SEMATEC
IT Training Center

دوره مرکز عملیات امنیت (تحلیلگر سطح 1) – SOC Tier1

خلاصه دوره مرکز عملیات امنیت:

دوره SOC مقدمه ای بر مرکز عملیات امنیت و استانداردهای استقرار و طراحی آن به همراه بررسی کامل اجزای مرکز عملیات امنیت و در نهایت پیاده سازی فرآیندهای عملیاتی یک مرکز عملیات امنیت در محیط آزمایشگاهی با کمک SplunkEnterprise ارائه خواهد گردید. دوره SOC تلفیقی از دوره های استاندارد مؤسسه SANS به همراه دوره Security+ ارائه می گردد.

در این پکیج دوره های (SSCP/Security+, SANS SEC 450, SANS SEC 504, Splunk Fundamental) تدریس خواهد شد.

پیش نیاز دوره مرکز عملیات امنیت:

تسلط بالا بر مفاهیم TCP/IP و لایه های شبکه

آشنا به مفاهیم Network+

مخاطبین دوره مرکز عملیات امنیت:

کارشناسان و تحلیلگران مرکز عملیات امنیت (سطح یک)

کارشناسان امنیت شبکه (سطح یک)

ممیزهای امنیت اطلاعات

سرفصل دوره:

Section1: History & Overview

- Security Operation Center
- SIEM
- Incident Management

Section 2: What is SOC?

- Modules
- Process
- Technology
- People

SEMATEC
IT Training Center

- Network Monitoring
- Log Management
- Incident Response
- Automated Actions

Section 3: Processes and Procedures in SOC

- Analytical Process
- Intrusion Analysis Process
- Training Process
- Subtle Event Process
- Operational Process
- Event Management Process
- Daily Operation Process
- Reporting Process
- Technologic Process
- Design Process
- Configuration Management Process
- System Administration Process
- Business Process
- Metric Process
- Process Improvement Process
- Business Continuously Process

Section 4: Technologies

- SIEM
- Data Gathering and Mechanisms
- Log Management and Log Types
- Correlation Engine
- FIM/SCM
- Antiviruses
- IPS/IDS
- Patch Management
- DLP

Section 5: Peoples

SEMATEC
IT Training Center

- Operators Levels
- Job Titles

Section 6: Lab (Splunk ES)

- Event Gathering
- Log Analysis
- Dashboards and Reports