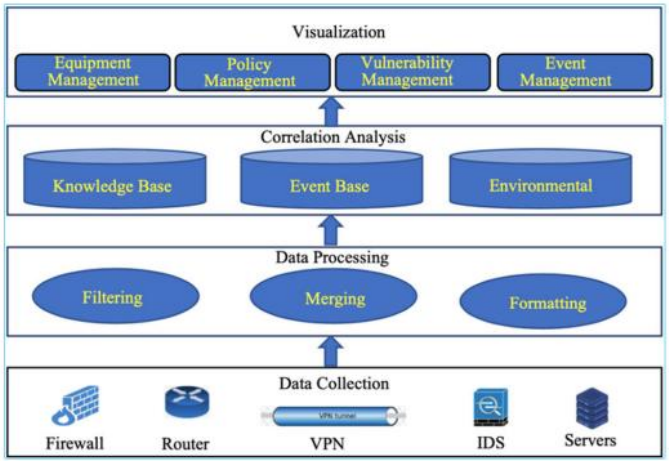
BAB III
PELAKSANAAN KERJA PROFESI

3.1 Bidang Kerja

Selama masa pelaksanaan kerja profesi di PT NOOSC Security Global, praktikan diarahkan pada posisi *Cyber Security Intern*, ditempatkan pada posisi *Security Operation Center Analyst* (SOC), *Cybersecurity Analyst*, *Cybersecurity Engineer,* dan VAPT *and Project Manager*. Pada kegiatan kerja praktik di posisi SOC *Analyst*, praktikan melakukan kegiatan pemantauan dan analisis ancaman keamanan siber dalam proyek pengamanan infrastruktur digital perusahaan. Posisi ini bertujuan untuk meningkatkan keamanan jaringan dan data perusahaan melalui deteksi dini ancaman dan respon insiden. Pada **Gambar 3. 1** menggambarkan model arsitektur SOC secara umum, yang menunjukkan empat komponen yaitu: *data collection, data processing, correlation analysis,* dan *visualization*. Salah satu model SOC yang diusulkan oleh Bidou dkk mendefinisikan SOC, yang terdiri dari lima bagian: *event generators, event collectors, message databases, analysis engines,* dan *reaction management software*.



Gambar 3. 1 Arsitektur SOC
Sumber: Shahjee, 2022

Security Operation Center Analyst (SOC) adalah pusat operasi keamanan siber organisasi. Tujuan utamanya adalah untuk mendeteksi dan merespons insiden dan ancaman keamanan di seluruh infrastruktur organisasi. SOC *Analyst* dikelola oleh para profesional keamanan terlatih yang memantau sistem dan jaringan organisasi untuk mencari tanda-tanda ancaman siber, seperti *malware*, serangan *phishing*, dan aktivitas berbahaya lainnya. SOC Analyst menggunakan kombinasi *People*, *Process*, dan *Technology* untuk mengelola dan merespons insiden keamanan. Hal ini mencakup pemantauan peristiwa dan peringatan keamanan secara *real-time*, investigasi dan analisis insiden, serta respons dan remediasi. SOC juga berkolaborasi dengan departemen lain dalam organisasi, termasuk TI dan *compliance*, untuk memastikan bahwa kebijakan dan prosedur keamanan dipatuhi (Mughal, 2022). Sebagai bagian dari tim SOC *Analyst*, ada 5 bidang kerja yang mencakup beberapa aspek dalam pemantauan dan penanganan insiden keamanan sebagai berikut.

1. *Security Monitoring* yaitu praktikan bertugas untuk memantau sistem dan jaringan secara *real-time* menggunakan alat seperti SIEM (*Security Information and Event Management*), *firewall*, dan *Intrusion Detection System/Intrusion Prevention System*. Hal Ini mencakup pemeriksaan dan analisis *log* keamanan untuk mendeteksi anomali atau aktivitas yang mencurigakan, seperti upaya akses ilegal atau serangan siber.

2. *Threat Analysis* yaitu setelah mendeteksi adanya potensi ancaman, praktikan melakukan analisis mendalam terhadap data log dan indikator ancaman. Tujuan dari analisis ini adalah untuk mengidentifikasi apakah ancaman tersebut benar-benar valid, serta menentukan tingkat keparahan dan dampaknya pada sistem.

3. *Incident Response and Handling* yaitu jika ditemukan ancaman yang nyata, praktikan berperan dalam proses respon insiden, termasuk mitigasi serangan atau eskalasi ke tim yang lebih berpengalaman. Ini bisa berupa isolasi perangkat yang terinfeksi, pemutusan koneksi jaringan, atau pembersihan *malware*.

4. *Reporting and Documentation* yaitu praktikan bertanggung jawab untuk menyusun laporan mengenai insiden keamanan yang terjadi, aktivitas yang dipantau, dan tindakan mitigasi yang dilakukan. Laporan ini diserahkan kepada manajemen keamanan atau pihak terkait lainnya untuk evaluasi lebih lanjut.

5. Berkolaborasi dengan tim keamanan siber internal dan eksternal termasuk *Cyber Security Analyst* dan *Incident Response Team*.

Selain menjadi *Security Operation Center Analyst* (SOC), praktikan diberikan kesempatan untuk mengikuti program kerja profesi di posisi *Cybersecurity Analyst*. Tugas praktikan meliputi pembuatan presentasi, rekapitulasi tiket, visualisasi data untuk laporan tiket, kenaikan *coverage* Sophos dan jumlah *device* selama sebulan, analisis *log* untuk pembuatan *use case* pada *dashboard monitoring* SOC dan membuat panduan teknis untuk digunakan SOC. Selama proses ini, praktikan menggunakan beberapa aplikasi seperti Microsoft Excel, Canva dan Splunk untuk menyelesaikan proyek secara optimal. Hal ini memungkinkan para praktikan untuk meningkatkan keterampilan analisis data dan berkontribusi pada pemahaman yang lebih baik mengenai hasil analisis yang berguna bagi *Cybersecurity Analyst.*

Praktikan diberikan kesempatan untuk mengikuti program kerja posisi *Cybersecurity Engineer.* Tugas praktikan mencakup *dismantle server*, instalasi SIEM Wazuh, simulasi penyerangan ke Wazuh, membuat server dan konfigurasi *firewall*. Selama menjalani pekerjaan ini, aplikasi yang dibutuhkan seperti VMware, OS Ubuntu Live Server, PuTTY dan Pfsense.

Dalam proyek *Pilot Project Technical Security Assessment*, Praktikan diarahkan sebagai *Project Manager* yang memastikan kelancaran setiap tahap pekerjaan. Pada tahap awal, Praktikan melakukan inisiasi kebutuhan dengan mencatat dan menentukan kebutuhan pengguna terkait VAPT (*Vulnerability Assessment and Penetration Testing*). Langkah ini melibatkan diskusi untuk memahami apa yang diinginkan oleh pengguna, termasuk area yang akan diuji keamanannya dan risiko yang menjadi prioritas mitigasi. Hasil dari inisiasi kebutuhan ini membantu Praktikan dalam menetapkan *scope* proyek yang jelas, sehingga setiap aktivitas memiliki fokus yang sesuai dengan harapan pengguna.

Selanjutnya, Praktikan menyusun *timeline* proyek dengan menentukan kegiatan awal hingga akhir, menggunakan *kanban board* untuk pengelolaan tugas harian dan *gantt chart* untuk memetakan keseluruhan jadwal. Praktikan juga mendefinisikan *output* proyek berupa laporan teknis yang mencakup temuan kerentanan, analisis risiko, dan rekomendasi mitigasi. Dalam pelaksanaan, Praktikan memanfaatkan *tools* seperti Google Slide untuk penyampaian laporan, Tenable Nessus untuk pemindaian kerentanan, dan Canva untuk menghasilkan laporan yang informatif dan menarik.

3.2 Pelaksanaan Kerja

Kerja Profesi yang praktikan kerjakan dimulai dari 8 Juli 2024 sampai 7 Januari 2025, praktikan diarahkan ke divisi *Cyber Security Intern* yang mencakup program kerja dari *Security Operation Center Analyst*, *Cybersecurity Analyst*, *Cybersecurity Engineer*, *Vulnerability Assessment Penetration Testing* (VAPT) and *Project Manager*. Dimulai dari *Onboarding Cyber Security Intern*, pemahaman *job description*, pemberian materi, hingga ke penerapan program kerja yang diarahkan pembimbing, berikut **Tabel 3.1** merupakan *gantt chart* dari *timeline* praktikan selama KP di PT NOOSC Security Global.

Tabel 3. 1 Gantt Chart Timeline Praktikan

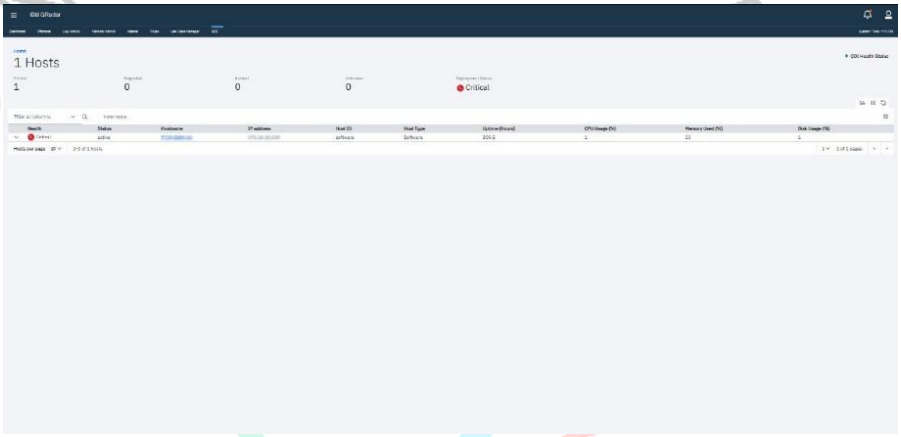
No	Kegiatan Praktikan	Juli				Agustus				September				Oktober			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	*Onboarding Cyber Security Intern*																
2	Pemberian materi oleh Pembimbing																
3	SOC *Analyst*																
4	*Cybersecurity Analyst*																
5	*Cybersecurity Engineer*																
6	VAPT *and Project Manager*																

3.2.1 Security Operation Center Analyst

Praktikan masuk ke kantor pada shift 1 yaitu pukul 07.00 WIB, berikut tugas –tugas yang dilaksanakan praktikan saat menjadi SOC *Analyst* di PT NOOSC Security Global:

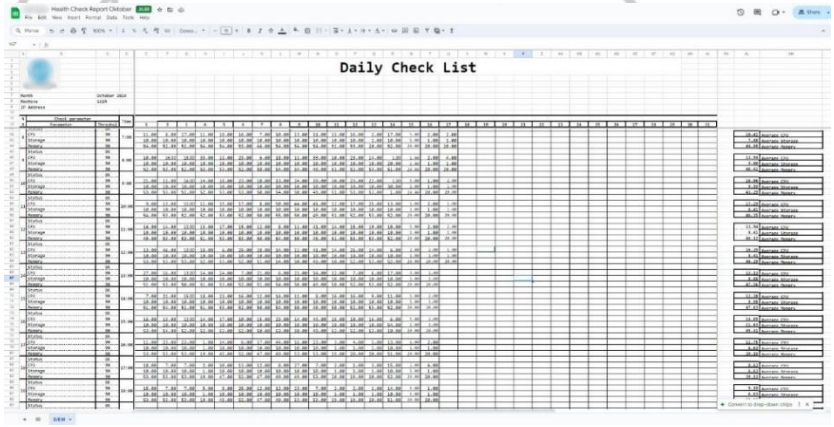
1. Pemeriksaan Health Check pada SIEM Qradar

   Pada **Gambar 3. 2** praktikan melakukan pemeriksaan *health check* Qradar. *Health check* pada SIEM adalah proses pemeriksaan rutin untuk memastikan bahwa sistem SIEM bekerja dengan optimal. Proses ini sangat penting bagi SOC karena memastikan sistem tetap berfungsi untuk mendeteksi ancaman dengan cepat dan tepat.



Gambar 3. 2 Health Check Qradar

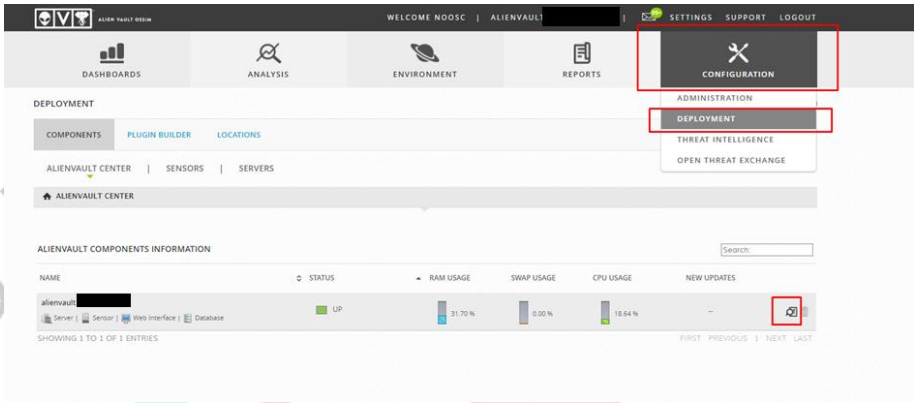
Setelah itu, **Gambar 3. 3** praktikan melaporkan hasil *health check* mencakup *CPU Usage, Memory Usage*, dan *Storage Usage* di Google Spreadsheet pada pukul 07.00 WIB dan seterusnya setiap satu jam sekali.



