SEMATEC
IT Training Center

سرفصل دوره SOC-Tier2

دوره SOC Tier 2 یک برنامه آموزشی پیشرفته است که به منظور آماده‌سازی متخصصان امنیتی برای انجام وظایف پیچیده‌تر و حساس‌تر در مرکز عملیات امنیت (SOC) طراحی شده است. این دوره افراد را از سطح ابتدایی (Tier 1) به یک سطح بالاتر (Tier 2) ارتقا می‌دهد، جایی که مسئولیت‌های بیشتری در زمینه تحلیل حوادث امنیتی و مدیریت تهدیدات به آن‌ها واگذار می‌شود.

اهداف دوره

اهداف یک دوره آموزشی برای نیروهای Tier 2 در مرکز عملیات امنیت (SOC) شامل تجهیز کردن آن‌ها به مهارت‌ها و دانش پیشرفته‌تری است که برای تحلیل عمیق‌تر و پاسخ به تهدیدات امنیتی پیچیده‌تر ضروری است. در زیر اهداف اصلی چنین دوره‌ای آورده شده است:

- آموزش تکنیک‌های پیشرفته برای تحلیل و تحقیق در مورد حوادث امنیتی که از سوی نیروهای Tier 1 تصاعد یافته‌اند.

- توسعه توانایی در تشخیص حملات پیچیده و مستمر (مثل APT ها) که نیاز به تحلیل دقیق‌تر دارند.
- کار با ابزارها و فناوری‌های پیشرفته مانند SIEM ، IDS/IPS،
- آموزش استفاده از اسکریپت‌نویسی و اتوماسیون برای تسهیل تحلیل و پاسخ به حوادث.

- آموزش مهارت‌های عملی برای پاسخ سریع و موثر به حملات پیچیده مانند بدافزارها، حملات شبکه‌ای، و حملات مهندسی اجتماعی.
- یادگیری تکنیک‌های پیشرفته در مهار، پاکسازی، و بازیابی سیستم‌های آلوده.

- تقویت مهارت‌های ارتباطی برای همکاری موثر با تیم‌های Tier 1 ، Tier 3، و سایر بخش‌های امنیتی و IT.
- آموزش مدیریت جلسات و گزارش‌دهی دقیق و جامع به مدیران و سایر تیم‌های مرتبط.

- آشنایی با تکنیک‌ها و تاکتیک‌های مورد استفاده توسط مهاجمین برای نفوذ و بهره‌برداری از سیستم‌ها.
- آموزش تجزیه و تحلیل تاکتیک‌ها، تکنیک‌ها، و پروسه‌ها (TTPs) مهاجمین بر اساس چارچوب‌هایی مانند MITRE ATT&CK.

- یادگیری روش‌های فعال برای جستجو و شناسایی تهدیدات در محیط‌های IT بدون وابستگی به هشدارهای خودکار SIEM.

- استفاده از تحلیل رفتاری و ناهنجاری‌ها برای کشف تهدیدات ناشناخته.

این اهداف به نیروهای Tier 2 SOC کمک می‌کند تا نه تنها بتوانند به طور موثرتر به تهدیدات پاســـخ دهند، بلکه بتوانند به صورت فعال تهدیدات را شناسایی و از آن‌ها پیشگیری کنند.

مخاطبان:

- کارشناسان امنیت سایبری که قصد دارند به سطح بالاتر (Tier 2) در SOC ارتقا پیدا کنند.
- افرادی که دارای تجربه در مانیتورینگ و تحلیل حوادث امنیتی هستند و می‌خواهند مهارت‌های خود را تقویت کنند.
- مدیران و کارشناسان امنیت

پیش‌نیازها:

- دانش و تجربه کار عملی با یک با ابزار .SIEM (بومی یا خارجی)
- آشنایی با مفاهیم اولیه امنیت شبکه و سیستم‌های اطلاعاتی.
- تجربه عملی در تحلیل ابتدایی حوادث امنیتی و کار در یک SOC به عنوان نیروی Tier 1. حداقل یکسال

مدت زمان دوره

این دوره در مدت زمان ۱۲۰ ساعت به صورت تئوری و عملی برگزار خواهد شد

سرفصل:

SEC511: Continuous Monitoring and Security Operations

- SECTION 1: Current State Assessment, SOCs
- and Security Architecture
- SECTION 2: Network Security Architecture
- SECTION 3: Network Security Monitoring
- SECTION 4: Endpoint Security Architecture
- SECTION 5: Automation and Continuous
- Security Monitoring
- SECTION 6: Capstone: Design, Detect, Defend

SANS SEC503: Network Monitoring and Threat Detection In-Depth

- SECTION 1: Network Monitoring and Analysis: Part I
- SECTION 2: Network Monitoring and Analysis: Part II
- SECTION 3: Signature-Based Threat
- Detection and Response
- SECTION 4: Building Zero-Day Threat
- Detection Systems
- SECTION 5: Large-Scale Threat Detection, Forensics, and Analytics
- SECTION 6: Advanced Network Monitoring and Threat
- Detection Capstone

EC-Council Certified Incident Handler (ECIH)

- Module 1: Introduction to Incident Handling and Response
- Module 2: Incident Handling and Response Process
- Module 3: First Response
- Module 4: Handling and Responding to Malware Incidents
- Module 5: Handling and Responding to Email Security Incidents
- Module 6: Handling and Responding to Network Security Incidents
- Module 7: Handling and Responding to Web Application Security Incidents
- Module 8: Handling and Responding to Cloud Security Incidents
- Module 9: Handling and Responding to Insider Threats
- Module 10: Handling and Responding to Endpoint Security Incidents