Diamond Model for Intrusion Analysis

Reading

45m

Status | Incomplete

Introduction

Previously, you learned how the Cyber Kill Chain Model helps threat hunters engage into intrusion analysis. In this reading, you will look at another model of intrusion analysis—the Diamond Model—and then compare how this model compares with the Cyber Kill Chain Model. You will also look at the concept of threat actors towards the end of the reading.

Reading

Diamond Model

The Center for Cyber Threat Intelligence and Threat Research put out the *Diamond Model* in 2013. It's a model of Intrusion Analysis that is used to describe cyberattacks and contains four parts: adversary, infrastructure, capability, and target. It helps to describe how to map an attacker's tactics, techniques, and procedures (TTPs) to build up threat intelligence.

> Read the following paper on the Diamond Model and how it works. While reviewing this short article, make a list of key steps you follow in the model and the approach you take to map TTPs using this model: The Diamond Model of Intrusion Analysis.

Cyber Kill Chain vs. Diamond Model

As you learned in the previous unit, Cyber Kill Chain is a concept that is centered on the defender, and it defines the steps that an attacker has to perform in order to effectively compromise their target and obtain the information they are looking for.

According to this line of thinking, all that is required of a defender is to remove only one link from a chain in order to make the subsequent steps that would have been problematic irrelevant.

Perhaps the biggest difference between the Diamond Model and the Cyber Kill Chain is that the Cyber Kill Chain strictly follows a linear narrative approach to analyze a cyber attack; one step leads to another. The Diamond Model was designed to track a threat actor over multiple intrusions.

However, the Diamond Model method puts a lot more emphasis on understanding the attacker, what tools and infrastructure they use, and why they do what they do, unlike the Cyber Kill Chain method.

The Diamond Model doesn't look at a series of events; instead, it looks at how features relate to each other. Instead of trying to find points of disruption in single attacks, it is meant to help you understand what kind of threat you are up against.

This is useful when dealing with more advanced attackers, like those who, once they get a foothold, set up other ways to get in and clean up the first infection. When you go through the Cyber Kill Chain event by event, you might be fooled into thinking that if you don't detect any more negative occurrences, the security measures you put in place worked.

Threat Actors

The term "cyber threat actors" refers to groups or individuals who, with the intention of causing harm, seek to gain unauthorized access to or otherwise affect the personal information, data, systems, and infrastructure of the victims, including the authenticity of the information that flows to and from them. This can be accomplished by exploiting vulnerabilities in an information system or exploiting the operators of the system. Because of the worldwide nature of the Internet, threat actors may operate from any location in the world and yet compromise the safety of the information systems of any institution, whether it is an organization or even a country. This is made possible by the globalization of the Internet.

> ⚠ In the upcoming lectures, your instructor will give you deep insight into the threat actors, their motivations, and their sophistication.

Conclusion

In this reading, you learned about the Diamond Model and how it compares to the Cyber Kill Chain Model. In the next reading, you will learn about another model used for analyzing cyberattacks: the MITRE ATT&CK framework.

Further Reading

You may go through the reading given here to get an in-depth understanding of the Diamond Model: [The Diamond Model of Intrusion Analysis](#).

✓ Mark Completed

Previous
Using Strategic Intelligence on Carbanak Report

Next
MITRE ATT&CK Framework

Lectures (1)

Work (5)

5 hrs

- Using Strategic Intelligence on Carbanak Report
- Diamond Model for Intrusion Analysis
- MITRE ATT&CK Framework
- Mapping to MITRE ATT&CK
- Models & Frameworks Exercise

Other (1)

W07D5 Schedule »