Gambar 3. 3 Pengisian Hasil Health Check Qradar

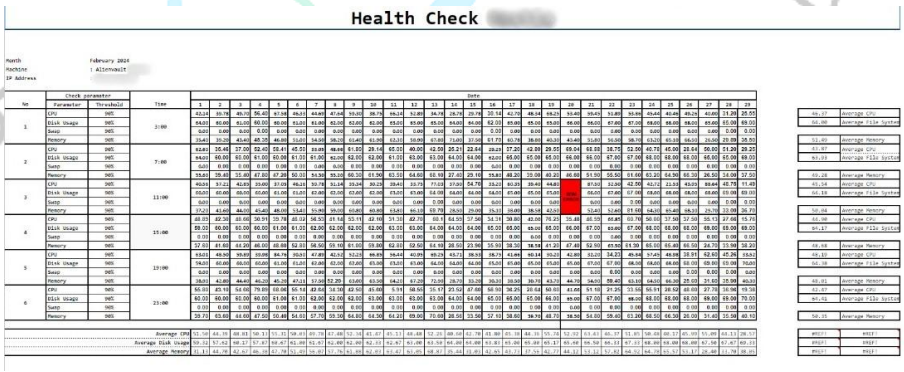
2. Pemeriksaan Health Check pada SIEM Alienvault

Pada **Gambar 3. 4** praktikan juga melakukan pemeriksaan *health check* untuk pengecekannya ke menu *configuration* setelah itu ke *deployment* yang berisi *CPU*, *Disk Usage*, *Swap*, dan *Memory* SIEM Alienvault pada pukul 07.00 WIB dan seterusnya setiap 4 Jam sekali.



Gambar 3. 4 Health Check Alienvault

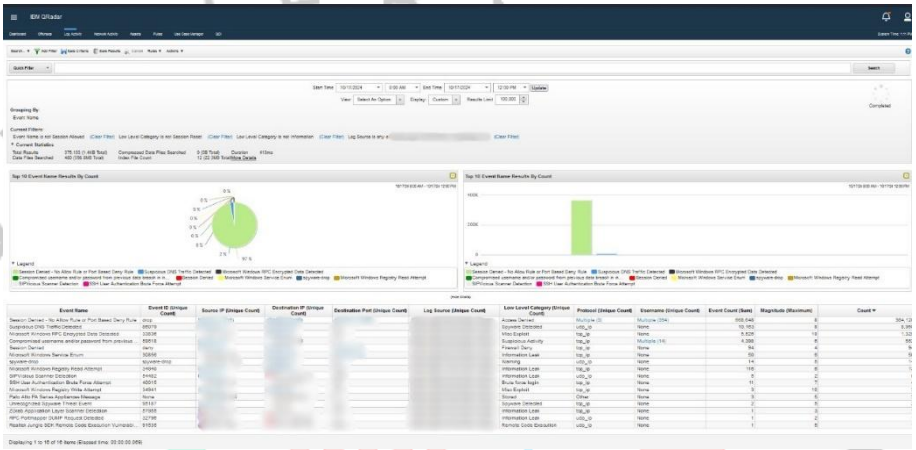
Setelah itu **Gambar 3. 5** praktikan mengisi hasil pemeriksaan ke Google Spreadsheet untuk memastikan kinerja optimal dari SIEM AlienVault dan mencegah *downtime* atau kelambatan dalam pemrosesan data keamanan.



Gambar 3. 5 Pengisian Hasil Health Check Alienvault

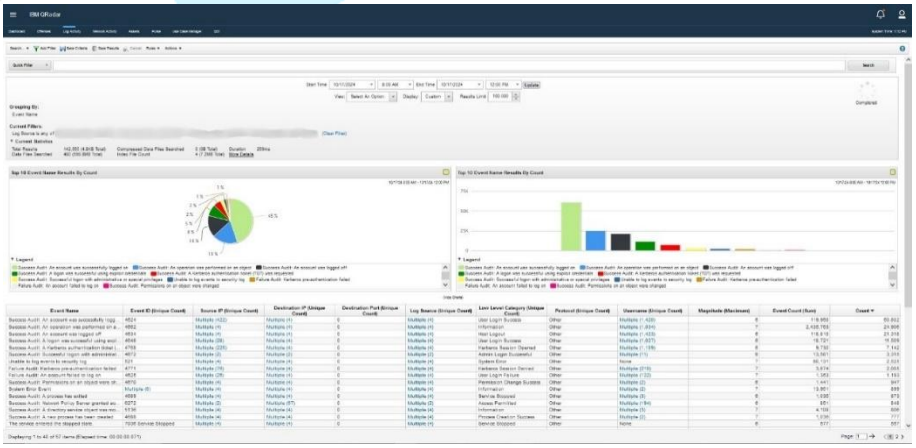
3. Laporan Operasional dari SIEM Qradar

Pada **Gambar 3. 6** Praktikan melakukan penarikan data dari *dashboard* Panorama dengan mengambil *top 5 event name, count, low level category,* dan *action.* Hal ini berguna untuk membantu praktikan dalam menyaring data yang paling penting dalam rangka menganalisis dan mengidentifikasi potensi masalah atau ancaman dalam sistem keamanan yang dipantau.



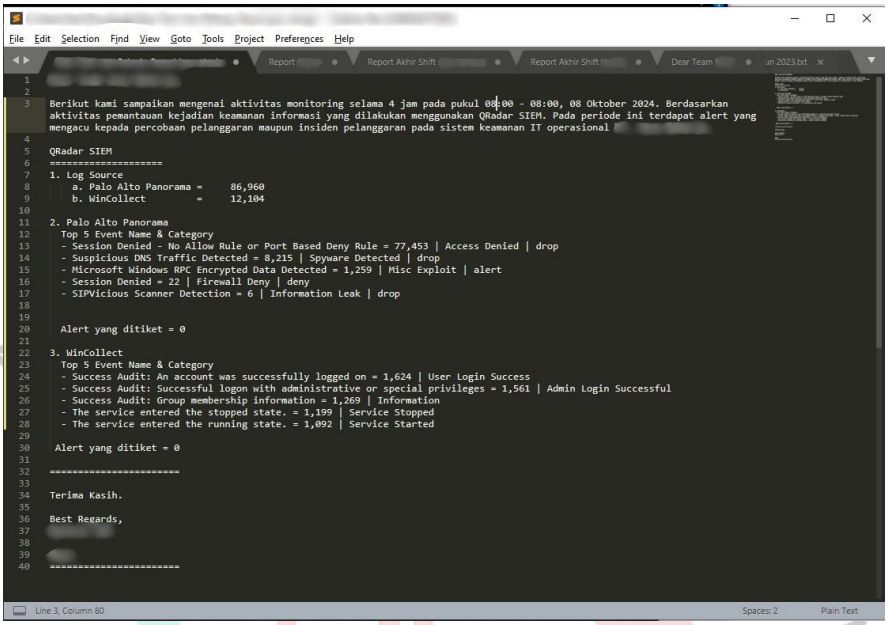
Gambar 3. 6 Dashboard Penarikan Data dari Qradar Panorama

Dibawah ini, **Gambar 3.7** menunjukkan penarikan data dari *dashboard* Wincollect dengan *start time* 04.00 dan 08.00 *end time*, dengan mengambil *top 5 event name, event count, low level category,* dan *action*.



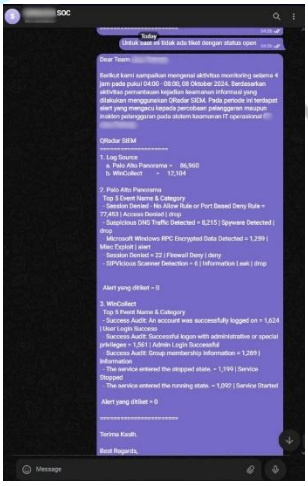
Gambar 3. 7 Dashboard Penarikan Data dari Qradar Wincollect

Setelah itu data yang sudah ditarik dari *dashboard* dimasukkan ke dalam *template* laporan operasional yang sudah disediakan di aplikasi Sublime Text pada **Gambar 3. 8** dibawah ini**.**



Gambar 3. 8 Template Laporan Operasional Qradar

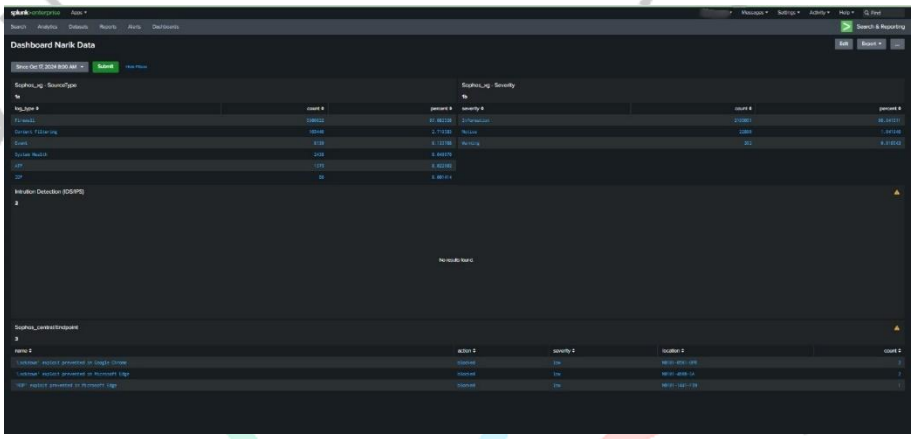
Setelah itu pada **Gambar 3. 9** praktikan mengirimkan laporan setiap 4 Jam sekali ke klien pada pukul 08.00 dan 12.00 disertai dengan total result log source Panorama dan Wincollect, *top 5 event name and category*, keterangan dan jumlah *alert* yang dibuatkan tiket oleh tim SOC setelah terjadinya insiden.



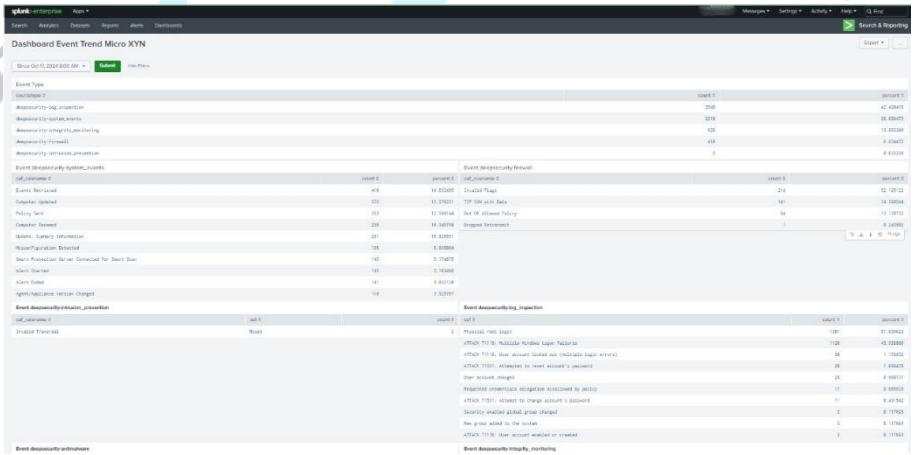
Gambar 3. 9 Pengiriman Laporan melalui Telegram

4. Laporan Operasional dari SIEM Splunk

Praktikan melakukan penarikan data dari SIEM Splunk pada **Gambar 3. 10** *dashboard* Sophos dan **Gambar 3. 11** *dashboard* Trend Micro dengan *start time* 04.00 *until now* untuk pengiriman laporan operasional pada pukul 08.00 dan *start time* 08.00 *until now* untuk Jam 12.00. Data yang ditarik termasuk Source Type, Severity, Event Attack, dan Ticket Details. Data tersebut sangat penting untuk pengelolaan insiden keamanan yang baik dan untuk meningkatkan keamanan secara keseluruhan.



Gambar 3. 10 Dashboard Penarikan Data Splunk untuk Sophos

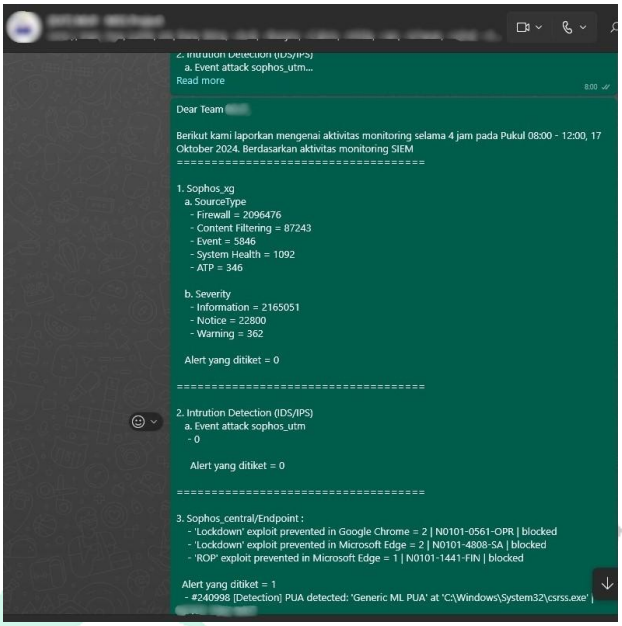


Gambar 3. 11 Dashboard Penarikan Data Splunk untuk Trend Micro

Jika data dari kedua dashbor Sophos dan Trend Micro sudah ditarik, setelah itu dimasukkan kedalam *template* laporan yang sudah disediakan tim SOC di aplikasi Sublime Text pada **Gambar 3. 12**.

Gambar 3. 12 Template Laporan Splunk

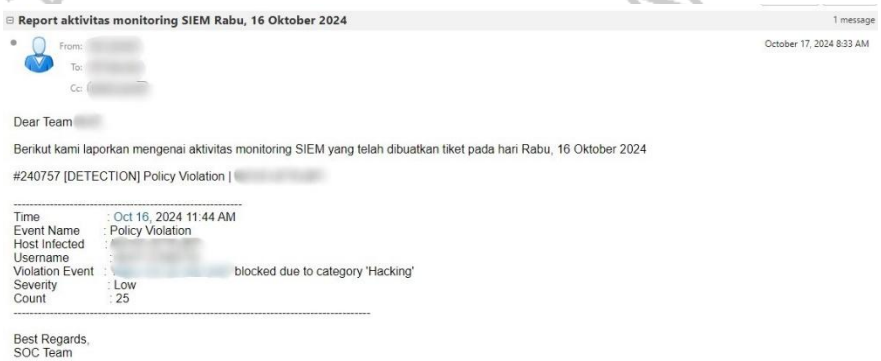
Pada **Gambar 3. 13**, setelah itu data yang sudah ditarik dimasukan ke *template* laporan operasional yang telah untuk mengirimkan laporan setiap 4 Jam sekali ke klien yang berisi keterangan *event* penting yang bisa menjadi indikasi ancaman keamanan atau aktivitas mencurigakan, jumlah dan keterangan alert yang dibuatkan tiket oleh tim SOC setelah terjadi insiden.



