Google Cloud

Lockheed Martin's Cyber Kill Chain® in practice

So far, you've learned that the Lockheed Martin Cyber Kill Chain® is a framework used to help analyze security attacks. The goal of using the Cyber Kill Chain® is to create actionable threat intelligence that can be used to improve security defenses, measure defensive performance, and plan for future prevention. These goals can be achieved by mapping attacks to each step of the Cyber Kill Chain®, and analyzing them to identify patterns. The steps of the Cyber Kill Chain® include:

1. **Reconnaissance**
2. **Weaponization**
3. **Delivery**
4. **Exploitation**
5. **Installation**
6. **Command and control**
7. **Actions on objective**

In this reading, you'll explore the Lockheed Martin Cyber Kill Chain® in more detail through a scenario involving compromised cloud IAM credentials.

Applying the Lockheed Martin Cyber Kill Chain® to a threat scenario

Many intrusions in cloud environments start with compromised account credentials like user accounts, passwords, or cloud access keys. Malicious actors might try to obtain account credentials as a way to gain access into the target environment. From there, they can launch their attack, maintain persistence, and identify critical assets. Then, they can collect and exfiltrate data.

Reconnaissance

In the reconnaissance step, a malicious actor collects information about their target. In this scenario, a malicious actor performs research on the organization they want to target. Then, they visit the company's website and social media profiles. Next, they identify employee names and job titles, and decide to focus on exploiting one particular employee. After doing some more searching, they identify the employee's code repository.

Identifying and addressing malicious reconnaissance can be challenging from a security perspective. But, organizations can be proactive by configuring environments to detect and alert their security teams when malicious actors are actively scanning. Organizations can also

take preventative measures, including: limiting the amount of information the organization makes publicly available, providing security awareness training to inform users of the risks of sharing information online, and sanitizing their online presence.

Weaponization

In the weaponization step, a malicious actor prepares their attack. In this scenario, the malicious actor crafts a phishing email aimed at the target organization's employee.

To defend against weaponization, organizations can leverage threat intelligence sources to

stay updated on existing and evolving threats, and identify and prioritize threats to improve defenses. They can also use security controls to block malicious payloads from entering their networks.

Delivery

In the delivery step, the malicious actor launches their attack. In this scenario, they send a phishing email and compromise the employee's account by tricking them into entering their credentials on a fake login page.

To defend during the delivery step, organizations can implement comprehensive security awareness training to educate end users on the dangers of clicking links from phishing emails, or installing unauthorized programs. This can help prevent attacks from being successfully delivered. Organizations can also implement security controls to identify and block malicious payloads from being delivered to their networks, like email filtering, web filtering, and data loss prevention solutions.

Exploitation

In the exploitation step, a malicious actor gains access to the target. In this scenario, after gaining access to the employee's account, the malicious actor locates plaintext account credentials by searching the repository's history. Then, they use these credentials to log into the target's corporate cloud environment. Next, they examine the resources in the cloud environment to locate the organization's critical assets and resources, like storage buckets and computer instances.

In this scenario, the organization can best defend against exploitation by providing user education, or informing users about different types of malicious strategies, along with steps to avoid them. Some other measures include an email threat protection solution, multi-factor authentication, and implementing least privilege access for all user accounts.

There are many other measures that can be used to defend against exploitation, including:

- Vulnerability management
- Security controls
- Security testing
- A dedicated, gardened administrative workstation for all admin tasks with no access to email or internet, and restricted login access
- Multi-factor authentication
- Context aware authentication to detect logins from multiple locations at one time
- An OAuth token with a limited lifespan
- Conditional access to only allow service and user accounts to log on to specific systems

Installation

In the installation step, a malicious actor's goal is to maintain access in the target's system. In this scenario, the malicious actor creates new user accounts in the corporate cloud environment to maintain their access to the target's systems.

To defend against exploitation and installation, organizations can configure intrusion detection systems, regularly patch software to address vulnerabilities, and block unauthorized access so attackers can't inflict more damage.

Command and control

In the command and control step, a malicious actor remotely controls the target's system. In this scenario, the malicious actor applies network policy in the corporate cloud environment to allow inbound and outbound traffic.

Malicious actors often use a system with specialized tools to control compromised systems. This is called the command and control, or C2 node. By allowing outbound traffic, the malicious actor in this scenario can communicate with their command and control node, and execute more attacks.

Monitoring network traffic and observing abnormal activity in the command and control step can help organizations identify and shut down communications with systems that have been compromised.

Actions on objective

In the actions on objective step, the malicious actor collects and exfiltrates the target's critical assets, like data containing personally identifiable information (PII). In this scenario, the malicious actor creates copies of the cloud storage volumes. Then, they exfiltrate these copies

using large data transfers out of the organization's cloud storage, and into their command and control server.

To defend against exfiltration, organizations can encrypt their data at rest, limit access to cloud storage volumes, and mask any PII.

Key takeaways

Understanding the Lockheed Martin Cyber Kill Chain®, and knowing how it can be applied to a workplace scenario, can help you anticipate and respond to the actions of malicious actors, and help keep your organization's systems safe. By identifying the appropriate step in the Cyber Kill Chain® to map to any situation, you can be more prepared to handle threats quickly and efficiently.

Resources for more information

Learn more about Lockheed Martin's Cyber Kill Chain® by checking out these resources:

- Lockheed Martin's Cyber Kill Chain® framework
- The MITRE ATT&CK Framework