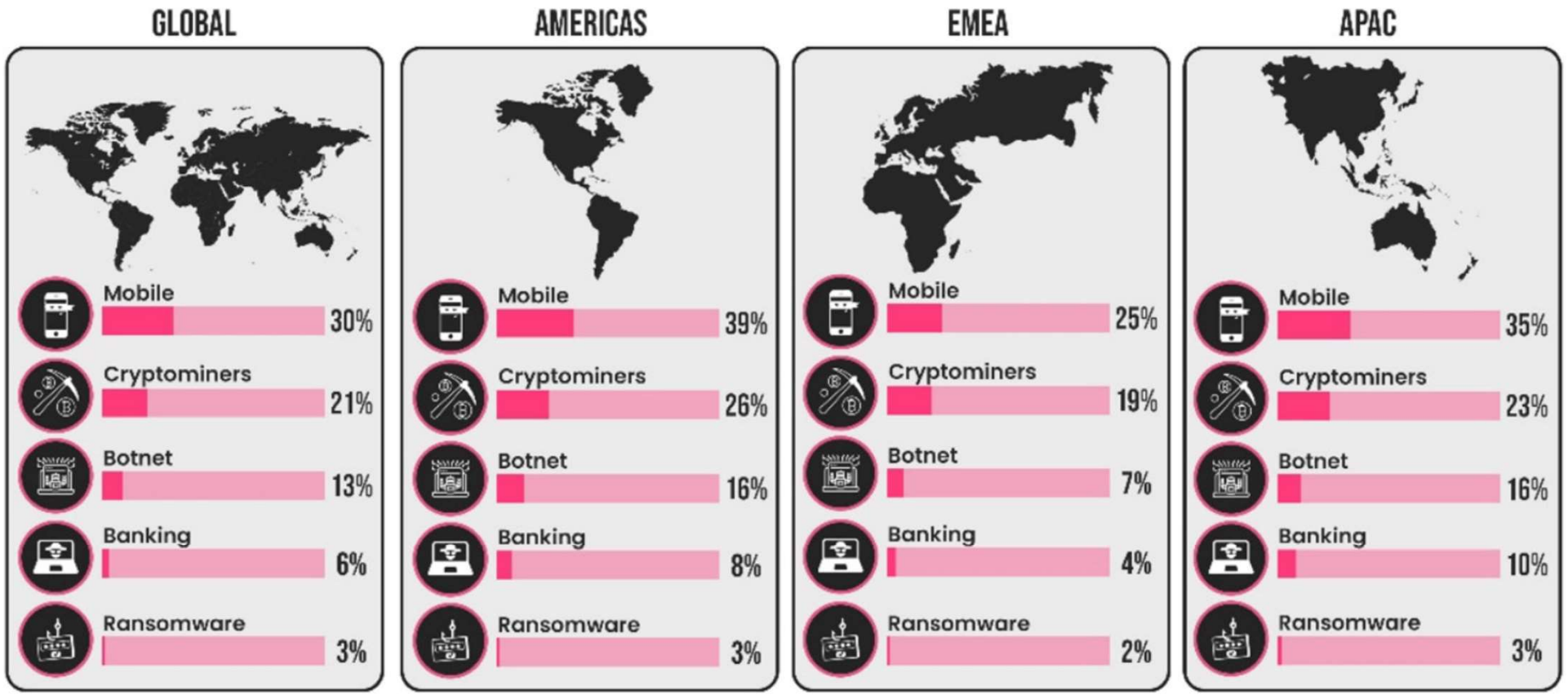
Sharing Implementasi Cyber Security di Perguruan Tinggi

