Slide 3- Threat Intelligence Classifications

1. It is typically used by senior leaders in an organization to make decisions about long-term plans and objectives related to cybersecurity. For example, strategic intelligence might involve analyzing trends and patterns in cyberattacks to determine where to invest resources or how to position the organization for future growth.
2. Technical Intelligence: It can be used to inform decisions about implementing specific technical controls and countermeasures to defend against cyber threats. Technical intelligence might include information on specific malware, zero-day exploits, or advanced persistent threats.
3. Tactical Intelligence: It includes information about the immediate environment, such as network traffic, system logs, and threat intelligence feeds, as well as information about the capabilities and intentions of attackers. Tactical intelligence is used to support decision-making at the operational level, such as determining the best course of action in response to a specific cyber incident.
4. Operational Intelligence: It typically includes data on things like vulnerability assessments, security incident response metrics, and security information and event management (SIEM) logs. Operational intelligence is used to optimize cybersecurity processes and make operational decisions, such as deciding where to allocate resources or how to improve efficiency in detecting and responding to cyber incidents.

Slide 5- Pyramid of Pain

Pyramid of pain is design to show the levels of how hard it will be for the adversary to make changes if they happened to get caught and attack again. For example, Hash Value, this one is tricky because even if the SOC Analyst has the malicious hash and can detect it in the system. However, it takes only 1 bit of change to have a completely different hash. So, if the hacker is sending a malicious file and he get detected, he just needs to change one 1 bit of that file and send it again.

1. Changing IP address is also easy. Usually, SOC analysts would block the malicious IP address however that would not stop the hacker from attacking again. They can use a technique used Fast Flux which allows multiple ip addresses associated with one domain name. So, unless you block the domain name, blocking an ip address doesn’t make the hacker’s job hard.
2. Domain name- Again easy. Even you can block a domain, the hacker can purchase another one. Unfortunately, unless you can find the hacker and prove is him and arrest him, there is no way to be save just by blocking domain names. Anyone can buy domains and they don’t need to show any identifications.
3. Host artifacts- Now it gets annoyed for the hacker because if he gets detected in this phase, he needs to change his attack tools and methodologies. This is time consuming, so it does get annoy.
4. Network Artifacts- the same thing it is annoying for him because again if he gets caught in this phase he needs to go and change his tools which gives the SOC Analyst more time to respond and detect the upcoming threats or remediate the existing ones.
5. Tools is hard- Because if the hacker is not able to attack your system than again, he must go and find new tools. It will be a game over for the attackers as they would need to invest some money into building a new tool.
6. TTPs- If you can detect and respond to the TTPs quickly, you leave the adversaries almost no chance to fight back. We will go over TTPs in the other slides.

Slide 6- Cyber Kill Chain

Cyber Kill Chain- It was created by Lockheed Martin.

Phases:

1. Reconnaissanceis discovering and collecting information on the system and the victim. An important concept to be familiar is OSINT. OSINT- Open- Source Intelligence. OSINT helps the hacker collect information about his victims. It is a good and bad tool depending on how it used. OSINT is used a lot by hackers for email harvesting.
2. Weaponizing- In this phase the hacker would create a way on how to reach the user and hack the system. For example, creating a malicious Microsoft Doc where a malicious payload is attached to it.
3. Delivery phase: Now that he built the weapon, he needs to deliver it to make some damages. One of the most spread but also effective ways to do it is
4. Phishing email. Other technique of delivery is watering hole attack. A watering hole attack is a targeted attack designed to aim at a specific group of people by compromising the website they are usually visiting and then redirecting them to the malicious website of an attacker’s choice.
5. Exploitation- Choosing what to exploit such as software, system, or server. The way the exploitation is carried is usually triggering the user to open an email attachment, exploiting hardware, using zero-day exploit, etc.
6. Installation- After the exploitation the hacker needs to keep persistence access. This is done by installing a web shell, a backdoor to the victim’s machine, modifying Windows services, etc.
7. C2- Command and Control- After the exploration and getting persistence, the hacker needs to remotely control and manipulate the victim’s machine. The way this is done is usually through HTTP or HTTPS protocols and if the user sends DNS requests than these requests are send to the hacker’s DNS.
8. Exfiltration- Unfortunately if things have reached this phase that means hacker already can collect the credentials from the users, Overwrite or corrupt data, Deleting the backups and shadow copies, etc.

Try Hack me- SOC Level 1- <https://tryhackme.com/paths>

Slide 7: The unified Cyber Kill Chain:

It was published in 2017 by Paul Pols and it was meant to be a expand of Cyber Kill Chain. The Unified Kill Chain was originally a university paper bringing together several Cyber Kill Chains by various industry contributors such as Laliberte, Nachreiner, Bryant, and Malone, but the real focus was on Lockheed Martin Cyber Kill Chain and MITRE ATT&CK. The unified Kill chain had 3 high level steps attackers can take:

1. Initial Foothold
2. Network Propagation
3. Action on Objectives

More information on each phase in the picture.

Slide8: The Diamond Model

Only 4 cores:

**Adversary: is the person who stands behind the cyberattack**

1. Adversary Operator: the hacker conducing the attack.
2. Adversary Customer: a person or group or country that will receive benefits from the attack.

**Victim: The person who is being attacked**

1. Victim Persona- people or company that is being target.
2. Victim Assets- The assets that are being attacked: such as systems, network, ip addresses, etc.

**Capability: any skills, tools or technique used by the hacker in the event**.

1. Capability capacity: all the vulnerabilities and exposures that the hacker can use.
2. Adversary Arsenal: is the set of capabilities that belong to the adversary.

**Infrastructure- any physical of logical interconnections that the adversary uses to attack. There are 3 types of infrastructure:**

1. Type1- the infrastructure owned or controlled by the adversary.
2. Type 2- includes malware staging servers, malicious domain names, etc.

Slide 9-10- Mitre Attack

Mitre is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The framework was developed by the MITRE Corporation, a non-profit organization that operates federally funded research and development centers, and it is widely used in the cybersecurity industry for threat intelligence, incident response, and defensive strategy development.

Mitre Attack developed three other framework that include:

CAR, Mitre Engage and Mitre Defend.

Car- provides a standardized approach for collecting and processing security data, and it includes a repository of pre-built analytics that can be customized and applied to various cybersecurity use cases.

Mitre Engage- The program includes various initiatives such as workshops, webinars, and collaborative projects, aimed at promoting the exchange of ideas and experiences, as well as improving cybersecurity knowledge and skills across different organizations and sectors.

Mitre Defend- The overall goal of Mitre Defend is to help SMBs (Small and Medium size business) to better understand and manage their cybersecurity risks, and to strengthen the overall cybersecurity ecosystem.

Sources:

1. Try Hack- SOC Path- <https://tryhackme.com/paths>
2. <https://gblogs.cisco.com/ca/2020/08/26/the-canadian-bacon-cisco-security-and-the-pyramid-of-pain/>
3. <https://www.sentinelone.com/blog/revisiting-the-pyramid-of-pain-leveraging-edr-data-to-improve-cyber-threat-intelligence/>
4. Cyber Threat Intelligence Integration Center (CTIIC)- <https://www.dni.gov/index.php/ctiic-home>
5. <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/>
6. <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>
7. <https://cyware.com/security-guides/cyber-threat-intelligence/what-is-the-diamond-model-of-intrusion-analysis-5f02>,
8. <https://attack.mitre.org/>
9. ChatGPT