Gambar 3. 13 Pengiriman Laporan Melalui WhatsApp

5. Laporan Status Tiket

Selanjutnya, pada pukul 08.00 WIB praktikan mengirim laporan status tiket monitoring SIEM yang telah dibuatkan tiket pada hari kemarin saat terjadinya alert, dengan tujuan untuk menindaklanjuti tiket yang sudah dibuat oleh tim SOC NOOSC kepada tim IT *Security* klien supaya dilakukan penyelesaian terhadap tiket tersebut yang berisi id tiket, waktu terjadinya serangan, nama serangan, *host* yang terinfeksi, *severity*, *count* beserta *detail* dari serangannya yang dapat dilihat pada **Gambar 3. 14** dibawah ini.



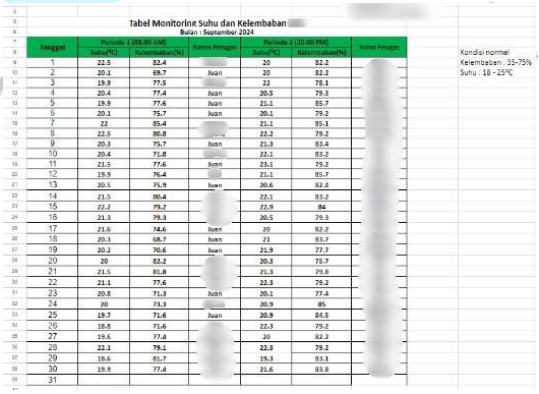
Gambar 3. 14 Laporan Status Tiket

6. Pemeriksaan Suhu dan Kelembapan pada Ruang Server

Pada **Gambar 3. 15** Praktikan melakukan pemeriksaan pada *Thermometer Digital Hygrometer* untuk melihat suhu dan kelembapan ruang server pada pukul 08.00 WIB.

Gambar 3. 15 Praktikan Memeriksa Suhu dan Kelembapan

Setelah diperiksa praktikan melaporkannya ke Google Spreadsheet SOC di **Gambar 3. 16** untuk membantu memastikan perangkat server beroperasi secara stabil dan mencegah risiko gangguan atau *downtime* yang bisa menghambat proses layanan serta keamanan data.



Tabel Monitoring Suhu dan Kelembaban

Bulan : September 2024

Tanggal	Periode 1 (08.00 AM)		Nama Penguji	Periode 2 (20.00 PM)		Nama Penguji
	Suhu(°C)	Kelembaban(%)		Suhu(°C)	Kelembaban(%)	
1	22.5	82.4		20	82.2	
2	20.1	69.7	Juan	20	82.2	
3	19.9	77.5		22	78.1	
4	20.4	77.4	Juan	20.5	79.8	
5	19.9	77.6	Juan	21.1	85.7	
6	20.1	75.7	Juan	20.1	79.2	
7	22	85.4		21.1	85.1	
8	22.5	80.8		22.2	79.2	
9	20.3	75.7	Juan	21.3	83.4	
10	20.4	71.8		22.1	83.2	
11	21.5	77.6	Juan	23.1	79.2	
12	19.9	76.4		21.1	85.7	
13	20.5	75.9	Juan	20.6	82.8	
14	21.5	80.4		22.1	83.2	
15	22.2	79.2		22.9	84	
16	21.3	79.3		20.5	79.3	
17	21.6	74.6	Juan	20	82.2	
18	20.3	68.7	Juan	21	83.7	
19	20.2	70.6	Juan	21.9	77.7	
20	20	82.2		20.3	75.7	
21	21.5	81.8		21.3	79.8	
22	21.1	77.6		22.3	79.2	
23	20.8	71.3	Juan	20.1	77.4	
24	20	73.3		20.9	85	
25	19.7	71.6	Juan	20.9	84.5	
26	18.8	71.6		22.3	79.2	
27	19.6	77.4		20	82.2	
28	22.1	79.1		22.3	79.2	
29	18.6	81.7		19.3	83.1	
30	19.9	77.4		21.6	83.8	
31						

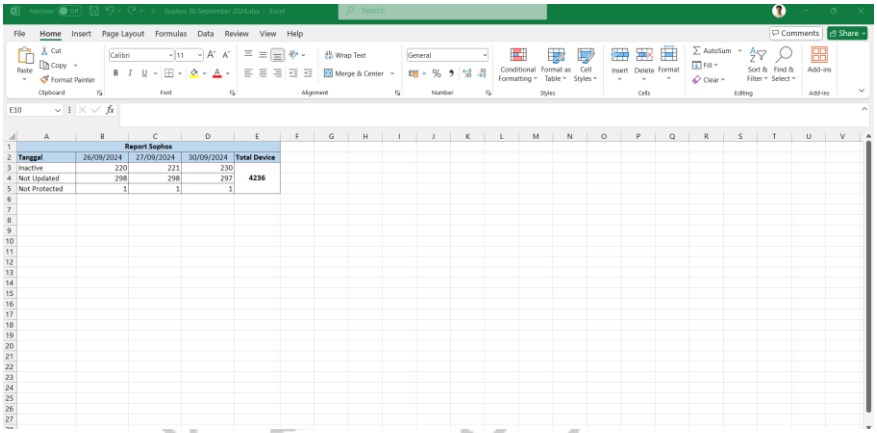
Kondisi normal
Kelembaban : 35-75%
Suhu : 18 - 25°C

Gambar 3. 16 Pengisian Hasil Pemeriksaan Suhu dan Kelembapan

7. Pengolahan Data untuk Laporan Harian Sophos dan Trend Micro

Pada **Gambar 3. 17** Praktikan melakukan pengolahan data menggunakan aplikasi Microsoft Excel untuk *daily report* Sophos dengan menggabungkan data dari Sophos baru dan yang lama. Penyusunan tanggal pada laporan adalah 3 hari termasuk hari ini guna memberikan informasi terkait laporan sebelumnya. Pada tahap ini, data mengenai status perangkat, seperti *inactive* (perangkat yang tidak aktif selama lebih dari 7 hari), *not updated* (perangkat yang belum diperbarui dalam waktu lebih dari 7 hari), dan *not protected* (perangkat yang tidak terlindungi), diidentifikasi dan dihitung untuk ditempatkan di kolom yang sesuai dalam *sheet Report*.

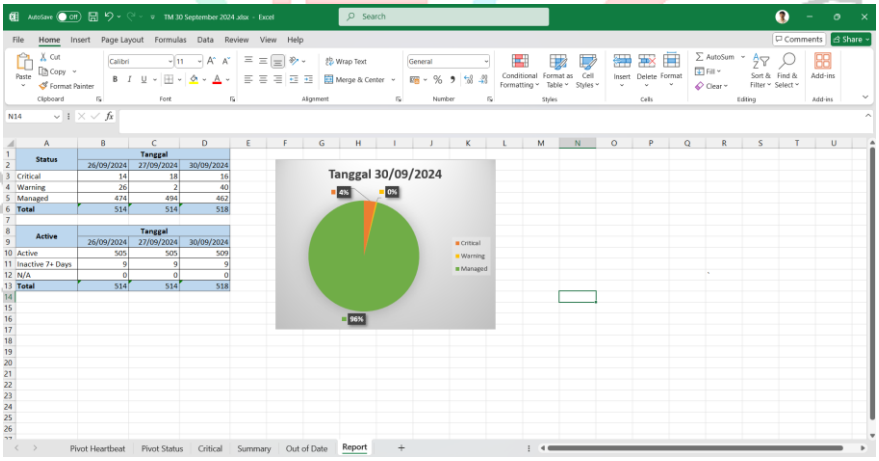
Praktikan mengidentifikasi perangkat yang mungkin memiliki kerentanan keamanan. Dengan mengisi kolom *not updated* dapat mengetahui jumlah perangkat yang belum diperbarui selama lebih dari 7 hari, yang berpotensi rentan terhadap ancaman keamanan baru. Sementara itu, kolom *not protected* menunjukkan perangkat yang tidak memiliki perlindungan aktif, seperti antivirus atau firewall, sehingga memungkinkan tim segera menindaklanjuti perangkat yang berisiko tinggi. Tahap ini membantu praktikan dalam memprioritaskan tindakan untuk memperkuat keamanan sistem. Setelah itu dilakukan perhitungan total perangkat, mengisi hasil jumlahnya ke kolom "*Total*" di *sheet* "*Report*." Setelah semua data terisi, kirim laporan melalui *email*.



Report Sophos				
Tanggal	26/09/2024	27/09/2024	30/09/2024	Total Device
Inactive	220	221	230	
Not Updated	298	298	297	4236
Not Protected	1	1	1	

Gambar 3. 17 Report Sophos

Selain itu pada **Gambar 3. 18**, Praktikan juga mengolah data untuk laporan harian Trend Micro ke *email* klien dengan menggunakan Microsoft Excel. Proses dimulai dengan mengunduh data dari *email*. Data tersebut kemudian disalin ke dalam file Excel *template* dari hari sebelumnya, dengan terlebih dahulu membersihkan data lama pada *Sheet Summary*. Langkah selanjutnya adalah melakukan analisis status perangkat dengan memfilter kolom "*Last Heartbeat*" untuk periode seminggu terakhir.



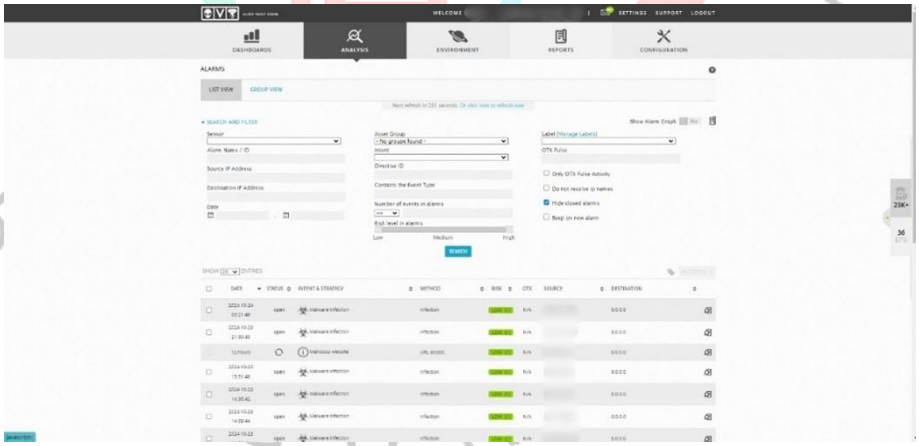
Gambar 3. 18 Report Trend Micro

Untuk mengkategorikan status perangkat, dimulai dengan mengisi nilai "*Active*" pada kolom K2 untuk perangkat yang aktif, kemudian dilanjutkan dengan mengidentifikasi perangkat "*Inactive 7+ Days*" untuk yang tidak aktif lebih dari seminggu. Data kemudian diproses menggunakan *Pivot Table* untuk menghitung statistik

status perangkat. Pengolahan data ini berguna untuk memantau *coverage* atau cakupan dari pembaruan sistem dan menganalisis hasil pembaruan yang telah dilakukan supaya tim klien dapat segera mengidentifikasi dan menindaklanjuti setiap anomali yang terdeteksi pada sistem.

8. Laporan Operasional dari SIEM AlienVault

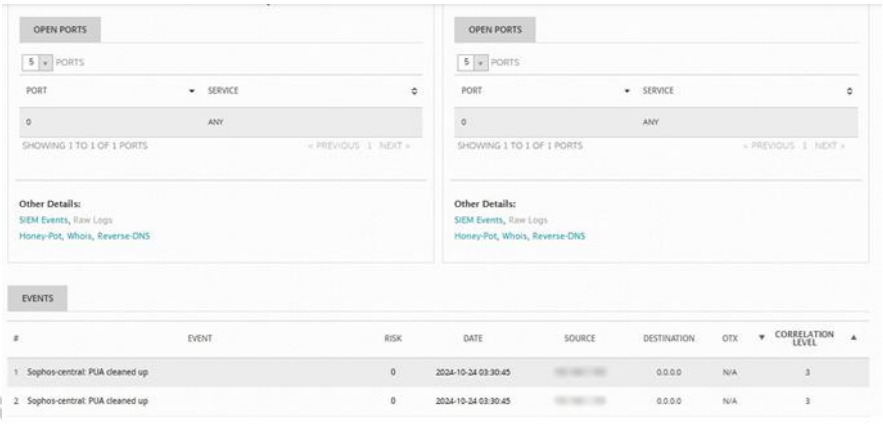
Pada **Gambar 3. 19** merupakan proses praktikan dalam pengiriman laporan operasional setiap 6 Jam sekali dari SIEM Alienvault yaitu dengan memeriksa terlebih dahulu secara lengkap *alert* atau serangan yang masuk dari pukul 03.00 – 09.00 untuk dilakukan pengiriman laporan pada pukul 09.00, dan 09.00 – 15.00 untuk dilakukan pengiriman laporan pada Jam 15.00 Sore hari saat akhir shift, berdasarkan gambar diatas terdapat *alert Malware Infection* yang terjadi pada tanggal 2024-10-24 pada Jam 03:21:46 yang memiliki *method infection* dengan tingkat risiko *low* dan sumber IP dari *alert* tersebut.



Gambar 3. 19 Tampilan Alert dari Alienvault

Setelah itu, pada **Gambar 3. 20**, praktikan melakukan pemeriksaan yang mendalam terkait informasi lengkapnya, pada gambar tersebut terdapat keterangan Sophos *cleaned up* yang artinya tidak ada insiden yang harus dibuatkan tiket ke klien, apabila ada maka keterangannya seperti Sophos *failed cleaned up* perlu dibuatkan tiket

dan *follow up* ke klien lewat *service desk* NOOSC atau *Open-Source Ticket Request System* (OTRS).



