#### 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.

Minggu Ke	<del>.</del> -	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

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

### 3.3 Uraian Pelaksanaan Magang RSITAS 3.3.1 Minggu 1 ULTIMEDIA

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.

Control center XG550 (SFOS 19.0.3 MR-3-Build517) C	51100WXVX6BC5E	Feedback 🛛 🖬 How-to g	uides Log viewer Help Admin Bima@PaninXG450Tier_1 ▼ Panin Dai-Ichi Life
System	Traffic insight		User & device insights
Performance Services interfaces VPN	Web activity 3 max   2 avg	Cloud applications	Security Heartbeat* 0 0 0 0 At risk Missing Warnings Connected Synchronized Application Control™
0/0 0/0 RED Wireless APs 0 811 Connected remote Live users	Hits every 5 minutes Allowed app categories Infrastructure 139,532.42M General Business 121,546.17M General Internet 102,986.58M Provy and Tunnel 39,413.5M	0% 50% 100% Network attacks Misc 10	31     1     426       New     Categorized     Total       Zero-day protection     0     21       Recent     Incidents     Scanned
4%         35%           CPU         Memory           5.5M8/s         4.1x           Bandwidth         Sessions           0%         0           Decryption capacity         Decrypt sessions	Allowed web categories Information Tec Financial services	scan Hits Blocked app categories	ATP UTQ 7 Jac 1 Sources blocked Acc. for 80% of risk
High availability: <u>A-P (M)</u> Running for 74 day(s), 21 hour(s), 20 minute(s)	Online Chat 5 Personal Networ 4 Search Engines 1 Hits	N/A 0	SSL/TLS connections % Decrypt and inspect Of traffic Click here
			Click on widgets to open details
Active firewall rules 82 18 392 WAF User Network	492 Scanned 257 Vesterday Wel Posterday Wel 2725 kB Use Vesterday Use	Messages ky apps seen ④ Alert New system firm sites seen d by top 10 web ④ Alert rs New RED firmwar	17:20 nware is available for download. <u>Click h</u> 3m ago e is available for installation. <u>Click here</u> 3m ago are is available for installation. <u>Click he</u>
320 290 2 Unused Disabled Changed	0 14 Intr New Yesterday	usion attacks 🕕	

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.



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.



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.

Lapor status (RESOLVED): Switch - Access LT	5 11							
zabbix@panindai-ichilife.co.id To: I <b>T - Datacenter</b>						n Reply 🍨 Reply	all 🤌 Forward 🔗 🔠 Wed 24-Apr-24 5	
Problem name: Interface GigabitEther 17:31:52 on 2024.04.24 Operational data: C	net1/0/2(GigabitEther Jurrent state: up (1) Pro	net1/0/2 Interface): L blem ID: 9357742	<b>.ink down</b> Problen	n started at 17:30:53 on	2024.04.	24 Problem has b	een resolved in 1m 0s at	
← Reply ← Reply all → Forward								

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.

