CrowdStrike University

CROWDSTRIKE UNIVERSITY

IDP 270
SECURING WORKFORCE IDENTITIES WITH FALCON IDENTITY PROTECTION

COURSE OVERVIEW

This course will cover Falcon Identity Protection and demonstrate how to configure, implement and utilize the data feeds from Falcon Identity Protection to secure your organization against credential-based attacks. Whether you want to monitor for weak or compromised passwords, analyze stale or stealthy administrators in your domain, or enforce MFA for high-risk users, this course will provide you the tools you need to leverage the Falcon Identity Protection toolset and lock down your domain.

WHAT YOU WILL LEARN

- Understand basic tenets of identity-based attacks, Zero Trust and identity protection
- Determine how Falcon IDP can help you gain visibility into your overall security posture
- Implement policy rules to enforce targeted controls against users and groups in your domain
- Perform threat hunting, analysis and light investigation from identity-based detections
- Recall how to integrate and configure Falcon IDP within your environment

PREREQUISITES

- Knowledge of computer networking concepts and protocols, and network security methodologies, privacy principles, cyber threats and vulnerabilities
- Completion of the IDP 170 eLearning course in CSU is recommended
- Familiarity with the Microsoft Windows environment
- Ability to comprehend course curriculum presented in English
- Understanding of Active Directory, Azure AD, and different types of authentication such as Kerberos and NTLM

REQUIREMENTS

- Broadband internet connection, web browser, microphone and speakers
- Dual monitors and headset are recommended

CLASS MATERIAL

Associated materials may be accessed from CrowdStrike University on the day of class.

1-day program | 2 credits

This instructor-led course includes a CrowdStrike Falcon platform walkthrough and hands-on exercises on Falcon Identity Protection.

Take this class if:
You are an identity protection administrator, identity protection policy manager, identity protection domain administrator or Falcon investigator

Registration
For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits. If you do not have access to CrowdStrike University, you need to purchase training credits or you need more information, please contact sales@crowdstrike.com.

CrowdStrike University

IDP 270: Securing Workforce Identities with Falcon Identity Protection

IDENTITY PROTECTION TENETS

- Understand the core principles of identity protection and Zero Trust
- Understand CrowdStrike's approach to Falcon Identity Protection
- Discover how Falcon Identity Protection solutions complement and reinforce traditional endpoint detection and response (EDR) solutions

DOMAIN SECURITY WITH IDENTITY PROTECTION

- Understand where Falcon Identity Protection fits in the cybersecurity framework
- Navigate and understand the Falcon Identity Protection module and sub-menus
- Assess domain security posture
- Analyze the risk associated with users in the domain
- Leverage custom insights and reports
- Identify risky users and entities in the domain
- Pivot from identity-based detections and incidents into analysis
- Identify the key attributes and related entities in identity-based detections

ANALYSIS AND THREAT HUNTING

- Articulate the differences between identity-based detections and incidents
- Understand and assess identity-based incidents
- Assess the risks and mitigation strategies of identity-based detections
- Navigate and understand an identity-based incident and timeline
- Pivot from identity-based incident/detection into analysis
- Navigate the Threat Hunter module and perform threat hunting in the domain
- Understand the basics of endpoint protection policies and how they relate to Falcon Identity Protection

POLICY RULES

- Understand the purpose of policy rules and policy groups
- Configure policy groups to manage rules
- Create and manage host groups in order to apply policy rules to specific groups
- Assess policy triggers and analytics
- Leverage policy rules to mitigate risks in the domain
- Build policy rules utilizing Zero Trust and risk scores
- Understand the importance of authentication traffic inspection and how to enable it in your domain

IDENTITY PROTECTION INTEGRATIONS

- Understand the integrations between Falcon Identity Protection and AD FS/PingFederate
- Navigate the configuration options for authentication integrations with Falcon Identity Protection
- Understand the requirements for authentication integrations
- Locate and understand how to leverage the help documentation for API configuration for authentication connectors
- Understand how Falcon Identity Protection integrates with the Falcon platform
- Create and manage configuration policies
- Create and manage subnets for virtual network segmentation
- Configure detection exclusions
- Generate and manage custom insights and custom reports
- Configure connectors for various systems such as Duo authenticator

FALCON FUSION WORKFLOWS FOR IDENTITY PROTECTION

- Navigate the Falcon Fusion module
- Understand the purpose of Falcon Fusion and how you can integrate workflows in Falcon Identity Protection
- Describe the workflow creation process
- Create a Falcon Fusion workflow from scratch
- Generate specific notifications based on a Falcon Fusion workflow
- Understand the triggers, conditions and actions used to build a Falcon Fusion workflow
- Integrate Falcon Fusion workflows within Falcon Identity Protection
- Understand how Falcon Fusion workflows can elevate visibility and reduce response time for identity-based detections and incidents