CrowdStrike University

CROWDSTRIKE UNIVERSITY

FHT 231
INVESTIGATING MALWARE WITH FALCON MALQUERY

COURSE OVERVIEW

Falcon MalQuery™ is the leading malware research tool in the industry. Its efficient, patent-pending indexing technology and robust search algorithms allow for intricate hunting throughout years' worth of malware samples. This course covers all angles of MalQuery's use, from beginner searches through advanced malware hunting with YARA.

PREREQUISITES

To obtain the maximum benefit from this class, you should meet the following requirements:

- Comprehend course curriculum presented in English
- Completion of FHT 100-level course material in CrowdStrike University (or experience using CrowdStrike® Falcon)
- Have intermediate knowledge of cybersecurity incident investigation and incident lifecycle
- Have working knowledge of windows and/or Mac/Linux
- Have some knowledge or experience in use of Linux command line

CLASS MATERIAL

Once registered for the course, associated materials may be downloaded from CrowdStrike University.

LEARNING OBJECTIVES

Students who complete this course should be able to:

- Use MalQuery Search, Hunt, and Monitor to categorize malware
  - Apply tools to known or suspected malware samples to extract potential functions
  - Differentiate use cases between MalQuery Search and Hunt
- Research malware samples to determine family relationships and other indicators
  - Determine if sample is malware, and if so, to which family it belongs
  - Analyze findings to determine possible actor attribution
- Utilize proper YARA rule-writing techniques to enable hunting
  - Create new YARA rules based on retrieved indicators
  - Apply intelligence analysis concepts to better use malware research techniques

This instructor-led course utilizes Falcon MalQuery™ to perform malware searches and includes ample hands-on time with the platform and tools that cover all facets of MalQuery's use.

1-day program | 2 credits

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.

CrowdStrike University

FHT 231 Investigating Malware with Falcon MalQuery

INTRODUCTION

- Who we are
- Who you are
- Administrative items
- Course overview/agenda

MALQUERY OVERVIEW

- The Falcon search engine
- Introduction to MalQuery
- Key benefits of using MalQuery
- MalQuery technical specifications
- How MalQuery fits in with other Falcon applications

MALQUERY SEARCH

- Search basics
  - Search the MalQuery database based on retrieved indicators
- Finding search parameters

INTRODUCTION TO YARA

- Introduction to YARA
- Rule structure
- Rule writing and implementation
- Modules, includes and extensions

MALQUERY HUNT

- Hunt basics
  - Hunt the MalQuery database with YARA based on retrieved indicators
- Reading hunt results

ADVANCED HUNTING

- Advanced rule types
- Stacking rules
- Advanced conditions
- Special string constructors

MALQUERY MONITOR

- Monitoring overview
  - Using MalQuery Monitor to enable prospective hunting capabilities
- New results

CONCLUSION