Report #24122727

BAB I PENDAHULUAN 1.1 Latar Belakang Kerja Profesi Cybersecurity atau keamanan siber adalah langkah yang diambil untuk melindungi sistem informasi dari berbagai potensi ancaman, baik itu serangan malware , peretasan, pencurian data, atau bentuk serangan siber lainnya. Di dunia yang semakin terkoneksi, perlindungan terhadap data dan sistem informasi tidak hanya menjadi tanggung jawab departemen IT, tetapi juga menjadi aspek kritis yang harus dikelola dengan cermat di seluruh organisasi.
Kerja profesi dalam bidang cyber security berperan penting dalam mengidentifikasi, menganalisis, dan mengurangi risiko keamanan yang mungkin terjadi. 6 Salah satu komponen utama dalam cyber security adalah monitoring dan analisis. Kegiatan monitoring dilakukan untuk memantau secara terus-menerus aktivitas dalam sistem, mendeteksi potensi ancaman, serta memastikan bahwa sistem berjalan dengan aman dan lancar. Sedangkan analisis cyber security mengacu pada pemahaman lebih dalam terhadap pola ancaman yang muncul, serta mengidentifikasi titik lemah dalam sistem yang perlu diperkuat. Monitoring dan analisis ini tidak hanya penting untuk mendeteksi serangan secara dini, tetapi juga untuk meningkatkan strategi keamanan yang diterapkan. Dengan terus melakukan evaluasi dan perbaikan berdasarkan data yang didapatkan dari monitoring dan analisis, perusahaan dapat mengurangi risiko keamanan dan meminimalisir kerugian yang muncul. Kerja profesi atau magang sebagai Cybersecurity Intern di PT NOOSC Security Global memberikan

kesempatan bagi praktikan untuk terlibat langsung dalam kegiatan yang terkait dengan keamanan siber. Sebagai bagian dari tim Security Operation Center Analyst , praktikan akan belajar tentang pemantauan real-time terhadap aktivitas jaringan dan sistem untuk mendeteksi potensi ancaman. Praktikan akan berlatih menggunakan berbagai alat keamanan siber, seperti Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Service Desk , Security Information and Event Management (SIEM), pengalaman ini sangat berharga untuk memahami bagaimana tim SOC beroperasi dan bagaimana informasi dikumpulkan serta dianalisis untuk memberikan respons yang tepat terhadap insiden siber. Di sisi lain, sebagai Cybersecurity Analyst , praktikan akan terlibat dalam menganalisis data kerentanan yang ada dan melakukan evaluasi terhadap potensi kerentanan dalam sistem seperti melakukan rekapitulasi tiket, serta praktikan akan belajar membuat use case untuk dashboard monitoring yang berguna untuk SOC. Pengalaman tersebut bermanfaat untuk mengembangkan wawasan mengenai proses deteksi dini dan respons cepat terhadap potensi ancaman keamanan siber di SOC. Praktikan diberikan kesempatan untuk mengikuti program kerja di posisi Cybersecurity Engineer . Dalam program ini, praktikan ditugaskan melakukan dismantle server , instalasi SIEM Wazuh, simulasi penyerangan ke Wazuh, serta pembuatan server dan konfigurasi firewall . Pengalaman tersebut memberikan pengalaman praktis yang mendalam di bidang keamanan siber.

