Blue Team Level 1 Certification

Introduction to BTL1

- ✓ Welcome to Blue Team Level 1:
 - 4 Topics

SECURITY FUNDAMENTALS DOMAIN

- - 1 Topic
- Soft Skills
- 7 Topics
- 5 Topics | 1 Quiz
- Networking 101
- 6 Topics | 1 Ouiz
- Management Principles 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- PA1) Introduction to Emails and Phishing
 - 7 Topics | 1 Quiz
- PA2) Types of Phishing Emails
 - 10 Topics | 2 Quizzes
- A PA3) Tactics and Techniques Used
 - 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email
 - 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and
 - 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions
 - 12 Topics | 1 Quiz
- PA7) Report Writing
 - 7 Topics | 1 Ouiz
- O PA8) Phishing Response Challenge
 - 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence
 - 7 Topics
- TI2) Threat Actors & APTs
 - 6 Topics | 2 Quizzes

O TI3) Operational Threat Intelligence

- 7 Topics | 1 Quiz
- O Section Introduction, Operational
- O Precursors Explained
- O Indicators of Compromise Explained
- O MITRE ATT&CK Framework
- O Lockheed Martin Cyber Kill Chain
- O Attribution and its Limitations
- O Pyramid of Pain
- Activity) End of Section Review Operational Intelligence
- TI4) Tactical Threat Intelligence
 - 7 Topics | 1 Quiz

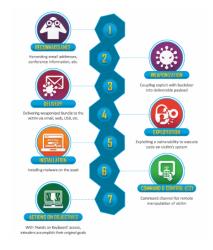
Lockheed Martin Cyber Kill Chain

Blue Team Level 1 Certification (Standard) > TI3) Operational Threat Intelligence > Lockheed M... IN PROGRESS

Threat Intelligence CYBER KILL CHAIN



The Cyber Kill Chain (CKC) framework was developed by Lockheed Martin in 2011 and it is an Intelligence Driven Defense model for the identification and prevention of cyber-attacks, specifically ones that can be classified as Advanced Persistent Threats (APTs). The CKC can help IT security teams and professionals develop strategies, $products, and \ plans \ to \ detect \ and \ contain \ attacks \ at \ different \ stages, \ resulting \ in \ a \ more \ secure \ IT \ environment. \ In$ $recent \ years, it \ has \ become \ the \ de-facto \ standard \ to \ describe \ how \ attacks \ can \ happen \ on \ a \ network. \ The \ CKC \ is$ split into seven different stages, with all seven stages needing to be completed to have a successful attack.



KILL CHAIN STAGES

[1] Reconnaissance:

Attackers: Malicious actors will conduct research on the target organization typically using both active and passive reconnaissance methods such as domain record lookups, public IP range port and vulnerability scanning, scouting out employees on social media, and more.

 $\textbf{Defenders:} \ \text{Activity conducted by the attackers at this stage will come in the format of precursors, such as IPs that also shows the attackers of the stage of the sta$ are performing port or vulnerability scanning, employees being approached by individuals that they do not know, and employees potentially receiving connection/friend requests on social media.

[2] Weaponization:

Attackers: Malicious actors create their own backdoor instead of purchasing commodity malware, and host this file on a domain they own. They then write a macro within a Microsoft Word document which connects to the attackerowned domain and downloads the malware to the system where the file was opened.

Defenders: It is extremely hard for the security team to detect this stage, as it is not happening within their environment therefore they have no visibility of what happens outside the organization (with the exception of cyber threat intelligence). Typical defenses should be employed such as anti-virus, email security, and system hardening.

TI5) Strategic Threat Intelligence 5 Topics 1 Quiz
TI6) Malware and Global Campaigns
6 Topics 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics 5 Topics
DF2) Forensics Fundamentals
10 Topics 5 Quizzes
DF3) Digital Evidence Collection
8 Topics 1 Quiz
DF4) Windows Investigations
3 Topics 3 Quizzes
DF5) Linux Investigations
4 Topics 2 Quizzes
DF6) Volatility
3 Topics 1 Quiz
O DF7) Autopsy
4 Topics 1 Quiz
SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics 1 Quiz
SI2) Logging
6 Topics 2 Quizzes
SI3) Aggregation
2 Topics 1 Quiz
SI4) Correlation
6 Topics 1 Quiz
SI5) Using Splunk
5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics 1 Quiz
IR2) Preparation Phase
10 Topics 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics 4 Quizzes
 IR4) Containment, Eradication, and Recovery Phase
5 Topics 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
○ IR6) MITRE ATT&CK
13 Topics 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH

O How to Start Your Exam

[3] Delivery:

Attackers: Malicious actors have crafted a spear-phishing email using information gathered on the target from OSINT sources. The email contains a Microsoft Office document with a malicious macro that will run malware in the context of the currently signed-in user.

Defenders: The security team should have email defenses in place such as attachment sandboxing which should be able to detect any malicious attachments such as immediately malicious binaries or malicious Word documents or PDFs

[4] Exploitation:

Attackers: Malicious actors have identified a vulnerability, that if exploited, can provide them with higher privileges than the current compromised account has, providing them with more access and the ability to perform more actions.

Defenders: The security team can prepare for this stage by hardening systems and performing vulnerability management processes to identify and remediate vulnerabilities that are both internal and externally present.

[5] Installation:

Attacker: Malicious actor installs a backdoor and deploys persistence tactics and techniques to ensure that they can keep a foothold within the infected system, allowing continuous access.

Defenders: The security team can deploy endpoint detection and response (EDR) software agents to potentially infected hosts to allow for the detection, investigation, and eradication of a malicious presence.

[6] Command and Control:

Attackers: The malicious actor installs malware that opens a channel between the malicious actor and remote machine, allowing them to send commands to the malware and attempt to gain the ability to complete step 7, actions on objectives.

Defenders: The defenders last step to fully stop the threat, prevention of command execution is key

[7] Actions on Objectives:

Attackers: The malicious actor was successful in their attack and has obtained keyboard-access, they are now able to attempt to complete any objectives they have.

Defenders: The defender must detect this stage as quickly as possible to prevent further damage and minimize the time that the attacker can complete their objectives.

IS IT OUTDATED?

Illustrating how cyber-attacks work has its issues. Attacks conducted by hackers, nation-states, and APT groups change over time and the model doesn't always show how the attack can take place. Numerous security researchers have noted that the cyber kill chain does not do a good job at describing insider threats, as well as the first two phases traditionally occurring outside of the defender's network, making it much harder to detect. In an effort to make the model work for more scenarios, MITRE combined its ATT&CK framework with the cyber kill chain to develop the Unified Kill Chain (UKC). The UKC consists of 18 unique attack phases that may occur during a cube attack and this includes things that the CKC left out; such as activities outside and within the network. Similar to the original CKC, the UKC can be used to analyze and defend against attacks that occur from APTs. So while the Cyber Kill Chain is still an important framework, others may be more appropriate.





