CYBRARY

Course Syllabus

Advanced Cyber Threat Intelligence

Instructor Name: Berriche Alyssa

Instructor Website: digitalys-mag.net

Instructor Contact: alyssa.berriche@digitalys-mag.net

Course Creation Date: 11/13/2019

Course Description and Goals

Course Description:

Cyber threats keep getting more complex and sophisticated and security teams cannot continue playing whack-a-mole. Basic methods and tools are no longer efficient against these emerging threats. This is why moving towards more data driven security is a necessity and of course all of this requires specific skills that you will be learning through this course. This course, Advanced Cyber Threat Intelligence, is built with the intelligence cycle in mind to create a consistent image and a logical sequence of how to build and leverage a Threat Intelligence program.

So, you will be interested to enroll in the course if you already have some basic knowledge about cyber threat intelligence and you are looking for a course to enhance your existing skills, or perhaps you are building a new Cyber Threat Intelligence program for your organization.

The advanced Cyber Threat Intelligence course will benefit security practitioners and individuals interested in preventing cyber threats. In this course, we will discuss how Threat Intelligence can help you leverage your existing data sources to extract useful information and how to find complementary information and intelligence from external sources. We will also explain how to get actionable data through the process of vetting and the importance of this task to reduce efforts on false positives investigations.

The next part will be dealing with analysis of intrusion and campaigns. It can help you structure your analysis using models and techniques like the Analysis of Competing Hypotheses, the Cyber Kill Chain and MITRE ATT&CK. A full part will be dedicated to campaign investigation and its sophisticated analysis methods such as Visual analysis and Heatmap analysis.
Another interesting part of the analysis is attribution. Working on complex investigations can often lead to create confusion or even push analysts to use shortcuts to come up with conclusions especially related to attribution. At some point, it becomes a handicap to think properly but if the analysts are unable to identify these issues, they won't be able to defeat them. For this reason, one of the modules will discuss biases and logical errors identification and giving advice on how to manage them.

And finally, one of the key concepts of Cyber Threat Intelligence is dissemination. Therefore, it is essential to choose the right format of intelligence to share based on your targeted audience (tactical, operational, strategic).

Prerequisites:
Students who desire to complete this course are required to have:

- Familiar with networking essentials
- Familiar with security terminology (Firewall, SIEM, IPS, …)
- Complete the "Intro to Cyber Threat Intelligence" course
- Basic OSINT knowledge
- Basic understanding of the Cyber Kill Chain
- Basic understanding of data analysis

Study Resources:
A separate document containing full list of references that were used to build this course, is provided

Course Goals: By the end of this course, students should be able to:

1. Run a threat intelligence program for an organization
2. Collect and select relevant intelligence to enhance detection and response
3. Analyze a campaign using ACH
4. Understand the mindset of modern attackers and adapt detection & response strategies based on Cyber Threat Intelligence analysis
5. Challenge and manage biases in intrusion analysis
6. Provide actionable advice about emerging threats
7. Build and disseminate threat intelligence reports based on the intended audience

Labs Used: No labs included in this course

Outline

Module 1 | Introduction
- Lesson 1.1 Course Introduction (7:50)
- Lesson 1.2 Introduction to Intelligence Lifecycle (7:09)

Module 2 | Collection
- Lesson 2.1 Introduction to Data Collection (4:11)
- Lesson 2.2 Internal Data Acquisition (6:38)
- Lesson 2.3 External Data Sources (7:07)
- Lesson 2.4 Private Data Sources Part 1 (8:37)
- Lesson 2.5 Private Data Sources Part 2 (3:42)
- Lesson 2.6 Community Data Sources (10:48)
- Lesson 2.7 Public Data Sources Part 1 (8:00)
- Lesson 2.8 Public Data Sources Part 2 (3:12)
- Lesson 2.9 Leveraging OSINT Part 1 (9:22)
- Lesson 2.10 Leveraging OSINT Part 2 (6:50)

Module 3 | Data Management and Processing
- Lesson 3.1 Introduction to Data Processing (6:14)
- Lesson 3.2 Common CTI Standards Part 1 (8:01)
- Lesson 3.3 Common CTI Standards Part 2 (4:01)
- Lesson 3.4 Storage and Integration (2:24)
- Lesson 3.5 Threat Intelligence Platforms (9:12)

Module 4 | Analysis
- Lesson 4.1 Introduction to Analysis (4:50)
- Lesson 4.2 Analysis of Competing Hypothesis (7:32)
- Lesson 4.3 Cyber Kill Chain and Diamond Model (10:45)
- Lesson 4.4 Cyber Kill Chain and Courses of Action Matrix (9:11)

Module 5 | Campaign Analysis

Lesson 5.1 Introduction to campaigns (4:58)
Lesson 5.2 Heatmap Analysis (6:02)
Lesson 5.3 Visual analysis (6:16)
Lesson 5.4 MITRE ATT&CK & MITRE Threat Groups Tracker (7:28)
Lesson 5.5 Threat Intelligence Naming Conventions (7:21)

Module 6 | Attribution

Lesson 6.1 Introduction to Attribution (8:02)
Lesson 6.2 Cognitive Biases (6:09)
Lesson 6.3 Logical Fallacies (6:32)
Lesson 6.4 How to Manage Biases (5:20)
Lesson 6.5 Nation-State Attribution Part 1 (7:53)
Lesson 6.6 Nation-State Attribution Part 2 (4:34)

Module 7 | Dissemination & Sharing

Lesson 7.1 Introduction to Dissemination (7:11)
Lesson 7.2 Tactical intelligence (7:28)
Lesson 7.3 Operational Intelligence (5:36)
Lesson 7.4 Strategic Intelligence (9:21)

Module 8 | Summary

Lesson 8.1 Summary (6:28)