Gambar 3. 20 Tampilan Detail Event dari Alert

Dikarenakan tidak ada maka praktikan menambahkan jumlah 1 insiden di *template* laporan yang sudah disediakan pada aplikasi Sublime Text pada **Gambar 3. 21** serta mengubah tanggal dan waktu laporan yang sesuai dengan Jam laporan operasional yang berlangsung. Laporan ini berfungsi untuk memberi tahu pihak terkait sehingga dapat mengambil langkah pencegahan atau mitigasi guna menjaga keamanan infrastruktur IT perusahaannya.

```
Dear Team

Berikut kami sampaikan mengenai aktivitas selama 6 jam, tanggal 08 Oktober 2024 03:00 - 09:00. Berdasarkan aktivitas pemantauan
kejadian keamanan informasi yang dilakukan menggunakan SIEM AlienVault dan Nagios. Pada periode ini terdapat alert yang mengacu
kepada percobaan pelanggaran maupun insiden pelanggaran pada sistem keamanan IT operasional

Alert AlienVault
==========================================

1. Suspicious Behaviour                              = 0 Insiden
2. Sophos - EC - Virus Detected and Blocked          = 0 Insiden
3. System Compromise - Malware Infection             = 0 Insiden
4. Bruteforce Authentication - Windows login         = 0 Insiden
5. Bruteforce Authentication - SSH                   = 0 Insiden
6. Bruteforce Authentication - HTTP                  = 0 Insiden
7. Bruteforce Authentication - Authentication Brute  = 0 Insiden
8. Bruteforce Authentication - HIDS Reported         = 0 Insiden
9. Malicious website - Exploit Kit - Exploit Kit     = 0 Insiden
10. Fortigate - PHP CGI Argument Injection           = 0 Insiden
11. WebServer Attack - XSS (Cross Site Scripting)    = 0 Insiden
12. WebServer Attack - SQL INJECTION (SQL INJECTION) = 0 Insiden
13. WebServer Attack - File Guessing                 = 0 Insiden
14. WebServer Attack - Attack Pattern Detection      = 0 Insiden
15. WebServer Attack - apache                        = 0 Insiden
16. F5 Web Attack - Command Execution                = 0 Insiden
17. F5 Web Attack - Non Browser Client               = 0 Insiden
18. AV Policy violation, ThunderNetwork P2P usage    = 0 Insiden
19. Windows - RDP Suspicious Access                  = 0 Insiden
20. Suspicious File - Infection                      = 0 Insiden
21. FortiGuard License Expiring                      = 0 Insiden
22. Malicious website - URL access                   = 0 Insiden
23. Malware Infection                                = 1 Insiden
24. Ransomware Infection                             = 0 Insiden
==========================================

Alert Nagios = 0

Alert Yang di tiketkan = 0

Untuk summary keseluruhan kejadian periode shift ini akan dikirimkan setiap akhir shift melalui email.

Terima kasih
```

Gambar 3. 21 Template Laporan Alienvault

9. Monitoring Seluruh SIEM klien

Sebagai *Security Operation Center Analyst* (SOC), tugas praktikan yaitu memantau sistem SIEM (*Security Information and Event Management*) seperti QRadar, AlienVault, dan Splunk pada klien pada **Gambar 3. 22** dengan memastikan bahwa seluruh aktivitas jaringan dan sistem yang dipantau berada dalam kondisi aman serta sesuai dengan kebijakan keamanan yang telah ditetapkan. Tugas ini meliputi pemantauan aktivitas jaringan secara *real-time*, identifikasi aktivitas mencurigakan, serta melakukan analisis terhadap log yang terkumpul di setiap SIEM tersebut.

Gambar 3. 22 Praktikan saat menjadi SOC Analyst

Setiap *platform* SIEM memiliki karakteristik dan kapabilitas yang berbeda, sehingga seorang SOC harus mampu mengoperasikan dan memahami cara kerja masing-masing, serta menyesuaikan pendekatan analisis sesuai dengan fitur yang disediakan. Dalam Qradar misalnya, fokus utamanya adalah pada korelasi log dan deteksi anomali untuk mengidentifikasi ancaman yang terdeteksi dalam aliran data. Sementara itu, AlienVault memiliki fitur yang lebih spesifik untuk deteksi ancaman berbasis *signature* dan *threat intelligence*, yang berguna untuk mendeteksi pola serangan yang telah diketahui.

Splunk, sebagai platform yang serbaguna, digunakan untuk memantau log secara mendalam, serta menganalisis dan mencari indikasi potensi ancaman dalam data yang lebih luas. Tugas ini menuntut ketelitian, pemahaman teknis, dan kecepatan dalam merespon berbagai peringatan atau anomali yang mungkin muncul atau terdeteksi dari sistem SIEM.

10. Pembuatan Tiket Jika Terdapat *Alert*

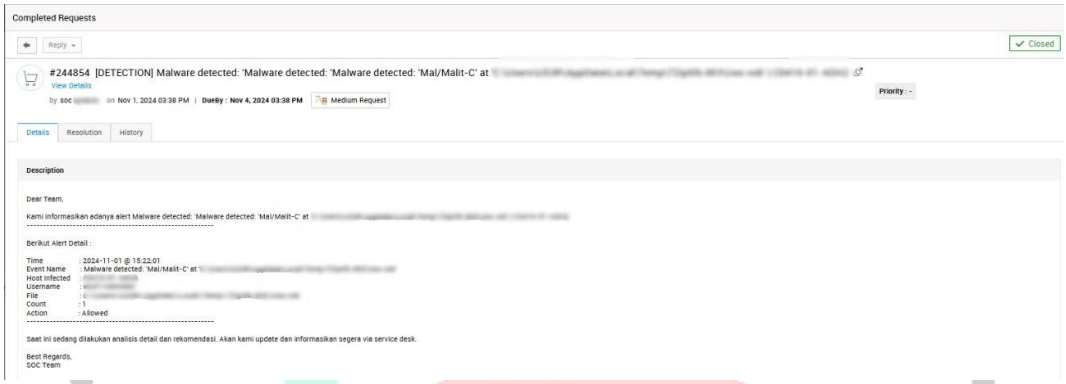
Praktikan melakukan pembuatan tiket dari *service desk* SOC. Kegunaan tiket bertujuan untuk mendokumentasikan dan menindaklanjuti setiap peringatan keamanan yang muncul seperti *malware*. Langkah pertama dalam pembuatan tiket adalah mengakses sistem ticketing yang tersedia, yaitu melalui *service desk* SOC. Setelah login menggunakan akun SOC, memilih menu "*Create New*" untuk membuat tiket baru. Dalam pembuatan tiket, kategori tiket ditentukan berdasarkan jenis alert yang terdeteksi. Sebagai contoh, untuk alert dari Sophos yang mengindikasikan adanya kode berbahaya pada perangkat desktop atau klien, kategori yang dipilih adalah "*Malicious Code Alert - Desktop/Client*".

Informasi ini penting untuk memastikan tiket diklasifikasikan dengan benar sehingga dapat ditindaklanjuti oleh tim yang berwenang. Setiap *field* pada *template* tiket tidak perlu diubah karena telah disesuaikan untuk memenuhi kebutuhan dokumentasi dan respon SOC. Berikut salah satu tiket pesan *first detection* dan *analysis* yang dibuat oleh praktikan:

- *First Detection*

Pada **Gambar 3. 23** dibawah ini, merupakan *Ticket First Detection* yang merujuk pada proses awal di mana sebuah sistem keamanan, seperti SIEM, mendeteksi aktivitas mencurigakan atau insiden keamanan dan menghasilkan tiket untuk melacak insiden tersebut. Gambar yang ditampilkan adalah contoh tiket yang telah *Closed* atau selesai di dalam *service desk* SOC. Tiket ini mencatat informasi tentang deteksi *malware* yang diberi nomor 244854.

Deskripsi tiket menunjukkan adanya *alert* deteksi *malware* dengan nama "Mal/Malit-C". *Malware* ini terdeteksi di suatu direktori pada perangkat pengguna di dalam jaringan. Informasi lengkap tiket mencakup informasi waktu deteksi *malware* pada 1 November 2024 pukul 15:22:01, *host* yang terdampak, nama pengguna terkait, nama *file* yang terinfeksi, dan jumlah 1 *event*.



Gambar 3. 23 Tampilan dari Pesan First Detection

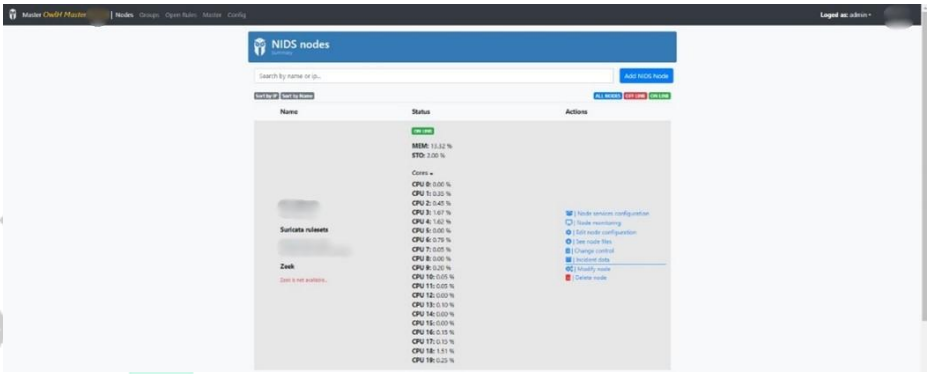
- *Analysis*

Setelah melakukan pembuatan pesan *first detection,* praktikan menambahkan mitigasi atau langkah-langkah yang dilakukan jika *host* atau perangkat klien sudah terinfeksi *malware,* disesuaikan dengan *alert* atau insiden yang terjadi pada **Gambar 3. 24**. Mitigasi yang praktikan tambahkan di pesan *analysis* berdasarkan hasil eskalasi dari *Cybersecurity Analyst*.

Gambar 3. 24 Tampilan dari Pesan Analysis

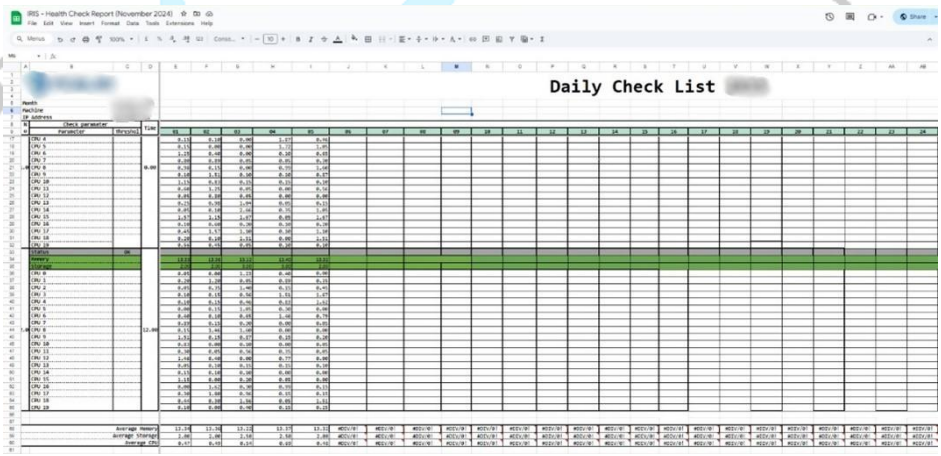
11. Pemeriksaan *Health Check* NIDS

Pada **Gambar 3. 25** praktikan melakukan kegiatan pemeriksaan kesehatan atau *health check* pada OWLH *Network Intrusion Detection System* (NIDS) klien.



Gambar 3. 25 Tampilan OWLH NIDS nodes

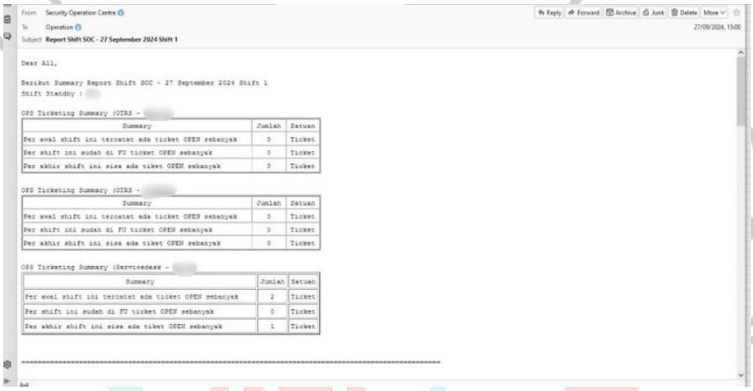
Setelah itu, mengisi hasil *health check* tersebut ke Google Spreadsheet yang telah dibuat oleh *internal* NOOSC berguna untuk memastikan bahwa sistem deteksi intrusi bekerja secara optimal dalam memantau dan mengidentifikasi potensi ancaman di jaringan pada **Gambar 3. 26**.



Gambar 3. 26 Pengisian Hasil Health Check NIDS

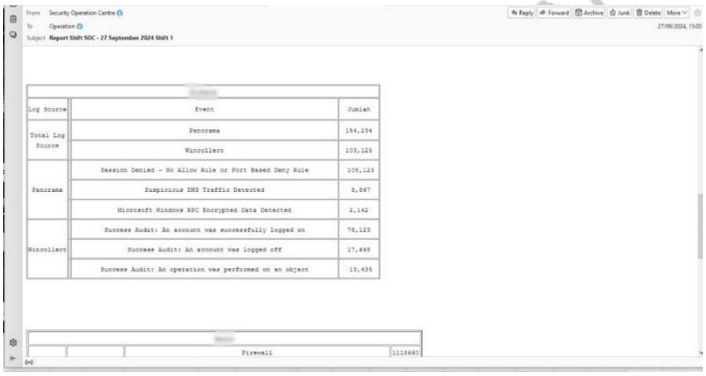
12. Laporan Akhir Shift

Sebelum selesai *shift* pada Jam 15:00, praktikan menarik data dari awal shift hingga akhir shift berguna untuk mengirim laporan akhir *shift* SOC ke tim *operation internal*. Pada **Gambar 3. 27** laporan ini berfungsi untuk mencatat semua aktivitas yang terjadi selama *shift*, termasuk insiden keamanan yang terdeteksi, jumlah tiket yang ditinggalkan *shift* sebelum praktikan bekerja, tiket yang dibuat selama shift praktikan berlangsung dan tiket yang ditinggalkan praktikan saat selesai *shift* pada **Gambar 3. 28**.



