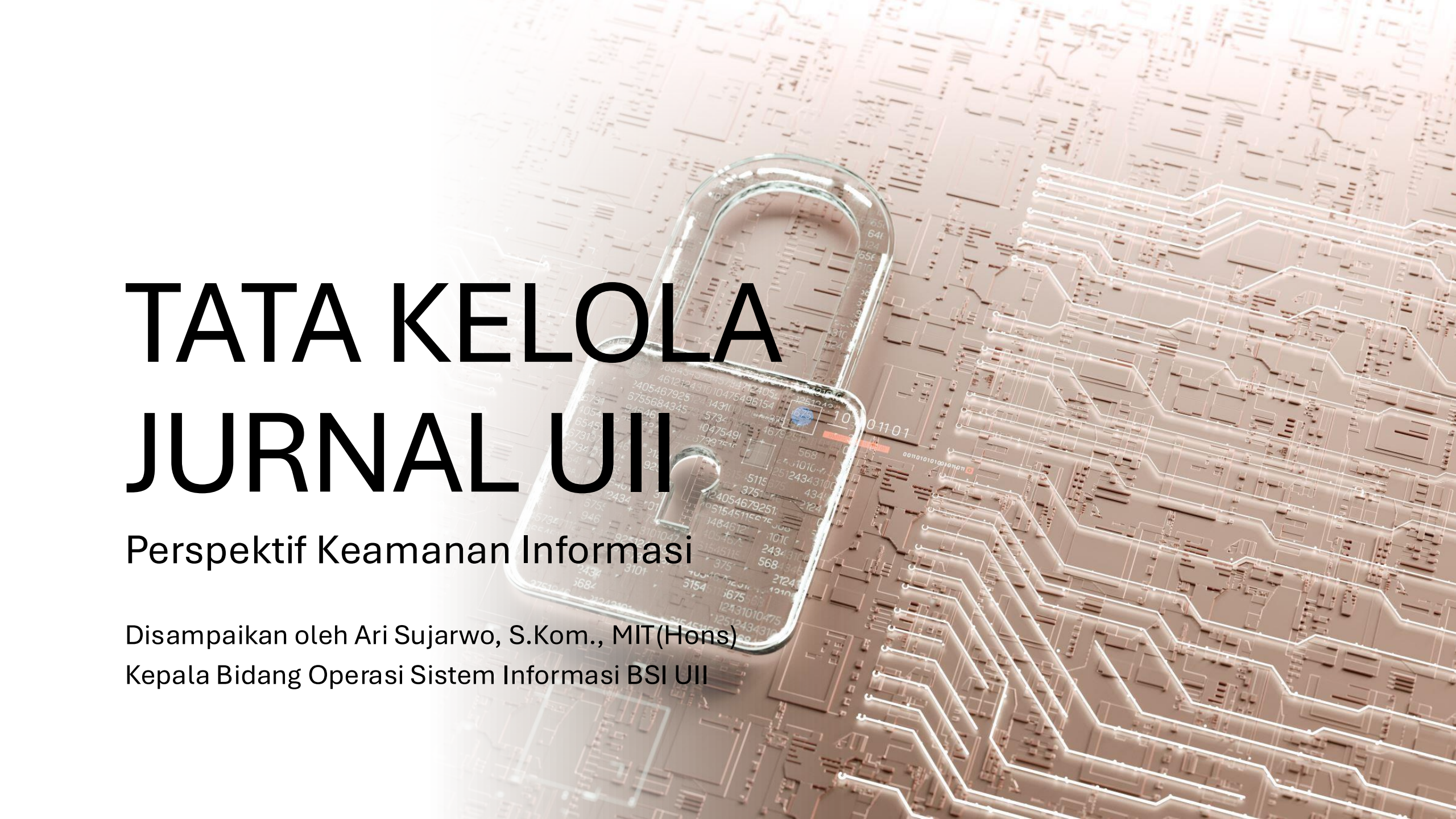


TATA KELOLA JURNAL UII

Perspektif Keamanan Informasi

Disampaikan oleh Ari Sujarwo, S.Kom., MIT(Hons)
Kepala Bidang Operasi Sistem Informasi BSI UII

UNIVERSITAS ISLAM INDONESIA

Ari Sujarwo, S.Kom., MIT (Hons)

Dosen di Program Studi Informatika, Universitas Islam Indonesia

Kepala Bidang Operasi Sistem Informasi, Badan Sistem Informasi, UII

Anggota klaster Sistem Informasi dan Sistem Siber, Jurusan Informatika, UII

Personal info:
sites.google.com/uii.ac.id/sujarwo

Kontak: ari.sujarwo@uii.ac.id

BIDANG ETIKA DAN HUKUM				
Status Peraturan:	BERLAKU			
Verifikasi	14 September 2020			

PERATURAN REKTOR UNIVERSITAS ISLAM INDONESIA
NOMOR 15 TAHUN 2020
TENTANG
KEBIJAKAN TEKNOLOGI INFORMASI DI LINGKUNGAN UNIVERSITAS ISLAM INDONESIA

