CROWDSTRIKE University

CQL 201:

Designing and Optimizing CQL Queries

Course Overview:

This comprehensive instructor-led training course provides cybersecurity professionals with the essential skills needed to effectively query, analyze, and visualize security data using CrowdStrike Query Language (CQL).

Participants will learn to interpret raw event data, construct efficient queries, optimize performance, and create meaningful visualizations for security investigations and reporting across the CrowdStrike Falcon® platform.

What You Will Learn:

In this course, you will learn how to:

- Analyze and interpret raw log data and understand how it's parsed into normalized formats within the CrowdStrike Falcon platform and CrowdStrike Falcon® Next-Gen SIEM
- Construct and execute effective CQL queries to extract specific security data from various sources
- Apply advanced query techniques including aggregation, joins, and data tables for complex investigations
- Create compelling data visualizations and reports for different audiences and use cases
- Identify and resolve query performance issues to optimize investigation efficiency
- Design and implement parameterized queries for reusable and flexible security analysis
- Leverage pre-built queries and save custom queries for future investigations

1-day program | 2 credits

This instructor-led course includes hands-on labs that allow you to practice and apply what you've learned

Take this class if you are:
an incident responder, Falcon analyst, Falcon Next-Gen SIEM analyst, security lead, or threat hunter

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.

Version: 6.2025

Recommended Prerequisites

- **CQL 101:** CrowdStrike Query Language Fundamentals 1
- **CQL 102:** CrowdStrike Query Language Fundamentals 2
- **FALCON 101:** Falcon Platform Essentials

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

Interpreting Event Data and Raw Logs

- Analyze raw log samples to identify key fields before and after CrowdStrike Parsing Standard (CPS) normalization
- Map original log fields to their normalized counterparts in the Falcon platform and Falcon Next-Gen SIEM
- Distinguish between parsed and unparsed log elements using @rawstring
- Troubleshoot parsing issues by comparing raw logs against processed versions
- Categorize different event types and identify common fields across the Falcon platform
- Navigate and utilize the event data dictionary for field definitions and relationships

CQL Components and Syntax

- Analyze existing CQL queries to determine their intended functions and scope
- Identify basic CQL syntax elements, operators, and filtering expressions
- Recognize proper field reference syntax for different data types
- Apply Boolean operators and query continuation syntax correctly
- Distinguish between different CQL operators and their specific functions

Build CQL Queries for Falcon

- Construct targeted queries to extract process execution, network connection, and authentication data
- Build multi-source queries that combine data from various event types
- Apply filtering and sorting techniques using Boolean operators and field-specific conditions
- Create time-range specific queries for focused investigations
- Implement exclusion filters and value comparison operators effectively
- Follow query writing best practices including proper order of operations and regex usage

Enriching and Extending Queries

- Apply aggregation functions including count(), groupBy(), and statistical functions for data summarization
- Implement timestamp manipulation and conversion techniques for time-based analysis
- Create joins between related event types using various methodologies
- Utilize defineTable() functionality for complex data manipulation and optimization
- Build time-based aggregations and correlations for trend analysis
- Design multi-level joins and temporal correlations for advanced investigations

Data Visualization

- Transform query results into timeline views and executive summaries
- Structure data outputs for incident response handoffs with standardized formats
- Select and configure appropriate visualization types based on security data characteristics
- Create interactive dashboards for dynamic security analysis
- Format data for various stakeholder audiences and use cases

Parameterized CQL and Utilizing Pre-built Queries

- Design and implement various parameter types including text, date/time, and multi-select options
- Create dependent parameters that respond dynamically to other selections
- Build reusable parameterized queries for common security investigations
- Load, modify, and optimize pre-built queries for specific investigation needs
- Establish effective query management practices including naming conventions and organization

CROWDSTRIKE
University