LAPORAN RESMI

PRAKTIKUM KEAMANAN JARINGAN

NOC dan SOC

Oleh :

Fisabili Maghfirona Firdaus 3122640051

D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

NOC

Network Operations Center berfokus pada instalasi jaringan, pemeliharaan, kinerja, dan ketersediaan. Tugasnya adalah memastikan bahwa akses jaringan, server, aplikasi, dan data selalu tersedia, dan memenuhi atau melampaui kebutuhan organisasi dan Service Level Agreements (SLA). NOC terutama berfokus pada penyampaian layanan dan aplikasi, pengoperasian, pemeliharaan, dan pencegahan/pemulihan dari bencana operasional dan alam: seperti banjir, gempa bumi, kebakaran, atau pemadaman layanan. NOC klasik adalah ruangan besar dan khusus yang menghadap atau berisi rak perangkat keras infrastruktur jaringan. NOC dapat dikelola secara internal, atau dikelola oleh penyedia cloud, penyedia layanan terkelola (MSP), atau penyedia pihak ketiga lainnya.

SOC

Security Operations Center berfokus pada semua hal yang terkait dengan keamanan:
Deteksi ancaman, pemasangan, pemeliharaan, pemantauan, analisis, respons insiden, dan forensik. SOC memastikan ketersediaan dan melindungi jaringan dengan membuat dan terus meningkatkan arsitektur dan infrastruktur keamanan yang melindungi sumber daya IT.
Mereka menjaga jaringan Anda dari ancaman rekayasa manusia seperti:

- Malware
- Virus
- Peretas
- Ransomware
- Serangan siber lainnya

Seperti NOC, SOC adalah lokasi terpusat tempat tim keamanan TI bekerja 24/7/365 untuk melindungi sumber daya IT. Tim SOC dapat bersifat internal, virtual, atau outsourcing. Di mana pun SOC berada, kemungkinan ada setidaknya satu orang yang menjabat sebagai Manajer atau Direktur SOC.

Perbedaan Tugas NOC & SOC

Perbedaan tugas akan ditampilkan pada tabel berikut:

Apa yang menjadi tanggung jawab NOC & SOC			
Tanggung Jawab	**Network Operations Center (NOC)**	**Security Operations Center (SOC)**	**Fokus pada**
Perbaikan Anti-Virus, malware & ransomware	✅ Ya	✅ Ya	Deteksi dan respons malware, virus, dan ransomware
Pelaporan kepatuhan audit	✅ Ya	✅ Ya	Kepatuhan terdokumentasi dengan persyaratan audit internal & eksternal untuk aset

Ketersediaan	☑ Ya	✕ Tidak	Pencadangan & pemulihan sistem/data, ketersediaan tinggi, pemulihan bencana
Analisis akar penyebab serangan siber	✕ Tidak	☑ Ya	Analisis & pahami akar penyebab serangan siber untuk mencegah serangan di masa mendatang
Manajemen perangkat & perangkat lunak	☑ Ya	☑ Ya	Penyebaran perangkat lunak/perangkat keras, penginstalan, pembaruan, pemecahan masalah & distribusi
Menegakkan kebijakan keamanan	✕ Tidak	☑ Ya	Pembuatan & penegakan kebijakan keamanan
Analisis forensik keamanan & data log peristiwa	✕ Tidak	☑ Ya	Analisis mendalam dari berbagai sumber mencari ancaman & tren keamanan
Tanggapan Insiden	☑ Ya	☑ Ya	Mengkoordinasikan & menerapkan respons insiden
Pantau dan kelola firewall & sistem pencegahan intrusi	☑ Ya	☑ Ya	Instalasi, administrasi, pembaruan, pengujian penetrasi, peretasan etis , dll.
Pemantauan kesehatan jaringan	☑ Ya	✕ Tidak	Memantau status jaringan, mendeteksi masalah jaringan yang memerlukan perhatian khusus, dan memperingatkan tim respons insiden saat terjadi peristiwa

			jaringan.
Pengawasan keamanan jaringan	✕ Tidak	☑ Ya	Mendeteksi pelanggaran keamanan dan memicu respons insiden
Menambal	☑ Ya	☑ Ya	Terapkan perbaikan & tambalan keamanan terbaru
Pertunjukan	☑ Ya	✕ Tidak	Pantau/pertahankan kecepatan & throughput jaringan agar sesuai dengan SLA
Memberikan keahlian keamanan	✕ Tidak	☑ Ya	Konsultasikan dengan entitas organisasi, pengguna, mitra bisnis, dan entitas luar untuk menerapkan metode dan alat keamanan
Keamanan	☑ Ya	☑ Ya	Pemantauan, penerapan alat, respons insiden
Analisis tren keamanan	✕ Tidak	☑ Ya	Selidiki & analisis data keamanan untuk menentukan apakah tren sedang berkembang seputar jenis peristiwa alarm keamanan tertentu
Izinkan & tolak daftar (daftar putih & daftar hitam fka)	✕ Tidak	☑ Ya	Memodifikasi dan memelihara daftar izinkan/tolak untuk situs web, email & proses lainnya