***Week1\_deliverables\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**MITRE ATT&CK Summary**

● **Initial access**: The first step of gaining entry to a target network or system. For

example, phishing, exploiting public-facing applications, or using stolen credentials.

● **Execution:** The second step of running malicious code on the compromised system.

For example, scripting, command-line interface, or remote file copy.

● **Persistence**: The third step of maintaining access to the system even after a reboot

or interruption. For example, registry run keys, scheduled tasks, or web shells.

● **Privilege escalation:** The fourth step of gaining higher-level permissions on the

system or network. For example, exploiting vulnerabilities, abusing service accounts,

or bypassing user account control.

● **Defense evasion:** The fifth step of avoiding detection by security tools or defenders.

For example, obfuscating files or commands, disabling security software, or

tampering with logs.

● Credential access: The sixth step of stealing or obtaining authentication information

of users or systems. For example, keylogging, credential dumping, or brute force.

● **Discovery**: The seventh step of gathering information about the environment,

network, or system. For example, network service scanning, system owner/user

discovery, or software discovery.

● **Lateral movement:** The eighth step of moving from one system to another within the

same network. For example, remote desktop protocol, pass the hash, or application

deployment software.

● **Collection:** The ninth step of gathering data of interest from the compromised

systems or network. For example, data from local system, data from network shared

drive, or data from cloud storage.

● **Exfiltration:** The tenth step of transferring the collected data to an external location or

server. For example, over command and control channel, over alternative protocol, or

over physical medium.

**CISA CSET Exploration**

*CSET Threat Intelligence Tool: This tool assists in collecting, analyzing, and*

*applying threat intelligence to assess an organization's vulnerabilities and*

*weaknesses*.

● **CSET Attack Surface Characterization Tool:** This tool helps identify an

organization's attack surface, highlighting potential points of vulnerability and areas

for improvement.

**Threat Post Report Analysis**

*The Threatpost report insights include:*

● **The rise of cryptojacking:** Cryptojacking is a type of cyberattack in which

attackers use infected devices to mine cryptocurrency without the owner's

knowledge or consent.

● **The increasing use of artificial intelligence (AI) in cyberattacks:** Attackers

are increasingly using AI to automate their attacks and make them more

effective.

● **The targeting of operational technology (OT) systems**: OT systems are

used to control industrial processes and critical infrastructure. Attackers are

increasingly targeting these systems to cause disruption or physical damage.

Trends that caught my attention are:

● **Supply chain attacks on the rise:** Supply chain attacks became more

sophisticated and frequent in 2023, with attackers targeting software vendors

and managed service providers to gain access to their customers' networks.

● **Evolving phishing tactics:** Phishing attacks continued to evolve in 2023,

with attackers using more sophisticated techniques to bypass traditional email

filters and trick users into clicking on malicious links.

**Annotated list of SANS Resources**

*Cyber Security Resources | SANS Institute: This is the main page for accessing*

*various free and exclusive online cybersecurity resources, news, tools, and more*

*provided by SANS. You can browse resources by focus area, such as cloud security,*

*threat intelligence, or incident response, or by type, such as webcasts, white papers,*

*or blogs. This page can help you stay updated on the latest trends and developments*

*in cybersecurity and learn from the experts in the field.*

● **Cyber Security Tools | SANS Institute:** This is a page where you can find open source

cyber security tools that support your work and help you implement better security.

You can search the lists to find the free tools available to help you get the job done.

Some of the tools include SIFT Workstation, REMnux, SOF-ELK, and more. These

tools can help you perform various tasks, such as digital forensics, malware analysis,

log analysis, and more.

● **Top 10 Most Popular Free Resources | SANS - SANS Institute:** This is a blog post

that lists the top 10 most popular free resources from SANS in the past year. You can

find links to webcasts, podcasts, posters, cheat sheets, and more on various topics,

such as OSINT, API security, software supply chain attacks, and more. These

resources can help you learn new skills, gain insights, and discover best practices in

cybersecurity.

