Professional Certificate in Geopolitical Risk Assessment

Security Threats and Vulnerabilities

Security Threats and Vulnerabilities Glossary

1. Adversary:
An individual, group, or entity that poses a threat or challenge to an organization's security. Adversaries can be external, such as hackers or terrorist organizations, or internal, such as disgruntled employees.

2. Backdoor:
A hidden or undocumented means of accessing a computer system or network, often created by malicious actors to gain unauthorized access.

3. Cyber Attack:
A deliberate attempt to compromise the confidentiality, integrity, or availability of information systems or data, typically carried out through digital means.

4. Data Breach:
An incident in which sensitive, confidential, or protected information is accessed, disclosed, or stolen without authorization, often resulting in harm to individuals or organizations.

5. Encryption:
The process of converting plaintext data into ciphertext to protect it from unauthorized access. Encryption is used to secure sensitive information and communication.

6. Firewall:
A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls help prevent unauthorized access to or from a private network.

7. Insider Threat:
A security risk posed by individuals within an organization who have legitimate access to systems and data but misuse their privileges for malicious purposes.

8. Malware:
Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Common types of malware include viruses, worms, trojans, and ransomware.

9. Phishing:
A type of cyber attack in which attackers impersonate legitimate entities to trick individuals into revealing sensitive information, such as passwords or financial data.

10. Ransomware:
A type of malware that encrypts a victim's files or locks them out of their system until a ransom is paid.

Ransomware attacks can cause significant financial and operational damage to organizations.

11. Social Engineering:
The use of psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise security. Social engineering attacks often exploit human vulnerabilities rather than technical flaws.

12. Threat Actor:
An individual or group responsible for carrying out malicious activities, such as cyber attacks or physical security breaches. Threat actors can be motivated by financial gain, political goals, or other reasons.

13. Vulnerability:
A weakness or flaw in a system, application, or network that could be exploited by attackers to compromise security. Vulnerabilities can arise from software bugs, misconfigurations, or human error.

14. Zero-day Exploit:
A cyber attack that targets a previously unknown vulnerability in software or hardware. Zero-day exploits are particularly dangerous because they can be used before a patch or update is available to fix the vulnerability.

15. Access Control:
The process of regulating who can access specific resources or information within an organization. Access control mechanisms include passwords, biometrics, and security tokens.

16. Authentication:
The process of verifying the identity of a user or system before granting access to resources. Authentication methods include passwords, smart cards, and biometric scans.

17. Biometrics:
Authentication techniques that use physiological or behavioral characteristics, such as fingerprints, facial recognition, or voice patterns, to verify a person's identity.

18. Denial of Service (DoS):
An attack that disrupts the availability of a service, system, or network by overwhelming it with a high volume of traffic or requests. DoS attacks can render a website or online service inaccessible to legitimate users.

19. Encryption Key:
A unique code or algorithm used to encrypt and decrypt data. Encryption keys are essential for securing sensitive information and ensuring confidentiality.

20. Incident Response:
The process of responding to and managing security incidents, such as data breaches, cyber attacks, or physical security breaches. Incident response aims to contain the incident, mitigate its impact, and restore normal operations.

21. Multi-factor Authentication:
An authentication method that requires users to provide two or more forms of verification before accessing a system or resource. Multi-factor authentication enhances security by adding an extra layer of protection against unauthorized access.

22. Patch Management:
The process of applying software updates, patches, and fixes to address security vulnerabilities and improve system performance. Patch management is essential for keeping systems secure and up-to-date.

23. Risk Assessment:
The process of identifying, analyzing, and evaluating potential risks to an organization's security. Risk assessments help organizations understand their security posture and prioritize mitigation efforts.

24. Security Policy:
A set of rules, guidelines, and procedures that define an organization's approach to security. Security policies outline expectations for employees, protect sensitive information, and ensure compliance with regulations.

25. Threat Intelligence:
Information about potential security threats, vulnerabilities, and adversaries that can help organizations anticipate and mitigate risks. Threat intelligence sources include security reports, threat feeds, and analysis of emerging threats.

