

IDP 270:

Securing Workforce Identities with Falcon Next-Gen Identity Security

Course Overview:

Strengthen your organization's defense against credential-based attacks with CrowdStrike Falcon® Next-Gen Identity Security. This comprehensive course teaches security professionals how to effectively implement and leverage Falcon Next-Gen Identity Security's powerful capabilities to protect workforce identities through a Zero Trust approach. Participants will learn to configure advanced identity protection controls, monitor authentication activities, and enhance visibility into your domains and security posture.

Through practical exercises and real-world scenarios, participants will master the essential components of modern identity protection. The course covers everything from initial configuration and policy implementation to advanced threat hunting techniques using identity-based detections. Special emphasis is placed on gaining actionable visibility into your security posture and implementing targeted controls to protect high-risk users and sensitive resources.

What You Will Learn:

In this course, you will learn how to:

- » Use Falcon Next-Gen Identity Security to apply Zero Trust principles
- » List the requirements for deployment and operation of Falcon Next-Gen Identity Security
- » Audit risks and assess the overall identity security posture in your domain
- » Describe how detections and incidents are generated, and how to investigate in an endpoint detection and response (EDR) context
- » Conduct identity-based threat hunting and analysis
- » Implement targeted policy controls for users and groups

1-day program | 2 credits

This instructor-led course includes a CrowdStrike Falcon® platform walkthrough and hands-on exercises on Falcon Next-Gen Identity Security

Take this class if you: are new to CrowdStrike Falcon Next-Gen Identity Security or want to understand where it fits in your security framework, want to enhance your skills as an identity protection administrator, or Falcon investigator; or are preparing for the CrowdStrike Certified Identity Specialist (CCIS) exam

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, need to purchase training credits, or need more information, please contact sales@crowdstrike.com.

Recommended Prerequisites

- » Knowledge of computer networking concepts and protocols, network security methodologies, privacy principles, cyber threats, and vulnerabilities
- » Completion of IDP 170: Falcon Next-Gen Identity Security Fundamentals is recommended
- » Familiarity with the Microsoft Windows environment
- » Understanding of Active Directory, Microsoft Entra ID, 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.

Topics

What is Falcon Next-Gen Identity Security?

- » Describe how Falcon Next-Gen Identity Security enables Zero Trust principles
- » Explain how Falcon Next-Gen Identity Security works with the Falcon platform

Falcon Next-Gen Identity Security Deployment

- » Summarize how Falcon Next-Gen Identity Security fits in the Falcon ecosystem
- » Enable Falcon Next-Gen Identity Security

Falcon Next-Gen Identity Security Baselines

- » Define Authentication Traffic Inspection (ATI)
- » Describe how baselining occurs

Auditing

- » Navigate the Domain Security Overview (DSO) page
- » Analyze Entity Business Card pages
- » Traverse the Users Dashboard
- » Create Custom Insights

Enforcement

- » Describe how policy rules work
- » Create policy rules
- » Validate policy rules

Falcon Fusion SOAR Workflows and Falcon Next-Gen Identity Security

- » Describe Falcon Fusion SOAR capabilities
- » Explain how Falcon Next-Gen Identity Security works with Falcon Fusion SOAR



