Security Operations Center (SOC)

Duration: 3 Days

Course Content

Pelatihan Security Operations Center (SOC) adalah program intensif yang dirancang untuk membekali peserta dengan pengetahuan dan keterampilan yang diperlukan untuk beroperasi dan mengelola sebuah pusat operasi keamanan yang efektif. Program ini menargetkan profesional IT dan keamanan siber yang ingin mengembangkan atau meningkatkan kemampuan dalam mendeteksi, menganalisis, dan merespons terhadap insiden keamanan siber.

Prerequisites

- Pengetahuan mengenai jaringan (osi layer & TCP/IP layer)
- Pengetahuan mengenai perangkat hardware
- Pengetahuan mengenai Operating sistem

Course Objectives

Setelah menyelesaikan pelatihan ini, peserta di harapkan dapat:

- Pemahaman Konsep Keamanan Siber
- Penerapan Kontrol Keamanan
- Keamanan Jaringan dan Sistem
- Deteksi Ancaman dan Respons Insiden
- Menerapkan keamanan data teknik keamanan data pada jaringan
- Kebijakan dan Prosedur Keamanan
- Kepatuhan dan Standar Keamanan
- Memahami dan menggunakan IDS/IPS teknologi

Course Outline

- Module 01: Introduction Cyber Six
- Module 02: Understanding Computer Network Defense
- Module 03: Tier 1, 2, 3 SOC
- Module 04: Administrative network security
- Module 05: Network Perimeter Security
- Module 06: Risk management

- Module 07: Endpoint Security windows
- Module 08: SIEM
- Module 09: Incident Respond