### M U L T I M E D I A N U S A N T A R A

AutoSave 💿 🕞 🍤 - 🤍 -		policies list - Excel • Saved	<ul> <li>&gt;</li> </ul>	Mohammad Bima 🛯 🔊 🔲	<b>E</b> –	•	×
File Home Insert Page	Layout Formulas	Data Review V	fiew Automate	Help 🖓	Comments	🖻 Share	~
Default	Page Layout	how Yoom 100% Zoo Yoo Sele	m to ction	ow D D Switch l D D Switch windows	Macros		
Sheet View Workboo	k Views	Zoom		Window	Macros		1
D46 🔻 i 🗙 🗸 🎜	bekalhidup.con	n, www.bekalhidup.com					`
A	В	с		D		E	
Name	Source	Destination		What		Action	1
5 INAT Servers 5 DNAT SMTP_Bekalhidup_GCP 1 DNAT TrendMicro to OSSIM 8 (C) DNAT Netscaler 13 9 (C) DNAT STP Xprint 0 DNAT ironport-Automail 1 (C) DNAT Ironport	WAN, IP_111.94.225.2, I WAN, IP_13.76.24.166_1 DMZ, LAN, WAN, Any hc WAN, IP_DBS_UAT, Hot WAN, Any host WAN, Any host	LAN, IP_202.158.23.78 LAN, IP_202.158.23.78 DMZ, IP_202.158.20.36 DMZ, Internet CBN [SFTP] DMZ, IP_202.158.20.46 DMZ, #POrtA1:12		SMTP TLS 587 SYSLOG #[C] DNAT Netscaler 12 #[C] DNAT SFTP Xprint PING , SMTP, SMTP TLS 587, SMTP. ICMP. ICMPy6. SMTP 1	SMTP-SSL, SMTP(S)	Accept Accept Accept Accept Accept Accept	
Microsoft 365 Rule           [C] DNAT Exchange Hybrid           [C] WAH-Hybrid HTTPS           Allow Exchange Hybrid to EXT           Allow Exchange AD Connect           7 Allow ALL to Office365	WAN, *.mail.protection Any zone, Any host Any zone, IP_170.10.10. Any zone, IP_170.10.10. Any zone WiFi-Networ	LAN, IP_202.158.23.70 #PortA1:9 WAN, Any host WAN, IP_20.190.128.0/18, IP_4 WAN, Microsoft 365	40.125.0.0/18, Microsof	SMTP hybrid.panindai-ichilife.cc HTTP, HTTPS, SMTP, ICMP HTTP, HTTPS, ICMP HTTP, HTTPS, SMTP, ICMP	b.id	Accept Forward Accept Accept Accept	
3 Allow UiPath Cloud 3 Allow Internal to Netscaler OTP 0 Allow Internal to AWS-DR	Any zone, IP_170.10.20. Any zone WiFi-Networ Any zone, IP_192.168.1	WAN, IP UIPath Cloud(HG), U Any zone, IP_10.0.0.22 WAN, Any host	liPath(HG)	HTTP, HTTPS, SMTP, ICMP Any service Any service		Accept Accept Accept	
2 SFTP FHI 3 ALL to API BCA - MASQ 4 Network Sementation	Any zone, Any host Any, zone, WIFI-Netwo Any zone, Any host	WAN, dev.ideal.panindai-ici WAN, ftp.fhnid.com WAN, IP_202.6.208.85_apiklik	kbca_ns11, IP_202.6.21f	HTTP, HTTPS TCP_2244 HTTPS, PING, ICMP, ICMPv6,	9443, 8182	Accept Accept Accept	1
ALL FLOOR MASO Allow LAN_SEGMENT to MGMT	Any zone, LAN_01_NET, Any zone, WIFI-Netwo	WAN, DMZ(Network),HCA Ne Management, Any host	twork, WIFI-Network, E	HTTP, HTTPS Any service		Accept Accept	
7 Allow LAN SEGMENT to DMZ 8 Allow FL6_Segment to DMZ	Any zone, WIFI-Networ Any zone, LAN_06_NET	DMZ, IP_10.0.0.16 DMZ, IP_10.0.0.233, IP_10.0.0.	235	Any service Any service		Accept Accept	
Allow DM2 access to LAN_SEGMENT     Outlook - Exchange Online Segmentat     Allow SETP DBDC LIAT - Segmented	Any zone, WIFI-Network	WAN, Exchange Online URLS	I_UI_NET, LAN_UB_NET,	ANY SERVICE HTTP, HTTPS, IMCAP, SMTP, TCP, 8005	UDP, ICMP, ICMPv6,	Accept	
2 LAN to DeutcheBank 3 Segment to ftp admedika	ANY zone, WIFI-Netwo ANY zone, WIFI-Netwo	WAN, DEMO DB, SFTP_Deust WAN, ftp.admedika.co.id	cheBack, DemoSFTP_D	SFTP_DB - Deutcshe Bank S TCP-2222	SFTP	Accept Accept	
Segment to SFTP SAS Business Portals	Any zone, IP_170.10.10.	WAN, sft-azsea.ondemand.s	as.com	PING , SSH		Accept	
WEB ADS	Any zone, Any host Any zone, Any host Any zone, Any host	#PortA1:15 #PortA1:14 #PortA1:0		workflow.panindai-ichilife ads.panindai-ichilife.co.id	e.co.id I	Forward Forward	
COVW ADSOUCE Panin Dai-Ichi Life     COVW PFA Portal Panin Dai-Ichi Life     COVW ADSOA Panindai-Ichi Life	Any zone, Any host Any zone, Any host Any zone, Any host Any zone, Any host	#PortA1:10 #PortA1:8 #PortA1:1		mservice.panindar-ichime		Forward Forward Forward	
New HIS-VW Link HTTPS     VW Link-Biznet     VW Link-Biznet     VW apis Panin Dai-ichi Life	Any zone, Any host Any zone, Any host Any zone, Any host	#PortA1:6 #PortA2:1 #PortA1:11				Forward Forward	
VW microsite Panin Dai-ichi Life [C] VW OWA HTTPS [C] VW Connector Panin Life [C] VW	Any zone, Any host Any zone, Any host Any zone, Any host	#PortA1:11 #PortA1:9 #PortA1:11				Forward Forward	
[C] VW AutoDiscover HTTPS     NAT Apple MDM	Any zone, Any host	#PortA1:9				Forward	1
DNAT Apple MDM HTTP	DMZ, LAN, WAN, Any he	DMZ, IP 202.158.23.78	: 4			Accept	
Sheeti						•	1

