

Cyber Kill Chain & Intrusion Analysis

Reading

40m



Status

Incomplete

Introduction

As a Blue Team member, it's important that you understand the nature of a cyber threat, the potential danger it imposes on your organization, and most importantly, the series of steps that the attacker follows to carry out the cyber attack. Therefore, it's important to understand the concept of *Cyber Kill Chain* that helps members of an SOC to trace stages of a cyber attack and analyze intrusion at every stage of the attack.

Reading



Read the following article to get an in-depth understanding of the Cyber Kill Chain:

<https://www.varonis.com/blog/cyber-kill-chain>

As you read the article, focus on the following areas:

- What is the Cyber Kill Chain and what is it used for?
- How the Cyber Kill Chain works.
- What are the different phases of the Cyber Kill Chain?
- How each phase contributes to stopping a cyber attack.



Reflection Question: Now that you understand different phases of a Cyber Kill Chain, think about the different telltale signs and signals, visible at each phase of the attack, as the attack progresses through the chain.

Conclusion

In this reading, you learned about the different phases of a Cyber Kill Chain. In the subsequent lectures, you will get an in-depth understanding of cyber threat, CTI, and Cyber Kill Chain.

Further Reading

The term or the idea of Cyber Kill Chain was first described in a study written by Lockheed Martin in 2009 and titled [Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains](#). Read the original study to dive deep into the Cyber Kill Chain model.

✓ Mark Completed

←

Previous
Threat Actors and Their Tactics

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

Let us know how we're doing




W07D4

Thu Aug 8

> Lectures (1)

✓ Work (7)

7 hrs

 [Project: Encryption](#)

 [Course Reflection](#)

 [Overview - Threat Defense Operations](#)

 [Understanding Cyber Threat Intelligence](#)

 [Threat Intelligence Platforms and Their Usage](#)

 [Threat Actors and Their Tactics](#)

 [Cyber Kill Chain & Intrusion Analysis](#)

> Other (1)

W07D4 Schedule »