BAB 3 PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Pelaksanaan program magang di PT Visionet Data Internasional dilakukan pada divisi Security Operation Center (SOC) Level 1, di bawah supervisi Bapak Hadi Ismanto selaku Kepala Departemen Security Services. Divisi SOC memiliki tanggung jawab utama untuk melakukan pengawasan, analisis, dan pelaporan terhadap alert yang muncul dari sistem SIEM dan EDR kepada PIC klien yang bersangkutan. Untuk meningkatkan koordinasi antar anggota SOC dilakukan weekly meeting via Microsoft Teams setiap hari Senin pukul 14.00 dimana satu atau dua anggota SOC melakukan sharing session berupa presentasi hal yang menarik bagi mereka atau bermanfaat untuk anggota SOC yang lain. Gambar 3.1 merupakan struktur subdivisi dari divisi Project Management Office.



Gambar 3.1. Struktur Divisi Project Management Office

SOC L1 memiliki beberapa tugas rutin yang perlu dilakukan setiap hari, salah satunya adalah melaporkan agen Visionet dan Lippo-Karawaci yang terputus dari *server* Wazuh maupun SentinelOne setiap pukul 10.00 ke grup WhatsApp masing-masing. Selain itu, pada pukul 14.00, dilakukan pelaporan khusus untuk agen Cinepolis yang terputus dari *server* Wazuh kepada PIC Cinepolis.

Untuk tugas mingguan, SOC L1 bertanggung jawab menyusun dan mengirimkan laporan yang berisi rekap *alert*, penambahan agen baru, dan penghapusan agen yang sudah tidak dipakai yang terdeteksi di SentinelOne selama 7 hari terakhir. Laporan ini disampaikan setiap hari Jumat sebelum pukul 12.00 kepada Bapak Hadi Ismanto selaku Kepala Departemen *Security Services*.

3.2 Tugas yang Dilakukan

Tugas yang dikerjakan adalah sebagai berikut.

- 1. Melakukan pengawasan terhadap sistem SIEM (Wazuh dan SOCFortress) dan EDR (SentinelOne) untuk memantau adanya *alert* yang menunjukkan aktivitas mencurigakan pada *endpoint*.
- 2. Menganalisis *alert* yang muncul, serta melaporkannya kepada PIC terkait apabila hasil analisis menunjukkan potensi ancaman atau aktivitas berbahaya.
- 3. Melaporkan secara harian status agen yang terputus dari SIEM maupun SentinelOne kepada PIC terkait.
- 4. Menyusun laporan mingguan yang berisi rekapitulasi *alert* yang muncul di SentinelOne sebagai bahan evaluasi dan dokumentasi.

3.3 Uraian Pelaksanaan Magang

Berikut adalah uraian semua kegiatan selama enam bulan yang dilakukan dalam pelaksanaan Magang di PT Visionet Data Internasional sebagai SOC L1 Engineer dalam tabel 3.1.

Pelaksanaan kerja magang diuraikan seperti pada Tabel 3.1.

Minggu k	Ke -	Pekerjaan yang dilakukan
1-2		Mempelajari cara melakukan monitoring sistem SIEM untuk
		klien Cinepolis, BPD DIY, dan untuk internal VDI, serta
		memahami prosedur eskalasi yang sesuai
3-4		Mempelajari cara melakukan monitoring sistem EDR
		SentinelOne untuk klien Lippo-Karawaci, dan internal VDI,
		serta memahami prosedur eskalasi yang sesuai
5-14		Melakukan <i>monitoring</i> terhadap kedua sistem, serta
		melakukan eskalasi ke PIC terkait
15		Melakukan transisi ke SOC L2 dengan cara mempelajari threat
		intelligence Recorded Future
16-19		Mencari vulnerability yang dapat dimasukkan kedalam
		playbook dan mencari adanya credential leak yang dapat
		dilaporkan menggunakan Recorded Future
20-23		Kembali ke SOC L1 dan melanjutkan tugas sebagai L1

3.3.1 Pipeline Standard Operating Procedure di divisi SOC PT Visionet Data Internasional

Pada hari pertama masuk ke kantor diberikan penjelasan mengenai tugas dari tim SOC PT Visionet Data Internasional (VDI). Tim SOC bertanggung jawab untuk melakukan pengawasan terhadap sistem SIEM yang digunakan oleh klien Cinepolis, BPD DIY, lingkungan internal VDI, dan Lippo-Karawaci serta sistem EDR yang digunakan untuk lingkungan internal VDI dan klien Lippo Karawaci. Gambar 3.2 menunjukkan *standard operating procedure* divisi SOC VDI.



Gambar 3.2. Pipeline Standard Operating Procedure SOC VDI

Berikut penjelasan lebih mendalam mengenai gambar 3.2:

1. Alert Detected

Sistem SIEM atau EDR akan mendeteksi adanya aktivitas yang mencurigakan, seperti percobaan *login* yang gagal berulang-ulang kali, adanya *file* yang ditandai sebagai sebuah malware, URL/IP yang mencurigakan, atau aktivitas diluar jam kerja.

2. Alert Masuk ke Dashboard

Aktivitas mencurigakan tersebut akan masuk ke *dashboard* monitoring sebagai sebuah *alert* sesuai dengan klien (Wazuh untuk Cinepolis/BPD DIY dan SOCFortress/SentinelOne untuk Internal VDI/Lippo-Karawaci).

3. Analisis Awal Oleh SOC L1

Akan dilakukan verifikasi awal terhadap *alert* yang muncul dengan cara mengidentifikasi *severity* dari *alert* sesuai dengan *playbook* yang telah dibuat (*Critical, High, Medium, Low*). Setelah itu akan diecek detail dari *alert* (Waktu terdeteksi, *source* IP, Hash *file, hostname*, nama *user*). Kemudian melakukan cek terhadap reputasi dari *file/IP/URL* menggunakan *threat intelligence* seperti VirusTotal, AbuseIPDB, URLVoid, dan Recorded Future.

