COURSE TABLE OF CONTENTS

ITSEC 220: Managing Exposure Risks with CrowdStrike Falcon® Exposure Management

OEM: CrowdStrike • Code: ITSEC 220

COURSE DESCRIPTION

Transform your organization's security posture with a structured approach to exposure management. In this instructor-led course, you will learn how to identify, assess, and reduce risk across your attack surface using CrowdStrike Falcon® Exposure Management. Through hands-on exercises, you'll gain visibility into assets and vulnerabilities spanning both internal and external environments. You'll configure key capabilities such as asset discovery, vulnerability assessment, and policy frameworks before progressing to operational workflows, reporting, and data integration. Harness advanced capabilities including AI-driven prioritization with ExPRT.AI and attack path analysis to stay ahead of threats and drive proactive risk reduction. By the end of this course, you will be able to implement, operationalize, and continuously improve an exposure management program within your organization.

AUDIENCE PROFILE

- A security analyst, vulnerability management specialist, IT security hygiene analyst, SOC manager, or security professional implementing exposure management programs

PREREQUISITES

- Foundational knowledge of vulnerability management concepts, including Common Vulnerabilities and Exposures (CVEs) and Common Vulnerability Scoring System (CVSS v3)
- Familiarity with security operations concepts such as asset management, risk prioritization, and incident response
- Basic understanding of enterprise IT environments (endpoints, cloud, and network infrastructure)
- Prior experience with the CrowdStrike Falcon platform (recommended)
- Comfort navigating web-based tools and interpreting dashboard data
- Broadband internet connection, web browser, microphone, and speakers
- Dual monitors and headset are recommended

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- Establish visibility into assets, vulnerabilities, and external exposure
- Configure asset discovery, scanning, and assessment policies
- Analyze vulnerabilities using AI-driven prioritization with ExPRT.AI
- Organize and operationalize exposure data using dashboards, filters, and grouping

- Integrate exposure management into workflows, reporting, and remediation processes
- Apply attack path insights to support risk-based prioritization and response

COURSE OUTLINE

Module 1: Foundation and Initial Discovery

- Explain vulnerability fundamentals and the evolving threat landscape using real-world adversary examples
- Describe single-sensor architecture benefits and unified platform visibility
- Navigate the Falcon Exposure Management console and key dashboards (Overview, Exposures, EASM, Assets)
- Identify visibility provided by Falcon sensor data, external attack surface management (EASM), and asset discovery

Module 2: Asset Discovery and Configuration

- Describe asset discovery approaches, including passive, active, and integration-based methods
- Configure Network Vulnerability Assessment (NVA) scans and third-party integrations
- Enable and customize configuration assessment policies for compliance monitoring
- Create asset criticality rules for business-aligned classification

Module 3: Risk Assessment and Prioritization

- Explain ExPRT.AI risk scoring and exploitation likelihood
- Compare traditional CVSS v3 scoring with AI-driven prioritization
- Interpret attack path visualizations for contextual risk analysis
- Analyze vulnerabilities across multiple data sources (NVA, Falcon Spotlight, third-party integrations)
- Create saved filters for consistent and repeatable analysis

Module 4: Operational Integration and Workflow Automation

- Generate and schedule vulnerability management reports for stakeholder communication
- Build application groups using dynamic criteria for asset organization
- Implement suppression rules with appropriate governance and justification
- Create team dashboards and saved filters to support operational workflows
- Manage external asset review processes and status tracking

Module 5: Advanced Capabilities and Continuous Improvement

- Configure vulnerability ticketing workflows and integrations
- Use attack path analysis to support proactive threat identification
- Apply exposure management capabilities to real-world scenarios
- Establish processes for ongoing optimization and program maturity