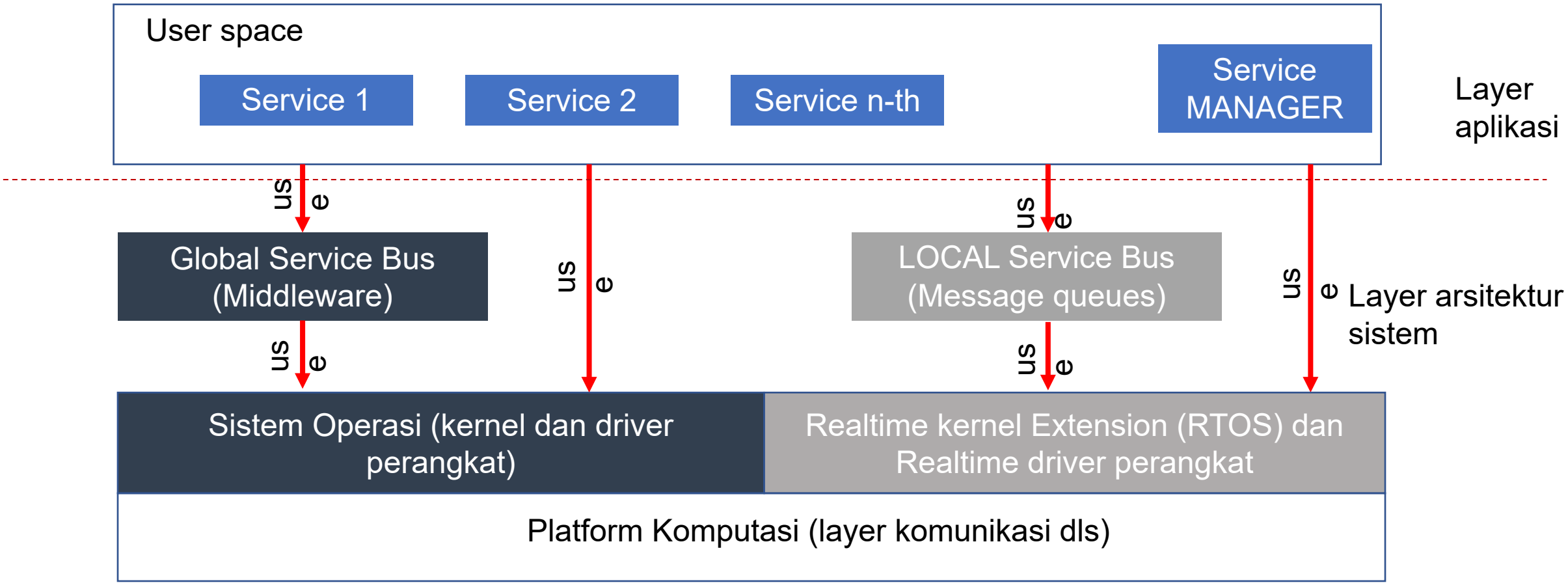
1. PENS Chapter
2. UI Chapter
3. BRIN Chapter

