BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Organisasi

Dalam pelaksanaan kerja magang di PT Panin Dai-ichi Life, ditempatkan dalam divisi *System Ops. and Security* dibawah pimpinan Bapak Ilyas selaku *leader System Operation*, Bapak Aris selaku pembimbing lapangan ditempatkan dalam divisi yang sama. Divisi *System Ops. and Security* bertanggung jawab memastikan sistem bekerja tanpa kendala, serta menyediakan alat yang diperlukan divisi lain, dan juga menjaga keamanan siber.

3.2 Tugas yang Dilakukan

Tugas yang dilakukan selama magang didapatkan dari tim *leader*, pembimbing lapangan, maupun staff PDL. Terdapat tugas harian untuk memeriksa infrastruktur dan jaringan untuk memastikan sistem siap tanpa kendala maupun anomali, tugas yang didapatkan dari staff PDL berupa tugas untuk *restore database* dan permintaan pembukaan *remote access* yang dapat dibuka melalui *firewall*. PDL juga memberikan tugas untuk migrasi *firewall* dari Sophos ke firewall Fortigate dari Fortinet, dan tugas migrasi *Web Application Firewall* sophos ke *Web Application Firewal* Akamai yang sudah berbasis *Cloud*. Pelaksanaan kerja magang diuraikan seperti pada Tabel 3.1.

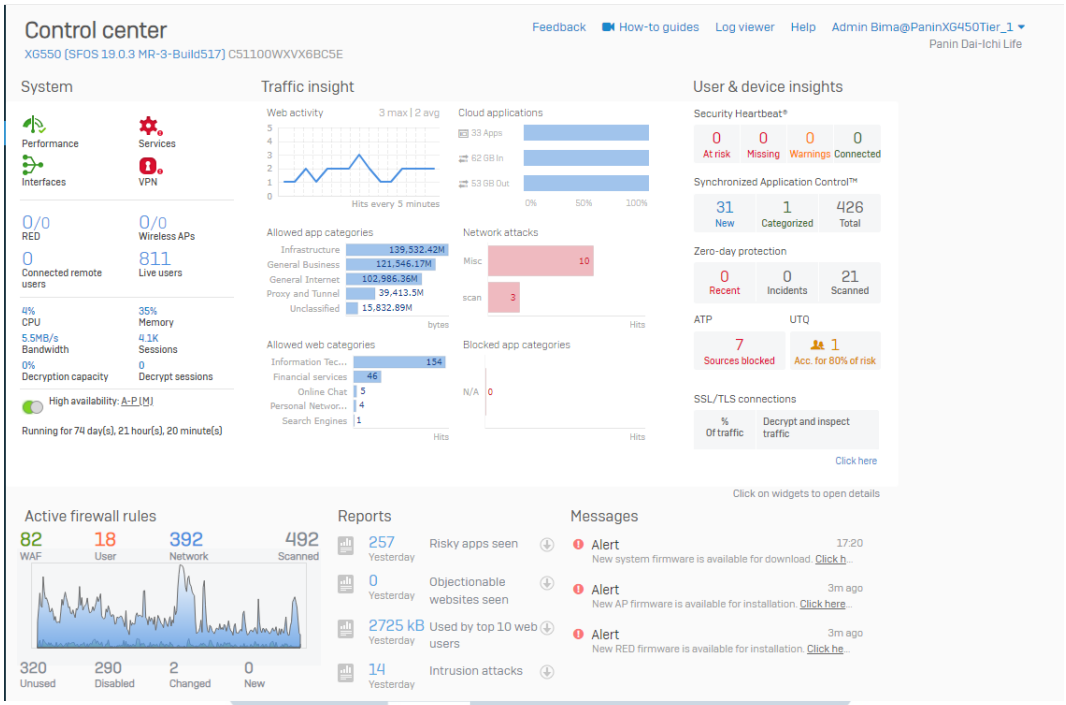
Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

Minggu Ke -	Pekerjaan yang dilakukan
1	Memahami dan mempelajari firewall Sohpos, prosedur daily check, Zabbix.
2	Membuat peta jaringan AP dan Switch pada Zabbix.
3	Membuat list Policies dan NAT Rules Sophos Firewall dan mempelajari Alienvault OSSIM.
4	Melakukan perbaikan dan scanning vulnerability degan Alienvault OSSIM.
5	Melakukan Update Patch,Feed, dan Troubleshooting AlienVault OSSIM.
6	Menyediakan Jaringan Internet untuk acara penting dan menyiapkan VMONE untuk memperbanyak sektor yang di monitoring.
7	Membuat list perangkat yang rentan, dan melakukan restoring database
8-11	Daily Check, Restore Database, and Request Remote Access.
12	Membuat Guide Working Instruction
13	Membuat list OS VM, Install Trelix Agent, Install Antivirus (gunanya agar patching menjadi lebih gampang karena tinggal di kontrol di pusat) dan juga konfigurasi zabbix
14	Set Up configuration fortigate, switch farm ke fortigate, menghubungkan switch farm ke fortigate, setting fortanalyzer license topologi vulnerability report.
15	Security Training, Meeting Akamai
16-20	Migration Phase 1-5

3.3 Uraian Pelaksanaan Magang

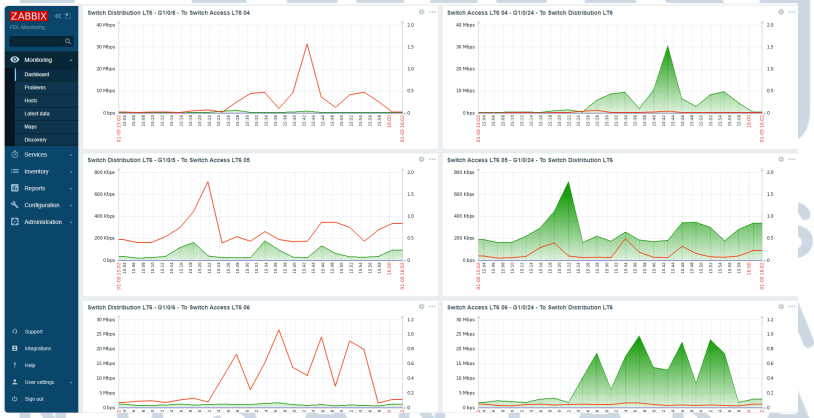
3.3.1 Minggu 1

Pada minggu pertama diperkenalkan dengan beberapa software yang akan dipakai seperti firewall sophos dan zabbix, serta diberikan pekerjaan harian untuk cek kesediaan sistem, kemudian diberikan tugas untuk list semua rules and policy yang ada pada firewall sophos.



Gambar 3.1. Firewall Sophos

Sophos adalah perangkat firewall yang dipakai PT Panin Dai-ichi Life untuk melindungi jaringan dari ancaman siber seperti malware, ransomware, bot, dan peretasan. Firewall Sophos dapat mengontrol dan memantau lalu lintas data yang masuk dan keluar dari jaringan perusahaan. Firewall Sophos juga melindungi data sensitif dari kebocoran serta mampu mendekripsi dan memeriksa lalu lintas TLS/SSL untuk mencegah kebocoran data.