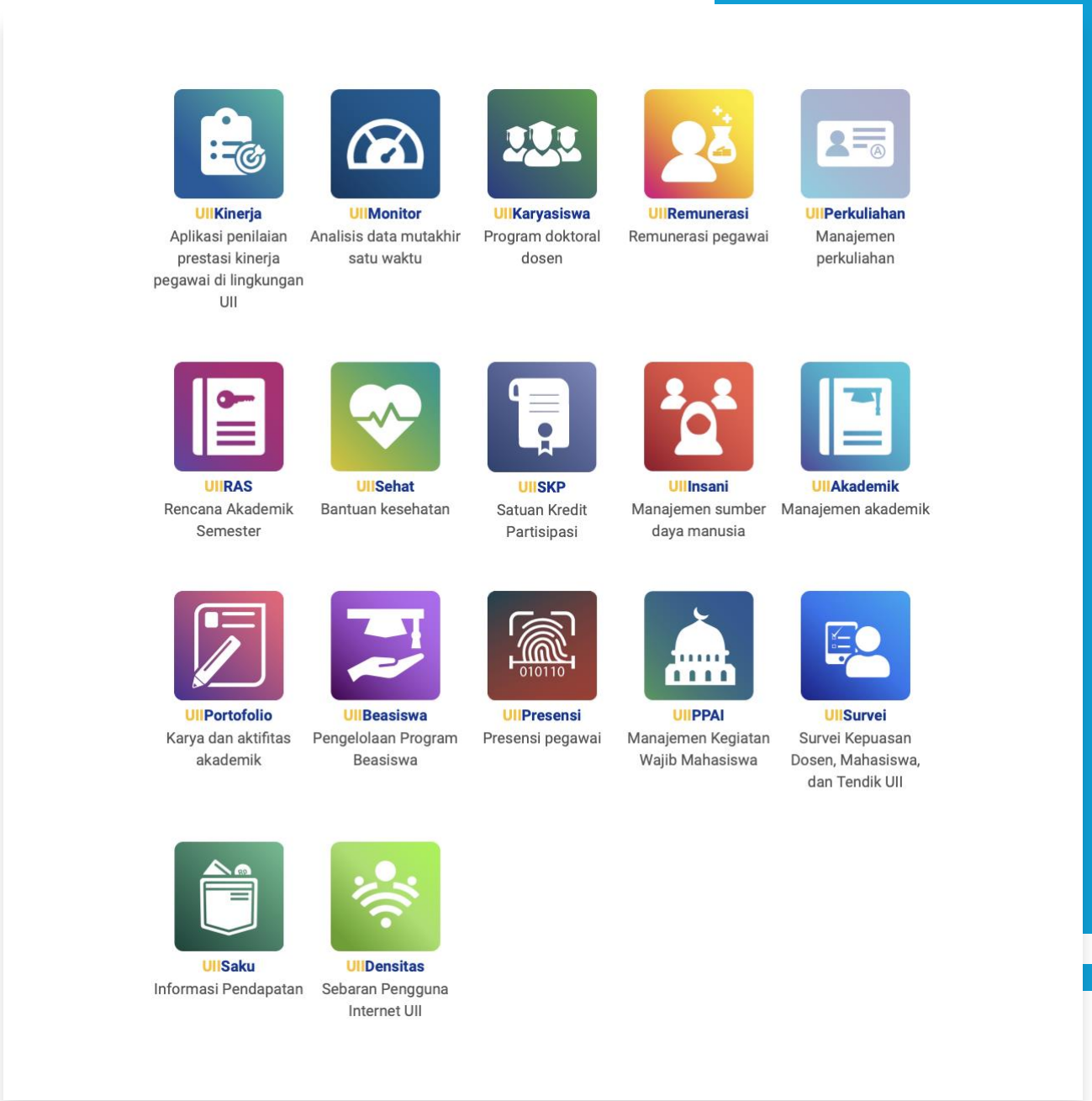
Bismillaahirrahmaanirrahim

REKTOR UNIVERSITAS ISLAM INDONESIA:

