CrowdStrike University

CROWDSTRIKE

FHT 231
INVESTIGATING MALWARE WITH FALCON MALQUERY

BUSINESS VALUE

Learn the components and use cases of CrowdStrike Falcon Malquery™, the world's largest repository of malicious files. This course includes an in-depth introduction to YARA to give researchers unparalleled hunting capabilities using Falcon Malquery.

AUDIENCE

Team members that conduct any type of incident response or malware research.

- **Threat Analysts**
- **SOC (security operations center) Analysts**
- **Malware Reverse Engineers**
- **Incident Responders**
- **Threat Team Managers**

DELIVERY: Instructor-led – virtual or on-site

COURSE LENGTH: Approximately eight hours of content and hands-on exercises

PREREQUISITES: General computer and operating system knowledge required

COST PER STUDENT: Two training credits

Learning Objectives

Students who complete this course should be able to:

- Use Falcon MalQuery features, including Search, Hunt and Monitor to categorize malware
- Research malware samples to determine family relationships and other indicators
- Utilize proper YARA rule-writing techniques to enable hunting

COURSE DESCRIPTION

FHT 231: INVESTIGATING MALWARE WITH FALCON MALQUERY

This one-day course introduces best practices for malware identification and familial determinations using the Falcon MalQuery search engine. The course begins with an overview of the technical specifications and benefits of using Falcon MalQuery and examines each of its major components, including Search, Hunt, and Monitor. There is also a comprehensive tutorial on YARA, which helps researchers understand how to properly utilize the hunting technologies MalQuery provides.

A successful graduate of FHT 231 understands how an unknown, potential malware file can be analyzed for indicators, and how those indicators can be used in MalQuery to identify possible malware family relationships. Malcode authors often reuse code and techniques, and MalQuery enables researchers to identify likely attribution and potential use cases of malware samples based on previous intelligence.

This course is best suited for a member of the organization's incident response team: analysts, SOC members, responders, managers and investigators. There are no prerequisite courses for FHT 231, but general computer knowledge is recommended.

This course includes numerous hands-on examples and instructor-led walk-throughs to reinforce learning.

COURSE OUTLINE

The course follows this agenda:

Introduction

- Course Overview
- Instructor/Student Introductions
- Administrative Notes

MalQuery Overview

- The Falcon Search Engine
- Introduction to MalQuery
- Key Benefits of Using MalQuery
- MalQuery Technical Specifications
- How MalQuery Fits in with Other Falcon Apps

MalQuery Search

- Search Basics
- Finding Search Parameters

Introduction to YARA

- Introduction to YARA
- Rule Structure
- Rule Writing and Implementation
- Modules, Includes and Extensions

MalQuery Hunt

- Hunt Basics
- Reading Hunt Results

Advanced Hunting

- Advanced Rule Types
- Stacking Rules
- Advanced Conditions
- Special String Constructors

MalQuery Monitor

- Monitoring Overview
- New Results

Conclusion

- Review of Lessons Learned
- Continuing Education at CSU