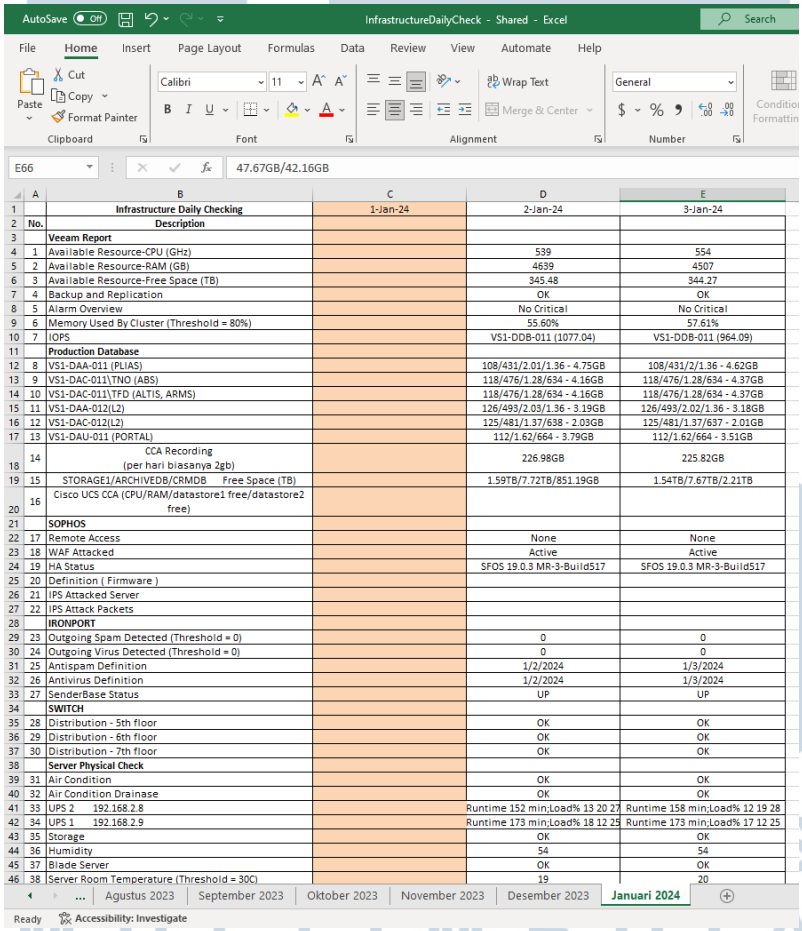


Gambar 3.2. Zabbix

Zabbix adalah software open source yang dipakai PT Panin Dai-ichi Life untuk memantau kinerja jaringan, server, aplikasi, dan layanan IT secara real

time. Zabbix dapat memberikan peringatan dini jika terdeteksi masalah pada jaringan untuk kemudian dapat ditangani ITSO. Zabbix dapat mengumpulkan data historis kinerja untuk analisis tren, data metrik yang dikumpulkan dapat divisualisasikan kedalam bentuk grafik maupun laporan untuk membantu dalam mengambil keputusan.

Pada minggu ini juga diberikan panduan kerja untuk melakukan daily checking atau pemeriksaan infrastruktur yang akan menjadi tugas harian selama pelaksanaan magang. Daily Checking ini meliputi pemeriksaan Veeam, Production Database, Firewall, Cisco Ironport, Swich, Server Physical Check, CCTV, OpenText Services, dan Cloud Services.



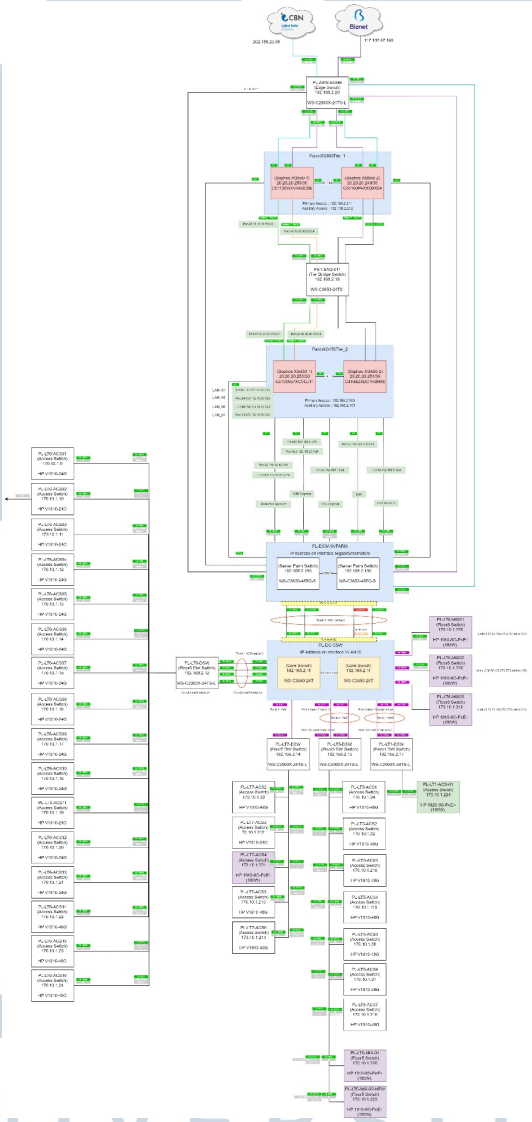
No.	Description	1-Jan-24	2-Jan-24	3-Jan-24
	Infrastructure Daily Checking			
	Veeam Report			
1	Available Resource-CPU (GHz)		539	554
2	Available Resource-RAM (GB)		4639	4507
3	Available Resource-Free Space (TB)		345.48	344.27
4	Backup and Replication		OK	OK
5	Alarm Overview		No Critical	No Critical
6	Memory Used By Cluster (Threshold = 80%)		55.60%	57.61%
7	IOPS		VS1-DDB-011 (1077.04)	VS1-DDB-011 (964.09)
	Production Database			
8	VS1-DAA-011 (PLIAS)		108/431/2.01/1.36 - 4.75GB	108/431/2/1.36 - 4.62GB
9	VS1-DAC-011\TNO (ABS)		118/476/1.28/634 - 4.16GB	118/476/1.28/634 - 4.37GB
10	VS1-DAC-011\TFD (ALTIS, ARMS)		118/476/1.28/634 - 4.16GB	118/476/1.28/634 - 4.37GB
11	VS1-DAA-012(L2)		126/493/2.03/1.36 - 3.19GB	126/493/2.02/1.36 - 3.18GB
12	VS1-DAC-012(L2)		125/481/1.37/638 - 2.03GB	125/481/1.37/637 - 2.01GB
13	VS1-DAU-011 (PORTAL)		112/1.62/664 - 3.79GB	112/1.62/664 - 3.51GB
14	CCA Recording (per hari biasanya 2gb)		226.98GB	225.82GB
15	STORAGE1/ARCHIVEDB/CRMDB Free Space (TB)		1.59TB/7.72TB/851.19GB	1.54TB/7.67TB/2.21TB
16	Cisco UCS CCA (CPU/RAM/datastore1 free/datastore2 free)			
	SOPHOS			
17	Remote Access		None	None
18	WAF Attacked		Active	Active
19	HA Status		SFOS 19.0.3 MR-3-Build517	SFOS 19.0.3 MR-3-Build517
20	Definition (Firmware)			
21	IPS Attacked Server			
22	IPS Attack Packets			
	IRONPORT			
23	Outgoing Spam Detected (Threshold = 0)		0	0
24	Outgoing Virus Detected (Threshold = 0)		0	0
25	Antispam Definition		1/2/2024	1/3/2024
26	Antivirus Definition		1/2/2024	1/3/2024
27	SenderBase Status		UP	UP
	SWITCH			
28	Distribution - 5th floor		OK	OK
29	Distribution - 6th floor		OK	OK
30	Distribution - 7th floor		OK	OK
	Server Physical Check			
31	Air Condition		OK	OK
32	Air Condition Drainase		OK	OK
33	UPS 2 192.168.2.8		Runtime 152 min;Load% 13 20 27	Runtime 158 min;Load% 12 19 28
34	UPS 1 192.168.2.9		Runtime 173 min;Load% 18 12 25	Runtime 173 min;Load% 17 12 25
35	Storage		OK	OK
36	Humidity		54	54
37	Blade Server		OK	OK
38	Server Room Temperature (Threshold = 30C)		19	20