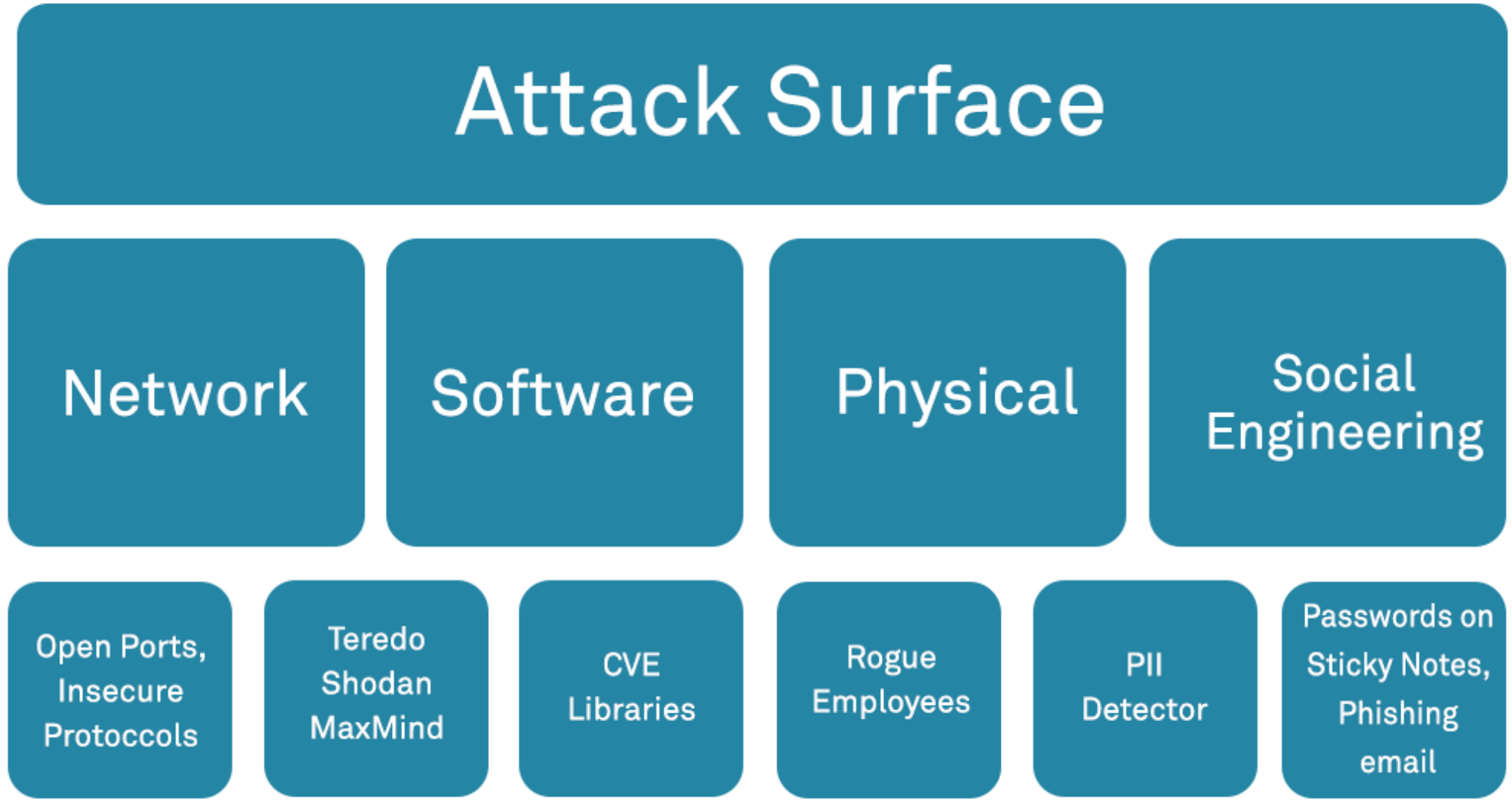
Menimbang
a. bahwa pemanfaatan teknologi informasi harus terus dikembangkan selaras dengan nilai-nilai dasar Universitas Islam Indonesia;
b. bahwa pemanfaatan teknologi informasi di lingkungan Universitas Islam Indonesia berperan penting dalam mewujudkan efektifitas dan

OJS Product Owner

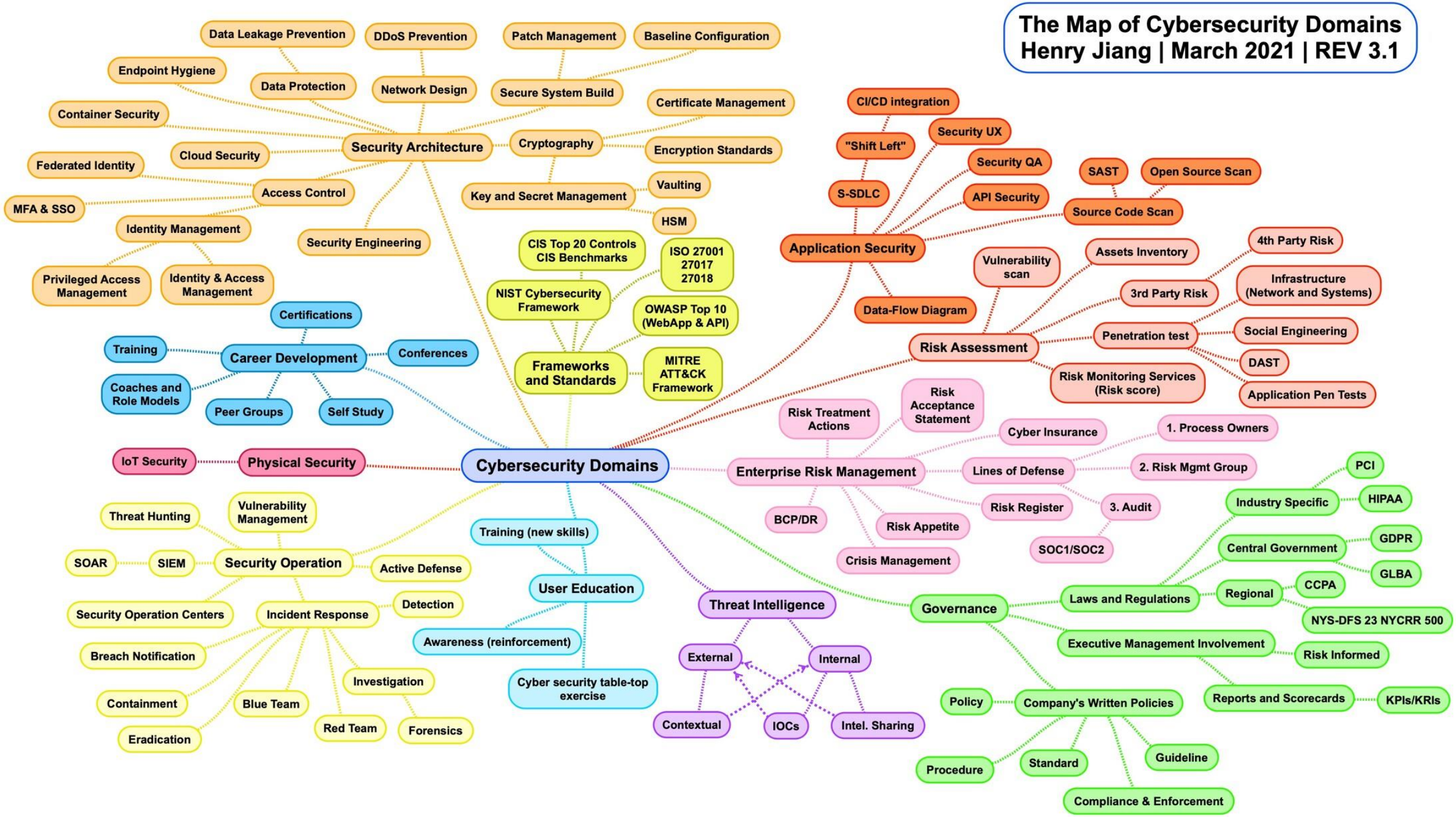
OJS UII belum memiliki *product owner*. Dampaknya: tidak ada peta *product vision*.