Praktikan juga diarahkan pada posisi Vulnerability Assessment Penetration Testing (VAPT) and Project Manager dalam proyek Pilot Project Technical Security Assessment . Pada tahap awal dimulai dengan inisiasi kebutuhan pengguna terkait VAPT, mencakup diskusi untuk menentukan area pengujian keamanan dan prioritas risiko. Berdasarkan inisiasi tersebut, Praktikan menetapkan scope proyek yang jelas, menyusun timeline menggunakan kanban board dan gantt chart , serta merancang hasil berupa laporan teknis berisi temuan kerentanan, analisis risiko, dan rekomendasi mitigasi. Untuk mendukung pelaksanaan, digunakan tools seperti Tenable Nessus untuk pemindaian kerentanan, Canva untuk desain laporan, dan Google Slide untuk presentasi hasil. Melalui program magang ini, praktikan akan memiliki kesempatan untuk bekerja dalam lingkungan kolaboratif yang mencakup tim profesional berpengalaman. Praktikan akan belajar tentang pentingnya komunikasi dan koordinasi dalam merespons insiden keamanan, serta bagaimana menciptakan budaya keamanan yang kuat di seluruh organisasi. Selain itu, praktikan akan mengembangkan jaringan profesional yang dapat membantu praktikan dalam pencarian pekerjaan di masa depan. 2 5 9 1.2 Maksud dan Tujuan Kerja Profesi 1.2 5 1 Maksud Kerja Profesi Maksud dari pelaksanaan kegiatan magang kerja profesi yaitu: 1. Melakukan pemantauan dan analisis keamanan sistem. 2. Mengembangkan dan mengimplementasikan solusi Keamanan. 3. Mendukung tim cyber security dalam penanganan insiden 1.2.2 Tujuan Kerja Profesi Tujuan dari pelaksanaan kegiatan magang kerja profesi yaitu: 1. Meningkatkan pemahaman tentang operasi keamanan siber. 2. Meningkatkan keterampilan teknis dan analis. 3. Menyiapkan diri untuk peran profesional di industri keamanan siber. 1.3 Tempat Kerja Profesi Praktikan melaksanakan kegiatan Kerja Profesi di PT NOOSC Security Global, yang berlokasi di Gedung Graha Mandiri, 2nd floor Jl. Imam Bonjol No. 61 Jakarta, 10310, Indonesia. 2 1.4 Jadwal Pelaksanaan Kerja Profesi Kerja Profesi dilaksanakan selama 6 bulan yang dimulai pada tanggal 8 Juli 2024 hingga 7 Januari 2025. Pelaksanaan kegiatan Kerja Profesi pada PT NOOSC Security Global dimulai saat praktikan masuk ke kantor Office Hour pada pukul 09.00–18.00 WIB,

setelah itu praktikan diarahkan pembimbing ke posisi SOC Analyst mengikuti jam kerja shift 1 SOC yaitu dimulai pada pukul 07.00–15.00 WIB dan kedua jam kerja tersebut bersifat on-site atau datang ke kantor. 1 B-1 BAB II TINJAUAN UMUM TEMPAT KERJA PROFESI 2.1 Sejarah Perusahaan Dimulai pada tahun 2010, melalui kemitraan strategis NOOSC kini telah menjadi layanan keamanan terkelola pilihan di Indonesia yang melayani beberapa lembaga keuangan dan jasa terbesar di negara ini. Perusahaan ini beroperasi pada Pusat Operasi Keamanan 24x7 khusus dengan perlindungan pemulihan bencana Profesional ahli, kredensial & catatan internasional yang dapat diverifikasi Praktik terbaik, proses pengiriman yang digerakkan oleh tingkat layanan (sesuai dengan ISO27001) Investasi R&D aktif yang mencakup ancaman & teknologi keamanan baru yang muncul. 2.2 Struktur Organisasi Struktur organisasi ini memberikan gambaran yang jelas tentang pembagian tugas dan tanggung jawab di dalam perusahaan. Berikut adalah penjelasan singkat dari setiap departemen dan posisinya terlihat pada Gambar 2. 2: Tingkat Tertinggi: ⊠ CEO: Merupakan pemimpin tertinggi perusahaan dan bertanggung jawab ata s visi, misi, dan strategi keseluruhan perusahaan. ⊠ COO: Bertanggung jawa b atas operasi sehari-hari perusahaan, memastikan semua departemen berjalan efisien dan efektif. Tingkat Manajemen: ⊠ Office Management: Mengelol a administrasi umum perusahaan. ⊠ Control & PMO: Mengelola proyek da n memastikan proyek berjalan sesuai rencana. ⊠ Strategy, Consulting & Sale s Marketing Division Head: Bertanggung jawab atas strategi bisnis, konsultasi, penjualan, dan pemasaran. ⊠ CyberSec Technology, Services an d Business Development Division Head: Bertanggung jawab atas pengembangan teknologi keamanan siber, layanan, dan pengembangan bisnis di bidang ini. Departemen dan Posisi: ⊠ HR & Legal Section: Mengelola sumber daya manusi a dan urusan hukum perusahaan. ⊠ Finance: Mengelola keuangan perusahaan. ⊠ ISO 27001 Auditor: Bertanggung jawab atas audit sistem manajemen keamanan informasi. ⊠ PMO Officer: Mengelola proyek-proyek khusus. ⊠ Operational Contr ol: Mengontrol operasi sehari-hari. ⊠ Strategic Consulting: Memberika n konsultasi strategis. ⊠ Account Executive Direct Sales: Bertanggung jawa

