

SOAR 200:

Implementing Security Automation with Falcon Fusion SOAR

Course Overview

Learn to design and implement security orchestration workflows using CrowdStrike Falcon® Fusion SOAR to enhance incident response and security operations efficiency.

This course provides practical skills to create workflow architectures incorporating triggers, conditions, and actions. Participants will explore intelligent triage workflows for alert classification and prioritization, develop multi-stage response orchestrations that coordinate actions across security systems, and learn automated remediation techniques for containment and eradication processes. Through hands-on labs and real-world scenarios, students will gain experience with testing methodologies, debugging techniques, and observability practices essential for maintaining workflow reliability in enterprise security environments.

What You Will Learn

- » Design and implement workflow architectures incorporating triggers, conditions, and actions.
- » Establish testing, debugging, and observability practices to ensure workflow reliability.
- » Design triage workflows that intelligently classify, prioritize, and initiate investigations.
- » Develop multi-stage response workflows that coordinate actions across security systems.
- » Build automated remediation workflows with containment and eradication actions.

1-day program | 2 credits

This instructor-led course includes various walkthroughs and hands-on learner exercises

Take this class if you are: a SOAR engineer, SOC engineer, security lead, or SIEM engineer

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

- » Fundamental knowledge of SOAR concepts
- » Recommended courses:
 - » **CQL 101:** CrowdStrike Query Language Fundamentals 1
 - » **CQL 201:** Designing and Optimizing CQL Queries
 - » **SOAR 100:** Falcon Fusion SOAR Fundamentals

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

Workflow Foundations and Architecture

- » Navigate user interfaces and locate key configuration areas
- » Identify core workflow components and features
- » Identify gaps between current capabilities and advanced automation needs
- » Configure trigger strategies utilizing conditional logic and multi-source correlation

Workflow Testing, Debugging, and Observability

- » Apply testing methodologies including individual unit testing
- » Implement systematic debugging techniques
- » Configure observability systems with alerting
- » Troubleshoot workflow failures using logging and diagnostic techniques

Triage Workflows

- » Configure scoring incorporating risk factors and threat intelligence
- » Implement contextual decision-making logic considering environmental awareness and asset criticality
- » Create investigation workflows that collect evidence and orchestrate tasks
- » Ensure appropriate prioritization of security events through workflow validation

Response Workflows

- » Orchestrate sequential and parallel response actions
- » Implement adaptive response pathways that contain escalation and de-escalation logic
- » Coordinate automated stakeholder communications

Remediation Workflows

- » Implement automated containment strategies
- » Design containment workflows across network and endpoint environments
- » Create eradication workflows that remove threats while preserving evidence