Dampak lanjutannya adalah kepada ketiadaan strategi dan teknis pelaksanaan pengamanan informasi.


Attack Surface
Network
Software
Physical
Social Engineering
Open Ports, Insecure Protoccols
Teredo Shodan MaxMind
CVE Libraries
Rogue Employees
PII Detector
Passwords on Sticky Notes, Phishing email

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1



Tata Kelola Jurnal UII

- Infrastruktur
- Keamanan Informasi
- Proses bisnis editorial

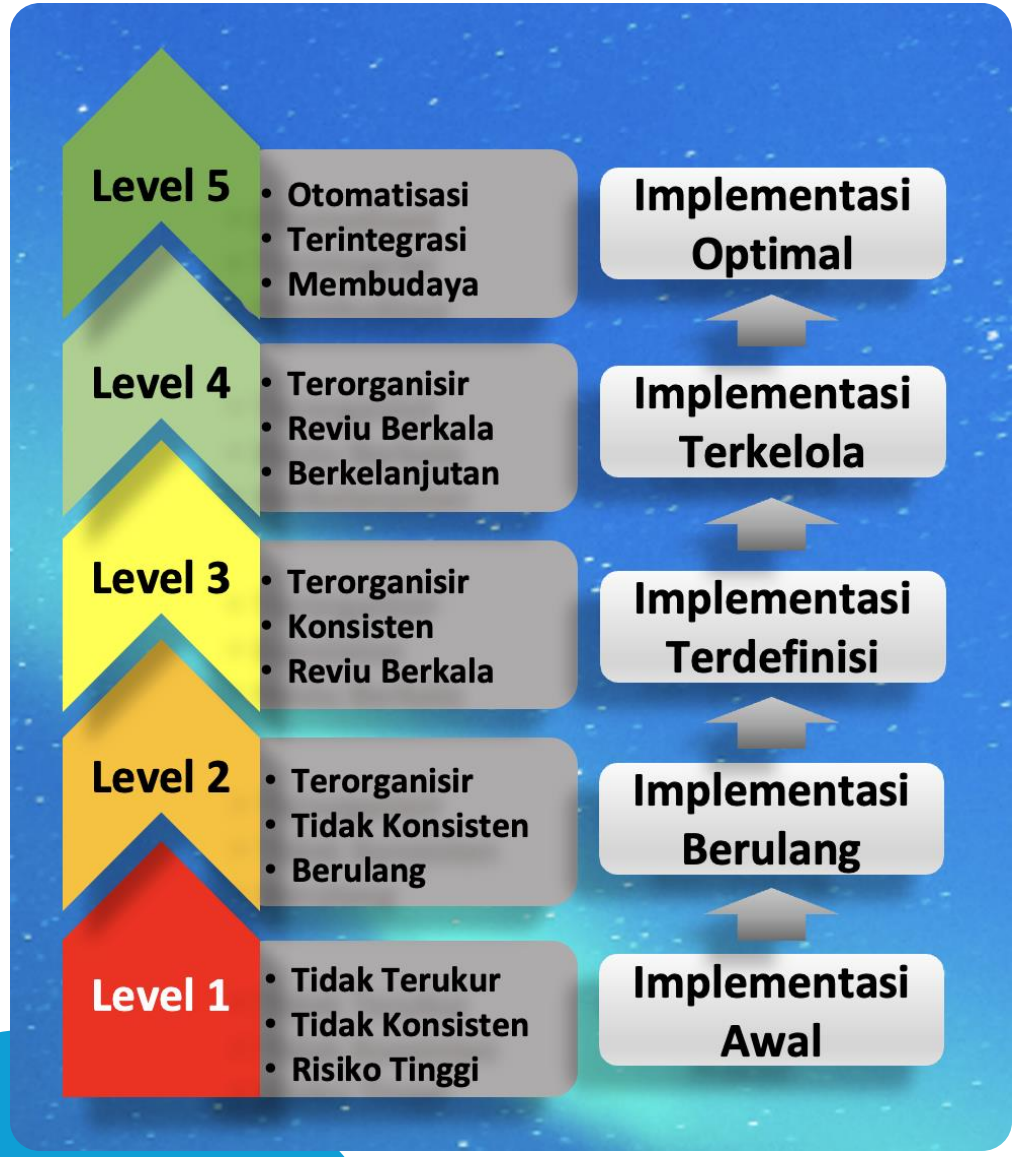
Infrastruktur

Universitas Islam Indonesia menyelenggarakan layanan jurnal melalui journal.uii.ac.id