b atas penjualan langsung. Account Executive Partner: Bertanggung jawa b atas penjualan melalui mitra. Sales & Tendering: Mengelola penjuala n dan tender. Digital Marketing & Content: Mengelola pemasaran digita l dan konten. Technical Security: Mengelola keamanan teknis. Produc t & Solutions Architect: Profesional yang bertanggung jawab untuk merancang dan mengembangkan solusi teknologi dan produk yang memenuhi kebutuhan bisnis dan pengguna. Manage Service Operation Section Head: Posis i manajerial dalam organisasi yang bertanggung jawab untuk mengelola dan mengawasi operasi layanan TI, dengan fokus pada penyampaian layanan yang efisien dan efektif kepada pelanggan. Security Operation Center Analyst : Sebuah unit yang bertanggung jawab untuk memonitor, mendeteksi, dan merespons insiden keamanan siber dalam suatu organisasi. Cybersecurit y Analyst: Berperan dalam menjaga keamanan informasi dan melindungi organisasi dari risiko yang terkait dengan ancaman siber. Dengan pengetahuan dan keterampilan yang tepat, mereka dapat mengidentifikasi dan mengatasi risiko, serta berkontribusi pada pengembangan strategi keamanan yang efektif. Cybersecurity Engineer: Profesional yang bertanggung jawa b untuk merancang, membangun, dan mengelola sistem dan infrastruktur keamanan siber dalam suatu organisasi. B-2 2.3 Kegiatan Umum Perusahaan PT NOOSC Security Global Gambar 2. 3 menyediakan layanan konsultasi dan profesional dengan profesional keamanan siber berpengalaman yang memberikan keahlian langsung dan memetakan rencana kebutuhan Klien yang mencakup aspek strategi, tata kelola, risiko, kepatuhan, dan jaminan. Dalam memandu dan berkonsultasi dengan organisasi untuk mengidentifikasi kesenjangan dan menyarankan solusi untuk mengisi kesenjangan tersebut guna meningkatkan efisiensi, dan memperkuat postur keamanan dan ketahanan siber berdasarkan praktik terbaik, kerangka kerja keamanan, standar industri, dan yang terpenting dari semuanya belajar dari pengalaman sejauh ini. Managed Security Services (MSS) yang dibagi ke dalam lima kategori utama. Berikut penjelasan lengkap untuk setiap layanan: 1. Managed Security Monitoring & Detection Services Layanan pemantauan secara real-time terhadap