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

٩								
NALYZE		Firewall rules		NAT rules	SSL/TLS	SSL/TLS inspection rules		
tivities	PV4 IPve	Disable filter	Watch: How to	use NAT	Add NAT rule 🗸 🗸	Disable		Delete
tion	Many n the MA	nasqueraded linked NAT (SNAT) r SQ rules with destination set onl	ules were created during migration. V y to WAN and turn on the default MAS	Ve didn't prune them automatically to Q rule at the bottom of the NAT rule tal Delete linked NAT rules (on	ensure there's no behavior change aft ble. For details, go to the online help. Iy MASQ; Destination: WAN] U	er migration	n. You can d Don't dele	elete Ite rules
	NAT type	<ul> <li>Status</li> </ul>	Rule ID	Hide linked NAT rule				Reset fill
		Name	Original	Translated	Interface	ID	Usage	
	= 🗌 41	fwl/424 migrated NAT R Firewall rule ID: 424	Source: IP_172.16.71.254172.1 Service: FTP. HTTP, HTTPS, PIN Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#26	<b>4</b> 0	Θ
	42	fw#928-migrated NAT R Firewall rule ID: 428	Source: IP_172.16.61.231.172.1 Service: FTP. HTTP, HTTPS, PIN Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#27	ф 0	Θ
	<b>4</b> 3	fw#54-migrated NAT Ru Firewall rule ID: 54	Source: Any host Service: HTTP, HTTPS, IMAP, Pl Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#28	<b>↑</b> 0	e
	≡ <mark> </mark> 44	fw#430 migrated NAT R Firewall rule ID: 430	Source: WIFI-Network , LAN Net Service: TCP-2222 Destination: ftp.admedika.co.id	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: 2024-01-12 14:00:01	#29	<b>1</b> 098	Θ
	≡ <mark> </mark> 45	fw#244_migrated_NAT_R	Source: Any host Service: HTTP Destination: IP_202.158.23.78	Source: Driginal Service: migrated_service_fw# Destination: IP_10.0.04410.0	Inbound: PortA7, PortA6, BRM Outbound: Any interface Last used: 2024-01-1214/23/48	#240	<b>1</b> 26K	Θ
	<b>=</b> 46	fw#249_migrated_NAT_R	Source: Any host Service: HTTPS Destination: IP_202.158.23.78	Source: Original Service: migrated_service_fw# Destination: IP_10.0.04410.0	Inbound: PortA7, PortA2, PortA Outbound: Any interface Last used: 2024-01-1214/28/40	#238	🛧 23К	Θ
	I 47	fw#258 migrated NAT R	Source: Any host	Source: Original	Inbound: PortA7, BRMgmt, Por	#224	<b>1</b> 0	$\Theta$

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.

DEPLOYMENT	
COMPONENTS PLUGIN BUILDER LOCATIONS	
ALIENVAULT CENTER   SENSORS   SERVERS	•
A ALIENVAULT CENTER 👌 ALIENVAULT [170.10.11.161] 👌 SOFTWARE - PACKAGES PENDING UPDATES	5
<b>E</b>	Ľ
v5.8.9 available! Patch	
As of Tuesday, November 16th, 2021, AT&T Gybersecurity is proud to announce that AlienVault USM v5.8.9 is generally available for all existing and new customers. If possible, we encourage users to first apply the upgrade to a test system to understand and learn the new functionality before upgrading production systems.	
RELEASE HIGHLIGHTS	3 <b>-</b>
The main goal for the v5.8.9 release is the OSSEC upgrade. OSSEC will be updated to the latest available version (v3.6.0).	
Beulder Hur OSSEC upgrade, hur following areas include one or more float/improvements: • Analysis – Trächts • Analysis – Trächts • Derivationen er – Vulnergalistics Environment – Vulnergalistics • Configuration – Administration – Main. • Configuration – Administration – Usar.	
Login page.	

