**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

What is the difference between false positive and negatives?