SIEM 220: Building Detection Rules and Dashboards in Falcon Next-Gen SIEM

OEM: CrowdStrike • Code: SIEM 220

COURSE DESCRIPTION

This instructor-led course teaches security practitioners how to build, test, tune, and deploy detection rules, custom dashboards, and reports in CrowdStrike Falcon® Next-Gen SIEM. Learners will work through the full detection and data cycle, identifying detection needs and leveraging CrowdStrike Query Language (CQL) to write custom detection rules. Students will build, validate, and tune detections from the ground up, visualize their findings through tailored dashboards and reports, and learn how to manage those detections and dashboards over time to keep pace in a rapidly evolving threat landscape.

AUDIENCE PROFILE

- A detection engineer or SOC lead responsible for Falcon Next-Gen SIEM content development

PREREQUISITES

- CQL 101: CrowdStrike Query Language Fundamentals 1
- CQL 102: CrowdStrike Query Language Fundamentals 2
- CQL 201: Designing and Optimizing CQL Queries
- SIEM 100: Next-Gen SIEM Fundamentals
- SIEM 106: Case Management Fundamentals
- 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:

- Evaluate detection rules for logic, scope, and alignment to organizational needs
- Build detection rules using CQL, utilizing both rule templates and custom query logic
- Use MITRE ATT&CK® as a reference framework to inform and validate detection logic
- Test, tune, and deploy rules matched to the needs of your environment
- Design custom dashboards tailored to specific business needs and use cases
- Configure custom reports
- Manage detection rule lifecycles and tune them for optimal threat visibility

COURSE OUTLINE

Module 1: Detection and Security Content in Falcon Next-Gen SIEM

- Define the role of detection engineers and content management
- Understand how different data sources impact your environment and how to manage them
- Understand the data lifecycle in your environment and where detection and content management live in that cycle
- Define the detection types in Falcon Next-Gen SIEM
- Utilize MITRE ATT&CK as a blueprint for detection engineering

Module 2: Detection Rule Development and Management

- Understand the detection rule development and management cycle
- Inspect and modify rules based on CrowdStrike-provided templates
- Apply documentation best practices to queries and dashboards, including comments, descriptions, and naming conventions
- Construct a correlation rule from scratch to detect a defined threat scenario
- Validate correlation rule performance and accuracy
- Understand detection rule update and maintenance needs and best practices

Module 3: Tuning and Optimizing Correlation Rules

- Apply threshold tuning techniques to increase visibility of true positive detections in the domain
- Evaluate rules for query efficiency
- Align detection rule needs to business needs and desired outcomes

Module 4: Building Tailored Dashboards

- Explore pre-built dashboards available in the Falcon platform
- Understand the widgets available and their use cases and requirements
- Configure filters for user filtering on dashboard results
- Scope dashboards and widgets for specific audiences and business cases
- Manage and maintain dashboards

Module 5: Scoping and Configuring Reports

- Describe the report types and export options available within Falcon Next-Gen SIEM
- Generate on-demand reports for specific audiences
- Understand scheduled reports and how they compare to scheduled searches

Module 6: Capstone: Building a Complete Security Visibility Practice

- Expand on the detection rules, dashboards, and reports configured throughout the course to enhance detection visibility