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*.

alienvault:/var/lib/rabbitmg/mnesia# cd /						
alienvault:/# ls						
None bin dev home initrd.img.old lib64 md5sum.txt			erv <mark>tap</mark>		vmlinuz.old	
awkprof.out boot etc initrd.img lib lost+found media				vmlinuz		
alienvault:/# dpkgconfigure -aforce-confiew						
E L Restanting RabbitMD Reserving Server (s.e. Pression Server)						
Setting in alienvalltani (5.8.17-9625)						
Installing new version of config file /etc/alienvault/api/default_tasks.um						
Installing new version of config file /etc/alienvault/api/messages.yml						
Installing new version of config file /etc/alienvault/api/triggers.yml						
Installing new version of config file /etc/init.d/alienvault-api						
# Host 12/,0.0.1 found: line 2						
Promeravapi/.ssn/knowi_nosts updated.						
# Host localhast found: line 2						
/home/avapi/.ssh/known_hosts updated.						
Original contents retained as /home/avapi/.ssh/known_hosts.old						
# 127.0.0.1:22 SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u8						
# localhost:22 SSH=2.0-OpenSSH_7.4p1 Debian=10+deb9u8						
# 127.0.0.1122 SSH=2.0-UpenSSH_7.401 Debian=10+de0508						
# localhost:22 SSH-2.0-OpenSSH 7.4p1 Debian-10+deb9u8						
# localhost:22 SSH-2.0-OpenSSH-7.4p1 Debian-10+deb9u8						
Enabling site alienvault-api.						
To activate the new configuration, you need to run:						
service apache2 reload						
Inserv: Service rabbitmd-server has to be enabled to start service allenva	auit-api					
[] Clean un rabbit queues: ] Starting ColoruBeat: colorubeattmofe d	no Zeuro tur	e tmofe i	(ru nosui	d noevec	relatime cize	-329
4180k.mode=755)	an sharr egg					
OK						
[] Starting CeleryD: celerydtmpfs on /run type tmpfs (rw,nosuid,noexec	relatime,s,	ize=3294:	180k,mode	=755)		
OK						
. ok Processing thiggers for plicework_proces2 (5.8.47-0672)						
Foldership (higgers to aller automatic apactez (0.0.1-5070)						
Setting up alienvault-dummu-framework (5.8,17-9678)						
deb http://data.alienvault.com/alienvault58/plugins-feed/ binary/						
alienvault:/#						_
			-	_	_	-
Combor 2 12 shall comm	and A	lion	vault	. E		
Gambal 5.12. Shen Comm	ина А	uen	vauu			

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.



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.



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

19 Optimalisasi Keamanan Aplikasi..., Moch. Bima, Universitas Multimedia Nusantara



Gambar 3.16. FortiAnalyzer Dashboard

#### Tampilan FortiAnalyzer Dashboard

High Severity Intrusions				Description
# Attack Name	CVE-ID	Intrusion Type	Counts	This indicates an attack attempt to exploit a buffer-overflow substability in the MySQL vaSSL module.
1 MySQLyaSSLBuffer.Overflo w	CVE-2008-0226	Buffer Errors	_	The vulnerability is caused due to impose handling of specially crafted packets which could lead to execution of arbitrary code or denial of service to target system.
2 🐞 Back.Orifice.Traffic	CVE-1999-0660	Malware	1	
3 PEAR.XMLRPC.XML.File.Code Injection	CVE-2005-1921	Code Injection		Affected Products
4 Apache.Struts.ClassLoader.P arameter.Interceptor				MySQL yaSSL version 17.5 and earlier.
5 🐞 HTTP.XXE				12
6 Adobe.ColdFusion.Administr ator.Page.Directory.Traversal	CVE-2010-2861	Path Traversal		12 Description
7 🐞 MS.Office.Word.Double.Free	CVE-2015-1650	Buffer Errors	~	7 This indicates the potential presence of a trojan horse known as BackOrlifice.
.Memory.Corruption				BackOrffice is a trojen which allows an intruder to take control of a target system.
			-87	
Medium Severity Intrusion	5			Affected Products
# Attack Name	CVE-ID	Intrusion Type	(	Counts
1 MS.Windows.SMB1.Request.Do	CVE-2011-1267	DoS		Any unprotected system is vulnerable to the attack
S				
2 Snort.TCP.SACK.Option.DoS		Anomaly		Description
3 SpringSource.Framework.XML.E xt.Entity.Information.Disclosure	CVE-2013-4152,CVE-2013-6429, CVE-2014-0054	Information Disclosure		This signature indicates detection of a TCP protocol anomaly of which a TCP packet containing a SACK option has a
4 MS.SMB.Server.Servername.Do S	CVE-2010-0022	DoS		unusual short length.
5 Obfuscated.javaScript.Access		Anomaly		Affected Products
6 Adobe.ColdFusion.filename.Dire ctory.Traversal	CVE-2013-3336	Path Traversal		Any host running TCP services

