Lecture Reading

Reading

1h - 1h30m

✓ Status Incomplete

Introduction

This reading focuses on subjects that will be covered by your instructor during the lecture. Make sure you review this page and take notes as you preparare for the upcoming lecture.

Part A: Reactive Versus Proactive Threat Detection

When it comes to finding a threat in an environment, hunting requires a more proactive strategy, as opposed to a reactive one, like most incident response teams do.

When alerts are generated, a reactive organization immediately initiates the incident response process. The warning may have originated from a third party, such as any three-letter agency, or it may have been generated internally by the organization's own network of security sensors. The most accurate depiction of a reactive strategy is that of an incident response team that, for the most part, sits about waiting to be called into action and places its faith in the authenticity of the alerts it is getting. The majority of firms build their incident response teams and processes as a reactive approach, which is perfectly acceptable as a starting point. In many instances, the majority of the incident response team is made up of augmentation workers who, as part of their regular roles, are generally responsible for a variety of other responsibilities. It is possible that the team becomes permanent if the company continues to expand in size or if it experiences an increasing number of occurrences.

When an organization realizes that it is not identifying its incidents early enough, the organization will transition from a “reactive organization” to a “hunting organization.” When we talk about hunting-based responses, we aren't suggesting that this is an "either/or" strategy. The majority of hunting companies likewise function as reactive organizations; however, they begin to assign their incident response team to actively engage and hunt for attackers within their environment. The hunting team will often be equipped with known malware, patterns of behavior, or certain threat actors' information to target them in their search.

Part B: Threat Hunting Hypotheses

Mostly, hunts begin with data gathered from different or external sources, such as from the Information Sharing and Analysis Center (ISAC) or three-lettered agencies (FBI, CIA, NSA, etc.), which provides useful information or IOCs such as URLs, hash values, network or host artifacts, IP addresses, etc. Incidents may sometimes trigger hunts, prompting participants to explain when and how something occurred.

In the cyber world, there are a large number of unknown risks. However, not every potential threat calls for a deep dive. This is where the **Hypothesis Approach** comes into play. As in the scientific world, in hypothesis-driven threat hunting, threat hunters make an informed assumption about a risk, develop a hypothesis based on this assumption, make the hypothesis the foundation of their investigation, and finally take steps to test it.

A hypothesis is an informed assumption about what you think could be happening in your environment, and it is the starting point for a hunt in a hypothesis-driven workflow. It can start or trigger either based on assumption or hunch. If you know what you're searching for, OSINT technologies and frameworks like MITRE ATT&CK may be quite useful.

Developing and evaluating hypotheses is an important aspect of danger hunting. Hunters generally construct hypotheses using a combination of data from sources such as frameworks, social intelligence, threat intelligence, and their own experiences in the field. The question "If I were to attack this environment, how would I do it?" is an example of a broad inquiry. "If I were to try to break into anything, what would it be? To what end would I be aiming?"

Other possible questions could include "Why do I see unusual traffic from printer IP addresses?" or "Why do I observe an unusual number of DNS requests from a single machine?".

> ℹ Go through this article to dive deep into the threat hunting hypothesis: Threat Hunting Hypothesis Examples: Prepare For a Good Hunt!

Part C: Compromise Assessment & Compromise Report

Most attackers are active in environments for a significant amount of time before being discovered. There were many attacks in recent years where the attackers were sitting in their environment for months and security teams were not aware of them, despite strong teams and processes, including reliable security controls being in place. Once the attacker gets access to the internal system, they have access to virtually all resources.

This is where a lot of organizations look for **Compromise Assessment**. If you want to know whether or not you've been breached, a compromise evaluation is what you need; the evaluation report thus developed is called a **Compromise Report**. As defined by Crowdstrike, "compromise assessments are high-level investigations where skilled teams utilize advanced tools to dig more deeply into their environment to identify ongoing or past attacker activity in addition to identifying existing weaknesses in controls and practices. The intent of the comprehensive assessment is to answer the critical question: 'Has my organization been breached?'"

> ⚠ It is important that you understand the difference between Compromise Assessment vs. Threat Hunting. Read the analysis below to learn more.

As explained by Crowdstrike, threat hunting is a proactive search for cyber threats that are already inside the infrastructure. Threat hunters develop hypotheses based on information gathered about new threats and combine that with knowledge about adversary tradecraft. They use threat intelligence to expose potential and ongoing attacker activity, and apply advanced analytics to detect suspicious behaviors among the massive amount of information captured by security systems. Threat hunting is an ongoing process.

A Compromise Assessment, on the other hand, is typically conducted on a periodic basis, oftentimes quarterly or monthly for point in time analysis and in some cases to meet regulatory requirements. The scope of a Compromise Assessment is also significantly greater than that of a threat hunt: a Compromise Assessment looks not only at IOCs and indicators of attack, but also at the reasons they may have occurred, what next steps are in order, and what actions can be taken to improve the organization's overall security posture.

Compromise Report Template

There is no standard format for a Compromise Report. However, it is recommended to include the following elements when creating a report:

- **Executive summary:** provide the overall scope of the assessment, the outcomes, and recommendations based on the assessment done. This is a high-level one- or two-pager executive summary.
- **Compromise Assessment:** this section provides more detailed findings and can be broken down into multiple sections, as given below:
    - Scope

    - Threats detected
    - Attribution
    - Detection timeline
    - Intrusion timeline
- **Recommendations and next steps:** these recommendations are to cover the gaps based on the certain frameworks or models you can use, such as the Cyber Kill Chain as one example.

Conclusion

Now that you have acquired basic understanding of the lecture topics, let's jump to the lecture for the day.

✓ Mark Completed

← Previous
Threat Hunting - Steps, Program & Maturity Model

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 »