INSTITUT TEKNOLOGI BANDUNG

CYBER ATTACK CATEGORIES BY REGION



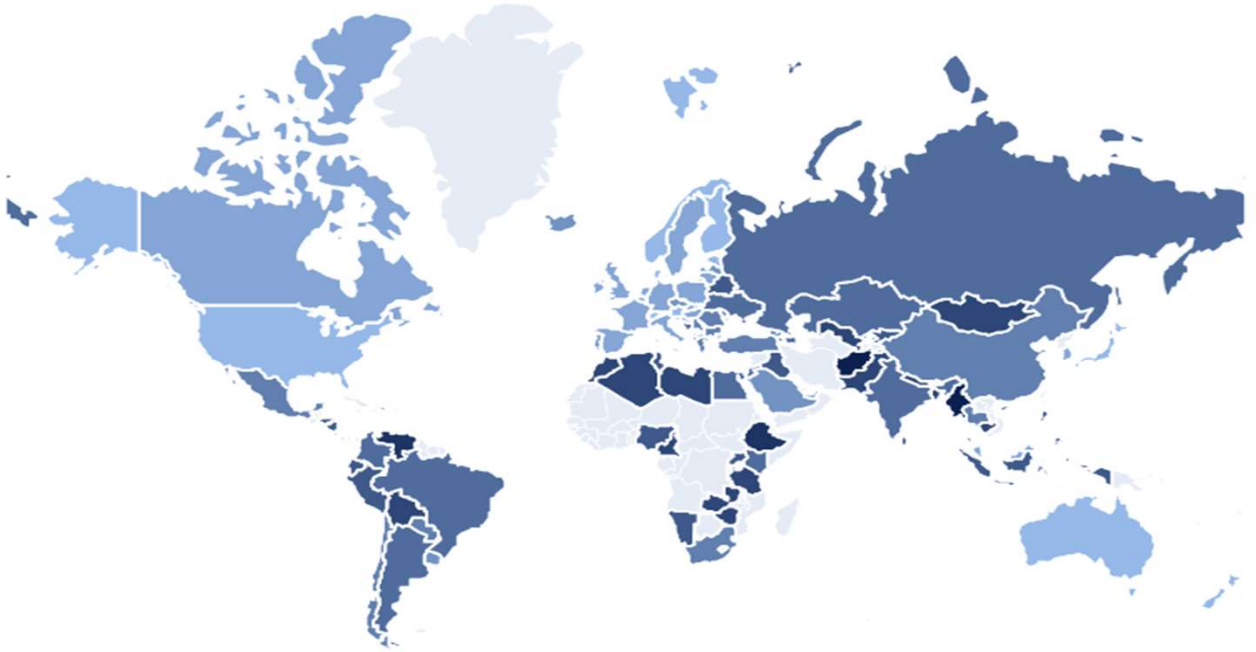
PasswordManagers.co

Global Cybersecurity Exposure Index 2020

From 0 to 1, the Cybersecurity Exposure Index (CEI) calculates the level of exposure to cybercrime by country. The higher the score, the higher the exposure.

Search

Country	Rank	Score
Finland	1	0.110
Denmark	2	0.117
Luxembourg	3	0.124
Australia	4	0.131
Estonia	5	0.134
Norway	5	0.134
Japan	6	0.138
United States	7	0.145
Austria	8	0.162
Switzerland	9	0.172



Exposure Index

Low Exposure — High Exposure

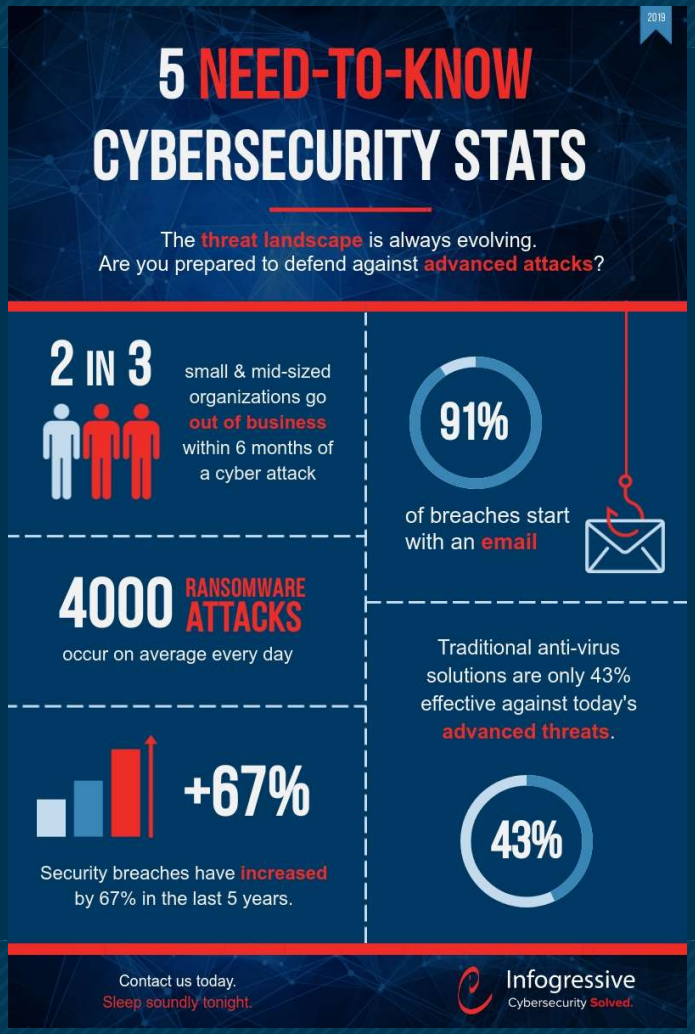
0.0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1.0

