MITRE D3FEND Model Learning Path

Develop an understanding of Operational Activity Mapping and Asset Inventory, crucial for safeguarding digital assets in an increasingly complex cyber landscape.

One of 3 MITRE D3FEND Learning paths from OffSec

Model | Harden | Detect

Learning Path Overview

The "MITRE D3FEND - Model" Learning Path equips learners with a robust framework for navigating the evolving landscape of cybersecurity. Tailored for cybersecurity professionals, particularly Incident Responders and SOC analysts, Security Engineers, System Administrators, and Information Security Managers, this integrated program systematically immerses learners in critical security principles, from assurance testing and security assessments to incident response and attacker methodologies. With a foundation built on the prestigious MITRE D3FEND techniques, participants gain a deep understanding of Operational Activity Mapping and Asset Inventory, crucial for safeguarding digital assets in an increasingly complex cyber landscape.

Techniques covered

- Asset Inventory
- Operational Activity Mapping

Learning objectives

- Gain a comprehensive understanding of integrating security measures throughout the software development process
- Equip learners with knowledge about various techniques employed by attackers on web applications
- Develop critical aspects of incident response, imparting knowledge about communication plans and fundamental response strategies for effectively managing and mitigating security incidents

Why complete the MITRE D3FEND Model Learning Path from Offsec?

This Learning Path is a crucial investment for organizations seeking to elevate their cybersecurity defenses. This concise, impactful program empowers learners with cutting-edge strategies in assurance testing, security assessments, incident response, and attacker methodologies. By integrating MITRE D3FEND techniques, this path ensures that participants can not only anticipate but effectively neutralize cyber threats, safeguarding critical organizational assets. By engaging in this Learning Path, your team will transform your organization's security posture, mitigate risks, and maintain operational excellence in the face of the unprecedented challenges of the modern digital security landscape.

Earning an OffSec MITRE D3FEND learning badge

Badge earners have demonstrated proficiency in assurance testing, security assessment, incident response, and web attack strategies aligned with the Asset Inventory and Operational Activity Mapping D3FEND techniques.

FAQ

What's the syllabus?

- Introduction to Assurance Testing
  - *The Context for Security Testing*
  - *Aligning Security Testing to the Business*
  - *Creating and Using Security Test Documentation*
- Introduction to Security Assessments
  - *Kali Linux in an Assessment*
  - *Types of Assessments*
  - *Formalization of the Assessment*
  - *Types of Attacks*
- Fundamentals of Incident Response
  - *Incident Response Frameworks*
  - *Roles and Responsibilities of Incident Response Teams*
- Incident Response Communications Plans
  - *The Importance of a Communications Plan*
  - *Communication Before a Crisis*
  - *Communication During a Crisis*
  - *Communication After a Crisis*
- Web Attacker Methodology
  - *Introduction to Web Application Assessments*
  - *Enumeration*
  - *Vulnerability Discovery*
  - *Exploitation*
  - *Post-Exploitation*
  - *Reporting*
- Secure Development Lifecycle
  - *Applying Security to the Software Development Lifecycle*
  - *Threat Modeling*
  - *Design Patterns and Reference Architecture*
  - *Static Analysis and Code Review*
  - *Vulnerability Scanning*
  - *Dynamic Analysis*
  - *Other Forms of Analysis*
  - *Incident Response*

What are the skills associated with this Learning Path?

- Common Attack Techniques: SOC Analyst
- Security and Compliance
- System Hardening
- Incident Response Processes

What are the job roles associated with this Learning Path?

- SOC Analyst
- System Administrator
- Incident Responder

Are there any prerequisites?

- No

Who is this Learning Path designed for?

Ideal for those committed to advancing their careers and securing their organizations, this learning journey positions participants at the forefront of cybersecurity, ready to tackle current and future challenges with confidence and expertise.

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

This self-paced path is designed for flexibility, typically taking 95 hours to complete. It includes text based content and 103 labs to reinforce training with hands-on experience.

Available on:

Learn Unlimited

Learn Enterprise