Understanding Cyber Threat Hunting

Reading

45m

Status | Incomplete

Introduction

This reading introduces you to Cyber Threat Hunting, shares key responsibilities of a hunting team, and helps you understand how the process of threat hunting is different from that of the incident response. Read on to learn more about Cyber Threat Hunting.

Reading

Read the following article to learn the basics of threat hunting: What is Cyber Threat Hunting?.

> As you read the article, focus on the areas listed below:

- How is threat hunting defined?
- Why do organizations engage in threat hunting?
- What are the different threat hunting methodologies?
- What are the key steps one needs to take to carry out threat hunting?

Once you have understood the basics of threat hunting, read the following article to dive deeper into the topic: What is threat hunting?.

> As you read the article, focus on the areas listed below:
>
> - Types of threat hunting
> - Important tools used for threat hunting

Threat Hunting vs. Incident Response

As described by Cybersixgill, the tools and techniques used in threat hunting are similar to those used when responding to security incidents. In both cases, Cyber Security analysts perform an in-depth analysis of systems to identify indicators of attack. The main difference between the two processes is the starting point: a known incident versus a potential threat.

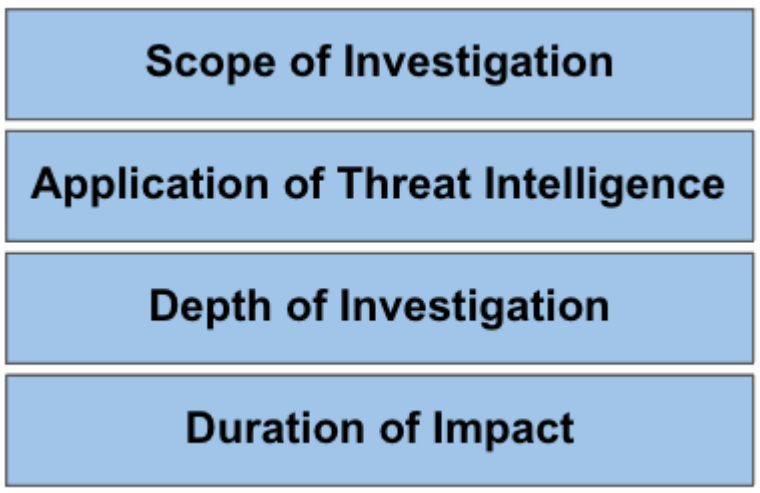

Figure 1: Differentiators Between Threat Hunting and Incident Response

While proactive and reactive investigations use similar techniques, they also have significant differences. Some major differentiators include:

Scope of investigation: when investigating a known attack, the scope of investigation is relatively limited as some links in the attack chain are known and the analyst needs to work forward and backward from there. Threat hunting can include a much wider scope of investigation because it involves looking into a completely unknown potential threat.

Application of threat intelligence: both reactive and proactive investigations use threat intelligence, but they use this data in different ways. Reactive analysis can use threat intelligence to identify incoming or ongoing threats. In contrast, proactive threat hunting uses threat intelligence to determine which threats that an organization may face and how they can be detected.

Depth of investigation: an incident response investigation only needs to go far enough to verify a threat and collect any necessary information for remediation. Threat hunting, on the other hand, needs to prove or disprove a theory, which can be more difficult.

Duration of impact: the desired end result of incident response is the removal of a present threat. Threat hunting can not only help with the remediation of past attacks but can also help to close visibility gaps and improve defenses for the future.

Source: Cyersixgill.com

Conclusion

Now that you have understood the basics of threat hunting and how it is different from a conventional incident response, you will move to the next reading to delve further into the basics of threat hunting and learn about threat hunting steps, threat hunting programs, etc.

✓ Mark Completed

Previous
Using Tactical Intelligence on Carbanak Report

Next
Threat Hunting - Steps, Program & Maturity Model

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 »