Share

made with infogram

Source:PasswordManagers.co

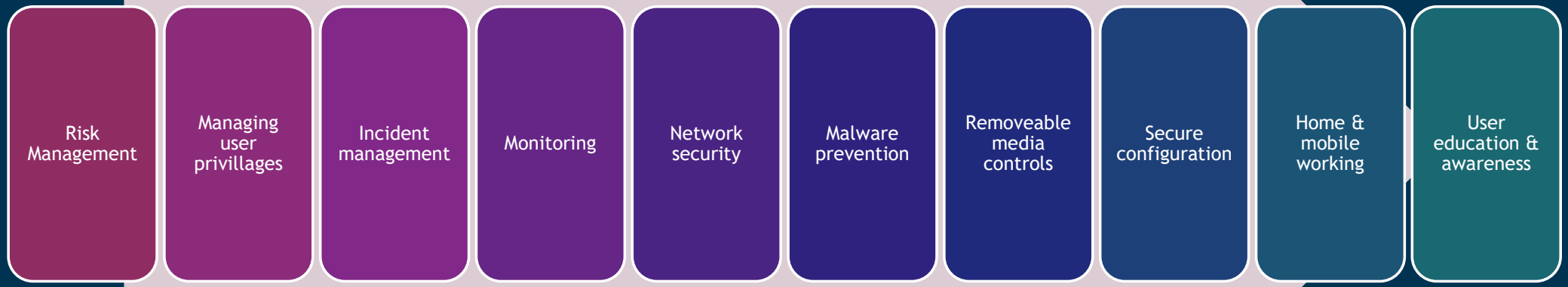
FAKTA DAN DATA TENTANG CYBERSECURITY



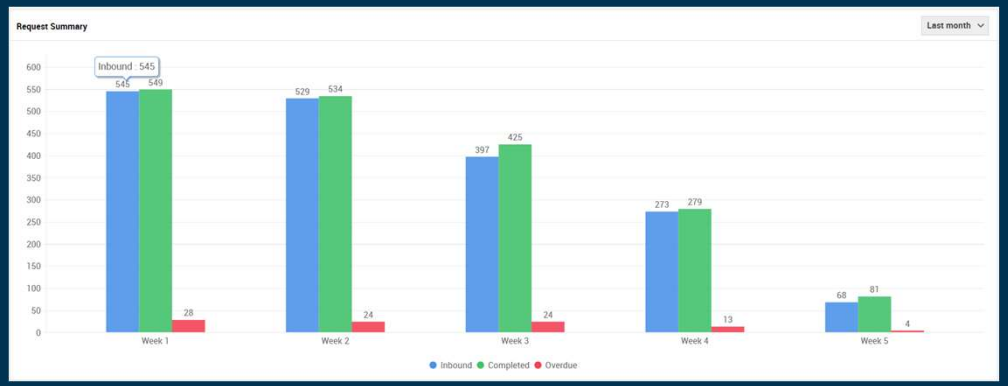
PERUBAHAN PARADIGMA TENTANG CYBERSECURITY

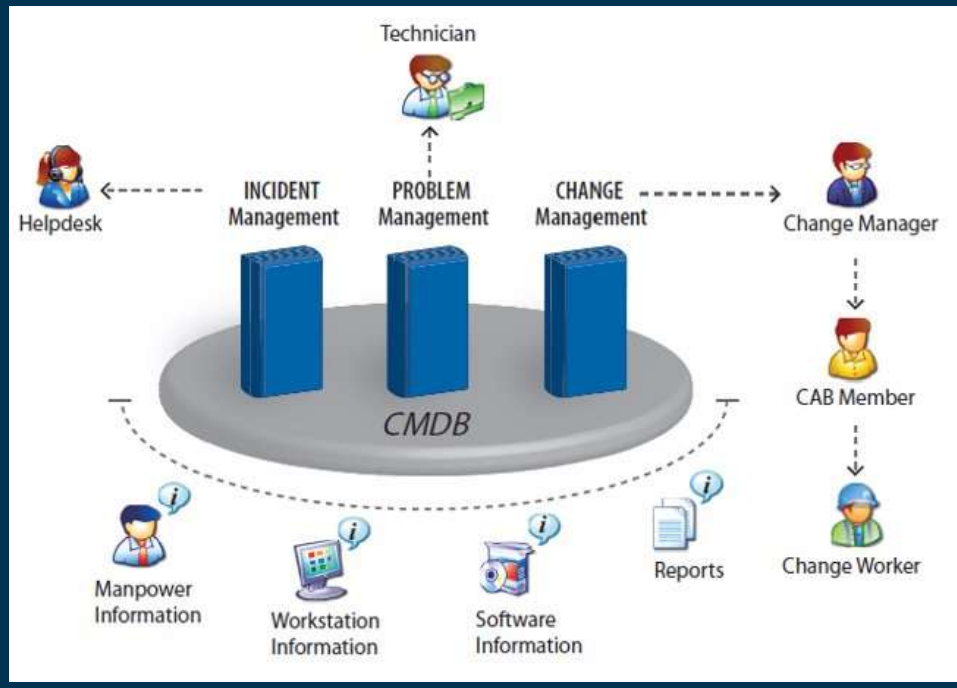
PARADIGMA LAMA		PARADIGMA BARU
Users are employees	→	Employees, partners, customers, bots, things
Corporate managed devices	→	BYOD & IoT
On-premises apps	→	Explosion of cloud apps
Monolithic apps	→	Composite apps & public restful APIs
Corporation network & firewall	→	Perimeter-less
Local packet tracking & logs	→	Explosion of signal