Menggunakan mesin web Open Journal System (OJS) versi 3

Diamankan dengan standar keamanan informasi Cyber Security Maturity (CSM) dari BSSN

Diperkuat dengan mesin firewall UII dan WAF dari CloudFlare



CSM

- **Tata Kelola** (kesadaran, audit, kontrol, pemenuhan, kebijakan, dan proses)
- **Identifikasi** (manajemen aset, inventaris, manajemen risiko, prioritas, pelaporan, dan klasifikasi)
- **Proteksi** (jaringan, aplikasi, pengguna, manajemen identitas dan akses, cloud, dan data)
- **Deteksi** (perubahan, monitor, peringatan, pemberitahuan, intelijen, dan pelaporan)
- **Respon** (penahanan, penanggulangan, pemulihan, Kegiatan Paska Insiden, dan pelaporan)

Tata Kelola		Identifikasi		Proteksi		Deteksi		Res
		1,24		0,83		0,83		
Kesadaran		Manajemen Aset	2,75	Jaringan		Perubahan	5,00	Penahanan
Audit		Inventaris	4,67	Aplikasi		Monitor		Penanggulang
Kontrol		Manajemen Risiko		Pengguna		Peringatan		Pemulihan
Pemenuhan		Prioritas		Manajemen Identitas dan Aset		Pemberitahuan		Kegiatan Paska Insiden
Kebijakan		Pelaporan		Cloud		Intelijen		Pelaporan
Proses		Klasifikasi		Data	5,00	Pelaporan		

20	10	Kesadaran	Apakah organisasi Anda memberikan pelatihan untuk karyawan tentang cara mengidentifikasi dan menyimpan, mengirim, mengarsipk
21	11	Kesadaran	Apakah organisasi Anda memberikan pelatihan untuk karyawan terkait kesadaran tentang penyebab kebocoran data secara tidak seng
22	12	Kesadaran	Apakah karyawan yang menangani data sensitif stakeholder / klien / konsumen / pelanggan dilatih tentang cara melindungi data terse
23	13	Kesadaran	Apakah organisasi Anda melatih staf secara khusus tentang kewajiban menjaga data privasi, termasuk hukuman terkait pengungkapan
24	14	Kesadaran	Apakah organisasi Anda melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan?
25	15	Kesadaran	Apakah organisasi Anda melakukan simulasi phishing setidaknya setiap tahun?
26	16	Kesadaran	Dalam pengembangan software/aplikasi di organisasi, apakah personel yang terlibat dalam pengembangan software/aplikasi telah me
27	17	Kesadaran	Apakah organisasi Anda memberitahukan kepada stakeholder / klien / konsumen / pelanggan Anda tentang teknik atau kerentanan si
28	18	Audit	Apakah organisasi Anda memiliki kebijakan mengharuskan penerapan perlindungan data pribadi? Dan apakah direviu secara berkala?
29	19	Audit	Apakah pemeriksaan background dilakukan untuk semua karyawan baru?
30	20	Audit	Dalam pengembangan software organisasi Anda, apakah menggunakan algoritma enkripsi dan direviu secara berkala?
31	21	Audit	Apakah organisasi Anda menggunakan tool vulnerability scanning secara mandiri, yang mana hasil vulnerability assessment digunakan
32	22	Audit	Apakah di organisasi Anda menggunakan akun khusus selain akun admin untuk melakukan vulnerability scanning?
33	23	Audit	Apakah setiap akun pengguna atau sistem yang digunakan dalam melakukan penetrating testing dikontrol dan dipantau untuk memast
34	24	Audit	Apakah organisasi Anda melakukan reviu security risk assessment? Dan apakah dilakukan secara berkala?
35	25	Audit	Apakah organisasi Anda melakukan reviu security risk treatment? Dan apakah dilakukan secara berkelanjutan?
36	26	Audit	Apakah organisasi Anda melakukan internal audit keamanan informasi secara berkala?