4. Validasi dan Keputusan Tindakan

Setelah dilakukan cek terhadap *alert* akan diketahui apakah *alert* tersebut merupakan sebuah *false positive* atau *true positive*. Jika *alert* tersebut *false positive* didokumentasikan tetapi tidak dieskalasi, tapi apabila *true positive* maka akan dilanjutkan dengan proses eskalasi.

5. Eskalasi ke PIC Klien

Eskalasi *alert* digunakan menggunakan email *Office Outlook*, grup Whatsapp, atau platform SDP VDI (khusus untuk *alert* internal). Eskalasi pertama dilakukan dengan waktu yang tidak melebihi 30 menit sejak *alert* muncul dan akan dilakukan *follow up* secara berkala sesuai dengan *severity* dari *alert* apabila tidak mendapat respon dari PIC klien. (*Critical*: tiap 2 jam, *High*: tiap 4 jam, *Medium*: tiap 8 jam, *Low*: tiap 24 jam)

6. Tindak Lanjut Oleh Klien

Klien akan melakukan respon seperti mengisolasi *endpoint*, melakukan *restart* pada agen, menghapus *file*, dll. Khusus untuk *alert* dari SentinelOne apabila perlu tim SOC L1 dapat melakukan *remote shell* ke *endpoint* untuk menghapus *file* yang tertandai sebagai *malware/virus*.

7. Dokumentasi

Setelah dilakukan langkah-langkah diatas, *alert* dimasukkan kedalam formulir *daily activity* untuk kemudahan L2 membuat *weekly report* tentang aktivitas keamanan siber dari klien yang nantinya akan disampaikan melalui *meeting* dengan klien.

Gambar 3.3 berikut merupakan tampilan formulir *daily activity* untuk Cinepolis, Bank Pembangunan Daerah Daerah Istimewa Yogyakarta (Bank BPD DIY), dan Visionet. Dalam formulir ini perlu diberikan informasi mengenai Nama *alert* yang muncul, ID dari *alert* untuk memudahkan identifikasi lebih lanjut, *Severity* dari *alert*, Nama klien, Nama petugas L1 yang melakukan eskalasi, Status eskalasi dari *alert*, Waktu *alert* muncul dan Waktu eskalasi *alert* dilakukan.

0	SOC Visionet Portal Daily Activity	/ Tickets *				∇ ⊑ ₽° ₫) [*] All Items ~	Issues grouped by perso	on assigne Issue	s grouped by priority	Issues grouped by	status ··· +	Add view
0	① ID ↓	(1) Issue	⊟ Issue descripti	Customers	⊘ Severity	Category	⊘ Status	Time/Date Det	Assigned to	O Detection Met	E List of Affecte	Ø Affected Asset	≕ List
1	2824	Threat Intel Alert – Linux Host Established	#337524 Threat Intel A	Internal	(† High)	Block IP	In progress	6/19/2025 12:56 PM	Makaio Kanaka	SIEM			
1	2823	FORTIGATE: Web Filter - Nmap Scanner Ev	MSSP BPD DIV 175031	BPD DIV	(† High)	Block IP	In progress	6/19/2025 12:36 PM	Makaio Kanaka	SIEM			
1	2822	OFFICE365 ACCESS FROM OUTSIDE INDO	OFFICE365 ACCESS FRO	Lippo-Karawaci	(† High)	Suspicious Activ	In progress	6/19/2025 11:34 AM	Alwi Dirgantara	SIEM			
1	2821	FORTIGATE: Web Filter - Potentially Unwan	MSSP BPD DIV 175021.	8PD DIV	(† High)	Block IP	In progress	6/19/2025 9:07 AM	Alwi Dirgantara	SIEM			
1	2820	FORTIGATE: Web Filter - Potentially Unwan	MSSP BPD DIV 175030	8PD DIY	(† High)	Block IP	In progress	6/19/2025 11:37 AM	Makaio Kanaka	SIEM			
1	2819	Threat Intel Alert – Linux Host Established	#337446 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 8:58 AM	Alwi Dirgantara	SIEM			
1	2818	Threat Intel Alert - Linux Host Established	#337444 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 8:55 AM	Alwi Dirgantara	SIEM			
1	2817	Threat Intel Alert – Linux Host Established	#337448 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 9:00 AM	Muhammad Haf	SIEM			
1	2816	Threat Intel Alert - Linux Host Established	#337447 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 8:56 AM	Muhammad Haf	SIEM			
1	2815	Threat Intel Alert – Linux Host Established	#337445 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 8:54 AM	Muhammad Haf	SIEM			
1	2814	Threat Intel Alert – Linux Host Established	#337439 Threat Intel A	Internal	(† High)	Block IP	Completed	6/19/2025 8:14 AM	Muhammad Haf	SIEM			
1	2813	SSHD authentication success outside offic	#337426 SSHD autheni	Internal	(† High)	Suspicious Activ	In progress	6/19/2025 6:17 AM	Owen Salim	SIEM			
1	2812	RDP Login success out of office hours	MSSP Cinepolis 175021	Cinepolis	(† High)	Suspicious Activ	In progress	6/19/2025 5:25 AM	Owen Salim	SIEM			
1	2811	Request Block IP SURICATA Security Alert	#332582 SURICATA Sec	Internal	(† High)	Block IP	Completed	6/19/2025 2:40 AM	M. Jalaluddin .8	SIEM			
1	Add new item	RDP Login success out of office hours	#337198 VERIFIKASI A	Internal	(† High)	Suspicious Activ	Completed	6/19/2025 2:17 AM	Owen Salim	SIEM			
1				_	\frown					_			

Gambar 3.3. Formulir Daily Activity Cinepolis, BPD DIY, dan VDI

Gambar 3.4 merupakan tampilan formulir *daily activity* untuk Lippo-Karawaci. Formulir ini berisi Waktu *alert* muncul, Sistem operasi dari *endpoint*, *Severity* dari *alert*, Status eskalasi dari *alert*, Nama petugas L1 yang melakukan eskalasi, Nama *endpoint* dan pengguna *endpoint* tersebut.