10 Steps to Cyber Security

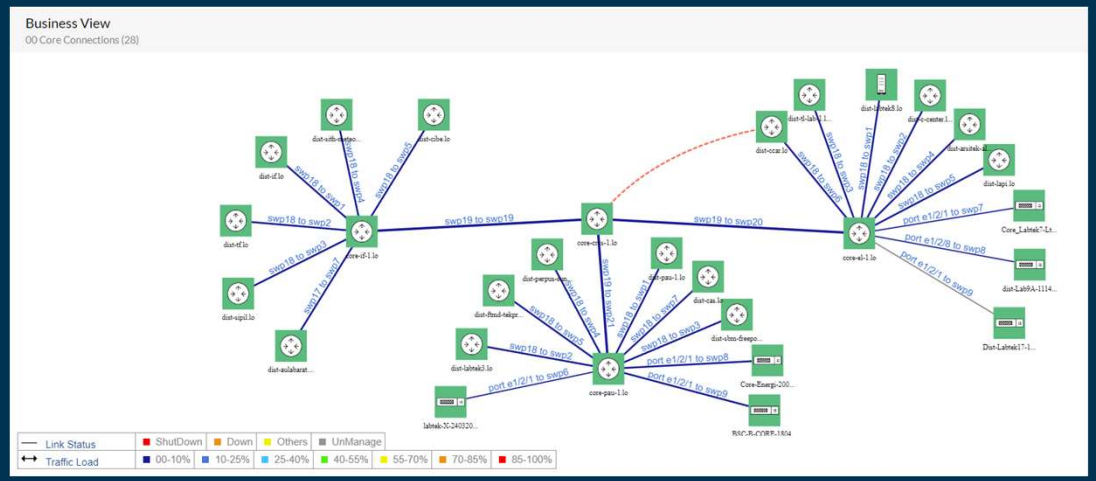


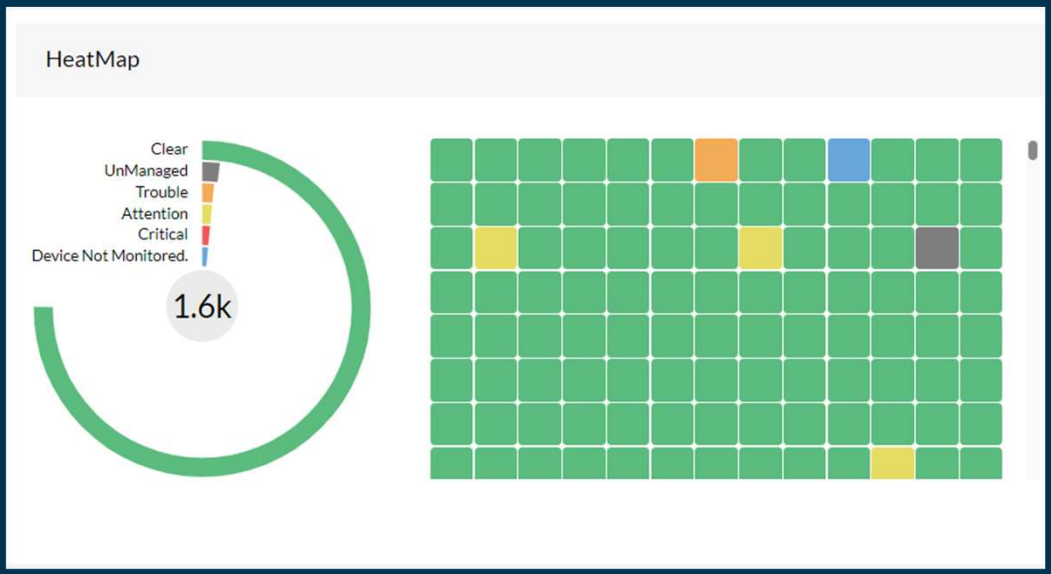
INCIDENT MANAGEMENT SERVICE DESK PLUS

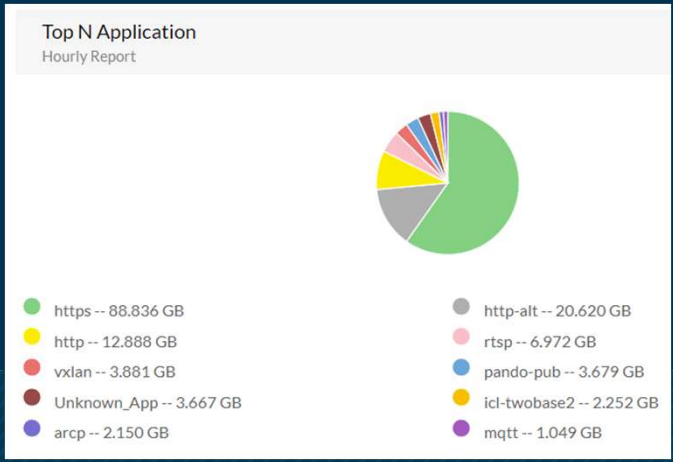




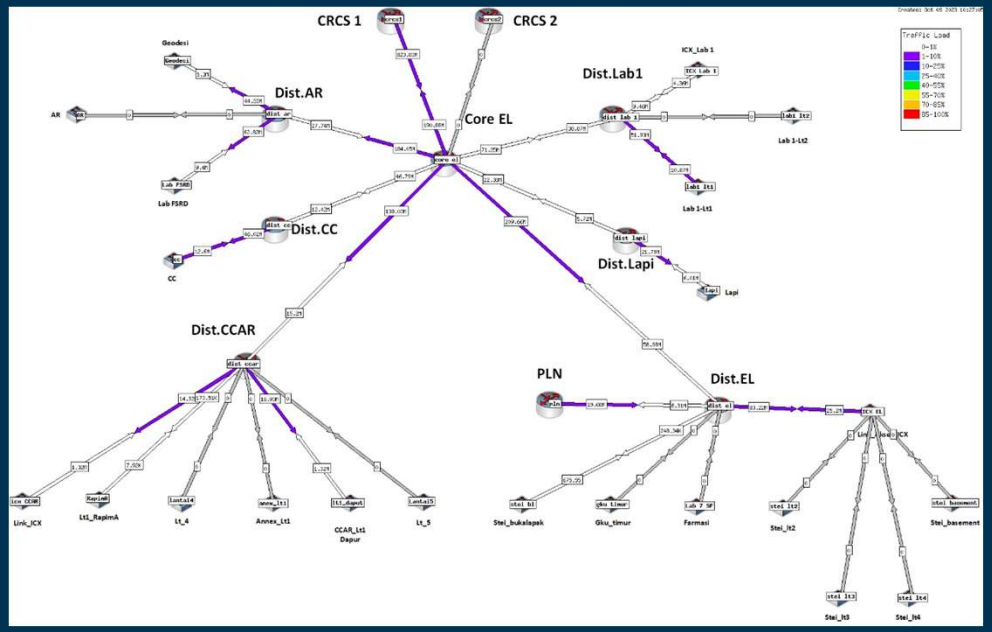
DASHBOARD OPERATIONAL MONITORING







DASHBOARD NETWORK ACTIVITY



Availability Map

Total hosts **up: 353** **warn: 2** **down: 107**

down down up up up up up up up up up
down down up down up down up up up up up
up up down up up up up down down down
down down up down down up up up down up