Gambar 3. 27 Ticketing Summary

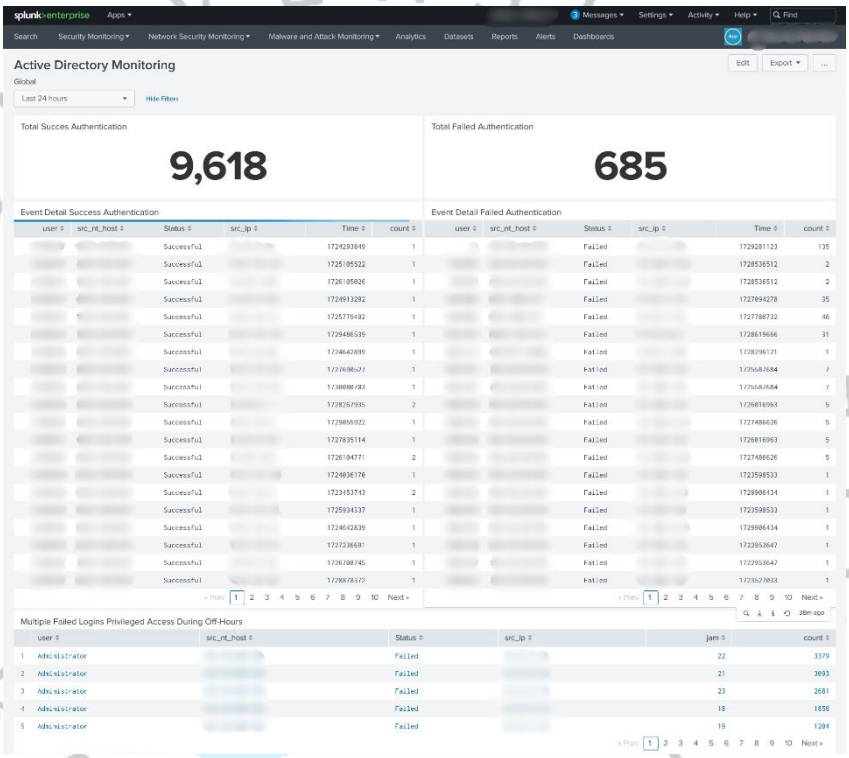
Dengan adanya laporan ini, tim yang akan mengambil alih *shift* selanjutnya dapat dengan cepat memahami situasi keamanan terkini, insiden yang masih memerlukan tindak lanjut, serta prioritas yang harus diutamakan.



Gambar 3. 28 Aktivitas Pada SIEM

3.2.2 Cybersecurity Analyst

Praktikan masuk kantor pada *Office Hour* yaitu pukul 09.00 WIB, tugas – tugas yang dilaksanakan praktikan saat menjadi *Cybersecurity Analyst* meliputi analisis *log* untuk pembuatan *use case* pada **Gambar 3. 29** adalah hasil *Dashboard Active Directory Monitoring* di SIEM Splunk dengan menggunakan *Search Processing Language* (SPL) penyusunan laporan tiket bulanan dan analisis data Sophos, dan pembuatan panduan teknis untuk operasional SOC. Berikut rincian tugas-tugas yang praktikan laksanakan:

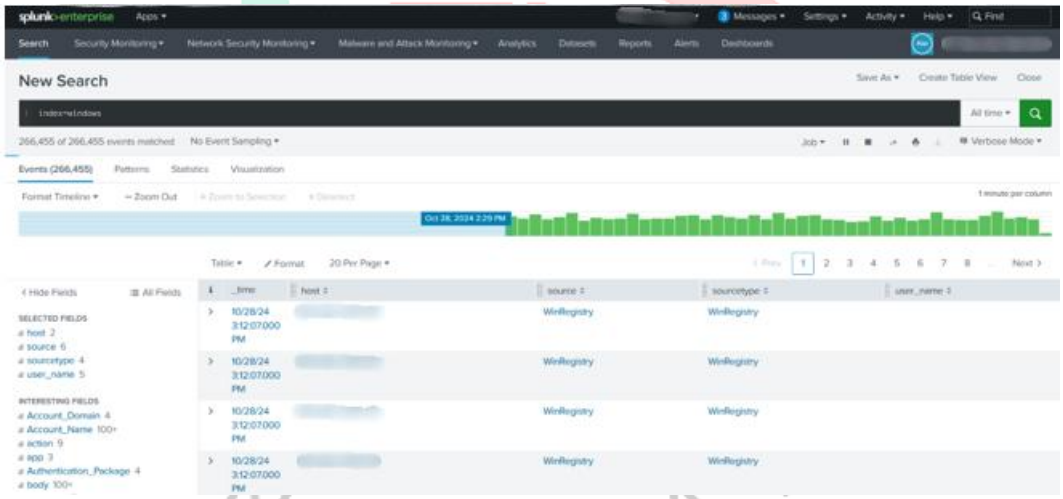


Gambar 3. 29 Tampilan Dashboard Active Directory Monitoring

1. Menentukan Tujuan *Use Case*

Pada kesempatan ini, Praktikan menganalisis *log* yang berkaitan dengan *use case Multiple Failed Logins Privileged Access During Off-Hours* atau Menangkap beberapa upaya login yang gagal pada akun dengan akses *privileged* selama jam-jam di luar jam kerja standar, misalnya di malam hari atau akhir pekan. Kejadian ini bisa jadi mencurigakan karena akses pada jam tersebut tidak umum untuk sebagian besar organisasi.

Kueri index=windows merupakan tempat penyimpanan data yang dikelompokkan berdasarkan kategori atau sumber tertentu. Pada **Gambar 3. 30** merupakan index "windows" yang biasanya menyimpan data *log* dari sistem berbasis Windows seperti *event logs*, *security logs*, atau aktivitas yang terkait dengan Windows.



Gambar 3. 30 Tampilan Query Search di Splunk

2. *Field* yang Diperlukan

Praktikan harus mencari *field* yang berkaitan, berikut kueri dari hasil analisis *log* yang praktikan buat untuk dapat membuat *use case* tersebut:

```
index=windows "tag::eventtype"=authentication EventCode = 4625
| eval Status=if(EventCode=4625, "Failed", "Successful")
| eval jam=strftime(_time, "%H")
| where jam>=18
| stats latest(_time) as Time, count by user, src_nt_host, Status, src_ip,
jam
| table user, src_nt_host, Status, src_ip, jam, count
| sort by count desc
```

Berikut penjelasan lebih lengkap mengenai kueri yang praktikan buat yaitu:

```
index=windows "tag::eventtype"=authentication EventCode
= 4625
```

- Memilih data dari indeks bernama windows yang memiliki *tag authentication* pada *eventtype* dan *EventCode* bernilai 4625. *EventCode* 4625 adalah kode yang biasanya mewakili upaya *login* yang gagal di Windows.

```
| eval Status=if(EventCode=4625, "Failed", "Successful")
```

- Menambahkan *field* baru bernama *status*. Jika *EventCode* bernilai 4625, maka *status* akan diatur sebagai *Failed*, dan jika tidak, akan diatur sebagai *Successful*.

```
| eval jam=strftime(_time, "%H")
```

- Membuat field baru bernama jam, yang mengekstrak jam (dalam *format* 24 jam) dari *field* *_time* sebagai data jam kejadian tersebut.

| where jam>=18

- Memfilter hasil hanya untuk kejadian yang terjadi pada atau setelah pukul 18.00. Ini biasanya menunjukkan aktivitas yang terjadi di luar jam kerja normal.

| stats latest(_time) as Time, count by user, src_nt_host, Status, src_ip, jam

- Mengelompokkan hasil berdasarkan beberapa *field* (*user*, src_nt_host, Status, src_ip, dan jam), lalu menampilkan waktu terbaru (latest(_time)) dari kejadian sebagai *Time*, dan menghitung jumlah kejadian pada kelompok tersebut sebagai *count*.

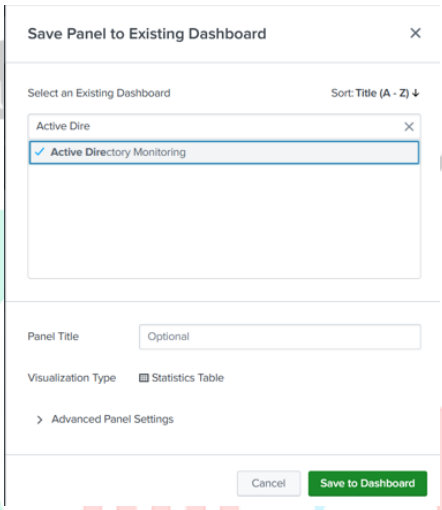
| table user, src_nt_host, Status, src_ip, jam, count

- Mengatur hasil dalam bentuk tabel dengan kolom *user*, src_nt_host, Status, src_ip, jam, dan *count* untuk menampilkan informasi yang lebih jelas.

| sort by count desc

- Mengurutkan tabel hasil berdasarkan *count* secara menurun, sehingga hasil dengan jumlah kejadian terbanyak muncul paling atas.

- Setelah dilakukan implementasi kuerinya, langkah selanjutnya adalah melakukan *Save As to Existing Dashboard* untuk memasukkan *use case* ke *dashboard* yang sudah dibuat yaitu *Active Directory Monitoring* yang dapat dilihat pada **Gambar 3. 31**.



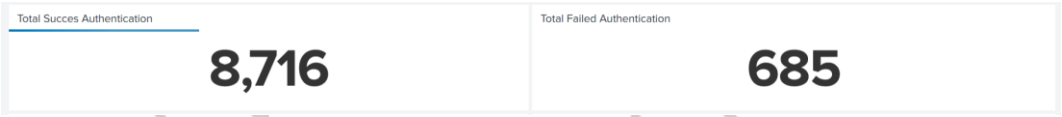
Gambar 3. 31 Save Panel to Existing Dashboard

Gambar 3. 32 tersebut menunjukkan log aktivitas yang mencatat upaya login gagal menggunakan akun pengguna dengan akses istimewa (*privileged access*) yang terjadi di luar jam kerja (*off-hours*). Semua upaya berasal dari alamat IP yang tercantum ke *host* yang tercantum, dengan status login Failed. Jumlah percobaan login yang gagal sangat tinggi, pada urutan pertama didapatkan jumlah 3379 kali pada jam 22 atau jam 10 Malam. Aktivitas ini perlu segera ditangani untuk mencegah pelanggaran keamanan.

Gambar 3. 32 Tampilan Multiple Failed Login Acces During Off-hours

Total Success Authentication dan *Total Failed Authentication*

Pada **Gambar 3. 33** merupakan dua kueri yang digunakan untuk menghitung jumlah unik pengguna yang berhasil *login* (*EventCode* 4624) dan jumlah unik pengguna yang gagal *login* (*EventCode* 4625) di sistem Windows, masing-masing disimpan dalam kolom total.



Gambar 3. 33 Tampilan Total Succes Authentication dan Failed

```
index=windows "tag::eventtype"=authentication EventCode
= 4624
| stats dc(user) as total
```

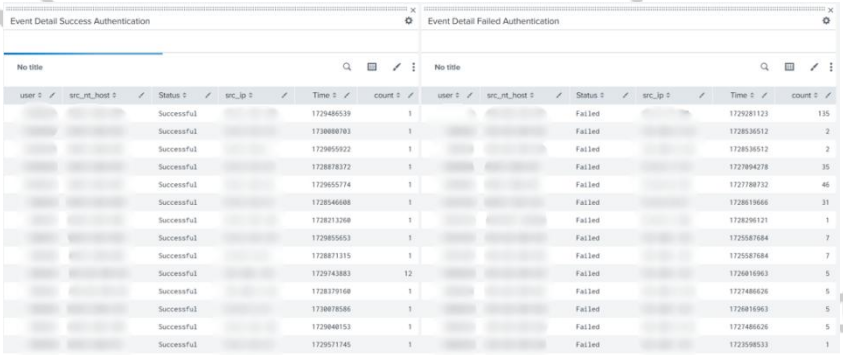
- Memilih data dari indeks bernama windows dengan *eventtype* bertag *authentication* dan *EventCode* bernilai 4624. *EventCode* 4624 biasanya digunakan untuk menunjukkan *login* yang berhasil di sistem Windows dan menggunakan fungsi dc (*distinct count*) untuk menghitung jumlah unik dari *user* yang berhasil *login* dan menyimpannya dalam kolom bernama total.

```
index=windows "tag::eventtype"=authentication EventCode
= 4625
| stats dc(user) as total
```

- Pemilihan data dari indeks bernama windows dengan *eventtype* bertag *authentication* dan EventCode bernilai 4625. *EventCode* 4625 adalah kode yang menunjukkan upaya login yang gagal dan menggunakan fungsi dc (*distinct count*) untuk menghitung jumlah unik dari user yang gagal *login* dan menyimpannya dalam kolom bernama total

Event Detail Success Authentication dan *Event Detail Failed Authentication*

Kedua kueri ini digunakan untuk mengelompokkan dan menghitung kejadian login berhasil (*EventCode* 4624) dan login gagal (*EventCode* 4625) berdasarkan pengguna, nama *host*, status, dan alamat IP, serta menampilkan waktu terakhir kejadian untuk masing-masing kelompok. Berikut **Gambar 3. 34** merupakan Tampilan dari *Event Detail Success and Failed*.