Gambar 3.3. Infrastructure Daily Check

3.3.2 Minggu 2

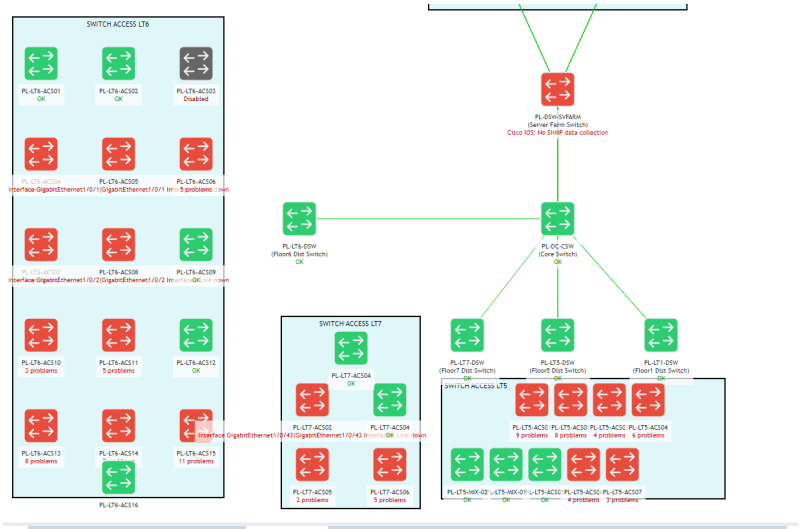
Pada minggu ini terdapat tugas membuat peta jaringan AP dan Switch Panin Dai-ichi Life dan mengintegrasikan pada software zabbix untuk dapat lebih mudah

memantau jaringan, hal ini dilakukan karena PDL sendiri belum memiliki gambaran topologi yang lengkap dan jika ada perangkat yang bermasalah akan sulit mencari tahu perangkat mana yang bermasalah, kemudian melanjutkan list policy firewall sophos.



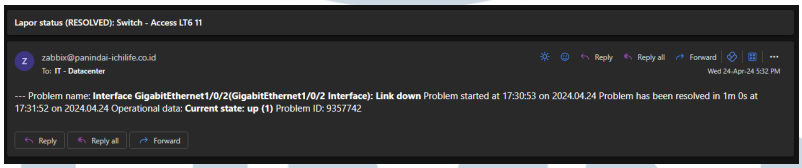
Gambar 3.4. Topologi Jaringan PT Panin Dai-ichi Life

Topologi jaringan pdl ini baru dibuat pada bulan Desember 2024 dan belum mencakup keseluruhan jaringan yang ada pada PDL. Peta topologi jaringan membantu memvisualisasikan struktur fisik atau logis dari sebuah jaringan komputer, gambar peta topologi menunjukan bagaimana perangkat-perangkat seperti komputer, router, switch, dll terhubung satu sama lain.



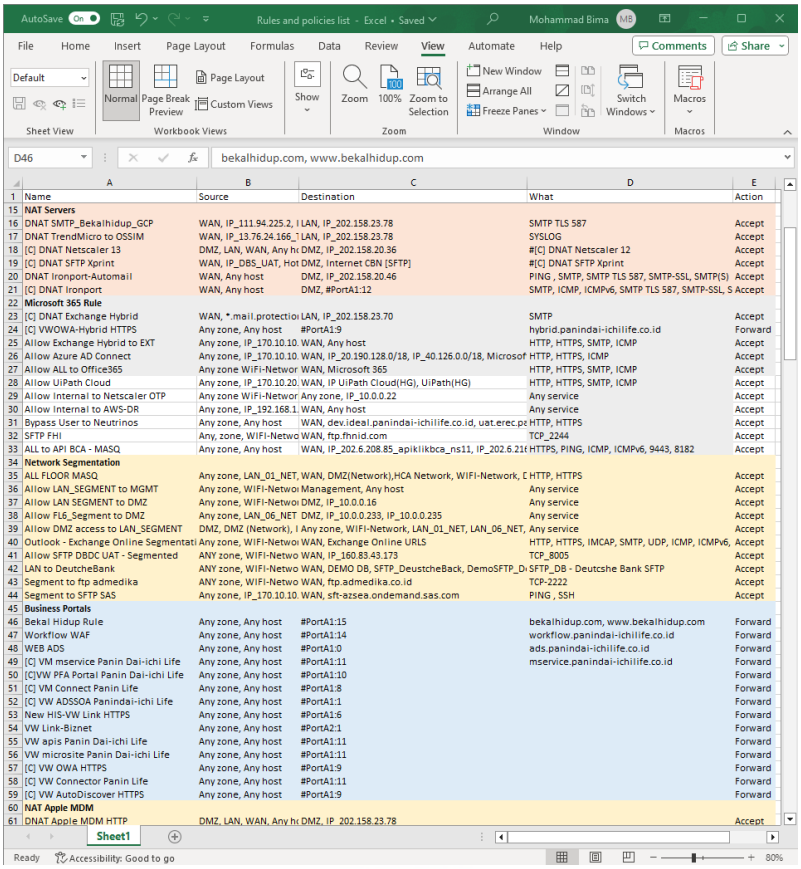
Gambar 3.5. zabbix network map

Dengan mengintegrasikan topologi pada Zabbix, ITSO dapat lebih mudah mendeteksi masalah atau gangguang pada infrastruktur jaringan PDL. Hal ini lebih optimal dan menghemat waktu dengan memanfaatkan fitur deteksi yang ada pada Zabbix.



Gambar 3.6. Laporan status zabbix melalui Email

Setelah itu terdapat tugs yang masih perlu diselesaikan, yaitu membuat list rules and policy pada firewall sophos, tujuan dari pembuatan list rules and policy ini adalah untuk mengetahui rules and policy mana yang aktif maupun tidak aktif, yang sering terpakai maupun jarang terpakai, yang kemudian list ini akan dipakai saat migrasi firewall sophos ke firewall fortigate.