up up up up down down down down down
down up up up up up up up up up up
up up down up up up up up up up up
up up up up up up up up up up up up
up up up down up up up up up up up down
up up up up up up up up up up up up
up up up up up down up up up up up down
up up up up up up up down down down up
down down down down down down up up up

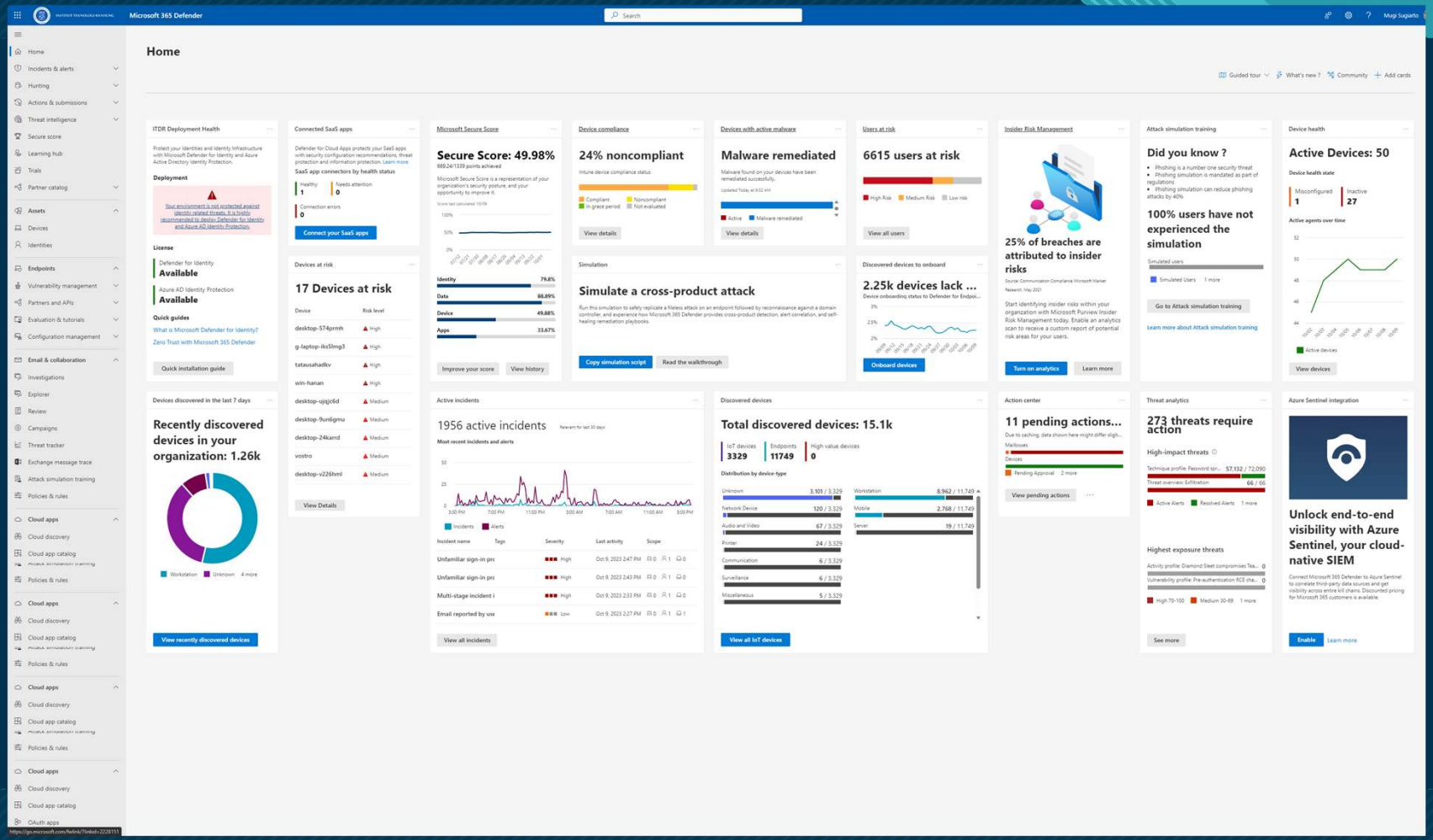
Device Summary

	Total	Up	Down	Ignore tag	Alert disabled	Disabled
Devices	476	355	107	2	11	4
Ports	19939	8293	9291	0	NA	2295
Services	27	22	1	0	NA	3