Gambar 3. 34 Tampilan Event Detail Success and Failed

index=windows "tag::eventtype"=authentication EventCode = 4624

- Memilih data dari indeks bernama windows dengan *eventtype* bertag *authentication* dan *EventCode* bernilai 4624. *EventCode* 4624 menunjukkan login yang berhasil di sistem Windows.

| eval Status=if(EventCode=4625, "Failed", "Successful")

- Menambahkan *field* baru bernama Status. Karena *EventCode* yang di-filter adalah 4624 (login berhasil), maka Status di sini akan ditetapkan sebagai "*Successful*" untuk semua hasil.

| stats latest(_time) as Time, count by user, src_nt_host, Status, src_ip

- Mengelompokkan hasil berdasarkan *user*, src_nt_host (nama *host* sumber), Status, dan src_ip (alamat IP sumber), lalu menampilkan waktu terakhir kejadian sebagai *Time*, serta menghitung jumlah kejadian untuk setiap kelompok dalam *count*.

index=windows "tag::eventtype"=authentication EventCode = 4625

- Memilih data dari indeks bernama windows dengan *eventtype* bertag *authentication* dan *EventCode* bernilai 4625. *EventCode* 4625 adalah kode untuk *login* yang gagal.

| eval Status=if(EventCode=4625, "Failed", "Successful")

- Menambahkan *field* baru bernama Status. Karena *EventCode* yang di-filter adalah 4625, maka Status akan diatur menjadi *"Failed"* untuk semua hasil.

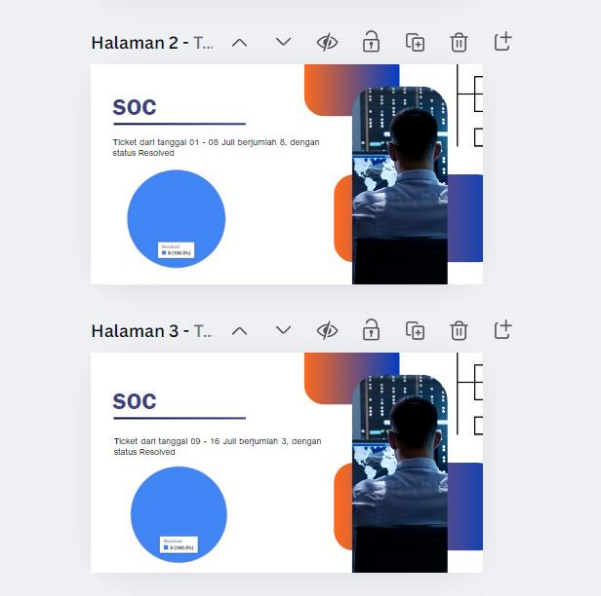
| stats latest(_time) as Time, count by user, src_nt_host, Status, src_ip

- Mengelompokkan hasil berdasarkan *user*, src_nt_host, Status, dan src_ip, lalu menampilkan waktu terbaru dari kejadian tersebut sebagai *Time*, dan menghitung jumlah kejadian untuk setiap kelompok sebagai *count*.

1. Penyusunan Laporan Tiket Bulanan dan Analisis Data Sophos

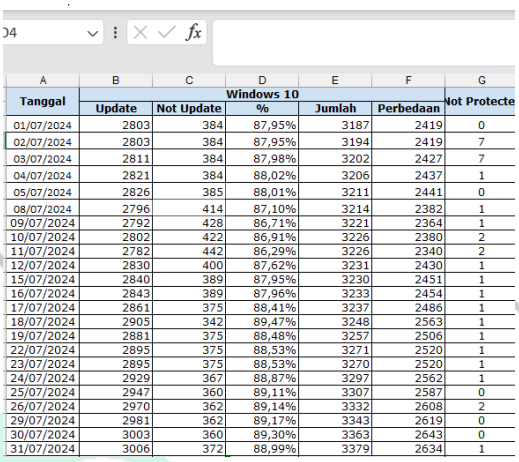
Tiket yang dibuat oleh tim SOC adalah catatan untuk melacak insiden keamanan atau aktivitas yang memerlukan perhatian khusus. Dalam laporan ini, setiap tiket diuraikan berdasarkan mingguan, menunjukkan jumlah tiket yang masuk dan status penyelesaiannya. Dalam **Gambar 3. 35** presentasi tersebut praktikan visualisasi rekapitulasi tiket per minggu di bulan Juli 2024 hasil nya adalah:

- 16-23 Juli terdapat lonjakan tiket hingga 14 disebabkan oleh peningkatan aktivitas atau insiden keamanan.
- 24-31 Juli puncak aktivitas dengan 26 tiket diselesaikan, menunjukkan kesibukan tim SOC di akhir bulan.



Gambar 3. 35 Visualisasi Tiket Sophos Mingguan

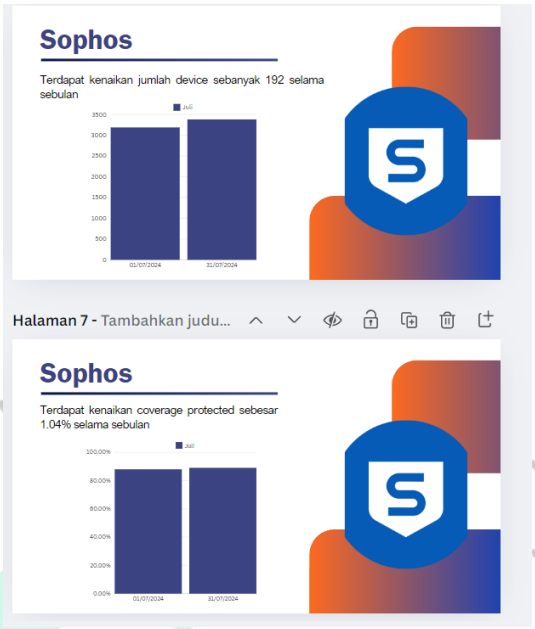
Pada **Gambar 3. 36** adalah data yang praktikan olah untuk melakukan visualisasi data Sophos dan merupakan laporan harian yang memantau kinerja perangkat oleh Sophos.



Tanggal	Windows 10					Not Protecte
	Update	Not Update	%	Jumlah	Perbedaan	
01/07/2024	2803	384	87,95%	3187	2419	0
02/07/2024	2803	384	87,95%	3194	2419	7
03/07/2024	2811	384	87,98%	3202	2427	7
04/07/2024	2821	384	88,02%	3206	2437	1
05/07/2024	2826	385	88,01%	3211	2441	0
08/07/2024	2796	414	87,10%	3214	2382	1
09/07/2024	2792	428	86,71%	3221	2364	1
10/07/2024	2802	422	86,91%	3226	2380	2
11/07/2024	2782	442	86,29%	3226	2340	2
12/07/2024	2830	400	87,62%	3231	2430	1
15/07/2024	2840	389	87,95%	3230	2451	1
16/07/2024	2843	389	87,96%	3233	2454	1
17/07/2024	2861	375	88,41%	3237	2486	1
18/07/2024	2905	342	89,47%	3248	2563	1
19/07/2024	2881	375	88,48%	3257	2506	1
22/07/2024	2895	375	88,53%	3271	2520	1
23/07/2024	2895	375	88,53%	3270	2520	1
24/07/2024	2929	367	88,87%	3297	2562	1
25/07/2024	2947	360	89,11%	3307	2587	0
26/07/2024	2970	362	89,14%	3332	2608	2
29/07/2024	2981	362	89,17%	3343	2619	0
30/07/2024	3003	360	89,30%	3363	2643	0
31/07/2024	3006	372	88,99%	3379	2634	1

Gambar 3. 36 Data yang Praktikan Olah Untuk Visualisasi

Pada **Gambar 3. 37** Sophos merupakan solusi keamanan yang dirancang untuk melindungi perangkat dari berbagai ancaman siber, seperti *malware* dan *ransomware*. Praktikan juga menganalisis data Sophos untuk melihat kenaikan jumlah perangkat terproteksi, laporan mencatat penambahan 192 perangkat baru yang dilindungi oleh *antivirus* Sophos selama bulan Juli. Hal ini menunjukkan upaya proaktif dalam memperluas cakupan perlindungan terhadap perangkat baru, yang dapat mencakup komputer, *server*, atau perangkat *endpoint* lainnya.

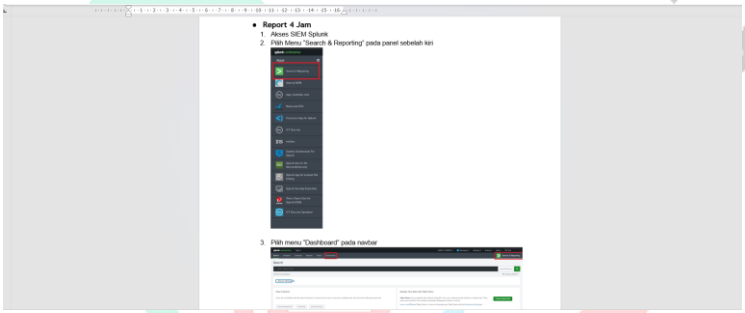


Gambar 3. 37 Visualisasi Data Sophos

Setelah itu, praktikan analisis peningkatan *coverage protected* atau cakupan proteksi Sophos terdapat peningkatan 1,04% dalam cakupan perlindungan selama Juli, yang mengindikasikan lebih banyak perangkat dalam lingkungan perusahaan kini berada di bawah perlindungan sistem keamanan. Meskipun peningkatannya terlihat kecil, dalam konteks skala besar ini bisa berarti ratusan perangkat baru mendapatkan perlindungan. Praktikan menggunakan *pie chart* dan diagram batang untuk memvisualisasikan data seperti jumlah perangkat yang terproteksi dan tingkat *coverage* perlindungan. Visualisasi membantu memberikan pemahaman cepat dan menyeluruh tentang tren serta pencapaian selama periode laporan.

2. Pembuatan Panduan Teknis untuk Operasional SOC

Pada **Gambar 3. 38** Praktikan membuat petunjuk tenis atau panduan teknis sesuai arahan Pembimbing Lapangan *Cybersecurity Analyst* yang berguna sebagai *transfer knowledge* dalam operasional SOC yang mengandung langkah-langkah detail tentang prosedur operasional yang harus dilakukan oleh tim SOC. Hal ini merupakan pengetahuan praktis yang berguna untuk anggota baru atau anggota yang kurang berpengalaman untuk melakukan tugas yang sama dengan standar yang telah ditetapkan serta memastikan bahwa pengetahuan teknis dapat diakses, dipahami, dan diterapkan dengan baik oleh tim SOC.



Gambar 3. 38 Panduan Teknis oleh Praktikan

Panduan teknis yang dibuat mencakup *daily report* Sophos, Trend Micro, status tiket, laporan operasional, dashboard monitoring, dan mekanisme *ticketing.* Panduan teknis ini berisi instruksi mengenai pembuatan laporan harian terkait perangkat lunak keamanan seperti Sophos dan Trend Micro, yang berisi status perangkat yang aktif dan tidak aktif. Selain itu, panduan ini juga menjelaskan mekanisme pembuatan status tiket, yang berfungsi untuk menindaklanjuti tiket yang dibuat kemarin dibuat oleh SOC. Laporan operasional yang terperinci mengenai pemantauan catatan aktivitas SIEM. Selain itu, panduan mengenai mekanisme *ticketing* seperti langkah-langkah pembuatan tiket dan mengkategorikan *alert* yang terjadi.

3.2.3 Cybersecurity Engineer

Praktikan masuk kantor pada *Office Hour* yaitu pukul 09.00 WIB, berikut rincian kegiatan yang dilaksanakan praktikan saat menjadi *Cyber Security Engineer:*

a. *Dismantle Server*

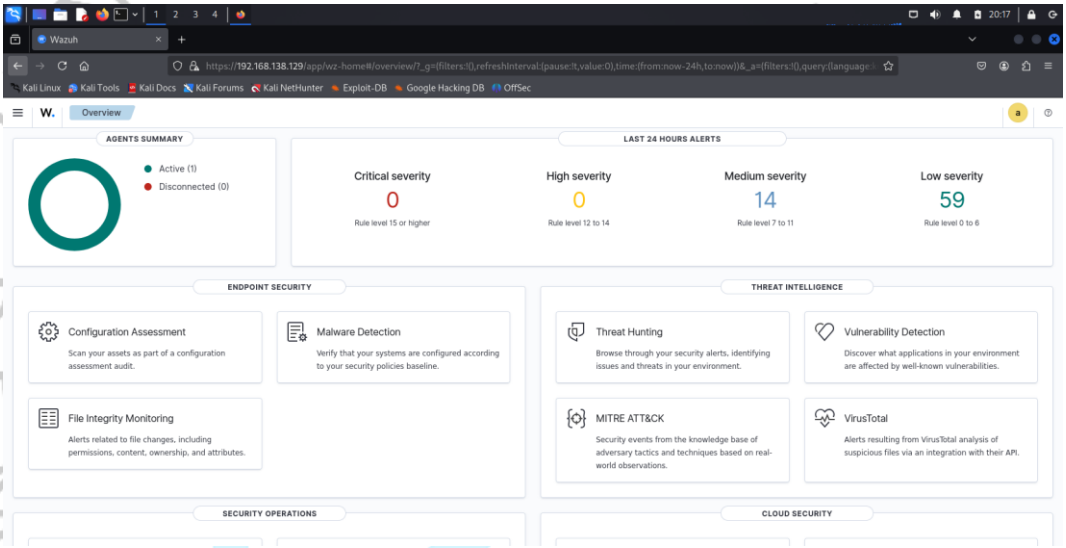
Pada **Gambar 3. 39** tanggal 16 Agustus 2024, praktikan dibimbing oleh pembimbing kerja untuk melakukan *dismantle server* di kantor klien guna menjalankan pengecekan internal serta menambahkan modul FO (*Fiber Optic*). kegiatan ini praktikan lakukan untuk memastikan sistem dapat beroperasi dengan lebih optimal sesuai kebutuhan klien.