● **Cyber Security Training, Degrees & Resources | SANS Institute**: This is the main

page for accessing various cyber security training, degrees, and resources offered by

SANS. You can find over 85+ cyber security courses, covering all specialties and

experience levels, and over 40 specialized GIAC cyber security certifications. You

can also find scholarship academies, degrees, and certificates from SANS.edu.

These options can help you improve your cyber security knowledge and capabilities

and advance your career.

● **Internet Storm Center | SANS Institute :** This is a page where you can access the

Internet Storm Center, a global incident alert network that monitors and reports on

the latest cyber threats and attacks. You can find daily infosec threat updates, live

streams, podcasts, diaries, and more from the ISC handlers and contributors. This

page can help you stay aware of the current threat landscape and learn how to

defend against cyber attacks.

***Week2\_deliverables\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**Threat Intelligence Report:**

*Title: Weekly Threat Intelligence Report*

*Executive Summary:*

This report summarizes the findings of our weekly threat intelligence analysis, highlighting the top 3-5 threats identified during the week. The analysis includes details such as attack patterns, potential impact, and relevant indicators of compromise (IOCs).

1. Threat: Phishing Campaign Targeting Employee Credentials

* Attack Pattern: Phishing emails disguised as legitimate communications from internal departments, prompting recipients to enter their credentials on fake login pages.
  + - Potential Impact: Unauthorized access to sensitive company data, compromise of employee accounts, potential data breaches.
    - IOCs: Suspicious email domains, URLs redirecting to phishing pages, spikes in failed login attempts.

1. Threat: Ransomware Attack Exploiting Remote Desktop Protocol (RDP)
   * + Attack Pattern: Exploiting unsecured RDP connections to infiltrate corporate networks, deploying ransomware payloads on compromised systems.
     + Potential Impact: Encryption of critical data, disruption of business operations, financial losses due to ransom demands.
     + IOCs: Suspicious RDP login attempts from external IP addresses, presence of ransomware executables on infected systems.
2. Threat: Supply Chain Compromise Through Third-Party Vendor
   * + Attack Pattern: Targeting vulnerabilities in third-party vendor software or services to gain unauthorized access to supply chain networks.
     + Potential Impact: Compromise of supply chain integrity, distribution of malicious payloads to downstream customers, reputational damage.
     + IOCs: Unusual network traffic between vendor systems and supply chain networks, indicators of unauthorized access to vendor accounts.

**Threat Prioritization List:**

1. Ransomware Attack Exploiting Remote Desktop Protocol (RDP)
   * Justification: Ranked highest due to the potential for significant impact on business operations and financial losses.
2. Phishing Campaign Targeting Employee Credentials
   * Justification: Ranked second due to the widespread nature of phishing attacks and the risk of unauthorized access to sensitive data.
3. Supply Chain Compromise Through Third-Party Vendor
   * Justification: Ranked third due to the potential for reputational damage and the complexities involved in addressing supply chain vulnerabilities.

***Week3\_deliverables\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Deep Dive on Prioritized Threats:

* *Threat: Advanced Persistent Threat (APT) Group X*
  + Conduct in-depth research on APT Group X, including their Tactics, Techniques, and Procedures (TTPs), motivations, and past attacks.
  + Analyze their preferred attack vectors, such as spear-phishing, watering hole attacks, or supply chain compromises.
  + Investigate their motivations, which could include espionage, financial gain, or sabotage.
  + Assess the potential impact of their attacks on your organization, considering factors like data exfiltration, disruption of operations, and reputational damage.
* *Threat: Ransomware Variant Y*
  + Dive deeper into the TTPs employed by Ransomware Variant Y, including initial access methods, encryption techniques, and command and control infrastructure.
  + Explore the motivations behind ransomware attacks, such as financial gain, political motives, or disruption of operations.
  + Examine recent incidents involving Ransomware Variant Y to understand their impact on victim organizations and sectors.
  + Analyze the potential consequences of a ransomware attack on your organization's operations, data integrity, and reputation.