26. Virtual Private Network (VPN):
A secure network connection that allows users to access the internet privately and securely. VPNs encrypt traffic and mask users' IP addresses to protect their privacy and security online.

27. Web Application Firewall (WAF):
A security solution that monitors and filters HTTP traffic between web applications and the internet. WAFs protect web applications from common threats, such as SQL injection, cross-site scripting, and DDoS attacks.

28. Zero Trust Security:
A security model that assumes no trust in users, devices, or networks, and verifies every access request before granting entry. Zero trust security aims to prevent unauthorized access and limit the impact of security breaches.

29. Advanced Persistent Threat (APT):
A sophisticated and targeted cyber attack carried out by a well-funded and organized group over an extended period. APTs often use multiple attack vectors to compromise high-value targets.

30. Botnet:
A network of compromised computers or devices controlled by a remote attacker to carry out malicious activities, such as DDoS attacks, spam campaigns, or data theft. Botnets can be used to launch large-scale cyber attacks.

31. Cross-Site Scripting (XSS):
A type of web vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. XSS attacks can steal sensitive information or execute unauthorized actions on behalf of the user.

32. Distributed Denial of Service (DDoS):
An attack that uses multiple compromised devices to flood a target system or network with traffic, causing a disruption in service. DDoS attacks can overwhelm servers and lead to downtime for websites or online services.

33. Encryption Algorithm:
A mathematical formula used to encrypt and decrypt data, ensuring confidentiality and integrity. Encryption algorithms include symmetric encryption (e.g., AES) and asymmetric encryption (e.g., RSA).

34. Firewall Rule:
A set of criteria that determines whether network traffic should be allowed or blocked by a firewall. Firewall rules are configured to enforce network security policies and protect against unauthorized access.

35. Incident Response Plan:
A documented set of procedures and protocols for responding to security incidents. Incident response plans outline roles and responsibilities, communication strategies, and steps to contain and mitigate the impact of an incident.

36. Keylogger:
A type of malware that records keystrokes on a computer or device, capturing sensitive information such as passwords, credit card numbers, or personal messages. Keyloggers are often used by cybercriminals to steal data.

37. Network Security:
The practice of securing networks from unauthorized access, data breaches, and cyber attacks. Network security measures include firewalls, intrusion detection systems, and encryption protocols.

38. Penetration Testing:
A security assessment conducted by ethical hackers to identify vulnerabilities in a system or network. Penetration testing simulates real-world attacks to test the effectiveness of security controls and measures.

39. Security Awareness Training:
Educational programs designed to raise awareness about security threats, best practices, and policies among employees. Security awareness training helps reduce human error and improve overall security posture.

40. Threat Hunting:
The proactive search for security threats within an organization's network or systems. Threat hunting involves analyzing logs, traffic patterns, and behavior anomalies to detect and respond to potential threats before they escalate.

41. Virtualization Security:
Security measures designed to protect virtualized environments, such as virtual machines, containers, or cloud platforms. Virtualization security safeguards against threats that target virtualized infrastructure.

42. Antivirus Software:
A security program that detects, prevents, and removes malware from computers and devices. Antivirus software scans files, emails, and web traffic for malicious content to protect against infections.

43. Blockchain Technology:
A decentralized and secure digital ledger that records transactions across a network of computers. Blockchain technology uses cryptographic techniques to ensure data integrity and prevent tampering.

44. Cryptography:
The practice of securing communication and data through encryption and decryption techniques. Cryptography protects sensitive information from unauthorized access and ensures confidentiality and integrity.

45. Data Loss Prevention (DLP):
A set of tools and policies that prevent sensitive data from being lost, stolen, or exposed. DLP solutions monitor and control data transfers to enforce security policies and compliance regulations.

46. Endpoint Security:
Security measures that protect endpoints, such as computers, mobile devices, and servers, from security threats. Endpoint security solutions include antivirus software, firewalls, and intrusion detection systems.

47. Incident Response Team:
A dedicated group of professionals responsible for responding to security incidents within an organization. Incident response teams coordinate efforts to contain, investigate, and recover from security breaches.