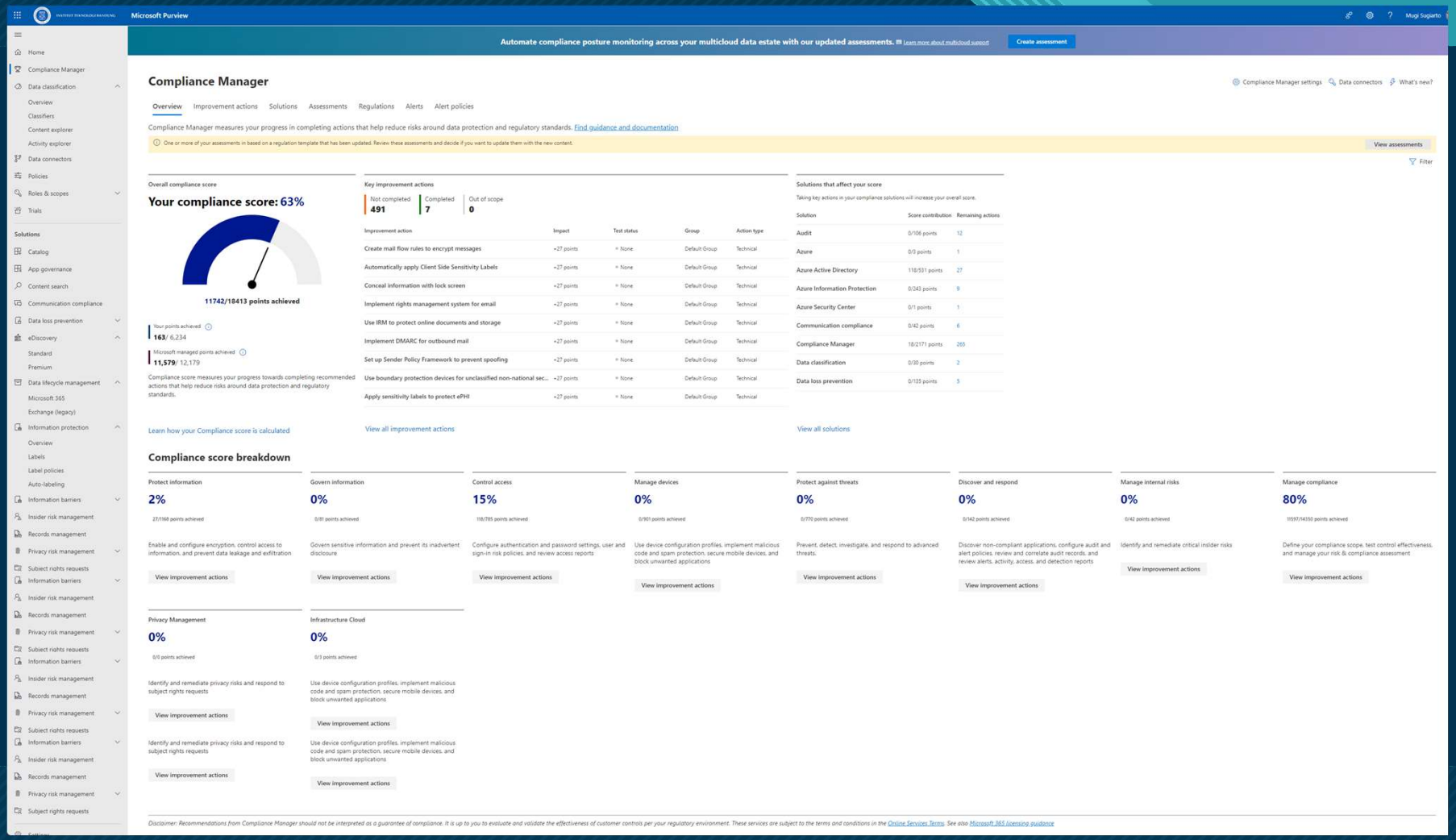
DASHBOARD MONITORING FIREWALL

Name	From Zone	To Zone	Source address	Source User	Destination address	Dynamic User Group	To Port	Application	Action	Severity
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
Wordpress-BruteForce	Zone_Un...	Zone_Trust	146.235.200.145		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
WordPress Login Brute Force Attack	Zone_Un...	Zone_Trust	192.18.130.225		167.205		80	web-browsing	reset-both	critical
XMRig Miner Command and	Zone_Trust	Zone_Un...	10.2.104.119		85.25.2		82	json-rpc	reset-both	critical