ancaman keamanan, incident management , dan insiden keamanan. Ini membantu organisasi mendeteksi dan merespon ancaman sebelum menjadi masalah besar. Security Log Management Pengelolaan log keamanan yang dihasilkan ole h berbagai sistem dan aplikasi. Security Event & Incident Managemen t Penanganan dan pengelolaan kejadian atau insiden keamanan secara terstruktur. Security Threat Alerting Pemberitahuan tentang ancaman ata u potensi serangan yang terdeteksi melalui pemantauan. 2. Managed Security Intelligence Services Layanan yang menyediakan informasi mendalam terkait nasihat strategis untuk membantu organisasi mengidentifikasi dan memitigasi potensi kerentanan atau ancaman keamanan. Fokusnya adalah pada penilaian risiko dan respons proaktif terhadap ancaman. Information Security Advisor y Memberikan saran terkait peningkatan keamanan informasi. Vulnerabilit y Assessment and Management Identifikasi dan pengelolaan kerentanan sistem untuk mencegah potensi serangan. Security Configuration Review Tinjaua n konfigurasi sistem untuk memastikan keamanan yang optimal. Threa t Hunting Proses aktif mencari ancaman keamanan yang tersembunyi dalam jaringan. Penetration Testing Menguji kerentanan sistem dengan mensimulasika n serangan dari luar. Attack Scenario Simulasi serangan untuk menguj i kesiapan sistem keamanan. 3. Managed Security Device Layanan ini mencakup pengelolaan dan pemeliharaan perangkat keamanan untuk memastikan perangkat tersebut selalu dalam kondisi optimal. Dukungan operasional rutin membantu menjaga keamanan sistem dan mencegah kerusakan. Administerin g Security Systems & Devices Pengelolaan perangkat keamanan yang ada di organisasi, termasuk firewall , IDS/IPS, dll. Operational Support o f Managing Security Devices Memberikan dukungan operasional harian untuk perangkat keamanan. Regular health check and liaison support Memastika n perangkat keamanan berfungsi dengan baik melalui pemeriksaan rutin. 4. Managed Incident Response and Handling Services Merupakan layanan respons dan penanganan insiden keamanan secara langsung. Proses ini melibatkan investigasi mendalam dan penerapan langkah-langkah untuk menanggulangi serta memitigasi dampak insiden. Information Security Log Forensic an

d Investigation Melakukan analisis forensik terhadap log untuk mengidentifikasi sumber dan dampak insiden keamanan. Incident Response an d Handling Penanganan insiden keamanan secara cepat dan efisien. Patchin g & Hardening Memperbaiki kerentanan dengan patch dan memperkuat sistem dari potensi serangan. B-3 5. General Technical Consultancy & Advisories Layanan konsultasi ini memberikan panduan teknis umum untuk meningkatkan keamanan IT organisasi secara keseluruhan, termasuk pengelolaan tim SOC, penilaian aset informasi, serta pelatihan kesadaran keamanan kepada staf. SOC Readiness Review Menilai kesiapan tim Security Operations Center (SOC) dalam menghadapi ancaman keamanan. SOC Design, Plan, and Implementatio n Membantu dalam perancangan dan implementasi pusat operasi keamanan. SO C Assessment Evaluasi terhadap kinerja dan efektivitas SOC. Informatio n Asset and Threat Identification Identifikasi aset informasi kritis dan potensi ancaman yang mungkin mempengaruhi mereka. IT Security Complianc e Monitoring Memastikan sistem sesuai dengan regulasi dan standar keamanan yang berlaku. Security Awareness Program Melatih staf tentang keamana n informasi dan praktik terbaik untuk menjaga keamanan. Phishin g Simulation Simulasi serangan phishing untuk menguji kesiapan dan kewaspadaan staf terhadap serangan siber. Berbagai layanan Managed Security Services yang mengacu pada pemantauan, intelijen, pengelolaan perangkat keamanan, respons insiden, dan konsultasi teknis. Hal ini membantu organisasi dalam melindungi aset informasi mereka, merespons ancaman keamanan dengan cepat, dan memastikan kepatuhan terhadap standar keamanan yang berlaku. 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 . 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. 3 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. B-4 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. 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. B-5 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. 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. 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. 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 . 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. 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. 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. 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. 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. 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. 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. 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. 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 . 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 B-6 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. 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 lapora n pada pukul 09.00, dan 09.00 – 15.00 untuk dilakukan pengiriman lapora n 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. 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). 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. 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. 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. B-7 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 Detectio n 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 . Analysis Setelah melakukan pembuatan pesan firs t 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 . 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. 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. 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. 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. 3.2.2 Cybersecurity Analyst Praktikan masuk kantor pada Office Hour yaitu pukul 09.00 WIB, tugas – tugas yan g 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: 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. 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 B-8 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. 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. index=windows "tag::eventtype"=authentication EventCode = 4624 | stat s dc(user) as total Memilih data dari indeks bernama windows denga n 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 = 462 5 | stats dc(user) as total Pemilihan data dari indeks bernama window s 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 . index=windows "tag::eventtype"=authentication EventCode = 4624 Memilih d ata 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-filte r 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 hasi l 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 Memi lih 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 yan g 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_n t_host, Status, dan src_ip, lalu menampilkan waktu terbaru dari kejadian tersebut sebagai Time , dan menghitung jumlah kejadian untuk setiap kelompok sebagai count . B-9 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 terdapa t lonjakan tiket hingga 14 disebabkan oleh peningkatan aktivitas atau insiden keamanan. 24-31 Juli puncak aktivitas dengan 26 tike t diselesaikan, menunjukkan kesibukan tim SOC di akhir bulan. Pada Gambar 3. 36 adalah data yang praktikan olah untuk melakukan visualisasi data Sophos dan merupakan laporan harian yang memantau kinerja perangkat oleh Sophos. 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. 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. 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. 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: 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. 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 . B-10 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 se rver Wazuh, seperti log , status perangkat, atau perubahan pada file yang sensitif. Praktikan menggunakan proses instalasi Wazuh Agent di Windows menggunakan file installer . 8 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. 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. 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. 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. 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. 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.

