OffSec

MITRE D3FEND
Detect Learning Path

Navigate through the intricacies of digital evidence handling, malware analysis, advanced platform attacks, and more.

MITRE | D3FEND™

One of 3 MITRE D3FEND Learning paths from OffSec

Model | Harden | Detect

Learning Path Overview

The "MITRE D3FEND - Detect" Learning Path offers a specialized foray into the critical realm of cyber threat detection and analysis. Designed for Incident Responders, SOC Analysts, Security Researchers, and Threat Hunters, this path presents a series of modules dedicated to equipping learners with the expertise to identify, analyze, and respond to cyber threats effectively. From digital forensics and static malware analysis to sophisticated techniques for hunting malicious users and detecting server-side attacks, participants will navigate through the intricacies of digital evidence handling, malware analysis, advanced platform attacks, and more.

Techniques covered

- File Analysis
- Identifier Analysis
- Network Traffic Analysis
- Platform Monitoring
- Process Analysis
- User Behavior Analysis

Learning objectives

- Equip learners with the expertise to identify, analyze, and respond to cyber threats effectively
- Understand digital forensics and static malware analysis to sophisticated techniques for hunting malicious users and detecting server-side attacks
- Integrate practical hunting methodologies for both Linux and Windows environments, alongside strategies for unearthing persistent threats and navigating network detections

Why complete the MITRE D3FEND Detect Learning Path from Offsec?

The "MITRE D3FEND - Detect" Learning Path empowers organizations by developing skilled professionals adept in the latest cyber threat detection and response techniques. Organizations will benefit from enhanced cybersecurity resilience, reduced incident response times, and a robust defense posture against evolving cyber challenges, ensuring operational continuity and safeguarding sensitive data and assets. This strategic investment in workforce development equips teams with the knowledge and tools to maintain a competitive edge in cybersecurity defense.

Earning an OffSec MITRE D3FEND learning badge

Badge earners have advanced skills in threat hunting, server-side attack defense, and persistent threat mitigation, fortifying digital infrastructures against evolving cyber threats and enhancing overall resilience.

FAQ

+ What's the syllabus?

- Incident Detection and Identification
  - *Passive Incident Alerting*
  - *Active Incident Discovery*
  - *Identifying False Positives*
  - *Identifying Attack Chains*
- Digital Forensics for Incident Responders
  - *Fundamentals of Digital Evidence Handling*
  - *Forensic Tools and Techniques*
  - *Malware Analysis*
- Basic Static Malware Analysis
  - *Initial Analysis: Investigating a Malicious File*
  - *Analyzing Phishing Attacks*
  - *Analyzing Compiled Malware*
- Hunting for Reflective DLL Injection
  - *DLL Injection Theory*
  - *Indicators of Compromise and Detection Strategies*
- Hunting for Malicious Users
  - *Introduction to Malicious User Hunting*
  - *Hunting Methodology on Linux and Windows*
  - *Hunting Methodology in Active Directory*
  - *Hunting in an Enterprise*
- Windows Server Side Attacks
  - *Credential Abuse*
  - *Web Application Attacks*
  - *Binary Exploitation*
- Windows Persistence
  - *Persistence on Disk*
  - *Persistence in Registry*
- Linux Server Side Attacks
  - *Credential Abuse*
  - *Web Application Attacks*
- Network Detections
  - *Intrusion Detection Systems*
  - *Detecting Attacks*
  - *Detecting C2 Infrastructure*

+ What are the skills associated with this Learning Path?

- Incident Detection and Identification
- Incident Evidence Preservation
- Monitoring, Intrusion Detection and Analysis
- User Behavior Analysis

+ What are the job roles associated with this Learning Path?

- Incident Responder
- SOC Analyst
- Security Researcher
- Threat Hunter

+ Are there any prerequisites?

- Linux Basics I
- Windows Basics I
- Linux Basics II
- Windows Basics II
- Threat Hunting Overview

+ Who is this Learning Path designed for?

MITRE D3FEND - Detect focuses on cyber threat detection, covering digital forensics, malware analysis, hunting tactics, and network detections, for roles like Incident Responders and SOC Analysts.

+ How long does the Learning Path take, and what is the format?

This self-paced path is designed for flexibility, typically taking 160 hours to complete. It includes text based content and 171 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise

OffSec

Learn more: offsec.com