Intelligence Fusion Practice:

* *APT Group X:*
  + Gather information from threat intelligence feeds, security blogs, research papers, and incident reports to build a comprehensive profile of APT Group X.
  + Cross-reference information from multiple sources to identify commonalities and discrepancies in their TTPs and motivations.
  + Look for indicators of compromise (IOCs) associated with APT Group X's activities to enhance threat detection and response capabilities.
* *Ransomware Variant Y:*
  + Aggregate data from threat intelligence platforms, malware analysis reports, and law enforcement alerts to gain insights into Ransomware Variant Y's behavior and evolution.
  + Analyze trends in ransomware attacks attributed to Variant Y, including target sectors, geographical distribution, and ransom demands.
  + Identify any gaps or conflicting information in your analysis and seek additional sources, such as cybersecurity forums or industry-specific reports, to validate findings.

**Source Credibility Assessment:**

* *APT Group X:*
  + Evaluate the credibility of sources reporting on APT Group X, considering factors like the reputation of the cybersecurity firm or research organization and their track record in threat analysis.
  + Assess the depth of analysis provided by the source, including the use of technical indicators, attribution methodologies, and contextual information.
  + Be mindful of potential biases or agendas that may influence the source's analysis, such as affiliations with government agencies or competitive interests.
* *Ransomware Variant Y:*
  + Verify the credibility of sources reporting on Ransomware Variant Y, paying attention to the expertise and experience of the security researchers or analysts involved.
  + Scrutinize the methodology used to attribute ransomware incidents to Variant Y, including the analysis of malware samples, network traffic, and ransom payment data.
  + Consider any potential conflicts of interest or incentives that may impact the objectivity of the source's findings, such as partnerships with cybersecurity vendors or regulatory agencies.

Mitigation Recommendations:

* *APT Group X:*
  + Implement proactive security measures, such as email filtering, endpoint detection and response (EDR), and network segmentation, to mitigate the risk of spear-phishing and lateral movement by APT Group X.
  + Enhance employee awareness and training programs to recognize and report suspicious activities indicative of APT campaigns, such as unusual email attachments or unauthorized access attempts.
  + Establish incident response protocols and threat hunting capabilities to detect and contain APT Group X's activities before significant damage occurs.
* *Ransomware Variant Y:*
  + Strengthen cybersecurity defenses with robust backup and recovery solutions, regularly backing up critical data to offline or immutable storage to mitigate the impact of ransomware attacks.
  + Implement endpoint security controls, such as application whitelisting, privilege management, and behavior-based detection, to prevent the execution of ransomware payloads and limit lateral movement.
  + Develop and rehearse ransomware response plans, including communication strategies, legal considerations, and coordination with law enforcement and incident response partners, to facilitate a timely and effective response to ransomware incidents.

***Week4\_deliverables\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

#### **Tool Selection: Zeek**

*Zeek (formerly known as Bro) is an open-source network analysis framework that provides a powerful platform for network traffic analysis. Its scripting language allows for the creation of custom scripts to extract and analyze data from network packets.*

#### Basic Functionalities of Zeek:

* Packet Capture: Zeek captures network traffic in real-time and logs it for analysis.
* Protocol Analysis: It dissects various network protocols and extracts metadata such as IP addresses, ports, and protocols.
* Signature-Based Detection: Zeek can detect known threats by matching patterns or signatures in network traffic.
* Custom Scripting: Users can write custom scripts to perform specific analysis tasks or to extend Zeek's capabilities.
* Metadata Extraction: Zeek extracts rich metadata from network traffic, enabling deeper analysis of network activity.

#### **Threat Analysis Templates:**

* *Threat Details Template:*
  + Threat Name
  + Threat Actor(s)
  + TTPs (Tactics, Techniques, and Procedures)
  + Indicators of Compromise (IOCs)
  + Impact Analysis
* *Analysis Template:*
  + MITRE ATT&CK Matrix Mapping
  + Tactics and Techniques Used
  + Tools and Malware Involved
  + Timeline of Events
  + Vulnerabilities Exploited
* *Mitigation Recommendations Template:*
  + Immediate Actions
  + Short-Term Remediation
  + Long-Term Prevention Strategies
  + Security Controls Enhancement