Playbook MSSP V 3.	.1 2 4		D Search for to	ols, help, and more (Alt + Q)							(0)
ome Insert Share	Page Layout Formulas	Data Review View Automate	Help Draw				Ċ	Comments	r∿• Catch up	∂ Editing ∨	85 Sha
Cut Copy Source Format Painter Clipboard	Arial v 10 v B I U D ab ⊡ v Fort Fort		p Text General ge & Center × \$€ × 9	v Conditional Format As Cell Number Styles	Insert Del	lete Format	∑ AutoSum v 2√ Q (88)				
$\checkmark [\times \checkmark f_{X} \circ]$											
В	с	D	E	F	G	н	1	J		к	
	14:10:30 AM	12:43		Windows 11 Pro 22621	Medium	Open	SentinelOne Cloud				
Selasa, 17 Juni 2025	10:37	12:03		Windows 11 Home Single Language 26100	Medium	Open	SentinelOne Cloud				
	15:01	15:54		Windows 11 Pro 22631	High	Open	Behavioral AI				
Rabu, 18 Juni 2025	8:46	9.04		Windows 11 Pro 26100	Medium	Open	On-Write Static Al				
	13:10	13:39		Windows 11 Pro 26100	Critical	Open	Behavioral Al				
	16:17	16:41		Windows 11 Pro 22621	Medium	Closed	SentinelOne Cloud				
	16:34			Windows 11 Pro 26100	Medium	Closed	SentinelOne Cloud				

Gambar 3.4. Formulir Daily Activity Lippo-Karawaci

3.3.2 Sistem SIEM

Security Information and Event Management (SIEM) adalah sistem yang digunakan untuk mengumpulkan, menganalisis, dan memantau log serta data keamanan dari berbagai perangkat dan sistem dalam suatu infrastruktur TI. SIEM menggabungkan dua fungsi utama, yaitu Security Information Management (pengelolaan informasi keamanan) dan Security Event Management (manajemen kejadian keamanan), untuk memberikan visibilitas secara real-time terhadap aktivitas jaringan dan mendeteksi potensi ancaman atau insiden keamanan. Dengan SIEM, tim keamanan dapat melakukan korelasi antar log dari berbagai sumber seperti firewall, endpoint, server, dan aplikasi, sehingga mempermudah dalam mengidentifikasi pola serangan, melakukan investigasi, dan menyusun respons yang cepat serta tepat terhadap insiden yang terjadi [6].

A Wazuh Cinepolis

Gambar 3.5	merupakan	tampilan	dari	wazun Cinepolis.	

Search			DQL	Cast 24 hours	Show dates C Ref
NOT full_log: is one of library, media × NOT	{"wildcard":{"data.dstuser":"marwan*"}} × NOT rule.id: 1001	800 × NOT data.cs1: wazuh-agent.exe × ④ Add filter			
Cinepolis Alerts by Rule ID					
mestamp: Descending	v id: Descending	v rule.description: Descending	v agent.name: Descending	~ Count	
14, 2025 @ 11:59:30.137	1749877169.306162885	Partition usage reached 95% (disk space monitor).	sysmon	1	
14, 2025 @ 12:59:30.168	1749880769.315910111	Partition usage reached 95% (disk space monitor).	sysmon	1	
14, 2025 @ 13:59:30.069	1749884369.168536834	Partition usage reached 95% (disk space monitor).	sysmon	1	
14, 2025 @ 14:59:30.556	1749887969.93371117	Partition usage reached 95% (disk space monitor).	sysmon	1	
n 15, 2025 Cortex XDR Log (:15:15:963 an 15, 2025 Cortex XDR Log 1:15:15:984			['SYSTEM']	MKGIT4RD2QM3	
un 15, 2025 Cortex XDR Log 1:15:03.097			['SYSTEM']	KKGIT48DZQW3	
iok Fortigate HD					
		1년 No results found			

Gambar 3.5. Dashboard Wazuh Cinepolis

Untuk klien Cinepolis beberapa alert yang perlu dilaporkan sebagai berikut:

А

(a) Windows Failed Login 5 Times in a Row

Alert ini muncul ketika terdapat percobaan *login* yang gagal sebanyak lima kali berturut-turut pada suatu *endpoint*, yang dapat mengindikasikan

upaya brute force atau akses tidak sah. Proses eskalasi dilakukan dengan menyertakan bukti *alert* kepada PIC klien dan menanyakan apakah aktivitas tersebut merupakan tindakan yang valid (sah) atau mencurigakan, guna memastikan apakah perlu dilakukan tindak lanjut lebih lanjut.

(b) *Cortex XDR terminated unexpectedly*

Alert ini muncul apabila Cortex XDR agen pada suatu *endpoint* terdeteksi sedang dalam kondisi tidak aktif, yang berpotensi menyebabkan *endpoint* kehilangan perlindungan dari ancaman. Sebelum dilakukan eskalasi, tim terlebih dahulu memastikan bahwa proses Cortex XDR benar-benar tidak aktif pada *endpoint* tersebut. Setelah validasi dilakukan, eskalasi dilanjutkan dengan pelaporan kepada PIC klien untuk meminta agar Cortex XDR diaktifkan kembali.

(c) Cortex XDR Wildfire Malware Event

Alert ini muncul ketika terdapat aplikasi pada *endpoint* yang terdeteksi oleh Cortex XDR sebagai malware. Sebelum dilakukan eskalasi, dilakukan verifikasi terlebih dahulu terhadap *hash* file aplikasi tersebut menggunakan platform *threat intelligence*. Jika hasil pengecekan menunjukkan bahwa file tersebut memang berbahaya, maka eskalasi dilakukan dengan melaporkan temuan tersebut kepada PIC klien untuk menghapus file tersebut.