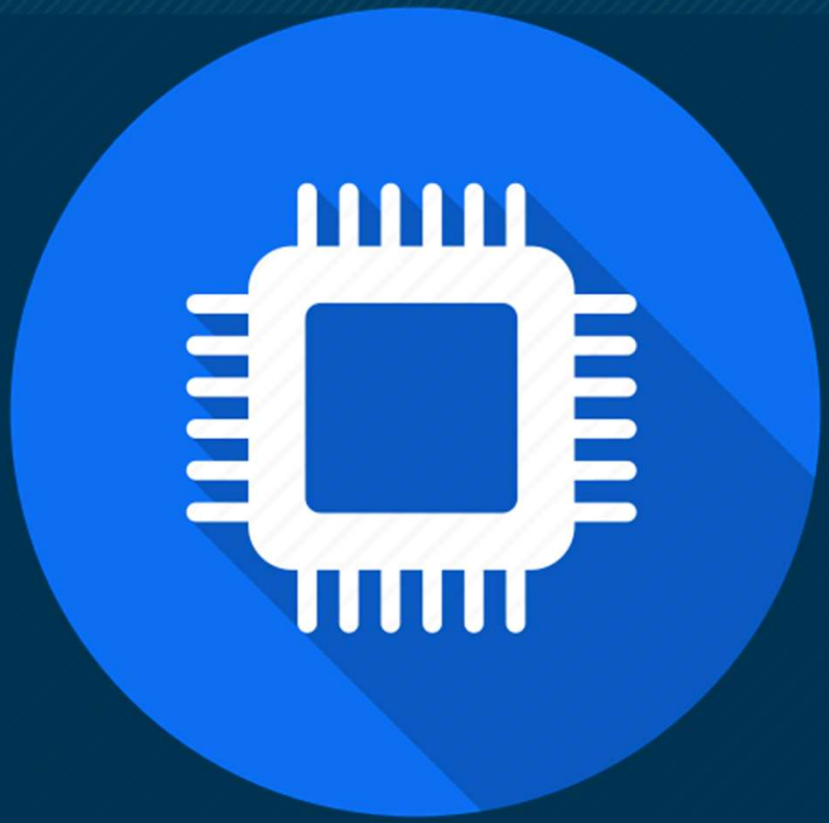
DASHBOARD 365 DEFENDER



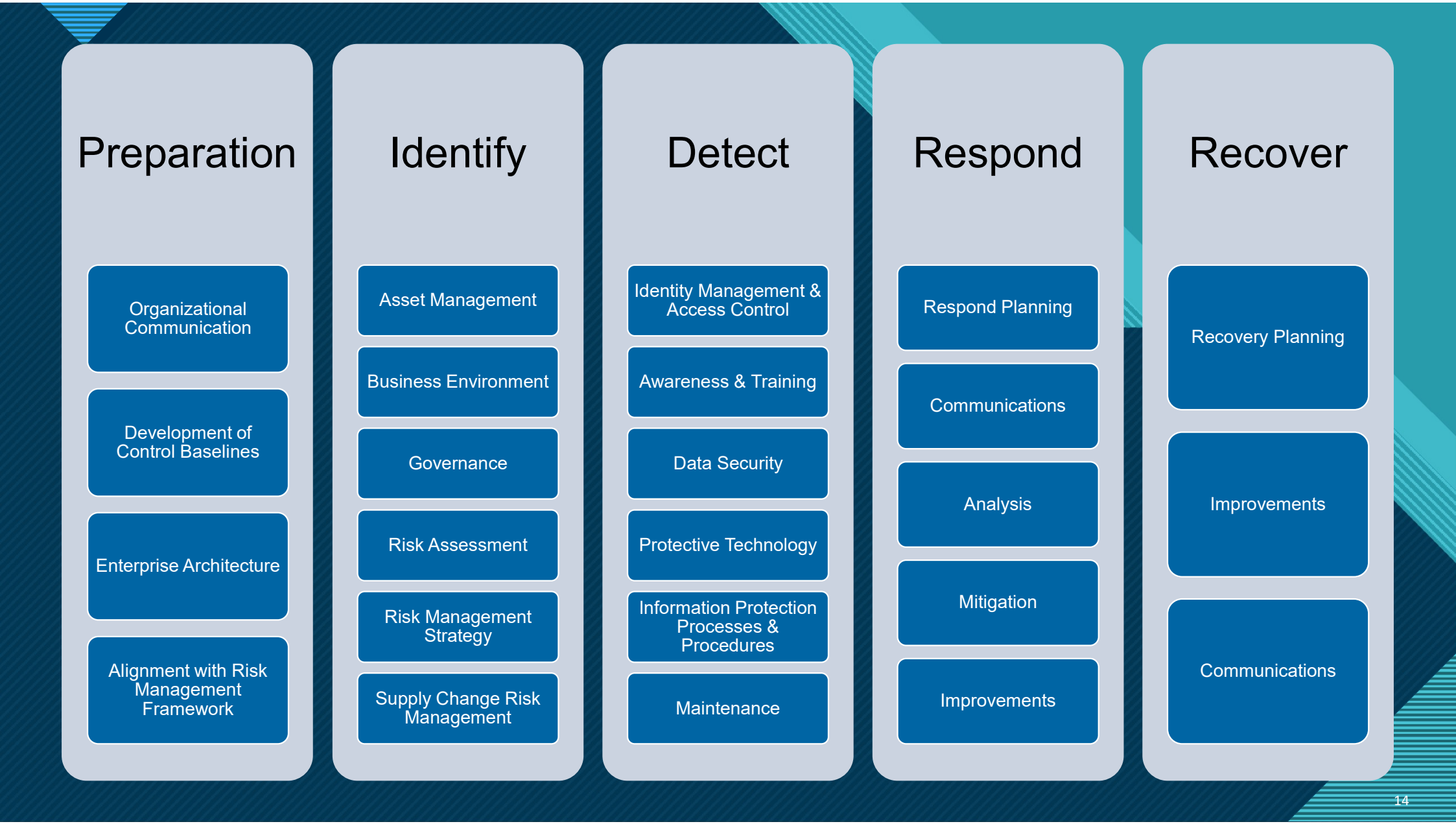
DASHBOARD COMPLIANCE MANAGER



NIST Cybersecurity Framework



- The NIST (US National Institute for Standard and Technology) Cybersecurity Framework is a set of guidelines for mitigating (manage and reduce) organizational cybersecurity risks
- Provides a common language for understanding, managing and expressing cybersecurity risk to internal & external stakeholders
- Can be used to help identify and prioritize actions for reducing cybersecurity risk and it is a tool for aligning policy, business and technological approaches to managing that risk