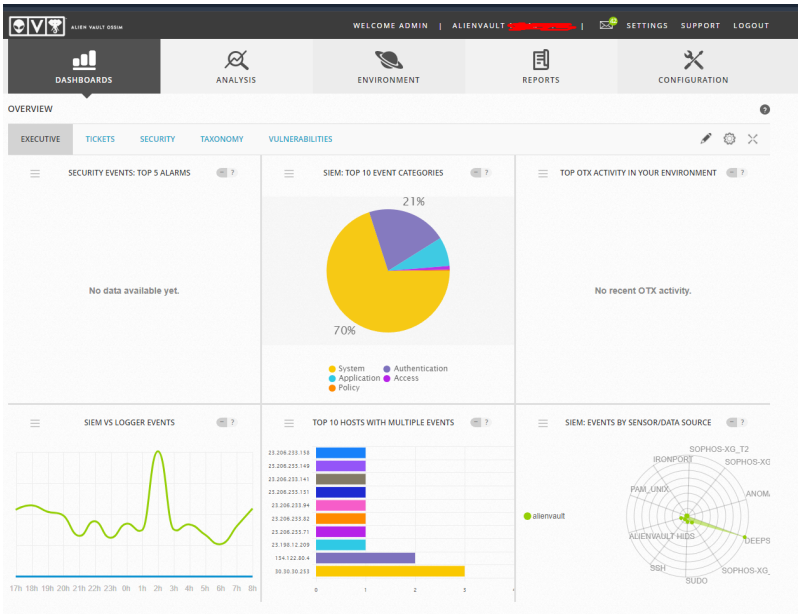


	Name	Source	Destination	What	Action
15	**NAT Servers**				
16	DNAT SMTP_Bekalhidup_GCP	WAN, IP_111.94.225.2, I	LAN, IP_202.158.23.78	SMTP TLS 587	Accept
17	DNAT TrendMicro to OSSIM	WAN, IP_13.76.24.166_1	LAN, IP_202.158.23.78	SYSLOG	Accept
18	[C] DNAT Netscaler 13	DMZ, LAN, WAN, Any h	DMZ, IP_202.158.20.36	#[C] DNAT Netscaler 12	Accept
19	[C] DNAT SFTP Xprint	WAN, IP_DBS_UAT, Hos	DMZ, Internet CBN [SFTP]	#[C] DNAT SFTP Xprint	Accept
20	DNAT Ironport-Automail	WAN, Any host	DMZ, IP_202.158.20.46	PING , SMTP, SMTP TLS 587, SMTP-SSL, SMTP(S)	Accept
21	[C] DNAT Ironport	WAN, Any host	DMZ, #PortA1:12	SMTP, ICMP, ICMPv6, SMTP TLS 587, SMTP-SSL, S	Accept
22	**Microsoft 365 Rule**				
23	[C] DNAT Exchange Hybrid	WAN, *.mail.protectio	LAN, IP_202.158.23.70	SMTP	Accept
24	[C] VWOWA-Hybrid HTTPS	Any zone, Any host	#PortA1:9	hybrid.panindai-ichilife.co.id	Forward
25	Allow Exchange Hybrid to EXT	Any zone, IP_170.10.10.	WAN, Any host	HTTP, HTTPS, SMTP, ICMP	Accept
26	Allow Azure AD Connect	Any zone, IP_170.10.10.	WAN, IP_20.190.128.0/18, IP_40.126.0.0/18, Microsof	HTTP, HTTPS, ICMP	Accept
27	Allow ALL to Office365	Any zone WiFi-Networ	WAN, Microsoft 365	HTTP, HTTPS, SMTP, ICMP	Accept
28	Allow UiPath Cloud	Any zone, IP_170.10.20.	WAN, IP UiPath Cloud(HG), UiPath(HG)	HTTP, HTTPS, SMTP, ICMP	Accept
29	Allow Internal to Netscaler OTP	Any zone WiFi-Networ	Any zone, IP_10.0.0.22	Any service	Accept
30	Allow Internal to AWS-DR	Any zone, IP_192.168.1.	WAN, Any host	Any service	Accept
31	Bypass User to Neutrinos	Any zone, Any host	WAN, dev.ideal.panindai-ichilife.co.id, uat.erec.pa	HTTP, HTTPS	Accept
32	SFTP FHI	Any, zone, WiFI-Netwo	WAN, ftp.fhnid.com	TCP_2244	Accept
33	ALL to API BCA - MASQ	Any zone, Any host	WAN, IP_202.6.208.85_apiklikbca_ns11, IP_202.6.21	HTTPS, PING, ICMP, ICMPv6, 9443, 8182	Accept
34	**Network Segmentation**				
35	ALL FLOOR MASQ	Any zone, LAN_01_NET,	WAN, DMZ(Network),HCA Network, WIFI-Network, L	HTTP, HTTPS	Accept
36	Allow LAN_SEGMENT to MGMT	Any zone, WIFI-Networ	Management, Any host	Any service	Accept
37	Allow LAN SEGMENT to DMZ	Any zone, WIFI-Networ	DMZ, IP_10.0.0.16	Any service	Accept
38	Allow FL6_Segment to DMZ	Any zone, LAN_06_NET	DMZ, IP_10.0.0.233, IP_10.0.0.235	Any service	Accept
39	Allow DMZ access to LAN_SEGMENT	DMZ, DMZ (Network), I	Any zone, WIFI-Network, LAN_01_NET, LAN_06_NET,	Any service	Accept
40	Outlook - Exchange Online Segmentati	Any zone, WIFI-Networ	WAN, Exchange Online URLS	HTTP, HTTPS, IMCAP, SMTP, UDP, ICMP, ICMPv6,	Accept
41	Allow SFTP DBDC UAT - Segmented	ANY zone, WIFI-Networ	WAN, IP_160.83.43.173	TCP_8005	Accept
42	LAN to DeutcheBank	ANY zone, WIFI-Networ	WAN, DEMO DB, SFTP_DeustcheBack, DemoSFTP_D	SFTP_DB - Deutcshe Bank SFTP	Accept
43	Segment to ftp admedika	ANY zone, WIFI-Networ	WAN, ftp.admedika.co.id	TCP-2222	Accept
44	Segment to SFTP SAS	Any zone, IP_170.10.10.	WAN, sft-azsea.ondemand.sas.com	PING , SSH	Accept
45	**Business Portals**				
46	Bekal Hidup Rule	Any zone, Any host	#PortA1:15	bekalhidup.com, www.bekalhidup.com	Forward
47	Workflow WAF	Any zone, Any host	#PortA1:14	workflow.panindai-ichilife.co.id	Forward
48	WEB ADS	Any zone, Any host	#PortA1:0	ads.panindai-ichilife.co.id	Forward
49	[C] VM mservice Panin Dai-ichi Life	Any zone, Any host	#PortA1:11	mservice.panindai-ichilife.co.id	Forward
50	[C]VW PFA Portal Panin Dai-ichi Life	Any zone, Any host	#PortA1:10		Forward
51	[C] VM Connect Panin Life	Any zone, Any host	#PortA1:8		Forward
52	[C] VW ADSSOA Panindai-ichi Life	Any zone, Any host	#PortA1:1		Forward
53	New HIS-VW Link HTTPS	Any zone, Any host	#PortA1:6		Forward
54	VW Link-Biznet	Any zone, Any host	#PortA2:1		Forward
55	VW apis Panin Dai-ichi Life	Any zone, Any host	#PortA1:11		Forward
56	VW microsite Panin Dai-ichi Life	Any zone, Any host	#PortA1:11		Forward
57	[C] VW OWA HTTPS	Any zone, Any host	#PortA1:9		Forward
58	[C] VW Connector Panin Life	Any zone, Any host	#PortA1:11		Forward
59	[C] VW AutoDiscover HTTPS	Any zone, Any host	#PortA1:9		Forward
60	**NAT Apple MDM**				
61	DNAT Apple MDM HTTP	DMZ, LAN, WAN, Any h	DMZ, IP_202.158.23.78		Accept

Gambar 3.7. List Rules and Policy

3.3.3 Minggu 3

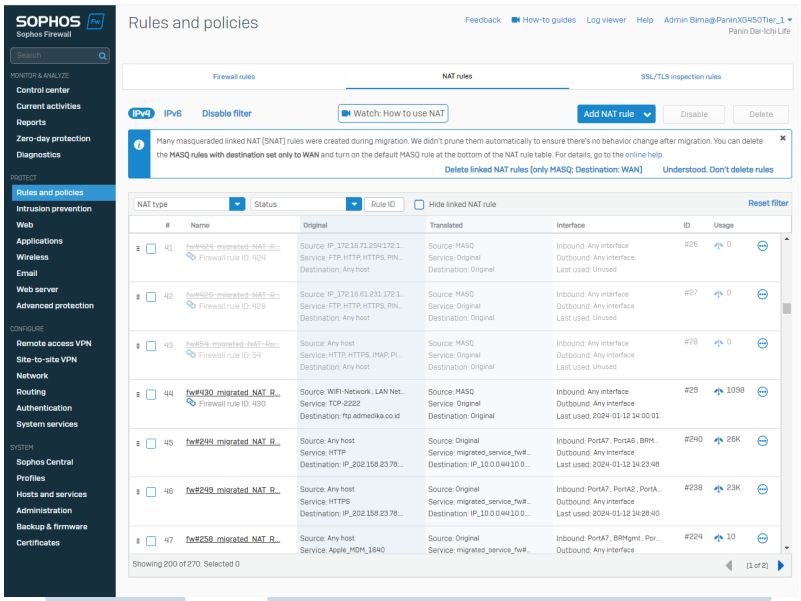
Pada minggu ketiga diperkenalkan dengan Alienvault OSSIM, kemudian mempelajari Alienvault OSSIM dan juga membuat list NAT rules yang ada di sophos firewall.



