COURSE TABLE OF CONTENTS

AIDR 200: Securing Workforce AI Usage with Falcon AIDR

OEM: CrowdStrike • Code: AIDR 200

COURSE DESCRIPTION

Your employees are already using AI. The question is whether you know where, how, and at what risk. As AI tools proliferate across the workforce, the threats multiply: sensitive data slipping into chat interfaces, shadow AI applications bypassing IT oversight, and well- meaning employees unknowingly creating compliance violations. This course equips IT security policy creators with the skills to architect intelligent CrowdStrike Falcon® Guardian monitoring frameworks that catch risky behaviors before they become breaches. You'll configure specialized detectors for malicious prompts and sensitive data exposure, build access and prompt rules tailored to your organization's risk profile, and validate your policies using the Guardian Sandbox before pushing them to enforcement. Through hands-on labs and real-world scenarios, you'll analyze AI usage patterns and fine-tune configurations to eliminate gaps while maintaining robust protection. You'll leave with the expertise to enable your workforce to harness AI's productivity gains, without sacrificing security, compliance, or data control.

AUDIENCE PROFILE

- an IT Security: • Administrator responsible for managing AI tool usage across your organization • Analyst investigating AI- related policy violations or data exposure risks • Compliance manager ensuring your organization meets regulatory requirements for AI usage

PREREQUISITES

- Familiarity with basic security concepts such as data loss prevention, access control, and compliance frameworks
- Basic knowledge of the CrowdStrike Falcon® platform
- Basic knowledge of AI security-related terminology (if new to AI security, see AIDR 090: AI Security Basics and Best Practices)
- Completion of AIDR 100: Falcon Guardian Fundamentals
- Completion of AIDR 101: Configuring the Falcon Browser Collector
- 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:

- Analyze employee AI activity and prompt data to identify policy gaps and implement iterative improvements
- Configure Falcon Guardian policies that detect and prevent unauthorized shadow AI usage and sensitive data from being shared with AI models

COURSE OUTLINE

Module 1: Mitigating AI Risks with Falcon Guardian

- Recognize common AI risks in the enterprise and explain why they create security gaps: data leakage and personally identifiable information (PII) exposure, shadow AI usage, compliance violations, and intellectual property loss
- Identify key AI regulations and their implications: NIST AI RMF, EU AI Act, ISO/IEC 42001, HIPAA, CCPA, and APPI
- Explain what Falcon Guardian does and how it addresses AI-related compliance risks
- Identify unapproved AI tool usage and data leakage risks across your environment

Module 2: Configuring Falcon Guardian Policies

- Configure policy settings and build a site access rule
- Create an inspection rule that routes browser vs. network-sourced AI traffic to distinct access and prompt rules
- Create access rules that block or limit AI use
- Configure prompt rules and detectors for sensitive data, such as Confidential and PII Entity, Secret and Key Entity, Code Detection, Language Controls, Competitor Mentions, and Topic/Content Filters
- Apply enforcement actions such as Report, Mask/Partial Mask, and Block
- Test policies in the Guardian Sandbox, interpret enforcement results, and refine configurations to address policy gaps

Module 3: Capstone Exercise: Balancing Security with User Productivity

- Combine access rules and prompt rules into a unified, comprehensive policy
- Apply a decision framework to determine which rule types and detectors address a given risk
- Evaluate trade-offs between security enforcement and user productivity
- Design and implement a policy solution for a multi-risk business scenario