48. Least Privilege:
The principle of granting users the minimum level of access required to perform their duties. Least privilege reduces the risk of unauthorized access and limits the impact of security incidents.

49. Network Segmentation:
The practice of dividing a network into separate segments or subnetworks to improve security and performance. Network segmentation isolates sensitive data and restricts access to critical resources.

50. Public Key Infrastructure (PKI):
A system of digital certificates, public and private keys, and registration authorities used to secure communication and verify the authenticity of users. PKI enables secure encryption, authentication, and digital signatures.

51. Security Incident:
An event that compromises the confidentiality, integrity, or availability of information systems or data. Security incidents require a response to contain the impact and prevent further damage.

52. Threat Landscape:
The current state of security threats, vulnerabilities, and risks facing organizations. The threat landscape is dynamic and continuously evolving, requiring organizations to adapt their security measures accordingly.

53. Vulnerability Assessment:
A systematic evaluation of systems, applications, or networks to identify and prioritize security vulnerabilities. Vulnerability assessments help organizations understand their risk exposure and take corrective actions.

54. Zero-Day Vulnerability:
A previously unknown security flaw in software or hardware that is exploited by attackers before a patch or update is available. Zero-day vulnerabilities pose a significant risk to organizations until a fix is released.

55. Access Control List (ACL):
A list of permissions that define who can access specific resources or perform certain actions within a system or network. ACLs are used to enforce access control policies and restrict unauthorized activities.

56. Botnet Attack:
A coordinated attack launched by a network of compromised devices under the control of a malicious actor. Botnet attacks can overwhelm servers, disrupt services, and steal sensitive information.

57. Cybersecurity Framework:
A structured set of guidelines, best practices, and controls to help organizations manage and improve their cybersecurity posture. Cybersecurity frameworks provide a roadmap for implementing security measures and mitigating risks.

58. Digital Forensics:
The process of collecting, preserving, and analyzing digital evidence to investigate security incidents or cyber crimes. Digital forensics techniques help identify culprits, reconstruct events, and support legal proceedings.

59. Encryption Key Management:
The process of generating, storing, distributing, and revoking encryption keys to ensure data security and confidentiality. Encryption key management is critical for protecting sensitive information.

60. Incident Response Plan Testing:
A practice of validating and improving an organization's incident response plan through simulations, tabletop exercises, or drills. Incident response plan testing helps identify gaps, refine procedures, and build readiness for security incidents.

61. Man-in-the-Middle (MitM) Attack:
A type of cyber attack in which an attacker intercepts and alters communication between two parties without their knowledge. MitM attacks can steal sensitive information, manipulate data, or impersonate legitimate entities.

62. Network Security Monitoring:
The continuous monitoring of network traffic, devices, and systems for security threats and anomalies. Network security monitoring helps detect suspicious activities, prevent breaches, and respond to incidents promptly.

63. Password Policy:
A set of rules and requirements for creating, managing, and storing passwords securely. Password policies enforce strong password practices to protect user accounts and prevent unauthorized access.

64. Security Incident Response Team (SIRT):
A specialized team responsible for managing and responding to security incidents within an organization. Security incident response teams coordinate efforts to contain, investigate, and recover from security breaches.

65. Threat Actor Attribution:
The process of identifying and attributing cyber attacks to specific individuals, groups, or entities. Threat actor attribution helps understand motives, tactics, and potential future threats.

66. Vulnerability Management:
The process of identifying, prioritizing, and remediating security vulnerabilities in systems, applications, or networks. Vulnerability management helps minimize risk exposure and strengthen security defenses.

67. Zero Trust Architecture:
A security model that assumes no trust in users, devices, or networks and verifies every access request before granting entry. Zero trust architecture focuses on continuous authentication, strict access controls, and least privilege principles.

68. Application Security:
The practice of securing software applications from security threats, vulnerabilities, and attacks. Application security measures include secure coding practices, penetration testing, and secure development lifecycles.