Gambar 3.6 merupakan eskalasi salah satu *alert* yang muncul pada Wazuh Cinepolis.

Territ					
10: 1					Inu 6/12/2025
Cc: I					
Dea					
We have identified a fil	e removal event on th	ie system	nvolving the following software :		
- c:\program files	(x86)\winpcap\unin	stall.exe			
- c:\program files	(x86)\winpcap\rpca	pa.exe			
↓ timestamp: Descending	v agent.name: Descendi	 agent.ip: Descending 	v rule.description: Descending	 id: Descending 	~ Count
Jun 12, 2025 @ 08:59:48.505			Custom FIM: Uninstallation Attempt c:\program files (x86)\winpcap\uninstall.exe	1749693588.105090087	1
			Custom FIM: Uninstallation Attempt c Iprogram files (x86)/winpcapirpcapil eve	1749893588 105081113	
This activity was detect	ted by our File Integri rm whether this action	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detect Could you please confi Thank you.	ted by our File Integri	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detec Could you please confi Thank you.	ted by our File Integri	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detec Could you please confi Thank you. Best Regards,	ted by our File Integri	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detec Could you please confi Thank you. Best Regards,	ted by our File Integri	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detect Could you please confi Thank you. Best Regards,	ted by our File Integri	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detec Could you please confi Thank you. Best Regards, Ignasius Denni Soc - Security Operation	ted by our File Integri rm whether this actio	ty Monitoring system	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance?		
This activity was detec Could you please confi Thank you. Best Regards, Ignasius Denni SOC - Security Operation UPH Gedung CL 5, JL M	ted by our File Integri rm whether this action rm whether this action rm whether this action rm whether this action restored the second	ty Monitoring system on was part of a legitir 10-2 Lippo Karawaci 110	and flagged as a possible uninstallation attempt. nate software uninstallation or system maintenance? • Tangerang 15811		

Gambar 3.6. Contoh Eskalasi Alert Cinepolis

B Wazuh BPD DIY

Ν

Gambar 3.7 merupakan tampilan dari Wazuh BPD DIY.

← → C 🛛 😣 Not s								. ९ 🖈	
🔠 🚺 WhatsApp 🛭 🕤 Playbook א	ISS 😈 SOC	LIVDIUP 🖭 M	iail - SOC VISI	SOC VIS	aonec P 👦 Carbonio 🧧 sentinei Oi		SDP ServiceDe	. 👦 TheHive - L	
W. Dashboards Dashboard Aler	t Level 12+						Full screen Share Clo	ne Reporting	🖉 Edit 🛛 M
Search					DQL	• ~	Jun 13, 2025 @ 06:	30:00.000 → now	C' Refrest
NOT SOC Agent ×									
lert Lovel 12+						Grafik Ru	le Level 12+		
é.					ÎÎ	30 -			• 12
llert(s)	Rule ID	✓ ↓ Rule Level	~ Count						• 13
FORTIGATE: Web Filter - Phishing URL Event	900074	13	6			25 -			
FORTIGATE: Web Filter - ZGrab.Scanner Event	900076	12	12			20			
ORTIGATE: IPS - Nmap Scanner Event	900077	12	8						
ORTIGATE: Web Filter - Potentially Unwanted Pro	900078	12	4			tuno 15			
Frend Micro Apex One: Virus/Malware Event	800002	12	2			ŭ	27		
Wazuh agent disconnected	504	12	1			10			
			33						
						5.			
					I		4	R.	
							12: Rule Level	13: Rule Level	
					1				
N U. 20180			1-12 of 12	(1)	Disconnect Agent				
Time agent.name data.hostname	id	rule.description	data.dstip	data.srcip	4			na eee anachtanachte	
Jun 13, 2825 RSYSLOG 183.23.175.1	174977698	FORTIGATE: Web Filter -	192.168.13.84	20.171.8.156	↓ timestamp: Descending ∨ agent.id: Descen	nding	v agent.name: Descer	iding ~ Count	ř
88:88:21.165	23	zurau.acanner Event			Jun 13, 2025 @ 13:20:01.956 054		TI-OPR-31	1	
08:08:21.163	1/49/7698 1.3713784 21	ZGrab.Scanner Event	192.108.13.84	20.1/1.8.156					
Jun 13, 2025 RSYSLOG 103.23.175.13 0 08:08:21.155	16 174977698 1.3713647 86	FORTIGATE: Web Filter - ZGrab.Scanner Event	192.168.13.84	20.171.8.156					
Jun 13, 2025 RSYSLOG 103.23.175.1	16 174977698 1.3713588	FORTIGATE: Web Filter - ZGrab.Scanner Event	192.168.13.84	20.171.8.156					
00.00.21.133	84		-	_		_			



Untuk klien BPD DIY beberapa alert yang perlu dilaporkan sebagai berikut:

(a) FORTIGATE: Web Filter - ZGrab.Scanner Event

Alert ini muncul ketika terdapat source IP yang ditandai oleh sistem Fortinet sebagai aktivitas ZGrab, yaitu alat pemindaian port yang sering digunakan oleh pelaku ancaman untuk mengumpulkan informasi dari server target [7]. Sebelum dilakukan eskalasi, source IP tersebut diverifikasi terlebih dahulu menggunakan platform threat intelligence. Jika hasil verifikasi menunjukkan bahwa IP address tersebut tergolong berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

(b) FORTIGATE: Web Filter - Phishing URL Event

Alert ini muncul ketika terdapat URL yang ditandai oleh sistem Fortinet sebagai aktivitas phishing, yaitu upaya penipuan untuk memperoleh informasi sensitif seperti kredensial atau data pribadi melalui media digital [8]. Sebelum dilakukan eskalasi, URL tersebut diverifikasi terlebih dahulu menggunakan platform *threat intelligence*. Jika hasil verifikasi menunjukkan bahwa URL address tersebut berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

(c) FORTIGATE: Web Filter - Nmap Scanner Event

Alert ini muncul ketika ada source IP yang ditandai oleh sistem Fortinet melakukan Nmap scanning ke sebuah destination IP. Nmap adalah sebuah alat yang digunakan untuk melakukan scanning terhadap suatu jaringan untuk melihat port/layanan mana yang terbuka [9]. Sebelum dilakukan eskalasi, source IP tersebut diverifikasi terlebih dahulu menggunakan platform threat intelligence. Jika hasil verifikasi menunjukkan bahwa IP address tersebut tergolong berbahaya, maka eskalasi dilanjutkan kepada PIC klien untuk ditindaklanjuti.

