Threat Hunting - Steps, Program & Maturity Model

Reading

1h

Status | Incomplete

Introduction

In the previous reading, you were introduced to the basics of threat hunting. In this reading, you will dive deep into some of those basics: learn more threat hunting steps, learn how to structure a threat hunting program, and finally, if a threat hunting program is already in place, how to develop it further using a maturity model.

Reading

Threat Hunting Steps

You briefly read about the threat hunting steps in the previous reading. Here is another reading that gives detailed insight into the steps you need to take to carry out threat hunting: What is Cyber Threat Hunting?.

> As you read What is Cyber Threat Hunting?, focus on the key steps a Blue Team member follows when conducting threat hunting in an organization.

> ⚠ Note, there is no specific industry standard with regard to the cyber hunting steps, however the ones shared here are definitely the ones popular in the industry.

Threat Hunting Program

Threat hunters can help build defenses as they work with offensive security teams to identify potential threats and build stronger threat barriers. Therefore, an effective threat hunting program is essential to track the threats before they attack the IT infrastructure of your organization.

> Read How to develop a successful threat-hunting program to learn more about putting together a hunting program for your organization.

As you read, focus on the following:

- Best practices for developing a successful threat hunting program
- How you would implement/customize each best practice as per the requirements of your organization

Threat Hunting Maturity Model

> Read the article given here with a focus on the threat hunting maturity model: What is Cyber Threat Hunting? Definition, Techniques & Steps

Conclusion

Now that you have strengthened your knowledge of threat hunting even further, it is time for a knowledge check exercise to assess how much you have learned so far.

Further Readings

1. Here is a short webinar and a good blog about the threat hunting framework; this also includes some case studies: Threat Hunting Frameworks and Methodologies: An Introductory Guide
2. Here is another reading that shares a different approach of the step-by-step threat hunting process (as was mentioned, there is no industry standard when it comes to threat hunting steps): Build a Cyber Threat Hunting Plan With This Step-by-Step Process
3. Read the following article to deep dive into the development of the threat hunting program: The Makings of a Successful Threat-Hunting Program

✓ Mark Completed

← Previous
Understanding Cyber Threat Hunting

Next
Lecture Reading →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W08D1

Mon Aug 12

› Outline & Notes (1)

› Lectures (1)

⌄ Work (5)

6 hrs

- </> Analysis of Intelligence Reports
- </> Using Tactical Intelligence on Carbanak Report
- Understanding Cyber Threat Hunting
- Threat Hunting - Steps, Program & Maturity Model
- Lecture Reading

W08D1 Schedule »

Powered by Lighthouse Labs.