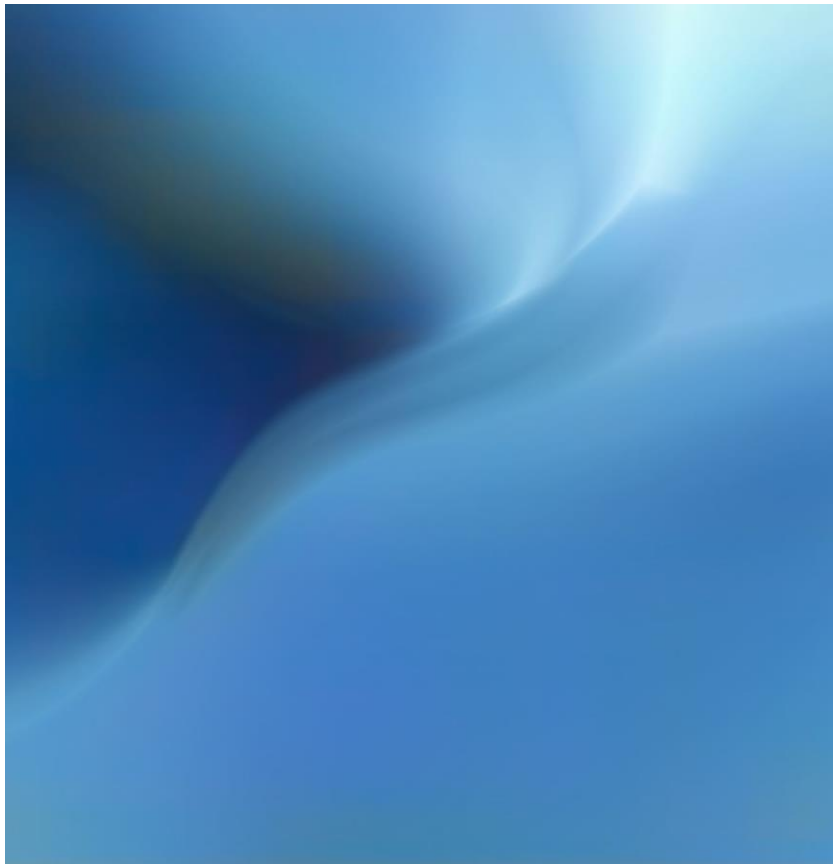
Asesmen Risiko Jurnal UII

Infrastruktur

- Gangguan pada server (storage/mem/cpu/...)
- Domain tidak aktif (blokir oleh Pandi/...)
- OJS mengalami serangan cyber (malware/slot/...)
- Internet UII mengalami gangguan (FO putus/fire event/...)

Proses bisnis jurnal

- Inactive users (dormant account/injeksi malware/...)
- Inactive journals (jurnal yang stop penerbitan/...)
- Manual editorial procedures (submisi dari luar sistem?/...)
- Integritas informasi (invalid papers?)
- OJS Plugin install/operations (penambahan plugin/...)
- Mail sendings (delivery errors/...)



Keamanan Informasi

Confidentiality

Informasi hanya boleh dibaca oleh pihak-pihak berkepentingan

Pada konteks jurnal:

Author	Reviewer	Editor

Integrity

Kebenaran informasi yang termuat dapat dipercaya, memiliki sumber valid

Dalam konteks jurnal:

Manuskrip yang diunggah betul milik author	Makalah yang terpublikasi termuat dalam wadah web terpercaya	Tautan betul menampilkan makalah yang diharapkan