Gambar 3.8. OSSIM Dashboard

Alienvault OSSIM (Open Source Security Information and Event Management) adalah sebuah sistem keamanan yang berbasis open source yang digunakan untuk mengelola dan menganalisis log keamanan dari berbagai sumber, seperti sistem operasional, aplikasi, dan perangkat keras. OSSIM berfungsi sebagai sistem keamanan yang dapat mendeteksi, mengidentifikasi, dan mengatasi ancaman keamanan yang terjadi pada sistem operasional perusahaan[3] . AlienVault OSSIM digunakan untuk:

1. Monitoring Keamanan
2. Analisis Keamanan
3. Pengawasan Kualitas Sistem
4. Pengawasan Kompabilitas Sistem

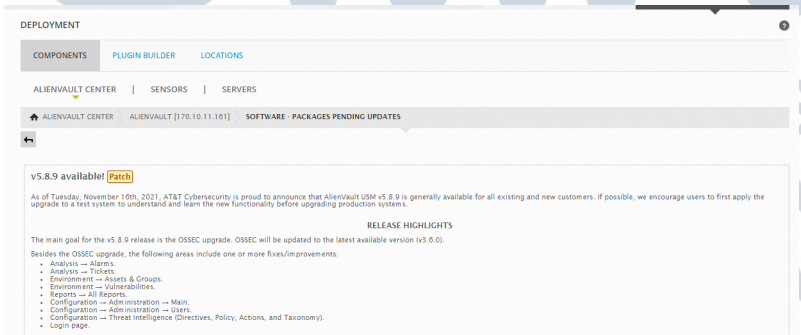


Gambar 3.9. NAT Rules Sophos Firewall

Setelah cukup mempelajari AlienVault OSSIM, terdapat tugas untuk membuat list NAT rules yang terdapat pada firewall Sophos, tujuan dari membuat list NAT rules ini sama dengan tujuan pembuatan list rules and policy.

3.3.4 Minggu 4

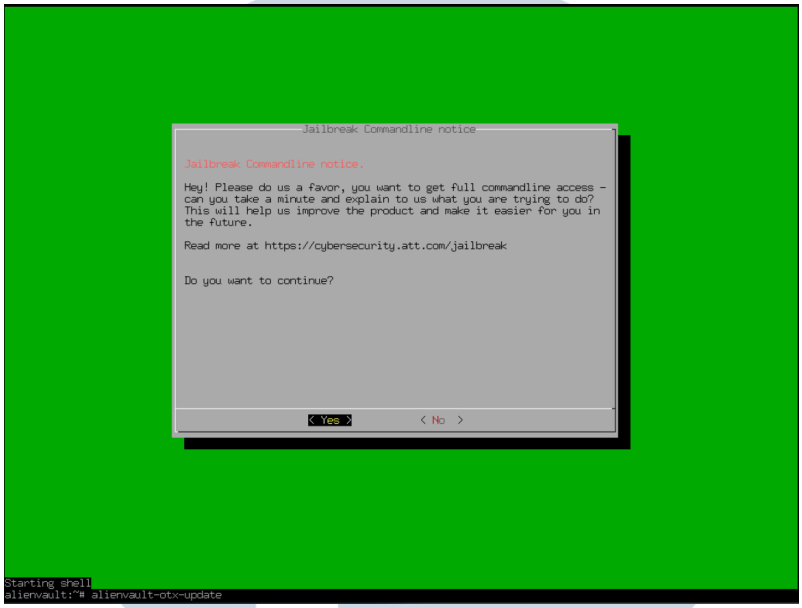
Pada minggu ini tugas yang dilakukan adalah melakukan pembaruan versi dan perbaikan pada Alienvault OSSIM karena PDL tidak pernah melakukan update maupun scanning sejak 2021, setelah memperbaiki dan memperbarui versi dari Alienvault OSSIM, kemudain melakukan scan kerentanan pada Alienvault OSSIM dan menemukan banyak kerentanan.



Gambar 3.10. Software Update Alienvault

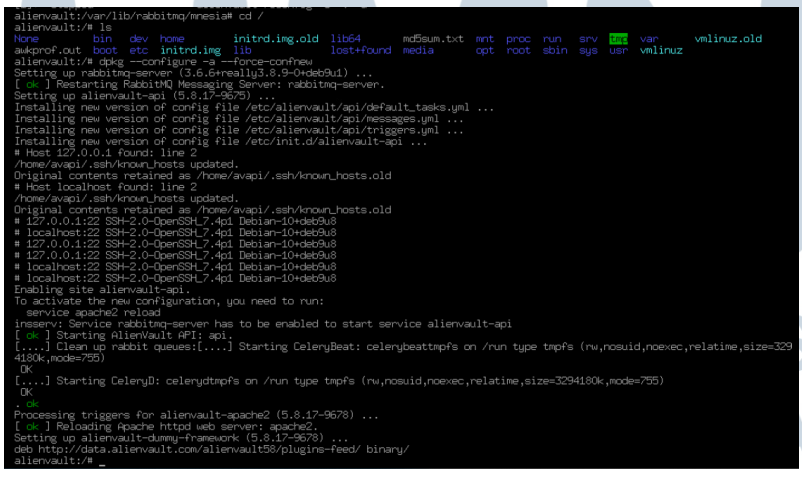
Alienvault yang digunakan oleh PDL adalah versi v5.8.5 dan terdapat update

versi v5.8.9 yang rilis pada 16 November 2021, sementara versi terbaru pada saat magang adalah versi v5.8.17 yang dirilis pada 14 november 2023.



Gambar 3.11. Alienvault Jailbreaking

Update Alienvault dapat dilakukan melalui *command shell* yang dapat diakses dengan melakukan *jailbreaking* pada OS Alienvault OSSIM yang ada pada *virtual machine*.



Gambar 3.12. *shell command Alienvault*

Jalankan command alienvault-update -c -v -d untuk melakukan update Alienvault OSSIM, command ini akan menjalankan update ke versi yang tersedia.