(d) Trend Micro Apex One: Virus/Malware Event

Alert ini muncul ketika sistem Trend Micro mendeteksi adanya virus pada suatu *endpoint*. Tindak lanjut yang dilakukan adalah menganalisis terlebih dahulu jenis dan karakteristik virus yang terdeteksi, termasuk jalur infeksi dan potensi dampaknya terhadap sistem. Setelah analisis dilakukan dan dipastikan bahwa ancaman tersebut signifikan, maka dilakukan eskalasi kepada PIC klien untuk penanganan lebih lanjut.

Gambar 3.8 merupakan eskalasi salah satu *alert* yang muncul pada Wazuh BPD DIY.



Gambar 3.8. Contoh Eskalasi Alert BPD DIY

C SOCFortress Internal VDI

Berikut merupakan tampilan dari SOCFortress Internal VDI.

G II VISIONET ~		Q Search or jump to	📾 ctri+k	 0 a 🔮
Home > Dashboards >	L1 Dashboard > Monitoring Dashboard > View panel			
Filter + Filters + Fi	liters +			🗘 Refresh 1m ×
Detail of Alert !!				
> 2022 - 46 - 10 11 126 - 66 - 10 > 2022 - 46 - 10 11 126 - 66 - 10 > 2022 - 46 - 10 11 126 - 66 - 10 > 2022 - 46 - 10 16 - 86 - 26 - 71 > 2022 - 46 - 10 68 - 26 - 71 > 2022 - 46 - 10 68 - 26 - 71 > 2022 - 46 - 10 68 - 26 - 71 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 21 - 48 > 2022 - 46 - 10 68 - 27 - 24 - 48 > 2022 - 46 - 10 28 - 21 - 48 > 2022 - 46 - 10 28 - 21 - 48 > 2022 - 46 - 10 28 - 21 - 48 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 > 2022 - 46 - 10 28 - 21 - 38 </th <th>The problem is a second by the problem is a second to the problem is a sec</th> <th>• 14 # # # # # # # # # # # # # # # # # #</th> <th></th> <th></th>	The problem is a second by the problem is a second to the problem is a sec	• 14 # # # # # # # # # # # # # # # # # #		
> 2025-06-14 17:15:20.977	RDP Login success on weekend by User js-putra.febriko on VM	I-WSJB3VPRD-UP.		

Gambar 3.9. Dashboard SOCFortress Internal VDI

Hampir semua proses eskalasi untuk sistem internal VDI dilakukan melalui platform SDP VDI, yang merupakan sistem pelaporan dan manajemen insiden

internal perusahaan. Sebagian lainnya dieskalasikan menggunakan outlook atau Beberapa *alert* yang perlu dieskalasikan pada SOCFortress VDI antara lain:

(a) RDP Login Success out of office hour

Remote Desktop Protocol (RDP) merupakan sebuah alat yang digunakan untuk mengakses lingkungan *desktop* dan *server* dari jarak jauh [10]. *Alert* ini muncul ketika terdapat pengguna (user) yang berhasil melakukan *login* ke *endpoint* menggunakan protokol RDP di luar jam operasional, yaitu antara pukul 17.00 hingga 07.00. Aktivitas seperti ini dianggap tidak wajar dan berpotensi mengindikasikan akses tidak sah, sehingga perlu segera dilakukan eskalasi kepada tim ITSD tanpa perlu analisis lanjutan.

(b) Log4j RCE attack attempt detected

Alert ini muncul ketika sistem mendeteksi adanya upaya serangan *Remote Code Execution* (RCE) yang mengeksploitasi kerentanan pada platform Log4j. Log4j adalah sebuah *library open-source* gratis yang mengimplementasikan *logging framework* [11]. RCE adalah sebuah kerentanan yang memungkinkan penyerang untuk menjalankan kode mereka dalam mesin korban [11] [12]. Sebelum dilakukan eskalasi, dilakukan pengecekan terlebih dahulu terhadap *source IP* menggunakan platform *threat intelligence*. Jika IP address tersebut teridentifikasi sebagai malicious, maka eskalasi segera dilakukan kepada tim ITSD untuk melakukan blok terhadap IP tersebut.

Berikut merupakan tampilan dari SDP Visionet.