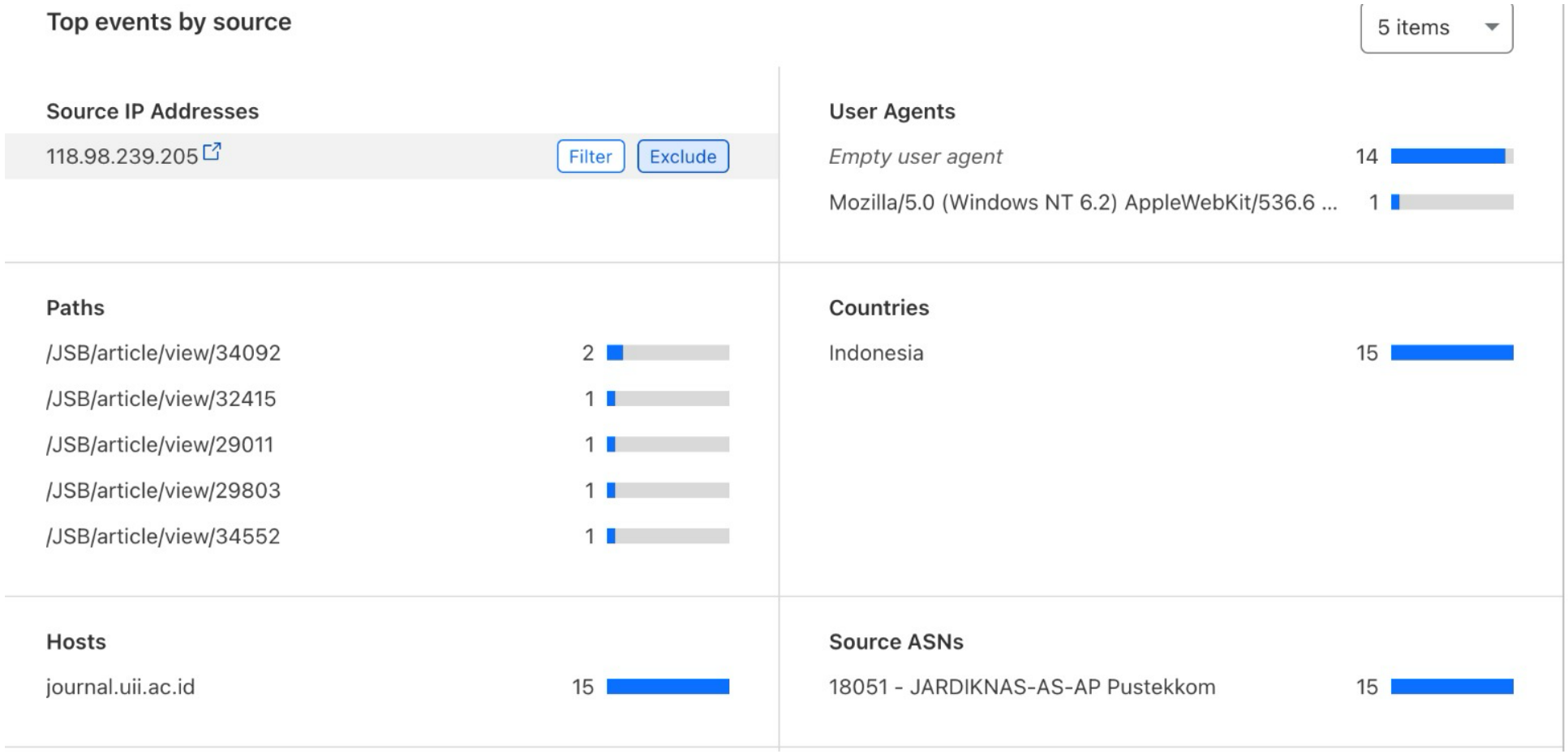
Availability

Makalah dan web secara umum tersedia kapan saja pengakses memerlukannya

Dalam konteks jurnal:

Halaman jurnal dan makalah di dalamnya dapat diakses dengan baik tanpa terjadi hambatan	Sistem-sistem lain seperti garuda dapat mengakses sistem dengan baik, misal untuk kepentingan crawling

Pada issue Garuda <<>> Journal UII, masuk dalam kategori mana?



Issue judi slot, masuk dalam kategori mana?

CIA harus dipastikan tepat

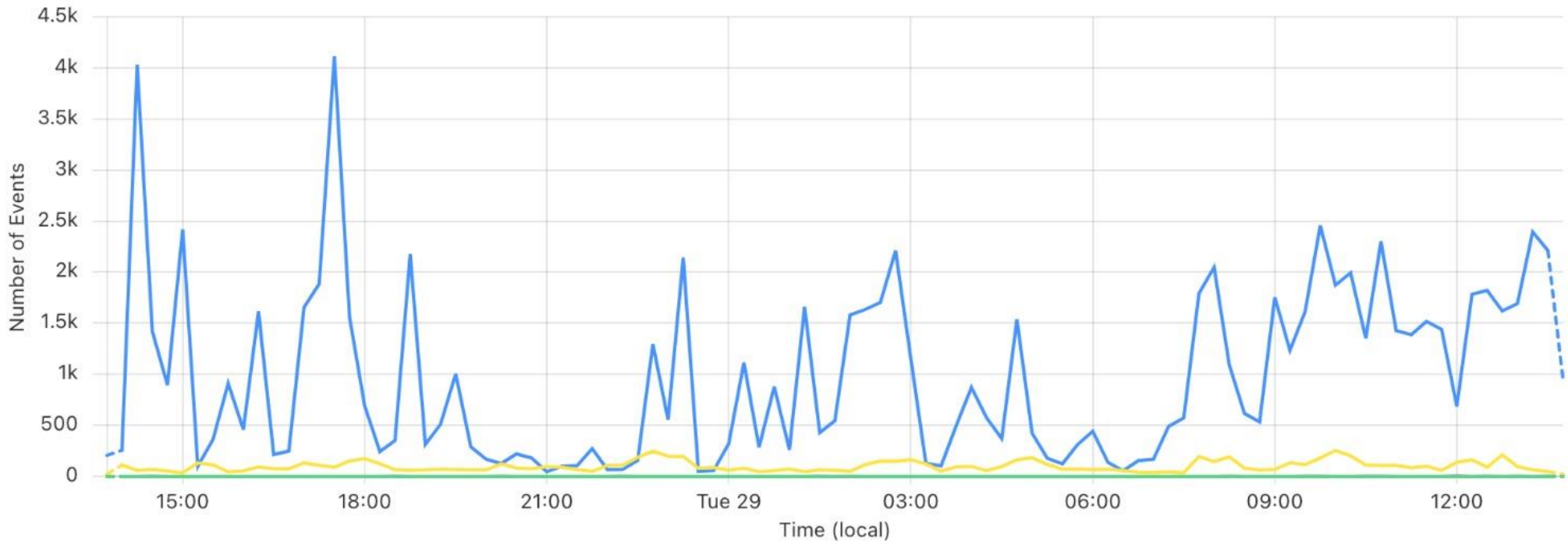
- Faktor:
  - Arsitektur hosting/datacenter
  - Arsitektur server
  - Arsitektur OJS
  - Rancangan theme dan plugin
  - Pengaturan hak akses admin/reviewer/author
  - Evaluasi rutin sistem menyeluruh
  - Pembaruan sistem terencana
  - Sumber daya komputasi dan manusia harus dipastikan cukup

Events summary

About Firewall Events

Action | Host | Country | Source ASN | Source IP | Path | ...

Total	Block	Skip	Managed Challenge	Log
103.59k	94k	9.54k	47	12



Host equals journal.uii.ac.id

France

Paths

/	1.25k
/wp-admin/js/about.php	765
/wp-login.php	735
/.well-known/acme-challenge/cloud.php	726
/index	590

Countries

Singapore	36.92k
France	Filter Exclude
United States	11.89k
Netherlands	6.82k
Hong Kong	5.23k

Hosts

journal.uii.ac.id	103.59k

Source ASNs

14061 - DIGITALOCEAN-ASN	40.87k
39351 - ESAB-AS	33.96k
15169 - GOOGLE	8.27k
208046 - COLOCATIONX-DATACENTER Dedica	7.96k
57678 - CATTECHNOLOGIES-AS	5.23k