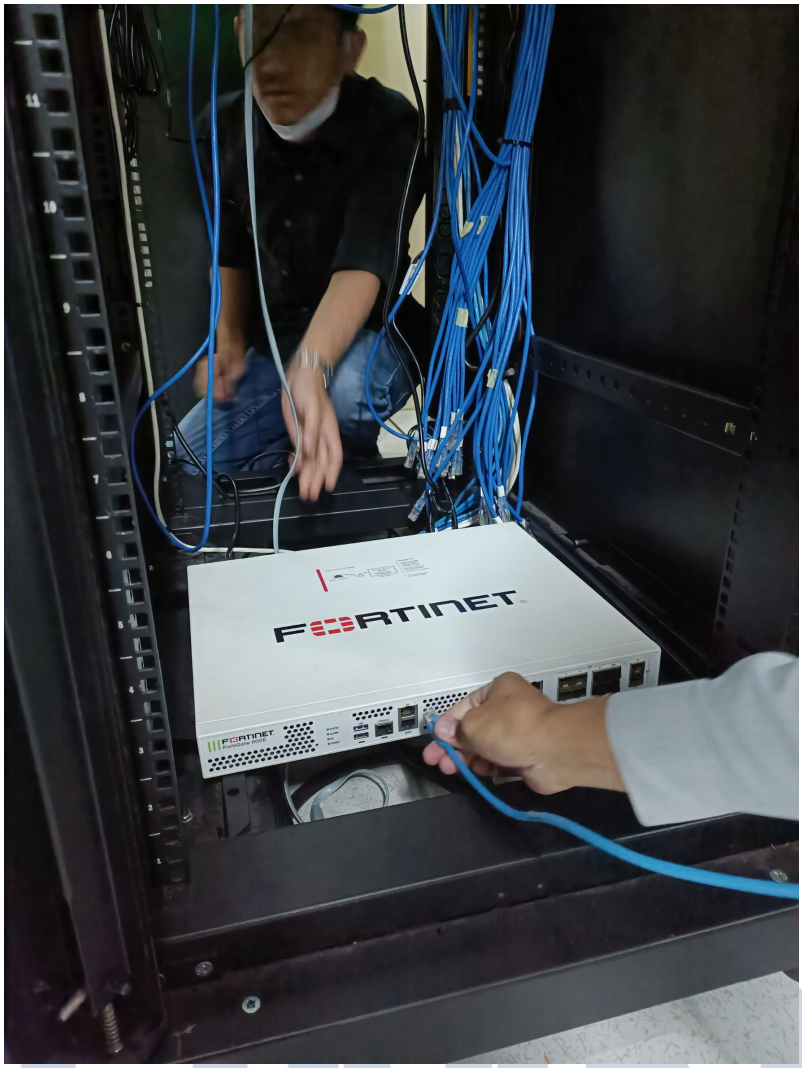
3.3.5 Minggu 5-13

Pada minggu 5 hingga 13 tugas yang dilakukan adalah sebagai berikut:

- Melakukan *Daily Checking*
- Tim ITSO menyediakan jaringan internet untuk acara penting dari perusahaan, serta menyiapkan VMONE untuk memperbanyak sistem yang dapat dilakukan pemeriksaan berkala.
- Membuat list perangkat-perangkat yang memiliki kerentanan di perusahaan, kemudian melakukan restore database yang diminta.
- Membuat panduan petunjuk kerja agar karyawan baru dapat dengan mudah mengerjakan pekerjaanya.
- Membuat daftar VM yang ada di Panin Dai-ichi Life yang kemudian akan diinstall Trelix Agent yang akan mempermudah untuk Panin Dai-ichi Life dalam melakukan perbaikan kerentanan, seperti install antivirus secara masal.

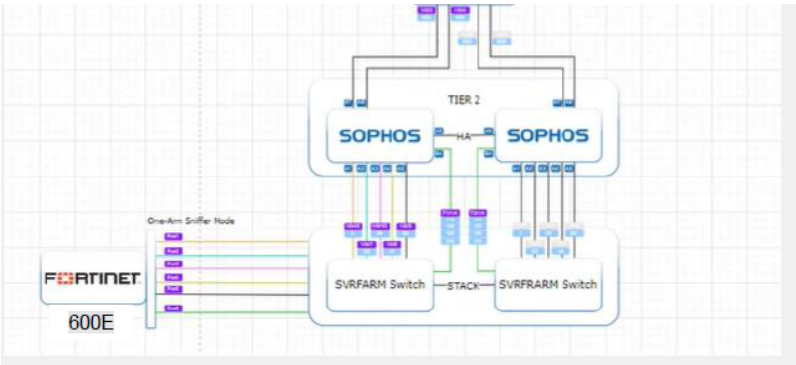
3.3.6 Minggu 14

Panin dai-ichi Life merencanakan akan melakukan migrasi firewall sohpos ke firewall lain. Kemudian tim ITSO melakukan uji coba bertahap dengan fortigate dari fortinet dengan menghubungkan switch farm ke fortigate, setting fortanalyzer, license fortanalyzer, membuat ulang topologi jaringan Panin dai-ichi Life, serta testing vulnerability report.



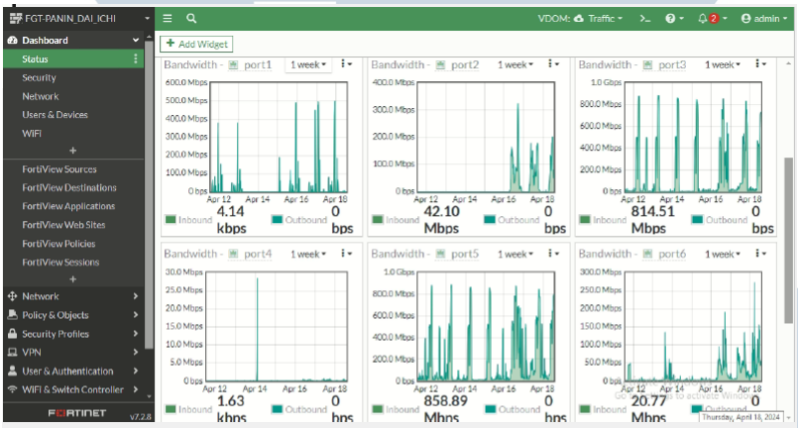
Gambar 3.13. Pemasangan Perangkat FortiGate

Perangkat fortigate dari fortinet yang dihubungkan dengan *switch farm* untuk dilakukan uji coba, perangkat ini dipasangkan pada rak server di ruangan *datacenter* Panin Dai-ichi Life.



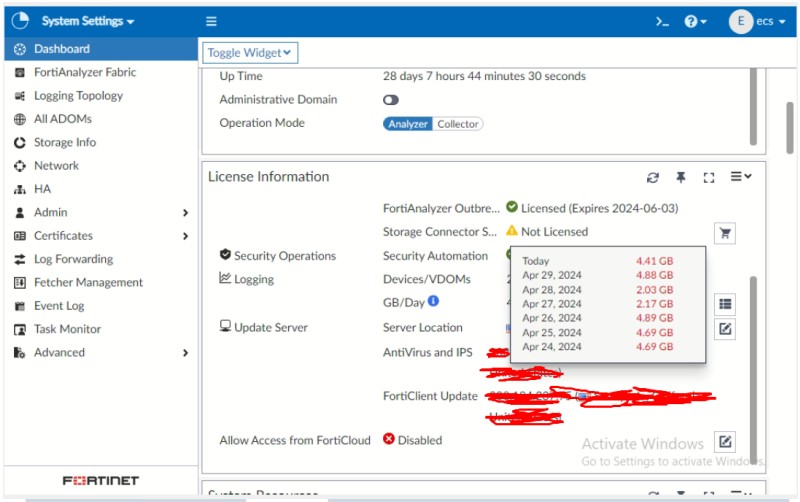
Gambar 3.14. Topologi FortiGate

FortiGate dipasangkan sebagai *mirroring port/sniff port*, sehingga tidak langsung menggantikan firewall sophos. Karena pemasangan ini hanyalah uji coba perangkat firewall baru dan Panin Dai-ichi Life belum memutuskan akan menggantikan sophos dengan firewall lain.



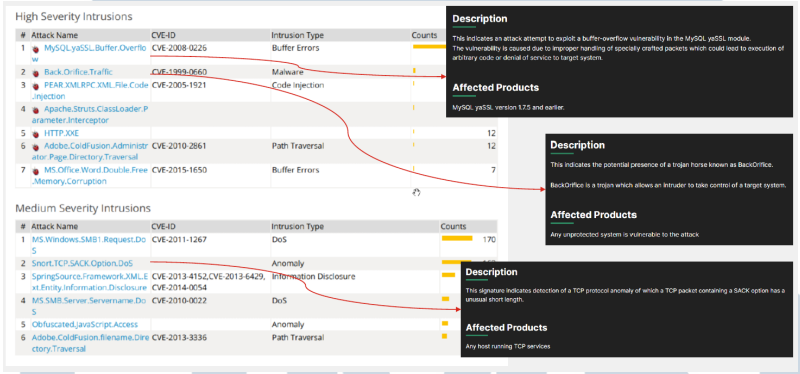
Gambar 3.15. Fortigate Dashboard

Tampilan Fortigate *Dashboard* yang menerima data lalu lintas pada switch farm Panin Dai-ichi Life.



