The Cyber Killer Chain was developed by Lockheed Martin to identify and prevent cyber intrusions. There are seven steps to the Cyber Kill Chain. Focusing on these steps helps analysts understand the techniques, tools, and procedures of threat actors.

When responding to a security incident, the objective is to detect and stop the attack as early as possible in the kill chain progression. The earlier the attack is stopped; the less damage is done and the less the attacker learns about the target network.

The Cyber Kill Chain specifies what an attacker must complete accomplishing there goal.

If the attacker is stopped at any stage, the chain of attack is broken. Breaking the chain means the defender successfully thwarted the threat actor's intrusion. Threat actors are successful only if they complete Step 7.

Note: Threat actor is the term used throughout this course to refer to the party instigating the attack. However, Lockheed Martin uses the term "adversary" in it's description of the Cyber Kill Chain. Therefore, the terms adversary and threat actor are used interchangeably in this topic.

The figure depicts the steps of the Cyber Kill Chain in a numbered vertical list. The steps of the Cyber Kill Chain are explained in detail in the next sections of the text.

Reconnaissance

Reconnaissance is when the threat actor performs research, gathers intelligence, and selects targets. This will inform the threat actor if the attack is worth performing. Any public information may help to determine the what, where, and how of the attack to be performed. There is alot of publicly available information, especially for larger organizations including news articles, websites, conference proceedings, and public-facing network devices. Increasing amounts of information surrounding employees is available through social media outlets.
The threat actor will choose targets that have been neglected or unprotected because they will have a higher likelihood of becoming penetrated and compromised. All information obtained by the threat actor is reviewed to determine it's importance and if it reveals possible additional avenues of attack.
The table summarizes some of the tactics and defences used during the reconnaissance step.

Adversary Tactics	SOC Defenses
Plan and conduct research: • Harvest email addresses • Identify employees on social media • Collect all public relations information (press releases, awards, conference attendees, etc.) • Discover internet-facing servers • Conduct scans of the network to identify IP addresses and open ports.	Discover adversary's intent: • Web log alerts and historical searching data • Data mine browser analytics • Build playbooks for detecting behaviour that indicates recon activity • Prioritize defence around technologies and people that reconnaissance activity is targeting

Weaponization

The goal of this step is to use the information from reconnaissance to develop a weapon against specific targeted systems or individuals in the organization. To develop this weapon, the designer will use the vulnerabilities of the assets that were discovered and build them into a tool that can be deployed.
After the tool has been used, it is expected that the threat actor has achieved there goal of gaining access into the target system or network, degrading the health of a target, or the entire network. The threat actor will further examine network and asset security to expose additional weaknesses, gain control over other assets, or deploy additional attacks.
It is not difficult to choose a weapon for the attack. The threat actor needs to look at what attacks are available for the vulnerabilities they have discovered. There are many attacks that have already been created and tested at large.
One problem is that because these attacks are so well known, they are most likely also

known by the defenders. It is often more effective to use a zero-day attack to avoid detection methods. A zero-day attack uses a weapon that is unknown to defenders and network security systems.
The threat actor may wish to develop there own weapon that is specifically designed to avoid detection, using the information about the network and systems that they have learned. Attackers have learned how to create numerous variants of there attacks in order to evade network defences.
The table summarizes some of the tactics and defences used during the weaponization step.

Adversary Tactics	SOC Defense
Prepare and stage the operation: • Obtain an automated tool to deliver the malware payload (weaponizer). • Select or create a document to present to the victim. • Select or create a backdoor and command and control infrastructure.	Detect and collect weaponization artefacts: PS: Are you a Nigerian resident abroad and you need to send money to your loved ones back home ? The stress is over now! Send money to Nigeria using the MonieWorld app. It's fast, easy and has great rates! MonieWorld is powered by Moniepoint. Sign up with my link https://spoo.me/iy8taz • Ensure that IDS rules and signatures are up to date. • Conduct full malware analysis. • Build detections for the behaviour of known weaponizers. • Is malware old, “off the shelf” or new malware that might indicate a tailored attack? • Collect files and metadata for future analysis. • Determine which weaponizer artefacts are common to which campaigns.

Delivery

During this step, the weapon is transmitted to the target using a delivery vector. This may be through the use of a website, removable USB media, or an email attachment. If the weapon is not delivered, the attack will be unsuccessful.
The threat actor will use many different methods to increase the odds of delivering the payload such as encrypting communications, making the code look legitimate, or obfuscating the code.
Security sensors are so advanced that they can detect the code as malicious unless it is altered to avoid detection. The code may be altered to seem innocent, yet still perform the necessary actions, even though it may take longer to execute.
The table summarizes some of the tactics and defences used during the delivery step.

Adversary Tactics	SOC Defense
Launch malware at target: • Direct against web servers • Indirect delivery through: ◦ Malicious email ◦ Malware on a USB stick ◦ Social media interactions ◦ Compromised websites	Block delivery of malware: • Analyze the infrastructure path used for delivery. • Understand targeted servers, people, and data available to attack. • Infer intent of the adversary based on targeting. • Collect email and web logs for forensic reconstruction.

