Blue Team Defender

Security Operations & Analysis

This course introduces the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know. you will learn the stages of security operations: how data is collected, where it is collected, and how threats are identified within that data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

You Must Know!

Duration:
40 Hours

Who Should Attend?
Security Analysts, Incident Investigators, Security Engineers and Architects, Technical Security Managers, SOC Managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC, and Anyone looking to start their career on the blue team

Course Pre-Requisites
A basic understanding of TCP/IP and general operating system fundamentals is needed for this course. Being accustomed to the Linux command-line, network security monitoring, and SIEM solutions is a bonus. Some basic entry-level security concepts are assumed.

Main Topics:

- Defensible Network Concepts
- Corporate Network Architecture
- Endpoints, Logs & Files
- Triage & Analysis
- Continuous Improvements & Automation

Course Modules

Module 1 – Introduction to the Blue Team Mission, Tools & Operations

- SOC Overview
- Defensible Network Concepts
- Events, Alerts, Anomalies, and Incidents
- Incident Management Systems
- Threat Intelligence Platforms
- SIEM
- Automation and Orchestration
- Who Are Your Enemies?

Module 2 – Understanding your Network

- Corporate Network Architecture
- Traffic Capture and Analysis
- Understanding DNS
- DNS analysis and attacks
- Understanding HTTP and HTTPS
- Analyzing HTTP for Suspicious Activity
- How SMTP and Email Attacks Work
- Additional Important Protocols

Module 3 – Endpoints, Logs & Files

- Endpoint Attack Tactics
- Endpoint Defense In-Depth
- How Windows Logging Works
- How Linux Logging Works
- Interpreting Important Events
- Log Collection, Parsing, and Normalization
- Files Contents and Identification
- Identifying and Handling Suspicious Files

Module 4 – Triage & Analysis

- Alert Triage and Prioritization
- Perception, Memory, and Investigation
- Mental Models for Information Security
- Structured Analysis Techniques
- Analysis Questions and Tactics
- Analysis OPSEC
- Intrusion Discovery
- Incident Closing and Quality Review

Module 5 – Continuous Improvements, Analytics & Automation

- Improving Life in the SOC
- Analytic Features and Enrichment
- New Analytic Design, Testing, and Sharing
- Tuning and False Positive Reduction
- Automation and Orchestration
- Improving Operational Efficiency and Workflow
- Containing Identified Intrusions
- Skill and Career Development

תל אביב

המרץ 2