Visi					Q & D (
🗍 All My	(Requests -				076
D	Subject	Created Date	J∱ Status	Resolved Date	Assigned To
03348	SSH Login success out of office hours by user vmin.local on vn-zbmtap01-cb.visionet.co.id	Mar 10, 2025 05:29 AM	Closed	Mar 10, 2025 08:47 AM	Tech Muhammad Sant
03068	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - NB-MTR-ATM-01-CB.	Mar 8, 2025 11:45 PM	Closed	Mar 8, 2025 11:51 PM	Tech Christian Andreanto
02923	Report SOC Monitoring Malicious Sentinel One Event - vn-cbpx1vdrc-gt.visionet.co.id 10.172.192.248	Mar 8, 2025 03:42 PM	Closed	Mar 10, 2025 02:02 PM	Tech Johan Wardono
02922	Report SOC Monitoring Malicious Sentinel One Event - vn-cbpx1vdrc-gt.visionet.co.id 10.75.8.5	Mar 8, 2025 03:25 PM	Closed	Mar 10, 2025 02:03 PM	Tech Johan Wardono
02851	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - NB-MTR-ATM-01-CB.	Mar 8, 2025 06:11 AM	Closed	Mar 8, 2025 06:16 AM	Tech Muhammad Niza
02831	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-VCWS1VDRC-GT	Mar 8, 2025 04:45 AM	Closed	Mar 10, 2025 02:05 PM	Tech Johan Wardono
02766	SSH Login success out of office hours by user vmin.local on vn-cbpx2vprd-up.visionet.co.id .	Mar 8, 2025 01:34 AM	Closed	Mar 10, 2025 11:45 AM	Tech Johan Wardono
02764	SSH Login success out of office hours by user vmin.local on vn-cbpx1vprd-up.visionet.co.id .	Mar 8, 2025 01:15 AM	Closed	Mar 10, 2025 11:42 AM	Tech Johan Wardono
02746	SSH Login success out of office hours by user main.vn = 5 on vn-zbmtap02-uph	Mar 7, 2025 11:42 PM	Closed	Mar 10, 2025 11:42 AM	Tech Bagus Padma
02745	SSH Login success out of office hours by user main.vn $ = 5 $ on vn-zbmbx03-cb.visionet.co.id	Mar 7, 2025 11:41 PM	Closed	Mar 10, 2025 11:41 AM	Tech Bagus Padma
02470	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - NB-MTR-ATM-01-CB.	Mar 7, 2025 06:25 AM	Closed	Mar 7, 2025 06:32 AM	Tech Andrie Syahriandy
02467	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-DB-MON-UPH.	Mar 7, 2025 05:46 AM	Closed	Mar 7, 2025 09:58 AM	Tech Heri Cahyono
02465	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-JUMPBOXPUB-UPH	Mar 7, 2025 05:43 AM	Closed	Mar 7, 2025 09:59 AM	Tech Dedik Nurdiantoro
02464	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-VCWS1VPRD-UP.	Mar 7, 2025 05:42 AM	Closed	Mar 7, 2025 09:59 AM	Tech Dedik Nurdiantoro
02412	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - NB-MTR-ATM-01-CB.	Mar 7, 2025 01:22 AM	Closed	Mar 7, 2025 01:24 AM	Tech Andrie Syahriandy
2376	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-Veeam-exCB01.	Mar 6, 2025 11:52 PM	Closed	Mar 7, 2025 08:34 AM	Tech Febriko Putra
2373	VERIFIKASI AKTIFITAS - RDP Login success out of office hours - VN-ADFS1VPRD-UP.	Mar 6, 2025 11:43 PM	Closed	Mar 6, 2025 11:53 PM	Tech Febriko Putra
2372	VERIEIKASI AKTIEITAS - RDP Login success out of office hours - VN-VCWS1VDRC-GT	Mar 6, 2025 11:36 PM	Closed	Mar 6, 2025 11-52 PM	Tech Febriko Putra

Gambar 3.10. SDP Visionet

3.3.3 Sistem EDR

Endpoint Detection and Response (EDR) adalah teknologi keamanan siber yang secara kontinu memantau aktivitas pada *endpoint* untuk mendeteksi adanya ancaman serta melakukan tindakan otomatis guna membantu mitigasi. *Endpoint* mencakup berbagai perangkat fisik yang terhubung ke jaringan seperti desktop, laptop, ponsel, mesin virtual, dan perangkat *Internet of Things* (IoT), yang semuanya dapat menjadi titik masuk bagi penyerang. Solusi EDR mencatat perilaku *endpoint* selama 24 jam penuh dan menganalisis data tersebut untuk mengidentifikasi aktivitas mencurigakan, seperti indikasi serangan ransomware. Selain mendeteksi, EDR juga mampu melakukan isolasi otomatis terhadap ancaman serta mengirimkan notifikasi kepada tim keamanan, yang kemudian dapat menggunakan data yang tercatat untuk menyelidiki secara rinci bagaimana insiden terjadi, apa saja yang terdampak, dan langkah penanganan yang perlu dilakukan selanjutnya [13].

Berikut merupakan tampilan dari EDR SentinelOne.

20 Monitoring Sistem SIEM dan EDR..., Ignasius Denni Hermawan, Universitas Multimedia Nusantara

JSANTA

←	→ C					а д д∣@:
		Mail - SUC VISI		Carbonio Sentinel C	one SDP ServiceDe	S TheHive - Login >>
\$	Cickel / ST Vicional Russ International - 33475		-		liate	
\$						Soc monitoring (current not for Soc L)
0	INCIDENTS THREATS THREAT SERVICES					
Q						
((-))						
*				Group by	Hash () No Items Selected 7 Threat Group:	100 Results 🗸 Columns 🧹 😰 Export
0				Endpoints 0 E Reported Tim		etecting Engine 👔 Initiated By 👔 Classification
R		Suspicious	Suspicious 🐱 Unresolved	MB-COR-TOMM Are 13th 202	5 • 12:46:21 Jun 13th 2025 • 12:49:47 (In-Write Static AI Agent Policy Malware
\$	V C Providence (+1 More)	Malicious		<u>NB-IT-NICH</u> Am 12th 202	5 + 12:25:58 Jun 13th 2025 + 12:25:58 5	entinelOne Cloud Agent Policy Malware
ŝ	AnstallZ_wait_tocpy (*1 Mare)	Suspicious		wn-asws1vprd-up Am 13th 202	5 • 11:04:44 Jun 13th 2025 • 11:04:46 P	pplication Control Agent Policy Malware
lis.		Suspicious	Suspicious Vinresolved	kg <u>un-asws1vprd-up</u> Am 13th 202	5 • 09:47:45 Jun 13th 2025 • 11:04:38 #	pplication Control Agent Policy Malware
<u>@</u>		Suspicious	Suspicious Unresolved	Krr <u>vn-asws1vprd-up</u> Am 13th 202	5 • 09:44:51 Jun 13th 2025 • 09:47:38 F	pplication Control Agent Policy Malware
\$		Suspicious	Suspicious Unresolved	V be un-asses layerd-up Are 13th 202	5 • 09:44:51 Jun 13th 2025 • 09:47:38 /	pplication Control Agent Policy Malware
	2 PM2DotNetHelper.exe (D1 Mage)	Malicious		V 106-202	5 • 08:35:28 Jun 13th 2025 • 08:35:30 (In-Write Static Al Agent Policy Malware
3"						

