CST 350 – Deriving Intelligence from Falcon Sandbox

Falcon Sandbox is the most advanced and powerful malware sandbox available. This half-day course enables analysts to utilize Falcon Sandbox's many features and covers the pivot from malware analysis to actionable intelligence. Students will learn how to retrieve Indicators of Compromise (IOC) from file, network, memory, and process activity related to the automated threat analysis available with the sandbox and understand the nature and complexity of the threat by matching indicators to current intelligence. Through this training, security teams will be empowered to gain unprecedented visibility into real-world threats and enable the teams to make faster and better decisions. This course includes numerous hands-on exercises to supplement the training.

PREREQUISITES

General technical knowledge is required. Experience with the Intelligence Cycle/Process or successful completion of CST 330 is suggested.

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

- Completion of FHT 100 & FHT 101 course material in CrowdStrike University (or experience using CS Falcon)
- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Be familiar with the Microsoft Windows environment

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:

- Summarize the various components and processes of Falcon Sandbox
- Submit files of interest to the Sandbox
- Analyze a Falcon Sandbox report
- Answer stakeholder Intelligence Requirements from Sandbox Reporting

The course includes hands-on labs that allow students to apply what they have learned in the workshop.

REGISTRATION

For a list of scheduled courses and registration access, please log into your CrowdStrike University account.
This course requires one (1) training credit. If you do not have access to CrowdStrike University, need to purchase training credits, or need more information, please contact sales@crowdstrike.com.

INTRODUCTION

- Who we are
- Who you are
- Admin items
- Course Overview/Agenda

SANDBOX OVERVIEW

- Intro to FalconX and Sandbox
- Comparison of Various FalconX Levels
- Sandbox Components
- Goals of Using Sandbox
- Sandbox Logs
- FalconX / Sandbox Quota System
- Sandbox OnPrem Solution
- Falcon Sandbox Bridge
- Sandbox 3rd Party Integrations

UPLOADING FILES TO SANDBOX

- Automatic Submissions
- Manual Submissions
- File Types Supported
- Submission Options

INGESTING THE SANDBOX REPORT

- Report Overview
- The Sandbox Analysis Pane
- Broad vs. Strict IOCs
- Calculated Risk Assessment &Threat Score
- User Roles in Report Generation & Reading
- The Report Summary Section
- The Network Activity Section
- The Advanced Analysis Section
- Report Formats
- MITRE ATT&CK Analysis

ANSWERING INTEL REQUIREMENTS FROM SANDBOX REPORTS

- Intel Reqs Pertaining to Sandbox
- Information Levels Feeding Analysis
- Delivering Assessments to Stakeholders
- Sandbox-Derived Answers to Intel Reqs
- Recursive Malware Analysis
- Threat Hunting with Previous Results

CONCLUSION

- Review of core concepts
- What's next