Gambar 3. 39 Praktikan Saat Melakukan Dismantle Server

Proof of Concept (PoC) sering digunakan untuk menguji kelayakan dan potensi dari suatu ide, produk, atau teknologi sebelum diinvestasikan lebih lanjut. Berdasarkan *timeline* PoC yang berjalan hingga tanggal 30 Agustus 2024, *dismantle* pada *server* PoC telah praktikan lakukan di kantor klien. Hal ini praktikan dan pembimbing kerja lakukan untuk melanjutkan proses evaluasi serta pengembalian perangkat terkait PoC.

b. Instalasi SIEM Wazuh, Wazuh Agent, dan Simulasi Penyerangan

Wazuh adalah platform SIEM (*Security Information and Event Management*) yang *open-source* dan digunakan untuk mengelola serta memantau keamanan sistem. Pada **Gambar 3. 40** praktikan diarahkan oleh pembimbing kerja untuk melakukan instalasi Wazuh dan memasang Wazuh *Agent*. Dalam hal ini praktikan menggunakan perangkat lunak *virtual machine* yang bernama VMware dengan menggunakan OS Kali Linux. Berikut penjelasan prasyarat dan langkah-langkah yang praktikan lakukan:

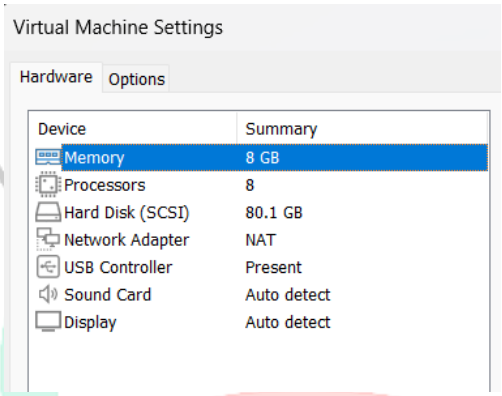


Gambar 3. 40 Tampilan SIEM Wazuh

Pada **Gambar 3. 41** Praktikan menggunakan OS Kali Linux untuk instalasi Wazuh karena dapat memberikan keunggulan karena sistem ini dirancang untuk keamanan siber, mendukung banyak alat tambahan, kompatibel dengan Wazuh Manager.

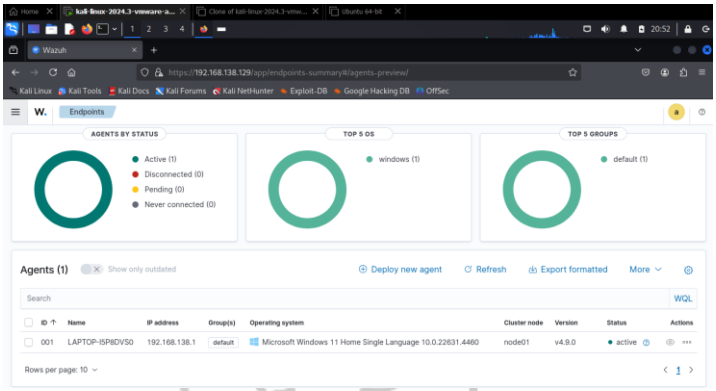
Gambar 3. 41 OS Kali Linux yang digunakan

Pada **Gambar 3. 42** praktikan memiliki spesifikasi 8 GB RAM, 8 CPU, dan 80.1 GB penyimpanan, sehingga cocok untuk menjalankan sistem operasi dan aplikasi berat, seperti Wazuh SIEM, *server*, atau pengujian keamanan dan konfigurasi jaringan *Network Address Translation* (NAT) untuk mempermudah koneksi internet VM melalui *host*.



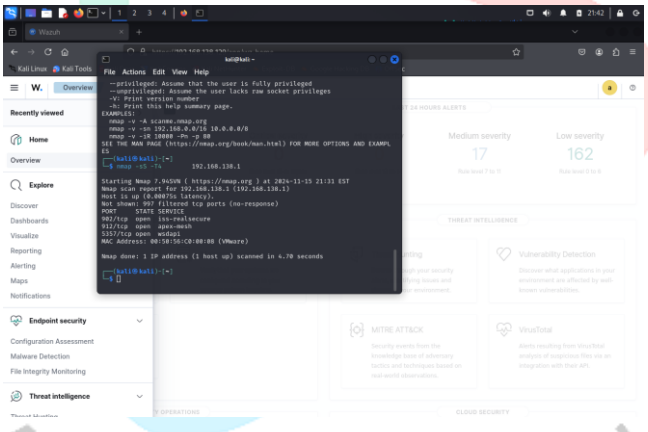
Gambar 3. 42 Spesifikasi Hardware dari VM

Setelah *server* Wazuh terpasang, langkah selanjutnya adalah memasang Wazuh Agent pada *local device* yang ingin dipantau seperti pada **Gambar 3. 43**. Wazuh Agent ini berfungsi untuk mengirimkan data keamanan dan aktivitas perangkat ke *server* Wazuh, seperti *log*, status perangkat, atau perubahan pada *file* yang sensitif. Praktikan menggunakan proses instalasi Wazuh Agent di Windows menggunakan *file installer*. Pertama, jalankan *file installer* dengan mengklik dua kali *file* tersebut. Proses instalasi akan dimulai. Pada setiap tahap, cukup klik tombol *Next* untuk melanjutkan hingga mencapai bagian konfigurasi agen. Di bagian ini, praktikan memasukkan alamat IP *server* Wazuh, yang dalam hal ini adalah 192.168.138.129, sebagai tujuan untuk mengirim log dan data keamanan. Selain itu, menggunakan *port default* 1514 yang digunakan oleh Wazuh untuk komunikasi antara agen dan *server*. Setelah selesai, lanjutkan proses instalasi hingga selesai, dan agen akan terkonfigurasi untuk terhubung dengan *server* Wazuh.



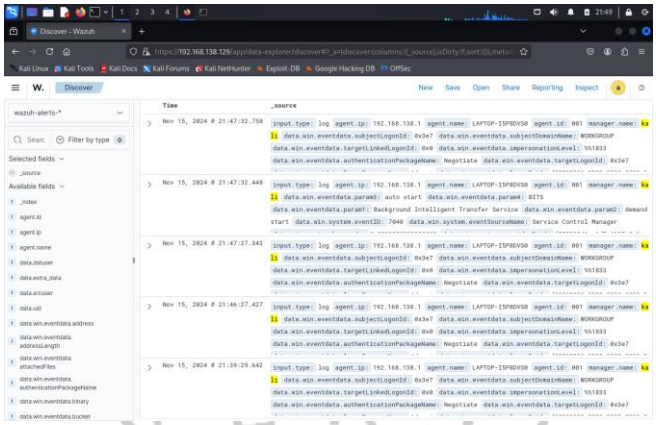
Gambar 3. 43 Wazuh Agent yang sudah dikonfigurasi

Untuk menguji efektivitas SIEM Wazuh, dilakukan simulasi serangan siber seperti pada **Gambar 3. 44**. Ini bisa berupa serangan sederhana praktikan melakukan pemindaian port dengan menggunakan Nmap yang bertujuan untuk memastikan bahwa sistem Wazuh dapat mendeteksi aktivitas mencurigakan, memberikan peringatan, dan mencatat peristiwa tersebut dengan akurat.



Gambar 3. 44 Simulasi Penyerangan ke Wazuh

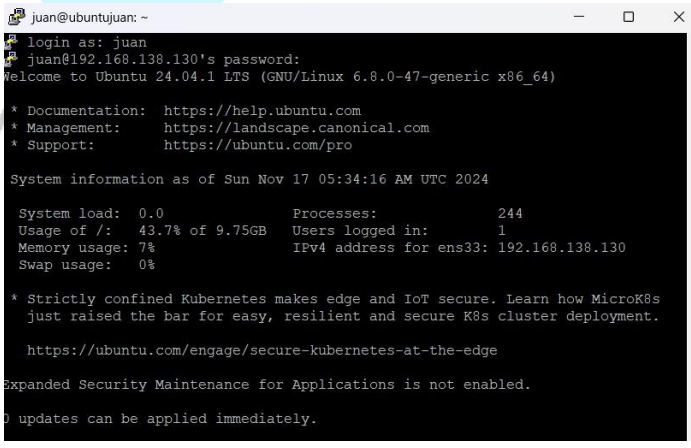
Pada **Gambar 3. 45** praktikan membuka halaman *discovery* untuk melihat *alert* di Wazuh didapatkan hasil bahwa terdapat aktivitas pemindaian aktivitas jaringan yang mencurigakan terdeteksi oleh SIEM Wazuh.



Gambar 3. 45 Alert yang Muncul Dari Penyerangan

c. Membuat *Server* dari *Virtual Machine*

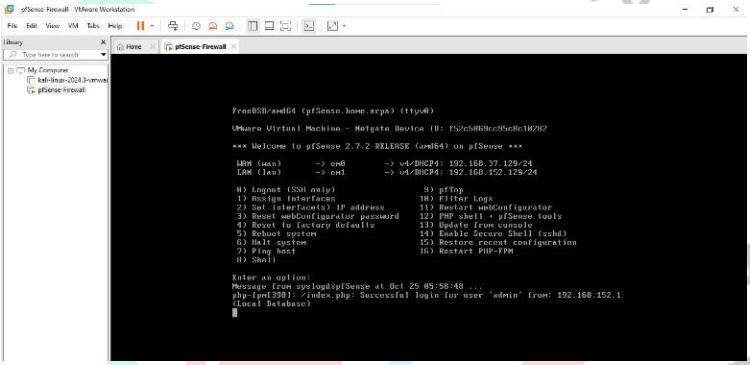
Praktikan membuat *server* dari VM menggunakan OS Ubuntu Live Server yang sudah terinstall dalam VM. Setelah itu praktikan melakukan konfigurasi OpenSSH di Ubuntu Server seperti instal Open SSH Server, pemeriksaan status SSH sudah berjalan atau belum, apabila sudah berjalan maka praktikan mencari alamat IP dari Ubuntu Server. Dalam pengujian koneksi, praktikan menggunakan PuTTY sebagai alat uji koneksi IP lokal ke *server* yang sudah dibuat. Pengujian koneksi dari PuTTY hanya memasukan alamat IP dari Ubuntu Server tadi, setelah itu menekan tombol *connect*, dan lakukan *login* pada *server* dari Ubuntu tersebut. **Gambar 3. 46** merupakan tampilan hasilnya.



Gambar 3. 46 Hasil Server yang Dibuat

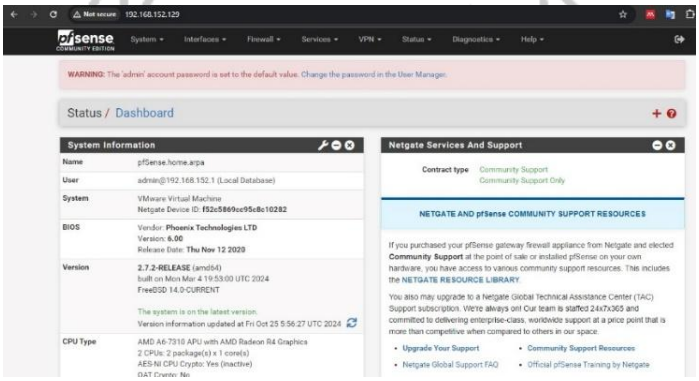
d. Pemasangan *Firewall* pfSense

Pada **Gambar 3. 47** pfSense adalah perangkat lunak firewall *open-source* yang bisa diinstal pada VM. *Firewall* berfungsi sebagai pengaman jaringan yang membatasi akses masuk dan keluar, penyaringan lalu lintas jaringan, serta melindungi sistem dari ancaman luar. Pada tahap ini, pfSense diinstal dan dikonfigurasikan praktikan. Langkah-langkahnya mencakup mengatur antarmuka jaringan, menentukan aturan *firewall*, dan menyesuaikan konfigurasi untuk mengamankan lalu lintas data di antara *server*, perangkat, atau jaringan yang terhubung.



Gambar 3. 47 Pfsense di VM

Pada Gambar **3. 48** merupakan *Dashboard Firewall* pfSense yang digunakan untuk mengontrol akses ke sistem dalam lingkungan pengujian. Dengan *firewall* ini, akses yang tidak diizinkan atau aktivitas mencurigakan dapat dibatasi, dan ini memberikan lapisan perlindungan tambahan dalam uji coba keamanan serta saat melakukan simulasi serangan.



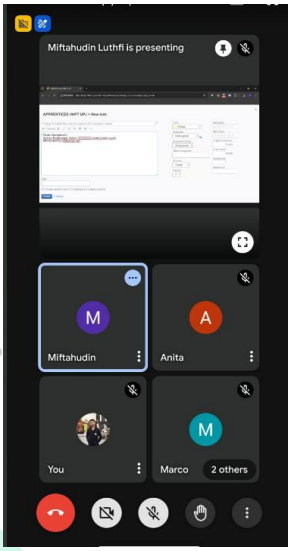
Gambar 3. 48 Dashboard pfSense

3.2.4 Vulnerability Assesment Penetration Testing and Project Manager

Vulnerability Assessment & Penetration Testing (VAPT) adalah suatu metodologi dalam melakukan uji keamanan terhadap suatu sistem *web application*. VAPT merupakan gabungan dari dua aktivitas yaitu, *Vulnerability Assessment dan Penetration Testing*. *Vulnerability Testing* merupakan aktivitas yang meliputi proses pemeriksaan sebuah celah atau kelemahan dari suatu *web application*. Sedangkan *Penetration Testing* adalah suatu proses simulasi penyerangan terhadap celah yang terdapat pada *web application* dan mengeksploitasinya (Ibrahim et al., 2022). Praktikan masuk kantor pada *Office Hour* yaitu pukul 09.00 WIB, berikut tugas – tugas yang dilaksanakan praktikan saat menjadi *Vulnerability Assesment Penetration Testing* and *Project Manager.*

1. *Meeting Pilot Project Technical Security Assessment* dengan Pembimbing

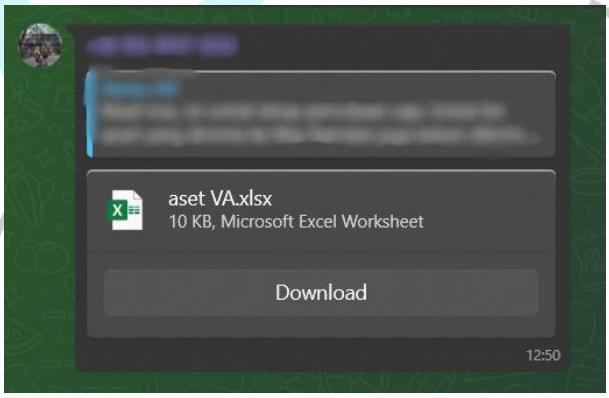
   Pada **Gambar 3. 49** merupakan *meeting pilot project Technical Security Assessment* dengan pembimbing dan *user*, dilakukan beberapa pembahasan penting, yaitu inisiasi kebutuhan seperti mencatat dan menentukan kebutuhan apa saja yang *user* ingin untuk dilakukan VAPT serta *scope* dari proyek *Technical Security Assessment*, penentuan *timeline* seperti menentukan kegiatan awal dan akhir dari sebuah proyek dengan membuat *kanban board* dan *gantt chart* sebagai *Project Manager*, serta mendefinisikan *output* dari proyek VAPT. Pertama, dilakukan diskusi awal untuk memahami kebutuhan dan tujuan proyek, serta persiapan yang diperlukan agar proyek dapat berjalan lancar. Selanjutnya, praktikan membuat *gantt chart* sebagai *timeline* proyek yang mencakup tahapan dan tenggat waktu penyelesaian setiap aktivitas, sehingga setiap langkah dapat dikelola sesuai jadwal dan memastikan semua anggota tim memahami kapan tiap bagian harus diselesaikan. Terakhir, dilakukan kesepakatan mengenai hasil akhir atau luaran yang diharapkan dari proyek, sehingga seluruh pihak memiliki pemahaman yang sama terkait *output* yang akan dicapai.



