MITRE D3FEND
Harden Learning Path

Learn hardening techniques for system security, covering input validation, secure coding, patch management, AppArmor/SELinux, and secure configurations for NGINX/MSSQL, with a focus on preventing credential attacks.

MITRE | D3FEND™

One of 3 MITRE D3FEND Learning paths from OffSec

Model	Harden	Detect

Learning Path Overview

Ideal for Software Developers, System Administrators, Cybersecurity Analysts, IT Security Engineers, and Network and Database Engineers, this Learning Path also serves as a vital resource for any professional tasked with the maintenance, development, and security of digital infrastructures. Through the exploration of MITRE Application Hardening, Credential Hardening, and Platform Hardening D3FEND techniques, learners will be equipped to anticipate and neutralize potential security vulnerabilities, making them indispensable in their roles. This Learning Path instills a proactive approach to cybersecurity, ensuring learners are prepared to protect and enhance their organization's digital assets in a rapidly evolving cyber landscape.

Techniques covered

- Application Hardening
- Credential Hardening
- Platform Hardening

Learning objectives

- Gain a solid foundation in input validation, secure web coding, and the intricacies of patch management for both Windows and Linux systems
- Dive into the implementation of security frameworks like AppArmor and SELinux
- Tackle the challenges of security misconfigurations, and master the secure configuration of vital technologies such as NGINX and MSSQL.

Why complete the MITRE D3FEND Harden Learning Path from Offsec?

The "MITRE D3FEND - Harden" Learning Path is, meticulously designed to elevate an organization's defense mechanisms. Organizations investing in this learning path will not only future-proof their systems against emerging cyber threats but also foster a culture of security-first thinking. This transformative program is an essential strategic asset, empowering teams to fortify their digital assets, ensure operational resilience, and maintain a competitive edge in the cybersecurity landscape.

Earning an OffSec MITRE D3FEND learning badge

Badge earners have demonstrated proficiency in web secure coding principles, emphasizing input validation fundamentals to prevent common vulnerabilities.

OffSec™
Learning Badge
MITRE ATT&CK Harden

FAQ

+ What's the syllabus?
- Input Validation Fundamentals
  - *User-Controlled Input*
  - *Validating Input*

- Introduction to Web Secure Coding
  - *Trust Boundaries*
  - *Untrusted Input Handling*
  - *Output Encoding and Character Escaping*
  - *File Handling*
  - *Parameterized Queries*

- Patching Windows Assets I
  - *Windows Update Components*
  - *Windows Update Releases*
  - *Windows Update Administration*
  - *Microsoft Update Catalog*
  - *Patch Management Program*

- Patching Linux Assets
  - *Understand Patching in Linux*
  - *Exploring the Git Patching Approach*
  - *Kernel Patching Basics*
  - *Operating a Patch Management Program*
  - *Automate the Patching Process*

- Introduction to AppArmor

- Introduction to SELinux

- Security Misconfigurations
  - *Hardening Servers and Applications*
  - *Application Runtime Parameters*

- Secure Configuration of NGINX
  - *Basic Platform Hardening*
  - *Applying Encryption*
  - *Hardening Message Flow*

- Secure Configuration of MSSQL
  - *Network Architecture and Security*
  - *Authentication and SQL Service Accounts*
  - *Escalation and Impersonation*
  - *Data Protection*

- Credential Attacks for Developers
  - *Password Attacks*
  - *Remediating Password Attacks*

+ How long does the Learning Path take, and what is the format?
This self-paced path is designed for flexibility, typically taking 130 hours to complete. It includes text based content and 210 labs to reinforce training with hands-on experience.

+ What are the skills associated with this Learning Path?
- Handling User Input
- Patch Management
- System Hardening

+ What are the job roles associated with this Learning Path?
- Software Developer
- System Administrator

+ Are there any prerequisites?
- Linux Basics 1
- Windows Basics 1

+ Who is this Learning Path designed for?
This Learning Path is tailored for cybersecurity professionals, particularly software developers and system administrators.

Available on:

Learn Unlimited   **Learn Enterprise**

OffSec™

Learn more: offsec.com