Gambar 3.16. FortiAnalyzer Dashboard

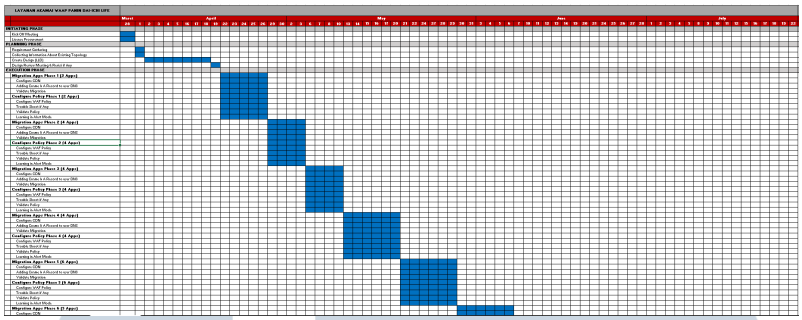
Tampilan FortiAnalyzer *Dashboard*



Gambar 3.17. Fortigate Vulnerability Report

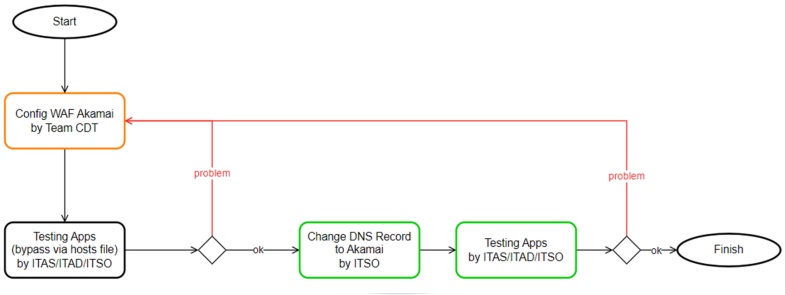
3.3.7 Minggu 15

Panin dai-ichi Life ingin meningkatkan keamanan siber dengan memberikan pelatihan security kepada karyawan Panin dai-ichi Life, kemudian ikut dalam projek migrasi WAF Sophos ke WAF cloud-based Akamai.



Gambar 3.18. Timeline Migrasi Akamai

Projek migrasi Web Application Firewall dari Sophos ke Akamai direncanakan akan dimulai pada awal bulan April hingga pertengahan bulan Juli.



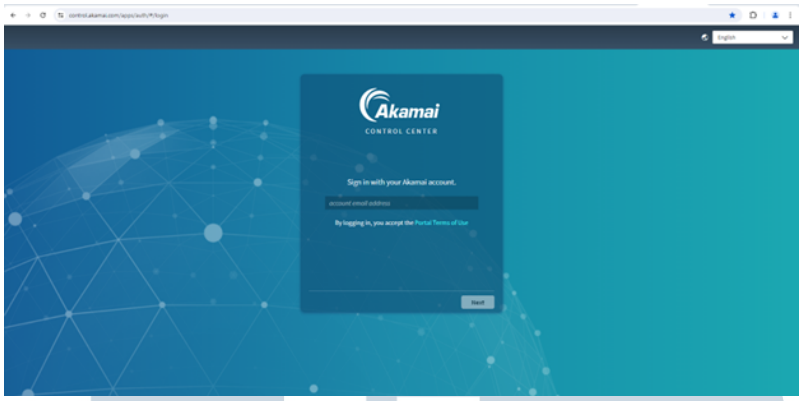
Gambar 3.19. alur migrasi akamai

Alur migrasi dimulai dengan melakukan konfigurasi WAF akamai terlebih dahulu yang akan dilakukan oleh tim CDT (Akamai), berbeda dengan WAF Sophos yang *build-in* dengan perangkat firewall Sophos sehingga tim PDL dapat melakukan konfigurasi WAF, sementara WAF Akamai berbasis *cloud* sehingga konfigurasi Akamai diserahkan pada tim CDT.

Setelah tim CDT selesai dengan konfigurasi Akamai, selanjutnya tim PDL melakukan testing aplikasi dengan melakukan *bypass via host files*, jika saat testing aplikasi web berhasil dimuat maka akan dilanjutkan dengan merubah DNS Record dan kembali testing aplikasi web.

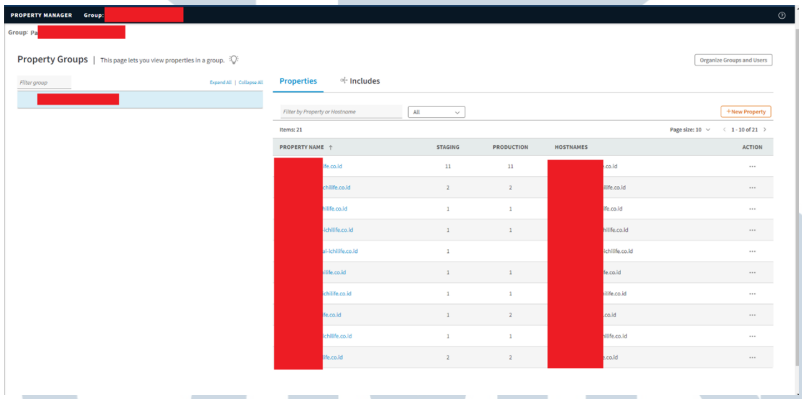
3.3.8 Minggu 16 - 20

Pada Minggu ini dilakukan migrasi tahap pertama hingga tahap ke lima dengan memindahkan 20 aplikasi dari WAF Sophos ke WAF Akamai.



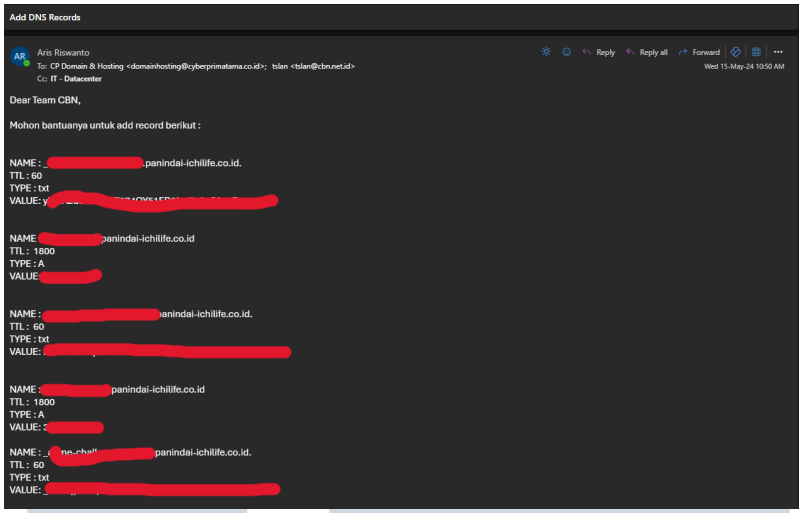
Gambar 3.20. Halaman Login Akamai Control Center

Akamai Control Center adalah sebuah sistem manajemen yang dikembangkan oleh Akamai Technologies, sebuah perusahaan teknologi yang berfokus pada pengembangan sistem keamanan dan jaringan. Sistem ini dirancang untuk membantu pengguna dalam mengelola dan mengawasi jaringan dan aplikasi yang menggunakan teknologi Akamai[4] .