https://github.com/Mata-Elang-Stable/MataElang-Platform

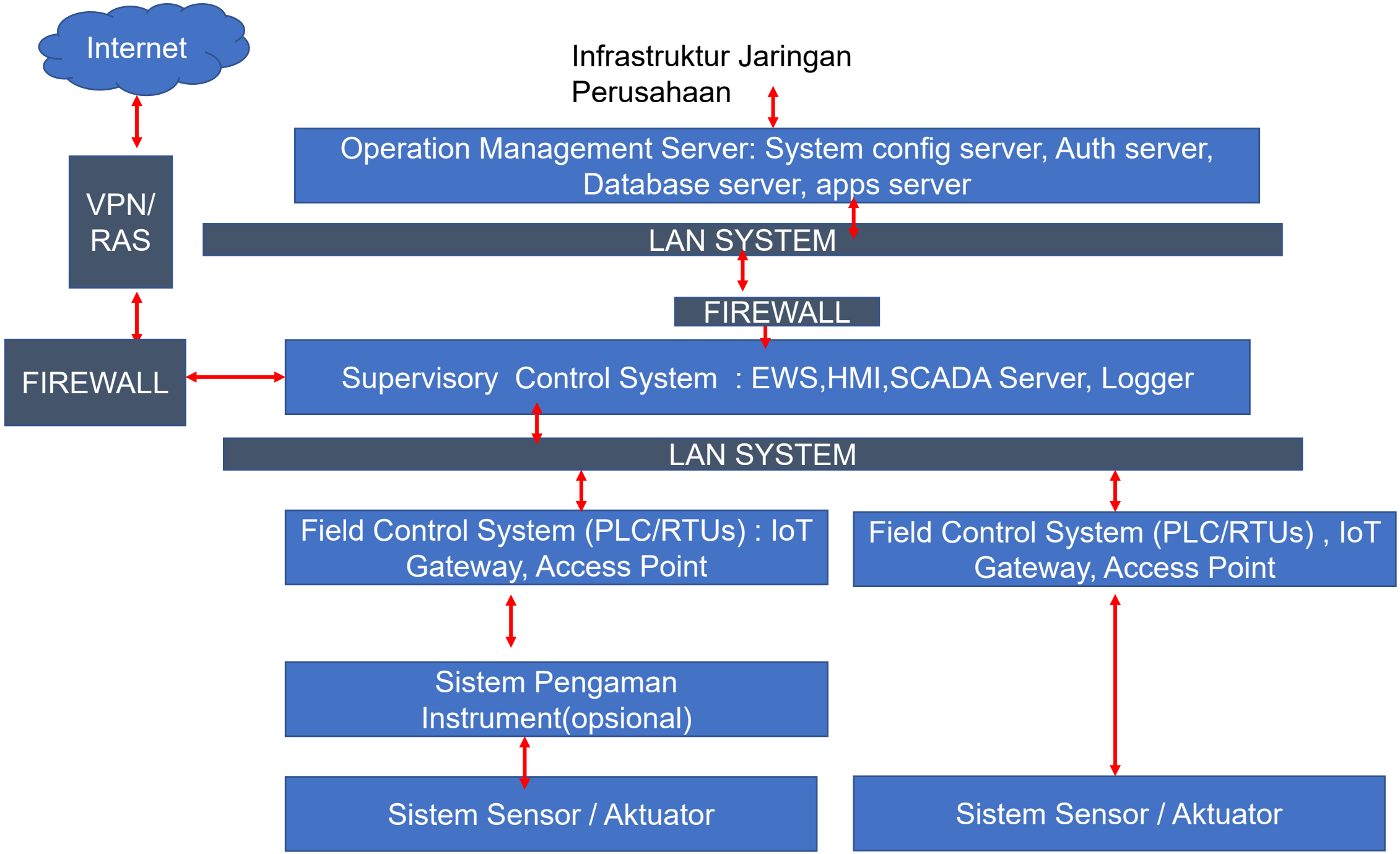
2019-now

Mata Elang Cloud IDS : Stable version

1. Board of Director : PENS dan DTE FT-UI
2. Managed from 2019-now
3. ME v1.0 and 1.1 were funded by JICA-UI Project



Logik sistem dari CPS : aplikasi, OS, RTOS ext. Serangan siber ke CPS semua berawal dari user space


Internet
Infrastruktur Jaringan Perusahaan
VPN/ RAS
Operation Management Server: System config server, Auth server, Database server, apps server
LAN SYSTEM
FIREWALL
FIREWALL
Supervisory Control System : EWS,HMI,SCADA Server, Logger
LAN SYSTEM
Field Control System (PLC/RTUs) : IoT Gateway, Access Point
Field Control System (PLC/RTUs) , IoT Gateway, Access Point
Sistem Pengaman Instrument(opsional)
Sistem Sensor / Aktuator
Sistem Sensor / Aktuator