Preparation
Organizational Communication
Development of Control Baselines
Enterprise Architecture
Alignment with Risk Management Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Supply Change Risk Management
Detect
Identity Management & Access Control
Awareness & Training
Data Security
Protective Technology
Information Protection Processes & Procedures
Maintenance
Respond
Respond Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

Pertanyaan Umum

- *What applications or portals are you users accessing corporate data?*
- *What apps contains business critical data?*
- *Are users leaves, how do you know they don't have corporate data stored on their personal device?*
- *Do users access email their personal cell phone?*
- *Are there business-critical pieces of data that would leave you exposed if a personal device was compromised?*
- *What would be the cost to company if this data was leaked?*
- *Are we compliant if data is leaked to unmanaged applications like a user's personal cloud storage?*
- *Do you want your users to be able to access corporate data securely from anywhere at any time?*
- *Do employees have access to corporate apps after they leave the company? How do you know if they do?*

ITB Cybersecurity Policy

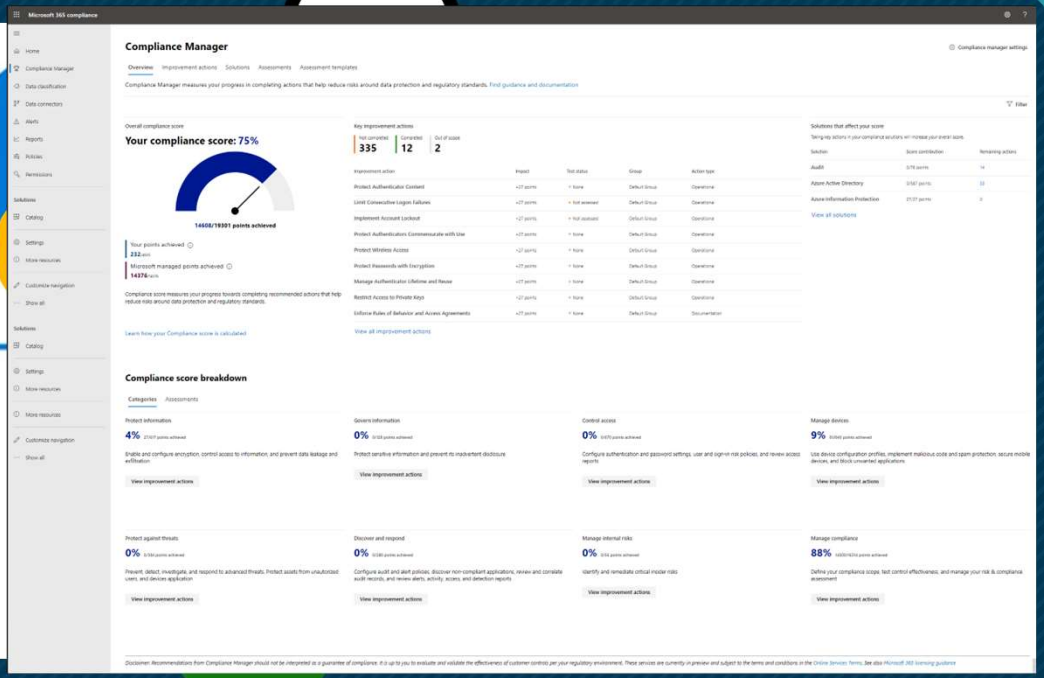
Optimizing Microsoft A3 License

Single Sign ON → Azure Active Directory

Microsoft Outlook Email

Mobile Device Management → INTUNE

Optimizing Windows Defender



KEBIJAKAN KEAMANAN DAN AREA PENGELOLAAN SMKI

- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
- Peraturan Badan Siber dan Sandi Negera Nomor 10 tahun 2020 tentang Tim Tanggap Insiden Siber
- Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik
- Permendikbudristek Nomor 8 Tahun 2022 Tentang SPBE Kemendikbudristek
- Persesjen Kemendikbudristek Nomor 11 Tahun 2022 tentang Sistem Manajemen
- Keamanan Informasi pada SPBE Kemendikbudristek

a. Keamanan personil;

b. Keamanan aset;

c. Keamanan akses;

d. Keamanankriptografi;

e. Keamanan fisik dan lingkungan;

f. Keamanan operasional;

g. Keamanan komunikasi;

h. Keamanan pengembangan dan pemeliharaan;

i. Keamanan pihak ketiga;

j. Manajemen insiden keamanan siber;

k. Manajemen keberlangsungan layanan SPBE Kementerian;

l. Pengendalian kepatuhan; dan

m. Audit keamanan SPBE Kementerian.

TASK EDU CISRT KEMENDIKBUD

- Mencatat insiden keamanan informasi TIK Kemendikbud RI
- Mendokumentasikan insiden keamanan informasi TIK Kemendikbud RI
- Meneruskan insiden keamanan informasi TIK Kemendikbud RI kepada pihak external yang berkompeten
- Memberikan telaah serta memberikan solusi atas insiden keamanan informasi TIK

CHALLENGE

TERIMA KASIH