Exploitation

After the weapon has been delivered, the threat actor uses it to break the vulnerability and gain control of the target. The most common exploit targets are applications, operating system vulnerabilities, and users. The attacker must use an exploit that gains the effect they desire.
This is very important because if the wrong exploit is conducted, obviously the attack will not work, but unintended side effects such as a DoS or multiple system reboots will cause undue attention that could easily inform cybersecurity analysts of the attack and the threat actor's intentions.
The table summarizes some of the tactics and defences used during the exploitation step.

Adversary Tactics	SOC Defense
Exploit a vulnerability to gain access: • Use software, hardware, or human vulnerability • Acquire or develop the exploit • Use an adversary-triggered exploit for server vulnerabilities • Use a victim-triggered exploit such as opening an email attachment or malicious weblink	Train employees, secure code, and harden devices: • Employee security awareness training and periodic email testing • Web developer training for securing code • Regular vulnerability scanning and penetration testing • Endpoint hardening measures • Endpoint auditing to forensically determine the origin of exploit

PEOPLE ALSO READ: The 10x ICT Instructor: Creating Multiple Income with ICT Skills

Installation

This step is where the threat actor establishes a back door into the system to allow for continued access to the target. To preserve this backdoor, it is important that remote access

does not alert cybersecurity analysts or users.
The access method must survive through antimalware scans and rebooting of the computer to be effective. This persistent access can also allow for automated communications, especially effective when multiple channels of communication are necessary when commanding a botnet.
The table summarizes some of the tactics and defences used during the installation step.

Adversary Tactics	SOC Defense
Install persistent backdoor: • Install webshell on a web server for persistent access. • Create a point of persistence by adding services, AutoRun keys, etc. • Some adversaries modify the timestamp of the malware to make it appear as part of the operating system.	Detect, log, and analyze installation activity: • HIPS to alert or block common installation paths. • Determine if malware requires elevated privileges or user privileges • Endpoint auditing to discover abnormal file creations. • Determine if malware is a known threat or a new variant.

Command and Control

In this step, the goal is to establish command and control (CnC or C2) with the target system. Compromised hosts usually beacon out of the network to a controller on the internet. This is because most malware requires manual interaction in order to exfiltrate data from the network.
CnC channels are used by the threat actor to issue commands to the software that they installed on the target.
The cybersecurity analyst must be able to detect CnC communications in order to discover the compromised host. This may be in the form of unauthorized Internet Relay Chat (IRC) traffic or excessive traffic to suspect domains.
The table summarizes some of the tactics and defences used during the command and control step.

Adversary Tactics	SOC Defense
Open channel for target manipulation: • Open two-way communications channel to CNC infrastructure • Most common CNC channels over the web, DNS, and email protocols • CnC infrastructure may be adversary owned or another victim network itself	Last chance to block operation: • Research possible new CnC infrastructures • Discover CnC infrastructure through malware analysis • Isolate DNS traffic to suspect DNS servers, especially Dynamic DNS • Prevent impact by blocking or disabling the CnC channel • Consolidate the number of internet points of presence • Customize rules blocking of CnC protocols on web proxies

PEOPLE ALSO READ: Understanding Diamond Model Of Intrusion Analysis

Actions on Objectives

The final step of the Cyber Kill Chain describes the threat actor achieving there original objective. This may be data theft, performing a DDoS attack, or using the compromised network to create and send spam or mine Bitcoin. At this point the threat actor is deeply rooted in the systems of the organization, hiding there moves and covering there tracks. It is extremely difficult to remove the threat actor from the network.
The table summarizes some of the tactics and defences used during the actions on the objectives step.

Adversary Tactics	SOC Defense
Reap the rewards of a successful attack: • Collect user credentials • Privilege escalation • Internal reconnaissance • Lateral movement through an environment • Collect and exfiltrate data • Destroy systems • Overwrite, modify, or corrupt data	Detect by using forensic evidence: • Establish incident response playbook • Detect data exfiltration, lateral movement, and unauthorized credential usage • Immediate analyst response for all alerts • Forensic analysis of endpoints for rapid triage • Network packet captures to recreate the activity • Conduct damage assessment

Action Point

Get My 66 Page eBook on How to Run Success Ads ON TikTok for 2,000 Naira. Click Here to Buy.

Get my 90 Page ebook on How to Run Ads on Facebook. Click here to buy now.

PS: Are you a Nigerian resident abroad and you need to send money to your loved ones back home? The stress is over now! Send money to Nigeria using the MonieWorld app. It's fast, easy and has great rates! MonieWorld is powered by Moniepoint. Sign up with my link

https://spoo.me/iy8taz

P.S.: If you need private online training on any of the ICT courses I offer here and you are in Nigeria, please send me a DM on my WhatsApp at **+2348103180831.** Please note that the Training will be 100percent online. It will be delivered via Zoom or Google Meet.

PS: I know you might agree with some of the points raised in this article or disagree with some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

Related posts:

1. The 10x Side Hustler. Ways of Creating Multiple Stream of Income
2. The 10x Whatsapp Group Administrator . Being a Leader With a Difference
3. The 10x Employee. Building Leaders in Our Organisations
4. Building a 10x Career. The Untaken Path to Career Growth