Gambar 3. 49 Praktikan saat Meeting Dengan Pembimbing Kerja dan User

2. Pengumpulan List Asset untuk Target *Vulnerability Assessment*

Pada **Gambar 3. 50** praktikan mengidentifikasi dan mencatat daftar aset atau sistem yang akan dilakukan *scanning* atau VA untuk mendeteksi kerentanannya. Aset ini bisa berupa perangkat keras, domain, atau data penting.

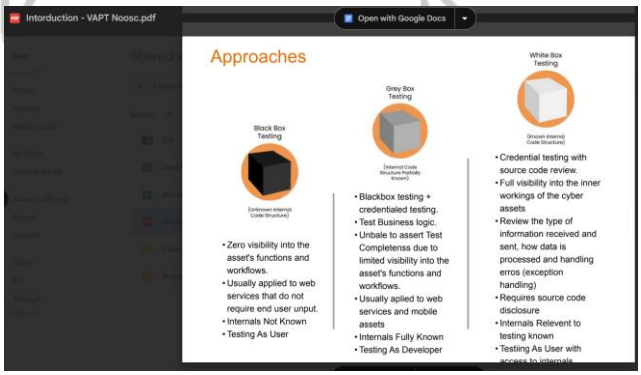


Gambar 3. 50 User Memberikan List Asset

3. Pemberian Materi Ethical Hacking

Praktikan diberikan materi oleh pembimbing sebagai bekal untuk melakukan VAPT pada asset yang ditargetkan. Penjelasan dari materi ini mengenai teknik-teknik *Ethical Hacking*, yaitu metode pengujian keamanan secara etis untuk menemukan potensi kelemahan sistem tanpa merusaknya. Berikut ringkasan mengenai ketiga jenis pengujian dalam **Gambar 3. 51** yaitu:

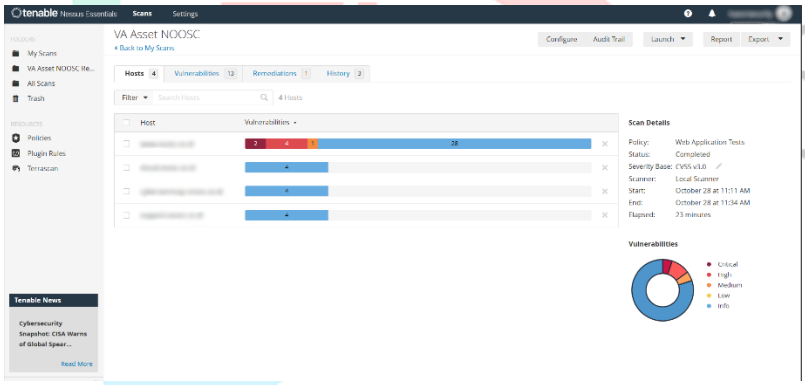
- *Black Box Testing* adalah pengujian tanpa pengetahuan internal sistem. Penguji bertindak seperti pihak luar atau pengguna eksternal yang mencoba mengeksploitasi sistem berdasarkan masukan yang tersedia. Fokusnya pada bagaimana sistem bereaksi terhadap serangan eksternal.
- *Grey Box Testing* merupakan pengujian dengan pengetahuan sebagian tentang sistem. Penguji memiliki akses terbatas ke informasi internal, seperti kredensial tertentu, sehingga dapat menguji lebih mendalam dibanding *Black Box*, tetapi tidak selengkap *White Box*. Pendekatan ini menggabungkan pengujian eksternal dan internal.
- *White Box Testing* pengujian dengan akses penuh terhadap sistem, termasuk kode sumber, alur kerja, dan data internal. Penguji dapat melakukan analisis mendalam untuk mengidentifikasi celah keamanan internal. Pendekatan ini memberikan hasil yang paling komprehensif.



Gambar 3. 51 Materi Ethical Hacking

4. Implementasi *Vulnerability Assessment*

Praktikan melakukan penilaian kerentanan pada aset-aset yang sudah terdaftar untuk mengetahui titik lemah atau risiko keamanan yang ada pada sistem tersebut. Pada **Gambar 3. 52** Tenable Nessus yang digunakan untuk melakukan *Vulnerability Assessment* (VA). Pada bagian atas, terlihat bahwa nama *scan* atau proyek yang sedang dilakukan adalah "VA *Asset* NOOSC", yang mengacu pada aset tertentu yang sedang dinilai keamanannya. Di bagian tengah, terdapat tabel yang menunjukkan daftar *host* aset yang dipindai. Setiap baris pada tabel mewakili satu host, dan kolom menunjukkan jumlah kerentanan berdasarkan tingkat keparahan, seperti *Critical, High, Medium*, dan *Low*. Sebagai contoh, *host* pertama memiliki 4 kerentanan *Critical*, 4 kerentanan *High*, dan 28 kerentanan *Medium*.



Gambar 3. 52 Praktikan Melakukan VA

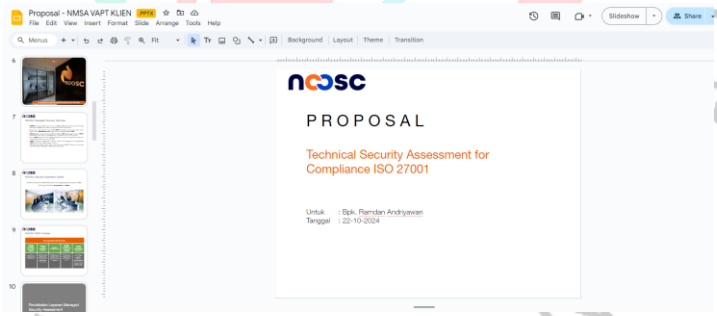
Pada sisi kanan, terdapat *Scan Details* yang memberikan informasi rinci terkait pemindaian. Informasi tersebut meliputi kebijakan yang digunakan dalam hal ini *Web Application Tests*, status pemindaian yang telah selesai *Completed*, penggunaan *Local Scanner*, tanggal dan waktu pelaksanaan scan, serta waktu yang dibutuhkan untuk menyelesaikan proses pemindaian, yaitu 29 menit. Selain itu, terdapat grafik pie yang menunjukkan distribusi kerentanan berdasarkan tingkat keparahan secara visual. Warna

merah mewakili *Critical*, kuning untuk *High*, biru untuk *Medium*, dan abu-abu untuk *Low*.

Proses *Vulnerability Assessment* dengan Tenable Nessus dimulai dengan melakukan pemindaian untuk mendeteksi kerentanan pada aset. Hasil pemindaian mengidentifikasi kerentanan pada setiap *host* dan mengkategorikannya berdasarkan tingkat keparahan. Data ini membantu menentukan prioritas perbaikan, di mana kerentanan dengan tingkat keparahan *Critical* harus segera ditangani karena berisiko tinggi terhadap keamanan.

5. Menyusun Laporan Proposal *Vulnerability Assessment*

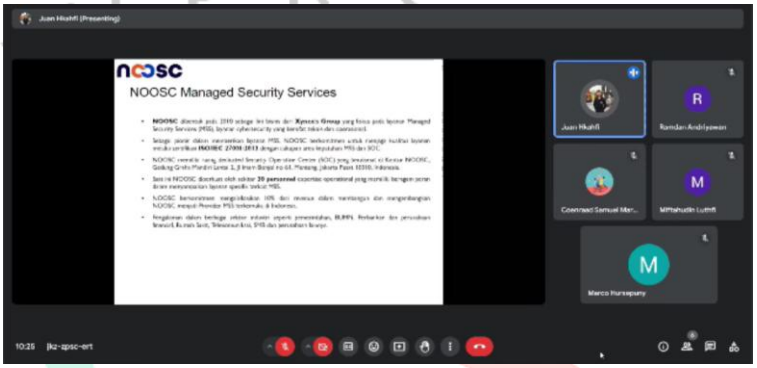
Pada **Gambar 3. 53** Praktikan menyusun dokumen proposal yang merangkum tujuan, metode, dan hasil yang diharapkan dari kegiatan *vulnerability assessment*, sehingga ada panduan dan persetujuan dari pihak terkait.



Gambar 3. 53 Laporan Proposal VA

6. Presentasi Proposal *Technical Security Assessment for Compliance* ISO 27001 dengan User dan Pembimbing

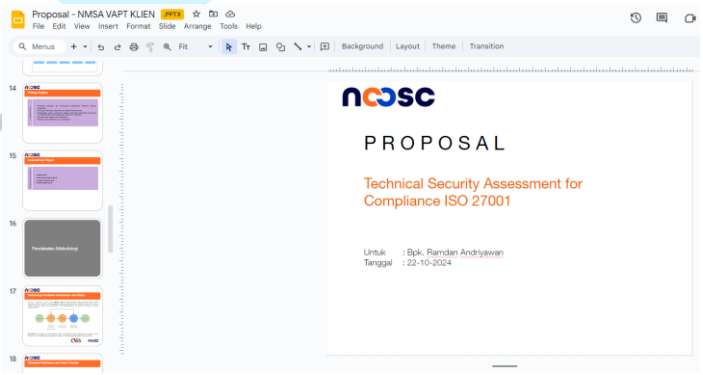
Pada **Gambar 3. 54** Praktikan menyampaikan isi proposal secara langsung melalui Google Meet kepada *user* dan pembimbing untuk mendapatkan masukan dan persetujuan terkait penilaian keamanan sesuai standar ISO 27001.



Gambar 3. 54 Praktikan Presentasi Dengan User dan Pembimbing

7. Melakukan Revisi Proposal *Technical Security Assessment for Compliance* ISO 27001

Pada **Gambar 3. 55** Praktikan memperbaiki proposal sesuai dengan masukan yang diterima agar rencana penilaian keamanan lebih relevan dan memenuhi standar yang ditetapkan.



Gambar 3. 55 Praktikan melakukan Revisi Proposal

8. Presentasi Laporan Hasil *Assessment Technical Security Assessment for Compliance* ISO 27001

Pada **Gambar 3. 56** Praktikan juga menyajikan hasil akhir dari *vulnerability assessment* yang telah praktikan lakukan kepada *user* dan pembimbing untuk menunjukkan hasil laporan yang sudah selesai dan area mana yang masih memerlukan perbaikan.

Gambar 3. 56 Praktikan Presentasi Terkait Hasil Laporan

3.3 Kendala yang Dihadapi

Selama menjalani kerja profesi, praktikan juga mengalami beberapa halangan yang berkaitan dengan pekerjaan. Yang pertama adalah penggunaan teknologi baru, di mana sangat sulit untuk mengoperasikan alat untuk keperluan *cyber security* seperti SIEM Wazuh dan penggunaan *firewall* pfSense. Hal ini disebabkan karena tidak adanya pengalaman praktikan di bidang ini sebelumnya. Selanjutnya, tantangan lain menjadi kendala dengan beragamnya koordinasi tim, terutama saat praktikan diharuskan untuk beradaptasi dengan komunikasi anggota tim dengan keterampilan teknis yang berbeda. Lalu terbatasnya waktu yang diberikan kepada praktikan dalam menyelesaikan tugas atau tes yang dibagikan dalam perbaikan tugas kerja terutama merevisi proposal dan presentasi laporan.

3.4 Cara Mengatasi Kendala

Selama menjalani kerja profesi, Praktikan mengalami beberapa kendala. Untuk mengatasi kendala-kendala tersebut, praktikan menerapkan berbagai pendekatan. Praktikan secara proaktif mempelajari panduan teknis dan meminta arahan lebih detail dari pembimbing terkait alat dan teknologi yang digunakan, sehingga dapat memahami teknologi baru dengan lebih baik. Dalam aspek komunikasi, praktikan meningkatkan keterampilan interpersonal dengan menyesuaikan cara berbicara dan mendengarkan masukan dari anggota tim lain, sehingga terjalin pemahaman bersama yang lebih baik. Selain itu, untuk mengelola tekanan waktu, praktikan menggunakan metode manajemen waktu seperti membuat *gantt chart* yang membantu merencanakan kerja secara terstruktur dan memprioritaskan tugas yang penting.

3.5 Pembelajaran yang Diperoleh dari Kerja Profesi

Selama kerja profesi, praktikan mendapatkan banyak pembelajaran berharga. Praktikan berhasil menguasai penggunaan teknologi baru, seperti SIEM Wazuh, VMware, PuTTY dan pfSense, yang sangat relevan dalam operasional keamanan siber. Selain itu, praktikan memperoleh pengalaman berkolaborasi dalam tim dengan latar belakang yang beragam, sehingga meningkatkan keterampilan komunikasi dan kemampuan bekerja sama. Praktikan juga belajar pentingnya fleksibilitas dan kemampuan belajar cepat untuk beradaptasi dengan tantangan di dunia kerja, terutama di industri keamanan siber. Tidak hanya itu, praktikan mengembangkan keterampilan teknis sekaligus kemampuan manajerial, seperti yang terlihat dalam pelaksanaan VAPT *and Project Manager* serta penyusunan presentasi laporan hasil analisis dan presentasi yang memberikan wawasan menyeluruh dalam mengelola proyek.