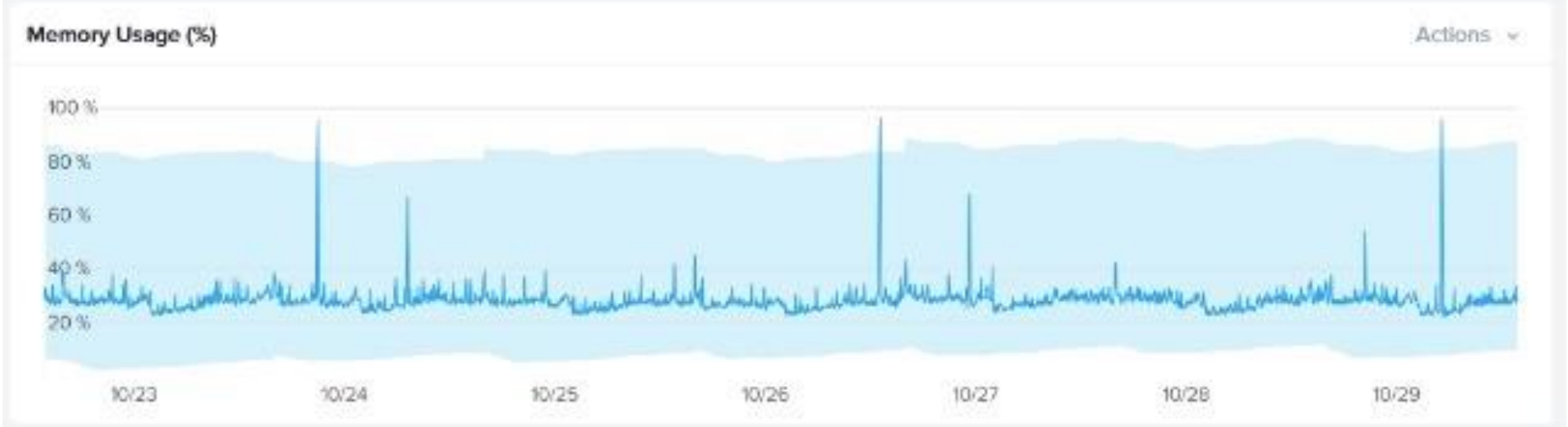
Firewall rules

Kebijakan Pengendalian User Agent Bot	57.29k
Kebijakan Blokir AS Number	22.14k
Bypass AS Google	9.41k
Kebijakan Pengendalian Wordpress dari Publik	8.24k
block .env	234

Rate limiting rules

No data


CPU Usage (%)
Actions
100 %
80 %
60 %
40 %
20 %
10/23
10/24
10/25
10/26
10/27
10/28
10/29


Memory Usage (%)
Actions
100 %
80 %
60 %
40 %
20 %
10/23
10/24
10/25
10/26
10/27
10/28
10/29

Disk Usage (%) Actions

Network Rx Bytes Actions

Daftar Akun Journal yang Terindikasi Terinfeksi Malware dan Mengalami Kebocoran

Segera lakukan RESET PASSWORD ATAU DISABLE AKUN

No	Username	Status
1	16524099	
2	aris	
3	chikaariadhita	
4	dalotaibi	
5	isfatimah@uii.ac.id	
6	piranhamas	
7	saptonojenar1982	
8	tri_hartono188	
9	tri188	
10	waritsulfirdaus	
11	sulistiyanengse	
12	waritsulfirdaus	
13	ajri	
14	JOhnma	

SOC UII Malware Scan Report.txt

```
SOC UII Malware Scan Report
====================================
Total dangerous files: 11

Dangerous Files scanned:
[+] Scanning ../target-journal/index.php
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/config.inc.php
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/plugins/generic/ojtPlugin/modules/ojtCopernicus/templates/
index.tpl
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/plugins/generic/ojtPlugin/modules/ojtCopernicus/templates/
settings.tpl
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/plugins/generic/ojtPlugin/modules/ojtCopernicus/templates/
issuesList.tpl
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/plugins/generic/ojtPlugin/modules/ojtCopernicus/vendor/spatie/
array-to-xml/LICENSE.md
YARA match found: [SuspiciousBackdoor]

[+] Scanning ../target-journal/plugins/generic/ojtPlugin/modules/ojtCopernicus/vendor/composer/
InstalledVersions.php
YARA match found: [SuspiciousBackdoor]
```

Proses bisnis editorial

Dilakukan oleh pemilik/pengelola jurnal di unit

Supporting system diberikan dari tim teknis Rumah Jurnal

Kebutuhan proses bisnis:

Korespondensi Penerbitan	Pencatatan dan payment	Monitoring proses bisnis	Monitoring sistem dan server

What to do?

- Update, update, update
- Komunikasi intensif dengan DPPM
- Rutin partisipasi di UIIAcademy oleh BSI
- Kontrol rutin user, plugin
- Kirim laporan jika ditemukan CVE (Common Vulnerabilities and Exposures/katalog celah kerentanan keamanan sistem informasi) baru
- Rumah Jurnal, pulang yuk!

Penutup

- Semua akan bergantung kepada sejauh mana visi produk layanan jurnal di UII
- Selama komitmen masih ada, penyelenggaraan jurnal di UII perlu diperjuangkan
- Cukupi kebutuhan sumber dayanya
- Tetapkan strateginya
- Belajar dari ahlinya

Selanjutnya, bagaimana dengan tata kelola keamanan *data riset* di UII?

Terima kasih