69. Cyber Threat Intelligence:
Actionable information about potential cyber threats, adversaries, and vulnerabilities that can help organizations proactively defend against security risks. Cyber threat intelligence informs security strategies, decision-making, and incident response.

70. Data Encryption Standard (DES):
A symmetric encryption algorithm used to secure data and communication. DES is a block cipher that encrypts data in 64-bit blocks using a 56-bit key.

71. Endpoint Detection and Response (EDR):
A security solution that monitors and responds to threats on endpoints, such as computers, mobile devices, and servers. EDR tools detect suspicious activities, investigate incidents, and contain security breaches.

72. Firewall Configuration:

The process of setting up and managing firewall rules, policies, and settings to protect networks from unauthorized access and cyber threats. Firewall configuration ensures proper traffic filtering and access control.

73. Incident Response Playbook:
A documented set of predefined procedures, guidelines, and checklists for responding to specific security incidents. Incident response playbooks help streamline response efforts, ensure consistency, and improve incident handling.

74. Key Management Service (KMS):
A cloud-based service that provides secure storage, generation, and management of encryption keys for cloud applications and services. KMS helps organizations protect sensitive data and comply with security requirements.

75. Network Security Architecture:
The design and implementation of security controls, protocols, and measures to protect network infrastructure from cyber threats. Network security architecture includes firewalls, intrusion detection systems, and access controls.

76. Physical Security:
Measures designed to protect physical assets, facilities, and resources from unauthorized access, theft, or damage. Physical security includes access control systems, surveillance cameras, and security guards.

77. Security Incident Response Plan:
A documented strategy outlining the steps, roles, and responsibilities for responding to security incidents within an organization. Security incident response plans help organizations coordinate efforts and minimize the impact of incidents.

78. Threat Hunting Team:
A specialized group of cybersecurity professionals responsible for proactively searching for security threats within an organization's network or systems. Threat hunting teams analyze data, investigate anomalies, and respond to potential threats.

79. Virtual Private Network Service:
A subscription-based service that provides secure and private network connections over the internet. VPN services encrypt traffic, hide users' IP addresses, and protect online privacy and security.

80. Web Application Security:
Measures designed to protect web applications from security threats, vulnerabilities, and attacks. Web application security includes secure coding practices, vulnerability scanning, and web application firewalls.

81. Advanced Encryption Standard (AES):
A widely used symmetric encryption algorithm that secures data and communication. AES encrypts data in fixed-size blocks using keys of 128, 192, or 256 bits for strong security.

82. Behavioral Analytics:
The use of machine learning and artificial intelligence to analyze user behavior and detect anomalies that may indicate security threats. Behavioral analytics help identify insider threats, account takeovers, and suspicious activities.

83. Cyber Threat Hunting:
A proactive approach to identifying and mitigating security threats within an organization's network or systems. Cyber threat hunting involves analyzing data, logs, and patterns to detect and respond to potential threats.

84. Data Encryption Key:
A cryptographic key used to encrypt and decrypt data securely. Data encryption keys protect sensitive information from unauthorized access and ensure confidentiality during transmission and storage.

85. Endpoint Security Solution:
Software or hardware tools that protect endpoints, such as computers, mobile devices, and servers, from security threats. Endpoint security solutions include antivirus software, firewalls, and intrusion prevention systems.

86. Incident Response Automation:
The use of automated tools and processes to streamline and accelerate the response to security incidents. Incident response automation helps organizations detect, contain, and mitigate threats more effectively.

87. Key Management System:
A centralized platform or service that manages encryption keys and cryptographic operations across an organization. Key management systems ensure secure key storage, distribution, and lifecycle management.

88. Network Security Controls:
Hardware or software mechanisms that enforce security policies and protect network infrastructure from cyber threats. Network security controls include firewalls, access control lists, and intrusion detection systems.

89. Security Incident Response Process:
A series of steps and actions taken to detect, investigate, and respond to security incidents within an organization. The security incident response process aims to contain and mitigate the impact of security breaches.

90. Threat Intelligence Sharing:
The practice of exchanging information about security threats, vulnerabilities, and indicators of compromise among organizations, industry sectors, or government agencies. Threat