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.

Δ

S



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].

PROPERTY MANAGER Group:					O
Group: Pa					
Description of the second					
Property Groups   This page lets you view properties in a group.					Organize Groups and Users
Filter group Expand All   Collope All	Properties of Includes				
	Filter by Property or Hostnome	All v			+New Property
	Items: 21				Page size: 10 $\ \sim \ \ \leq 1 \cdot$ 10 of 21 $\ >$
	PROPERTY NAME †	STAGING	PRODUCTION	HOSTNAMES	ACTION
	Becould	11	11	ico.id	
	chille.co.id	2	2	life.co.id	
	NITE co.id	1	1	He.co.id	
	-ichillife.co.id	1	1	Nifeco.id	
	al-Ichillie.co.Id	1		Ichilde.co.ld	
	ilite.co.id	1	1	fe.co.id	
	ichilife.co.id	1	1	ville.co.id	
	Re.co.ld	1	2	.co.id	
	ichill/e.co.id	1	1	sillfe.co.id	
	Recold	2	2	scould	
Gambar 3	3.21. Akam	ai Prop	erty I	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.



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.

					[ Logout	Change Password ]	a ç conaciós æ	Disclaimer	
	HOME	TRANSACTION	REPORT	INQUIRY	UPDATES	ATA FORUN			
	Training Schedule	Training Activities	Training History	Data Training					
	Training Name : *	: Please :	elect training name	~					
	Venue :*	: Please	select training name	A	V				
	Start :	Power	Speed						
	Eng . Kuota : *	Power	Care						
	Add	Basic P	inancial Planning inquistik Program (NLP)						
2000 ms	4000 ms	CPD 10 CPD 17 CPD 18 Berfikir Merekri	Kids Edu Plan     Customer Connect 2.1     Premier Heritage Plan     seperti Leader yang Sul     Premenang	ses	14000 ms	16000 ms	19000 ms	20000 ms	22000 ms
		Proses	Administrasi Bishis Baru Mananer yang Efektif						
		Proses Menjad CPD 19	Manager yang Efektif - Investment Essentials		Initiat	or and a second s	Size	Time	
uery.dataTables-1.10.min,	js?_=1717038136179	Proses Menjad CPD 19	Manager yang Efektif - Investment Essentials 200	xhr	loitist jauto	or -1.11.1.min.jz4	Size	Time 27.0 kB	6
Jery, data Tables-1.10.min, Hry-1.10.2.js?_=1717038	js?_=1717038136179 136180	Proses Menjad CPD 11	Administrasi Bishis Bario Manager yang Efektif - Investment Essentials 200 200	xhr xhr	Initiat japuto japuto	ər <u>=1.11.1.min.jg4</u> =1.11.1.min.jg4	Size	27.0 k8 82.2 k8	6
: Jery.dataTables-1.10.min, Jery-1.10.2.js?_=1717038 Jery-ui.custom.min.js?_=1	js?_=1717038136179 136180 1717038136181	Proses Menjad CPD 15	Administrasi Bishis Baru Manager yang Efektif - Investment Essentials 200 200 200	xhr xhr xhr	initiat jauto jauto jauto	or <1.11.1.min.jg4 <1.11.1.min.jg4 <1.11.1.min.jg4	Size	Time 27.0 k8 82.2 k8 61.0 k8	6 10 8
: uery.dataTables-1.10.min, uery-1.10.2.js?_=1717038 uery-ui.custom.min.js?_=171 uery.ui.core.min.js?_=171	js?_=1717038136179 136180 1717038136181 7038136182	Proses Menjad CPD 19	Administratis latisfie Saru Manager yang Elektif - Investment Essentials 200 200 200 200	xhr xhr xhr xhr	Initiat jauto jauto jauto jauto	r - <u>1.11.1.min.ja4</u> - <u>1.11.1.min.ja4</u> - <u>1.11.1.min.ja4</u>	Size	Time 27.0 k8 82.2 k8 61.0 k8 2.2 k8	6 10 8 5