Gambar 3.11. Dashboard EDR SentinelOne

Eskalasi untuk *alert* yang muncul pada SentinelOne dilakukan melalui Outlook secara langsung kepada pengguna *endpoint* yang terlibat. Nama pengguna biasanya sudah tercantum dalam *alert*, dan alamat email pengguna dapat diperoleh dari informasi tersebut. Sebelum dilakukan eskalasi, tim SOC L1 terlebih dahulu melakukan pengecekan terhadap *hash* file yang terdeteksi menggunakan platform *threat intelligence*. Jika *hash* file tersebut dikategorikan sebagai malicious, maka tim L1 akan segera mengambil tindakan dengan menggunakan fitur *remote shell* dari SentinelOne untuk menghapus file berbahaya tersebut secara langsung dari *endpoint*. Namun, apabila hasil pengecekan tidak menunjukkan bahwa file tersebut berbahaya, maka tim L1 akan menghubungi pengguna terkait untuk menanyakan legitimasi atau keabsahan file yang menjadi sumber *alert* tersebut. Berikut adalah bentuk eskalasi yang dilakukan melalui email *Office Outlook*.

COCIE					(· · ·)				() () () () () () () () () ()
SOF Vielonat					(++)	The Reply	Reply all	Forward	
To:									Thu 6/12/2025 12:33
Cc:									
De									
Telah terjadi secu Waktu: Jun 12, 20	rity incident pada End	point							
Source Hostname	e/IP/ User								
Severity High	Windows II FIO 20	100							
Al Confidence Los	ol: Malioious								
Threat File Name	in manorous								
\Device\HARDDI	SKVOLUME4\New fol	der\CheatEvolution\Che	atEvolution exe						
Statue: Killed and	Quarantined	der (Cheat Evolution (Che	att votation.exe						
Treat Status M	TIGATED A Confidence Lovel MALICI	OUS multer Workst. Undefined ~	heidere Status. Unresolved v]					
NETWORK HEATORY	FIGATED At Confidence Lower MALICI alem: KILLED © US QLARANTINEC 12, 2025 12:34-48 L 2025 12:34-48 L	CUS Index Veda: Undefined v	ind Q	nd this hash on Deny Visibility					
THERE AND A CONTRACT AND A CONTRACT FOR A CONTRACT AND A CONTRACT	TIGATED Af Confidence Level: MALICI wirr: KOLED 9 U1 QUARANTINEE 12. 2005 12: 34:46 12. 2005 12: 34:46 12. 2005 12: 34:46 12. 2005 12: 34:46 12. 2005 12: 34:46 12. 2005 12: 34:46	OUS Index webs: Undefined • • • 14 Outy 1 Site on the same make 1 Account / 1 Site / 1 Group	index Salar Unresolved v	nd thin hands on Deng Visibility Heart Nano Shanger File - Texensities Architects					
	TIGATED A Continues Level MALICI wirm: KOLED 9 J1 QUARANTINEE 12. 2025 12: 34-86 3 12. 2025 12: 34-86 3 Stratutions 3	OLS Indust tools Undefined • • • • • • • • • • • • • • • • • • •	instant Salara (Deressident) v and Q P S Carp Instant () Deneshard Instant ry - Keen Palay	nd this bank an Dung Vikibility Ball Nager Nager This					
Increase Market And Andrew Andre	Incarton Ad Continues Level MALICI Address Address Address Address 12, 2005 123.448 Address Address Address 12, 2005 123.448 Address Address Address Address Address Address Address Address Address Address Address Address Address Observert/MACCENVOLUME.com Thittee Statem Chanding Address Thittee Statem Chanding Address Thittee Statem Chanding Address	OUS have week to defined *	instant halos (Unseeding)	el Bik kadı en Deny Vikidely Kıcıl Narı Naral Fili					
Incrementary of the second sec	TIGATED A Gordanas Lovel MALLES Marrier KALED © 11 QUARANTINES 22,005 12,34.48 3,005 12,34.48 Dovient/ADCOSYCILLINE Film "Divise Marridonas"	OUS Indext Works Underfined • • • • • • • • • • • • • • • • • • •	Instant Salar Ubersahlmad u and Q Pa Cape Danks D Dankala 1 Matantah, Agen Dahy Tagan Dahyang Matantah Daham Salar Dahyang Matantah Dankala Salar Dahyang Matantah Matantah Daham Salar Dahyang Matantah Matantah Dahyang Matantah Daham Salar Dahyang Matantah Matanta	nd the last or Deep Vielding Heat Team Near Time					
Incrementary of the second sec	TIGATED A Continues Loss MALES According to the Males According to t	OUS Advanture Underflored	Instant Kalan Ukenseland v and Q Par Constant () Denalated Ministry Agen Palay Styles Styles Denalated () Denalated Ministry Agen Palay Styles Styles Denalated () Malant Denalated () Malant Denalated () Malant Denalated () Malant Denalated () Malant Denalated () Malant Denalated () Malant Malant	nd this bank on Drong Veikeling Konte Neur Indeed File					
Incrementary of the second sec		OUS Indust webs: Undefined • OUS Construction of the second reduct of t	And Carrier States (Unresolved) ~ ~	and the land at the probability State State State State					
Restance Market	TEGATED A Combined control MALEC A combined control MALEC QUARANTRACE A combined control MALEC QUARANTRACE Disposed bits	OD5 here wells: Undefined	interesting Unregalized or interesting Constraints interesting Constraints interesting interesting interesting interesting interesting int	d da hati n Duy Vabiy Int Nor Mar Nor Mar Fit I Manita Articla					
Incrementary of the second sec	INGATED A Contract Lond MALEC AND RELED O 11 QUARATIVE 2.2051123448 distuitations Visuaria/MCCOSYCULAR con 2.305123448 Visuaria/MCCOSYCULAR con 2.3051234 Visuaria/MCCOSYCULAR con 2.3051234 Visuaria/MCCOSYCULA	OUS have wells. Undefined • OUS City J form on the recent method Out J Annuel / 150/ 1 Group I Marked / 150/ 1 Group Interfedentiated	inter have Unexailered -	al da bak ar Day Vikilay Anter The Areanis & Control Mar The Areanis & Control CCD673 BIBLIAGN					
Received and the second	TIGATED A Continue torell MALECI Marcelline Marcelline QUARANTINE 2019 Marcelline QUARANTINE 2019 Marcelline QUARANTINE 2019 Marcelline Marcelline ChokenVADCORVCLUME.01A Marcelline Statistics To the stater Characteristics on the Statistics Statistics Statistics Statistics Statistics Statistics Statistics	OUS Indust Work: Undefined • OUS Charlest Work: Undefined • Out of first on the control endpe Date of first on the control endpe Date of the Charlest One of the Charl	Institute Ration (Unresultent) or and (Q) (Particular Statement) (Particular) Statement (Particular	Hit had at Day Vision Tart Not Net The Terrorities Address CRAPT RELINCY					
Restriction of the second seco	ITEATED & Control on MALEC Anno RELEO & U.1 QUARANTINES 2. 2005 12.54-00 Distribution Control Contr	OUS	Instant Kara Unresoluted v Control Control Co	nd da kuda ur Day Vahlay Jerri Ver Mar Terri Mar Terri Veranda 4 (1911) Ur Handa 1 (1911)					
Increase of the second	TEGATED a Combinest control MALEC Anime RELED 9.1 QUARANTINED 200513244 QUARANTINED 200513244 QUARANTINED 200513244 QUARANTINED 20040400000000000000000000000000000000	005	Instant Kara Unreaded y	nd da kuda ur Day Vahlay Jerr Ver Mar Day Mar					
Restance Market Restance Market Restance Market Restance Market Restance Market Restance Market Restance Rest	INGENED A Contract of MALEC And INFELED © U1 QUARANTEE 2. 2051 23:448 23. 2051 23:448 24. 2051 23:448 25. 2051 25. 2051 25. 2051 25. 2051 25.	005 Index Works: Undefined * 0 0 0 1 0 0 1	Institute Hairs Uterestitute	of the back at Data Value Particular Market States and Address and Addr Address and Address and Addre					