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 Assesmen t 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. 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. 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. 7 51 yaitu: ⊠ Black Box Testing adala h 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. B-11 ⊠ Grey Box Testing merupakan pengujian denga n 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 Bo x 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. 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 . 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. 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. 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. 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. 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. 4 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 B-12 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. BAB IV PENUTUP 4.1 Kesimpulan Tujuan Kerja Profesi berhasil tercapai dengan baik saat pelaksanaannya. Praktikan berhasil meningkatkan pemahaman tentang operasi keamanan siber melalui kegiatan monitoring sistem, analisis ancaman, dan penerapan solusi keamanan yang dilakukan secara langsung menggunakan berbagai alat keamanan seperti SIEM (Splunk, QRadar, AlienVault). Selain itu, keterampilan teknis dan analisis praktikan juga mengalami peningkatan dalam pengolahan data, pembuatan use case untuk dashboard monitoring , konfigurasi firewall , dan pelaksanaan Vulnerability Assessment dan Penetration Testing (VAPT). Pengalaman ini juga mempersiapkan praktikan untuk peran profesional di industri keamanan siber, dengan memberikan wawasan praktis, pelatihan soft skill dalam manajemen waktu dan komunikasi, serta kemampuan beradaptasi terhadap kebutuhan dunia kerja yang dinamis. Selama menjalani kerja profesi, praktikan menyadari bahwa banyak hal yang dipelajari di mata kuliah ternyata sangat membantu dalam menyelesaikan tugas sehari-hari. Salah satunya adalah mata kuliah Keamanan Informasi dan Administrasi Jaringan (IST104). Sebagai seorang Security Operation Center Analyst (SOC), praktikan sering menggunakan alat seperti SIEM Qradar, AlienVault, Splunk untuk memantau jaringan dan mendeteksi ancaman keamanan. Ilmu dari mata kuliah ini benar-benar terasa berguna karena memberikan dasar yang kuat dalam memahami cara kerja sistem keamanan. Selain itu, mata kuliah Perancangan dan Administrasi Basis Data (IST201) juga terasa manfaatnya ketika praktikan bekerja sebagai Cybersecurity Analyst . Dalam tugas ini, praktikan sering mengolah data dan menganalisis log menggunakan Splunk dan Microsoft Excel untuk membuat laporan operasional. Apa yang dipelajari di kelas, seperti cara mengelola dan menganalisis data, sangat membantu praktikan untuk memahami tugas dengan lebih mudah. Pengalaman sebagai Cybersecurity Engineer juga menunjukkan betapa pentingnya mata kuliah Pengembangan Aplikasi Perangkat Lunak (IST204). Tugas seperti instalasi SIEM Wazuh, konfigurasi Wazuh Agent, simulasi penyerangan, konfigurasi firewall

