BİLİŞİM ACADEMY

SOC LEVEL 1 ANALYST EĞİTİMİ

KURS İÇERİĞİ

KURS AÇIKLAMASI

Güvenlik Operasyonları Merkezi (SOC), bir kuruluşun ağını ve sistemlerini 7/24 izlemekle görevli BT güvenlik uzmanlarından oluşan bir ekiptir. İzleme aşağıdaki amaçlar için yapılır:

- *Ağdaki güvenlik açıklarını izleme:* Güvenlik açığı, bir saldırganın izin düzeylerinin ötesinde bir şeyler gerçekleştirmek için yararlanabileceği bir zafiyettir.

- *Politika ihlallerini keşfetme:* Bir güvenlik politikası, bir şirketin güvenlik tehditlerine karşı korunmasına ve uyumluluğun sağlanmasına yardımcı olmak için oluşturulmuş bir dizi kural ve prosedürdür.

- *İzinsiz girişleri tespit etme:* İzinsiz girişler, sistem ve ağ izinsiz girişlerini ifade eder. Bir örnek senaryo, web uygulamamızı başarıyla kullanan bir saldırgan olabilir. Başka bir örnek senaryo, kötü amaçlı bir siteyi ziyaret eden ve bilgisayarına virüs bulaştıran bir kullanıcı olabilir.

BU KURSU KİMLER ALMALI?

- Bilişim sektöründe yer almak isteyen öğrenci ve mezunlar,
- Kariyerini bilişim sektöründe ilerletmeyi düşünenler katılım sağlayabilir.
- Ağ Uzmanlığı alanında kariyer yapmak isteyenler
- Şirket ve Kurumlarda Ağ Yöneticisi/Ağ Teknisyeni pozisyonlarında görev alanlar/almak isteyenler
- CCNP sertifika kariyerinde ilerleyecekler
- 'Beyaz Şapkalı Hacker' olma yolunda CEH ve OSCP gibi sertifikasyon süreçlerine hazırlananlar

1.WINDOWS AND LINUX BASICS

1.1. Windows Fundamental

1.1.1. Understanding Operating System Configurations

1.1.2. Managing Files And folders

1.1.3. Understanding Operating System Maintenance

1.1.4. Active Directory Basics

2.SOC FUNDAMENTALS

2.1. Introduction to Cyber Defense Security

2.2. Areas of Defensive Security

2.2.1. Security Operation Center (SOC)

2.2.2. What is Threat Intelligence?

2.2.3. Digital Forensics and Incident Response (DFIR)

2.2.4. What is Malware Analysis?

2.3. Elements of Security Operations

2.3.1. Data Sources

2.3.2. SOC Services

2.3.3. SOC Roles

3.CYBER DEFENSE FRAMEWORKS

3.1. Pyramid of Pain

3.1.1. Hash Values

3.1.2. IP Addsress

3.1.3. Domain Names

3.2. Cyber Kill Chain

3.2.1. Reconnaissance, Weaponization, Delivery

3.2.2. Exploitation, Installation, C2

3.2.3. Actions on Objectives (Exfiltration)

3.3. MITRE Framework

3.3.1. Introduction to MITRE

3.3.2. CVEs, CVSS, TTPs

3.3.3. ATT&CK® Framework

4.CYBER THREAT INTELLIGENCE

4.1. Intro to Cyber Threat Intel

4.2. Threat Intelligence Tools

4.2.1. Threat Intelligence Classifications

4.2.2. UrlScan.io

4.2.3. Abuse.ch

4.2.4. Cisco Talos Intelligence

4.3. OSINT

4.3.1. OSINT Framework

4.3.2. Google Dorking

4.3.3. Socks Puppets

4.3.4. IP Analysis (VirusTotal, IP-Tracker, Scamalytics)

4.4. Yara

4.4.1. What is Yara?

4.4.2. Introduction to Yara Rules

4.4.3. Yara Modules

5.PHISING ANALYSIS

5.1. Phising Analysis Fundamentals

5.1.1. The Email Address

5.1.2. Email Delivery

5.1.3. Email Headers

5.1.4. Email Body

5.1.5. Types of Phising

5.2. Phising Email in Action

5.3. Phising Analysis Tools

6.NETWORK SECURITY AND TRAFFIC ANALYSIS

6.1. Traffic Analysis Essentials

6.2. Wireshark Basics

6.2.1. Tool Overview

6.2.2. Packet Dissection

6.2.3. Packet Navigation

6.2.4. Packet Filtering

6.2.5. Investigate Pcap Files

6.3. IDS/IPS Concepts

6.3.1. Introduction to IDS/IPS

6.3.2. Snort

7. ENDPOINT SECURITY MONITORING

7.1. Intro to Endpoint Security

7.2. Core Windows Processes

7.2.1. smss.exe

7.2.2. wininit.exe

7.2.3. svchost.exe

7.2.4. lsass.exe

7.2.5. winlogon.exe

7.2.6. explorer.exe

7.3. IDS/IPS Concepts

7.3.1. File and Disk Utilities

7.3.2. Networking Utilities

7.3.3. Security Utilities

7.3.4. System Information

7.4. Windows Event Log

7.4.1. Event Viewer

7.4.2.Event IDs

7.5. CrowdStrike EDR

7.5.1. Incident and Detection Concepts

7.5.2. CrowdScore

7.5.3. Dashboard

7.5.4. Process Tree

7.5.5. Investigate Detection

8. SECURITY INFORMATION EVENT MANAGEMENT

8.1. Introduction to SIEM

8.1.1. What is SIEM?

8.1.2. Why SIEM?

8.1.3. Log Sources and Log Ingestion

8.1.4. Analysing Logs and Alerts

8.2. Splunk Basics

8.2.1. Splunk Components

8.2.2. Navigating Splunk

8.2.3. Adding Data

8.3. Splunk Scenario (Investigation Fundamentals Logs)

8.3.1. Search Processing Language (SPL) Basic

8.3.2. Correlations

8.3.3. Create Report, Dashboard, Alert, Workflow