Gambar 3.12. Contoh Eskalasi EDR SentinelOne

Dalam laporan eskalasi ada beberapa hal yang perlu dicantumkan yaitu:

- 1. Nama endpoint
- 2. Waktu alert muncul di SentinelOne
- 3. Nama dan alamat IP pengguna
- 4. Operation System yang digunakan endpoint
- 5. Tingkat severity dari alert
- 6. Keputusan dari AI SentinelOne tentang seberapa berbahaya *alert*
- 7. Nama dan file path dari file yang terdeteksi
- 8. Bukti bahwa alert muncul berupa screenshot
- 9. Screenshot dari sebuah threat intelligence yang menunjukkan reputasi dari file yang terdeteksi
- 10. Analisa singkat mengenai file yang terdeteksi
- 11. Tindakan yang telah dilakukan oleh SOC dan saran tindakan bagi pengguna

<complex-block> Vertical Wirder Michael Mi

Berikut merupakan salah satu alert yang muncul di SentinelOne.

Gambar 3.13. Contoh Alert dari SentinelOne

Gambar 3.13 merupakan *screenshot* dari alert yang menyoroti hal-hal yang penting untuk diketahui oleh penerima laporan. Hal-hal yang perlu disoroti adalah Status dari *file* berbahaya, Waktu *alert* muncul, Informasi mengenai *file* seperti nama, *file path*, dan *hash*, *Engine* yang digunakan SentinelOne untuk mendeteksi *file*, Klasifikasi yang diberikan oleh SentinelOne untuk *file*, dan Informasi mengenai *endpoint*.

3.4 Kendala dan Solusi yang Ditemukan

Selama pelaksanaan kerja magang ini ditemukan beberapa kendala ketika melaksanakan tugas. Beberapa kendala yang ditemukan adalah sebagai berikut.

- Saat menjalani masa magang di divisi SOC L2 selama satu bulan, karena bukan merupakan pegawai tetap tidak diberikan akses untuk menggunakan VPN perusahaan.
- 2. Karena *alert* yang muncul di SentinelOne dilaporkan secara langsung kepada pengguna yang terkait, terkadang ditemukan *alert* dengan nama pengguna yang kurang jelas, seperti "*Administrator*". Hal ini dapat menyulitkan dalam proses identifikasi pemilik perangkat yang sebenarnya.

Dari berbagai kendala yang dialami selama kegiatan magang, berikut adalah solusi-solusi yang ditemukan untuk menangani masalah tersebut:

- 1. Diberikan tugas yang tidak memerlukan akses VPN, yaitu melakukan pencarian dan pemantauan berita terkait CVE serta *credential leak* menggunakan platform *threat intelligence* Recorded Future. Informasi yang diperoleh digunakan sebagai bahan analisis potensi ancaman yang mungkin berdampak pada klien maupun sistem internal perusahaan.
- 2. Melakukan koordinasi terlebih dahulu dengan PIC utama dari klien untuk mengidentifikasi nama pengguna dari *endpoint* terkait. Jika informasi tidak tersedia, maka dilakukan pelaporan kepada tim *IT Support* klien agar dapat ditindaklanjuti dan langsung dilaporkan ke pengguna *endpoint*.