pfSense, dan pembuatan server dari Virtual Machine membutuhkan pemahaman yang baik tentang pengembangan dan implementasi perangkat lunak, yang semuanya pernah dipelajari di mata kuliah tersebut. Pengalaman selama kerja profesi ini membuat praktikan sadar bahwa apa yang diajarkan di kampus bukan hanya teori belaka, tapi benar-benar berguna dan sesuai dengan apa yang dibutuhkan di dunia kerja. 4.2 Saran Setelah menjalani kerja profesi, praktikan memiliki beberapa saran yang bisa berguna untuk ke depannya. Pertama, kampus sebaiknya menambahkan lebih banyak sesi praktik langsung di kelas, terutama untuk mata kuliah yang berhubungan dengan keamanan jaringan atau pengelolaan basis data. Dengan begitu, mahasiswa bisa lebih terbiasa menggunakan alat-alat yang sering dipakai di dunia kerja, seperti SIEM atau Splunk. Selain itu, proyek kelompok juga penting karena di dunia kerja hampir semua tugas dilakukan secara tim. Jadi, lebih banyak tugas atau kegiatan kolaborasi di kampus pasti akan membantu mahasiswa belajar cara kerja sama dengan orang lain. Praktikan juga merasa penting untuk lebih mengenalkan teknologi terbaru di kampus. Selama magang, banyak alat dan teknologi baru yang belum pernah diajarkan di kelas. Kalau kampus bisa memasukkan pelatihan tentang alat-alat ini, pasti mahasiswa jadi lebih siap. Selain itu, sebaiknya magang dimulai lebih awal, misalnya di semester lima atau enam, supaya mahasiswa punya lebih banyak waktu untuk belajar dan beradaptasi dengan dunia kerja. Terakhir, kampus juga bisa membantu mahasiswa mempersiapkan soft skill seperti cara berkomunikasi dalam tim, membuat laporan, atau melakukan presentasi yang profesional. Hal-hal ini sering dilakukan di tempat kerja, dan kalau mahasiswa sudah terbiasa dari awal, pasti mereka akan lebih percaya diri. Dengan semua ini, mahasiswa akan lebih siap menghadapi tantangan di dunia kerja nanti. B-13

REPORT #24122727

Results

Sources that matched your submitted document.

IDENTICAL CHANGED TEXT

1.	INTERNET SOURCE **1.01%** cybersecmssp.noosc.co.id *https://cybersecmssp.noosc.co.id/id/tentang-kami/*	
2.	INTERNET SOURCE **0.32%** eprints.upj.ac.id *https://eprints.upj.ac.id/id/eprint/8987/11/BAB%20I.pdf*	
3.	INTERNET SOURCE **0.2%** www.biznetgio.com *https://www.biznetgio.com/news/soc-adalah*	
4.	INTERNET SOURCE **0.2%** eprints.upj.ac.id *https://eprints.upj.ac.id/id/eprint/1701/13/13.BAB%20III.pdf*	
5.	INTERNET SOURCE **0.2%** eprints.upj.ac.id *https://eprints.upj.ac.id/id/eprint/3633/11/11.%20BAB%20I.pdf*	
6.	INTERNET SOURCE **0.13%** aplikas.com *https://aplikas.com/blog/vulnerability-scanning/*	
7.	INTERNET SOURCE **0.13%** www.academia.edu *https://www.academia.edu/42142388/Unit_Pembelajaran_Visualisasi_Data*	
8.	INTERNET SOURCE **0.12%** vcube.co.id *https://vcube.co.id/belajar-obs-studio-cara-install-dan-setup-untuk-live-stream...*	
9.	INTERNET SOURCE **0.06%** kerma.esaunggul.ac.id *https://kerma.esaunggul.ac.id/upload/kerjasama/3557-Laporan%20Magang%20..*	