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

Reports	Feedback	How-ta guides Lag viewer Help Adr	In EmapPerintD-63Ter_1 *	Cale		Q Starch		AL Y			
				Quinan	Har I						
Exchements Applications & web Relation & Ethnich	-	Brial Compliance	Custon Victoria	Security (	Center F		olao.		Web Security 🖉		
Searc Beauty distances + View at +	FROM 2009-45-04	10 XX. 8004-60-04	(?)	Web Sec	urity Analytics	Samples ,	Wi vlevs 🕶				
Proceedings of the C & 1 Like 1 25 1 (50 1 300 1 200		Countrad. HTML	PDF CDV Bookmark Schedule	Requ	ests: 125,923	by Attack Gro	up				
		11 C. Page 1 of 35 (§ 30)	Co lo page	6							
			R					0	0		
Intrusion attacks			Des								
ataox	17 Hb					Total	Detection	175 077			
TO EVED AN EAST AND AN ADDRESS OF BUILDING ADDRESS.	1233		*			iotai	Detection.	123.322			
SCL under serent - possible sor mection attempt - OET parameter	208		~	2							
SOL use of please function with select - likely SOL intection	210										
SOL use of sleep function with and - likely SOL Intection	200		124			Hyperbarry 1					
SERVER: STREE Assoche Looiki contine remote code execution attamet.	270										
Removed the urgent flat and contar in TDP header	338					1037.10	M89.12	1659.20	1089.22	1039 24	May 25
FLE-STHER JACKSON BROENE DESERVATION FROM CODE HERVISON ADDRESS	78										
20Luce of concert function with select - they USL election	24 1		11	Requ	ests: 125.922						
SCAN Zorab Scanning Attempt Detected	64										
SERVER: WEBARR Adapting Look looping tempts code execution attempt	e1				Attack Ge	040			#Requests 4		
ERGRARE-Chill User-Arent Inners-malicitus user-arent shino - Hirai	50								autorio a		
A DESCRIPTION OF A DESC	10				Local Ella	inclusion.			45.479		
In the Hump of the Control Con					)	The second second					
SERVED WEAKED Anaring Antiquity] Disarting Transmal		Total Detection: 3144			Total Out	bound			37.650		
VPD-VP-WPBACQ Addres Connect Instrumentary moves the secondary	93				,				autana.		
TO TATE AN EAST CASE AND Dealters Instead alternal	20				Concertine	Perinting			10.812		
16 PVIP-WERAPP ATABLES CONTINUES COPE, expression insection attempt	37			1 4	1 0.092.2016	an an B			17,720		
SERVER-DTWER Microsoft Exchange Server CVE-2003-94972 Remote Code Executiv	0. 22				1	d to to add a s			12.001		
SOL unlending in comment characters - cossible sol intection attempt	22				j continano	a infection			10,901		
SERVER: WEBARR Adaption Configures Server 5 Endopint CvE 2021 25085 Inform	a. 33										
SERVED WERAT Morecol Exchange autodiscown server side wowed, formers after	1. 12			- F - F	j web Attac	X 1001			12,944		
INFORMATION PROPERTY AND A 23 YO F REPORT FROM CONTRACTOR	20 20										
					<ol> <li>SOL Islant</li> </ol>				11.926		
\$5.9459 MINORE ROUCH STUDY INTO A CODE EXECUTION AT ANY A	90				1 nder uber						
SERVER MACHE BOACH Prote Write out and the security strang. SERVER ORALL Prote Webland, Same write command execution strangs.	20 I				1 order others						

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:

$$Peningkatan deteksi = \frac{Jumlah deteksi Akamai - Jumlah deteksi Sophos}{Jumlah deteksi Sophos} \times 100$$
(3.1)

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

Peningkatan deteksi = 
$$\frac{125.922 - 3144}{3144} \times 100$$
 (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 .