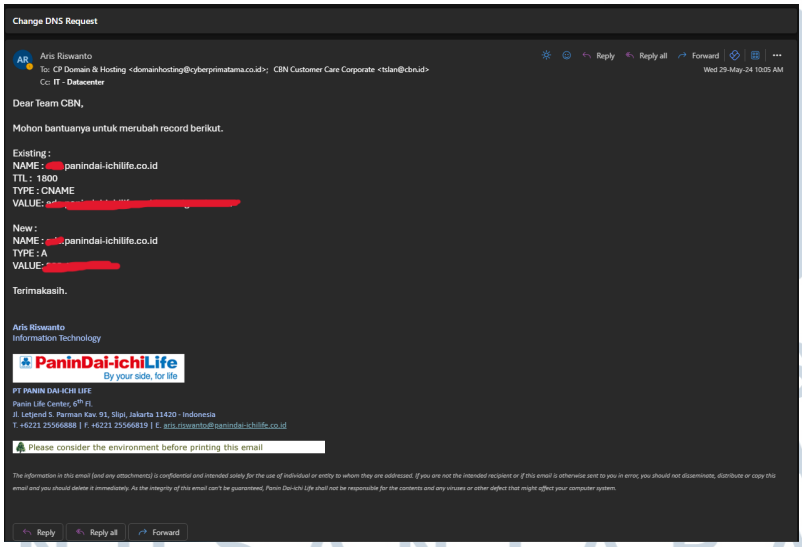
Gambar 3.21. Akamai Property Manager

Akamai Property Manager adalah sebuah sistem manajemen properti yang membantu pengguna dalam mengelola dan mengawasi properti digital mereka, termasuk aplikasi, situs web, dan jaringan. Sistem ini membantu dalam meningkatkan keamanan, mengoptimalkan kinerja, dan memudahkan pengguna dalam mengelola aplikasi.



Gambar 3.22. DNS Request

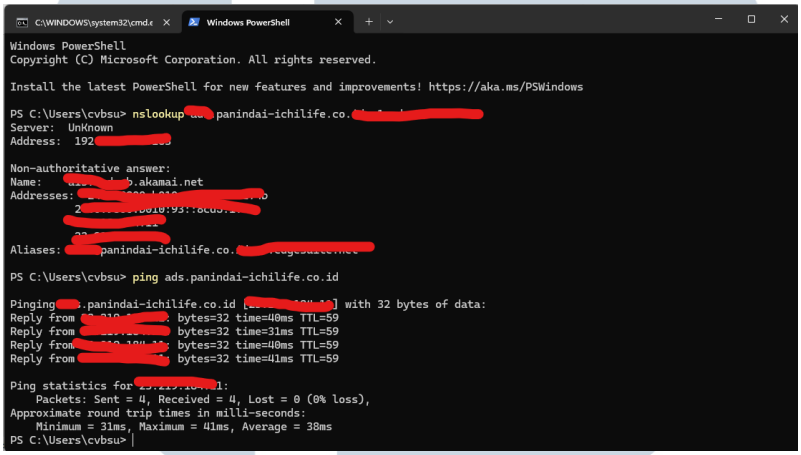
Dalam melakukan migrasi WAF dari Sophos ke Akamai, terdapat proses penting yang harus dilakukan, yaitu menambahkan TXT Record kepada ISP (Internet Service Provider) untuk verifikasi certificate. Proses ini bertujuan untuk memastikan bahwa certificate yang digunakan oleh Akamai adalah valid dan terverifikasi oleh ISP. Dengan demikian, ISP dapat memastikan bahwa certificate yang digunakan oleh Akamai adalah benar dan tidak tercemar oleh serangan keamanan.



Gambar 3.23. Change Request

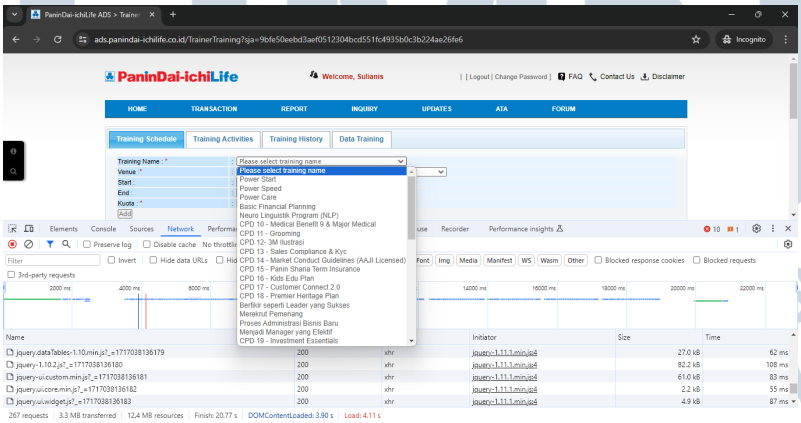
Setelah proses menambahkan TXT Record kepada ISP untuk verifikasi certificate berhasil, langkah selanjutnya adalah merubah existing record menjadi

CNAME record. Proses ini dilakukan untuk memastikan bahwa domain yang digunakan oleh Akamai dapat diarahkan ke server yang tepat. Dalam proses ini, existing record yang sebelumnya menggunakan nama domain akan digantikan dengan CNAME record yang mengarahkan domain ke server Akamai. Dengan demikian, domain yang digunakan oleh Akamai dapat diarahkan ke server yang tepat, sehingga dapat memastikan keamanan dan kinerja aplikasi yang lebih baik.



Gambar 3.24. Testing Bypass via host

Tes aplikasi web dengan menggunakan *file host*, dengan melakukan lookup nama domain (nslookup) ke nama host tujuan dan didapatkan respons dari server akamai.net yang menandakan aplikasi web telah berhasil dipindahkan ke Akamai.

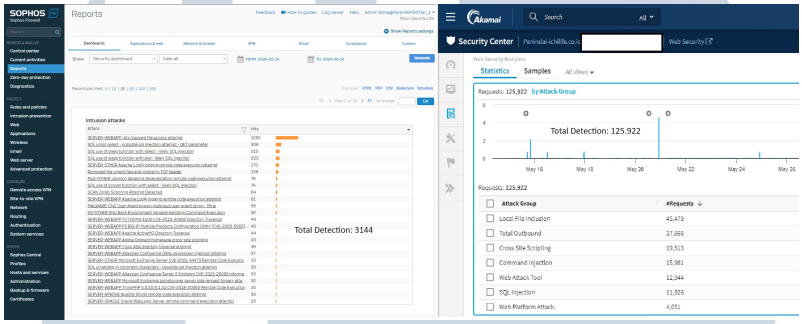


Gambar 3.25. Testing Web Application

Selanjutnya, alamat IP dan nama host yang didapatkan dari lookup nama domain disimpan pada file host, kemudian aplikasi web diakses dengan

mengunjungi URL nama host melalui browser, jika aplikasi web berhasil dimuat, maka migrasi telah berhasil.

3.3.9 Hasil Migrasi



Gambar 3.26. Perbandingan Deteksi Serangan Siber Pada Sophos dan Akamai

Pada periode 14 Mei 2024 hingga 14 Juni 2024, Sophos mendeteksi 3144 serangan, sementara Akamai pada periode yang sama mendeteksi 125.922 serangan. Migrasi WAF dari Sophos ke Akamai menunjukkan peningkatan deteksi serangan sebesar 3901,4%, yang dapat dihitung menggunakan rumus berikut:

$$\text{Peningkatan deteksi} = \frac{\text{Jumlah deteksi Akamai} - \text{Jumlah deteksi Sophos}}{\text{Jumlah deteksi Sophos}} \times 100 \tag{3.1}$$

Dengan demikian, peningkatan deteksi serangan sebesar 3901,4% dapat dihitung sebagai berikut:

$$\text{Peningkatan deteksi} = \frac{125.922 - 3144}{3144} \times 100 \tag{3.2}$$

3.4 Kendala dan Solusi yang Ditemukan

3.4.1 Kendala yang dihadapi

1. Kesulitan dalam berkomunikasi dengan tim ditempat magang, sehingga tidak dapat bekerja sama dengan efektif.
2. Ketidaktahuan akan tugas dalam divisi karena tidak adanya *training* sehingga pelaksanaan magang.

3.4.2 Solusi yang ditemukan

1. Cobalah lebih sering berkomunikasi, tidak harus berkomunikasi secara verbal, gunakan text.
2. Minta dan tawarkan bantuan pekerjaan untuk memaksimalkan pengalaman magang .