**WEEK 1 ASSIGNMENT**

1. What is the main goal of a security operations center (SOC)?
   1. To prevent security breaches and attacks
   2. To detect and respond to security incidents
   3. To implement security controls
   4. All of the above
2. What is the term for the process of identifying and responding to security threats and incidents?
   1. Vulnerability assessment
   2. Risk management
   3. Incident response
   4. Penetration testing
3. What is the name of the framework that outlines best practices for incident response management?
   1. NIST
   2. SANS
   3. ISO
   4. COBIT
4. Which of the following is a type of malware that infects a computer system and allows an attacker to control the system remotely?
   1. Virus
   2. Worm
   3. Trojan
   4. Spyware
5. What is the term for the unauthorized access to, or theft of, sensitive information?
   1. Phishing
   2. Spoofing
   3. Social engineering
   4. Data breach
6. What is the process of verifying the identity of a user before granting access to sensitive information or systems called?
   1. Authentication
   2. Authorization
   3. Encryption
   4. Digital signature
7. What is the term for a security control that helps prevent unauthorized access to systems and data?
   1. Firewall
   2. Intrusion detection system
   3. Access control
   4. Antivirus software
8. Which of the following is a type of attack that seeks to disrupt the availability of a website or online service?
   1. DDoS
   2. SQL injection
   3. Cross-site scripting
   4. Buffer overflow
9. What is the difference between false positive and negatives?

**WEEK 2 ASSIGNMENT**

1. What is Cyber defense framework and what are the processes in protecting organizational assets.
2. What is OSINT?
3. What is Email Harvesting?
4. What are some of the tool’s attacker can user for Reconnaissance?
5. Define attack surface and Attack Vector
6. What is the difference between Threat, Risk and Vulnerability?
7. Define a Malware and give 3 examples of malware and how would you mitigate a malware?
8. What is Cyber Kill chain and define the stages of Cyber Kill Chain?
9. What is Diamond Kill chain and what are the component included in each stage?
10. Define MITRE Attack and state all the stages involve with MITRE Attack
11. Define Unified Kill Chain and what are the benefits over other kill chains?
12. What is the name of the attack phase where an attacker employs techniques to evade detection?
13. Explain the Pyramid of Pain and how does that affect your network.
14. What Cyber attack have you defend before?
15. This term is referred to as a group of commands that perform a specific task. You can think of them as subroutines or functions that contain the code that most users use to automate routine tasks. But malicious actors tend to use them for malicious purposes and include them in Microsoft Office documents. Can you provide the term for it?
16. A malicious code that the attacker runs on the system is called what?
17. Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. What is the technique called?
18. What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker?

**WEEK 3 ASSIGNMENT**

1. What is Cyber threat Intelligence and how do you gather your information using OSINT tools?
2. Name some of the OSINT Tools available in gathering information.
3. Explain Threat Intel Classification and give examples of each control related to each intelligence.
4. Identify malware tools and explain how is used to mitigate alerts.
5. Give examples of network tools and endpoint tools.
6. Explain the difference between IDS/IPS]
7. Where do you get your cyber news and updates from?
8. Visit: <https://www.cisa.gov> and analyst current event and list recommended updates from CISA and FBI.
9. Explain Cyber Threat lifecycle:

Assuming Outbreak: FortiGate detected CISA Top 20 Vulnerability on Private Network. Use playbook to determine whether your organization is vulnerable to this attack.

**WEEK 4 ASSIGNMENT**

1. Define a network and the Peripheral within a network.
2. Give an example of network tools and how would you analyze network traffic.
3. What are network controls?
4. Which protocol is used for remote access to network devices?

a) RDP

b) SSH

c) ICMP

d) DNS

1. Which of the following is NOT a common network scanning tool?

a) Nmap

b) Wireshark

c) Angry IP Scanner

d) Netcat

1. Which layer of the OSI model is responsible for ensuring data integrity and flow control?

a) Physical

b) Data Link

c) Transport

d) Application

1. What is the difference between access control and threat control?
2. What is a VPN and what some of the benefits of VPN?
3. What is OSI Model and explain each step of the OSI Model?
4. What is Network Analysis and the benefits of Network Analysis?

**WEEK 5 ASSIGNMENT**

1. What is endpoint Security?
2. Can you explain how endpoint security works?
3. What are some common use cases for endpoint security?
4. What are the advantages of using endpoint security over other types of network security?
5. What are the different components that make up an endpoint security solution?
6. How can an endpoint security solution be configured to prevent users from downloading malware or viruses onto their workstations?
7. What is meant by “whitelisting”?
8. What are some examples of malicious behavior that an endpoint security solution might detect?
9. What is two-factor authentication?
10. What is an IPSec VPN tunnel?

**WEEK 6 ASSIGNMENT**

1. What is SIEM and what are some of the importance of having SIEM in your network?
2. Name some vendors with SIEM
3. What some of the role of SIEM for businesses?
4. What does SIEM stand for?

A) Security Information and Event Monitoring

B) Security Information and Event Management

C) Security Incident and Event Management

D) Security Incident and Event Monitoring

1. Name some of the Protocols for network centric?
2. What are some capabilities of SIEM?
3. Which of the following is NOT a primary function of a SIEM system?

A) Collecting security-related data from various sources

B) Correlating and analyzing security-related events

C) Providing intrusion detection and prevention capabilities

D) Performing vulnerability assessments

1. Which of the following is NOT a typical data source for a SIEM system?

A) Network devices (routers, switches, firewalls)

B) Servers (Windows, Linux, Unix)

C) Databases (Oracle, SQL Server)

D) Social media platforms (Facebook, Twitter)

1. What is the purpose of correlation rules in a SIEM system?

A) To detect security incidents by correlating related events from different sources

B) To determine the root cause of security incidents

C) To identify vulnerabilities in the network

D) To generate reports on security-related activities

1. What is the benefit of using a SIEM system for threat detection and response?

A) Faster incident response times

B) Improved accuracy of threat detection

C) Reduced false positive alerts

D) All of the above

1. What are some capabilities of SIEM?

**WEEK 7 ASSIGNMENT**

1. What is phishing and how would you define it?
2. Name types of phishing and how phishing email gets on your network.
3. How do you analyze phishing email?
4. How do you prevent phishing email?
5. What is DMARC, DKIM and SPF?
6. What are some protocols for email?
7. An email from your boss asks for the name, addresses, and credit card information of the company’s top clients. The email says it’s urgent and to please reply right away. You should reply right away. True or False?
   1. True
   2. False
8. You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:
   1. Reply to the text to confirm that you really need to renew your password.
   2. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.
   3. Click on the link. If it takes you to the vendor’s website, then you’ll know it’s not a scam.
9. Email authentication can help protect against phishing attacks. True or False?
   1. True
   2. False
10. If you fall for a phishing scam, what should you do to limit the damage?
    1. Delete the phishing email.
    2. Unplug the computer. This will get rid of any malware.
    3. Change any compromised passwords.