Course Outline

Cybersecurity with Metron

Course Summary

Description

This course will provide a comprehensive introduction to the capabilities of Metron. The student will begin with installing Metron. After learning Metron's domain specific languages (DSL), the Stellar Query and the Stellar Transformation Language, the student will create security telemetries, create enrichments, work with pluggable threat intelligence and understand the process of threat triage. The course will conclude with the student doing streaming enrichment and dashboarding with Kibana.

Objectives

After taking this course, students will be able to understand the material, know our labs and ask questions and with interactive discussions.

Topics

- Metron Installation, Overview, Architecture
- Creating a New Telemetry
- Creating a New Enrichment and Pluggable Threat Intelligence
- Threat Triage
- Streaming Enrichment and Dashboarding with Kibana

Audience

Individuals who want to understand the capabilities of Metron.

Prerequisites

An experiential or academic understanding of the need for centralizing the use and monitoring of capabilities provided by the tools of Cybersecurity such as pcap, netflow, bro, snort, fireye, and Sourcefire. The student should understand how software services can combine security information management (SIM) and security event management (SEM). The student should have an understanding of services that provide real-time analysis of security alerts generated by applications and network hardware-based operating system and command line scrip

Duration

Five Days/Lecture & Lab

Course Outline

Cybersecurity with Metron

Course Outline

I. Metron Installation, Overview, Architecture

II. Creating a New Telemetry

III. Creating a New Enrichment and Pluggable Threat Intelligence

IV. Threat Triage

V. Streaming Enrichment and Dashboarding with Kibana