Professional Certificate in Enterprise Security Architecture

Security Principles and Models

Security Principles and Models Glossary

Access Control:
Access control is a security measure that determines who is allowed to access a resource or perform a certain action. It involves authentication, authorization, and auditing to ensure only authorized users can access specific resources.

Authentication:
Authentication is the process of verifying the identity of a user or entity. This can be done through something the user knows (password), something the user has (smart card), or something the user is (biometric data).

Authorization:
Authorization is the process of determining what actions a user is allowed to perform after they have been authenticated. It involves setting permissions and privileges based on the user's role or identity.

Availability:
Availability is a security principle that ensures systems, services, and data are accessible when needed. This involves implementing redundancy, failover mechanisms, and disaster recovery plans to prevent downtime.

Confidentiality:
Confidentiality is a security principle that ensures sensitive information is only accessed by authorized users. This involves encryption, access controls, and data masking to protect data from unauthorized disclosure.

Cryptography:
Cryptography is the practice of encrypting and decrypting data to secure it from unauthorized access. It involves algorithms and keys to encode and decode information in a secure manner.

Defense in Depth:
Defense in depth is a security strategy that involves implementing multiple layers of security controls to protect against threats. This can include firewalls, intrusion detection systems, and encryption to create a robust security posture.

Encryption:
Encryption is the process of converting plaintext data into ciphertext to protect it from unauthorized access. It uses algorithms and keys to scramble data, making it unreadable without the correct decryption key.

Firewall:
A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks.

Identity and Access Management (IAM):
Identity and Access Management (IAM) is a framework of policies and technologies that ensure the right individuals have access to the right resources at the right time. It involves managing user identities, roles, and permissions to enforce security policies.

Intrusion Detection System (IDS):
An Intrusion Detection System (IDS) is a security technology that monitors network or system activities for malicious activities or policy violations. It can detect anomalies and raise alerts to notify security personnel of potential threats.

Least Privilege:
Least Privilege is a security principle that states that users should only be granted the minimum level of access required to perform their job functions. This limits the impact of a security breach by reducing the number of resources a compromised user can access.

Multi-factor Authentication (MFA):
Multi-factor Authentication (MFA) is a security method that requires users to provide two or more forms of verification before gaining access to a system. This can include something the user knows (password), something the user has (smart card), or something the user is (biometric data).

Network Segmentation:
Network Segmentation is the practice of dividing a network into smaller subnetworks to improve security. It limits the spread of threats and reduces the attack surface by isolating critical systems and data from less secure areas.

Penetration Testing:
Penetration Testing is a security assessment method that simulates real-world cyber attacks to identify vulnerabilities in a system. It involves ethical hackers attempting to exploit weaknesses to provide recommendations for remediation.

Principle of Least Privilege:
The Principle of Least Privilege is the practice of granting users the minimum level of access required to perform their job functions. This helps reduce the risk of unauthorized access and limits the impact of a security breach.

Risk Assessment:
Risk Assessment is the process of identifying, analyzing, and evaluating potential risks to an organization's

assets. It involves assessing the likelihood and impact of threats to determine the level of risk and prioritize security measures.

Risk Management:
Risk Management is the process of identifying, assessing, and mitigating risks to an organization's assets. It involves implementing security controls, policies, and procedures to reduce the likelihood and impact of threats.

Security Architecture:
Security Architecture is the design of a secure framework that outlines the organization's security controls, policies, and procedures. It involves defining security requirements, implementing security solutions, and aligning them with business objectives.

Security Controls:
Security Controls are safeguards or countermeasures that are put in place to protect an organization's assets. They can be technical, administrative, or physical controls that mitigate risks and enforce security policies.

Security Incident Response:
Security Incident Response is the process of detecting, analyzing, and responding to security incidents in a timely manner. It involves containing the incident, investigating the root cause, and implementing measures to prevent future incidents.

Security Model:
A Security Model is a framework that describes how security mechanisms are implemented to protect information and resources. It defines the rules, policies, and procedures that govern access control, authentication, and encryption.

Security Policy:
A Security Policy is a set of rules and guidelines that define how an organization protects its assets and enforces security controls. It outlines the requirements, responsibilities, and procedures for securing information and technology.

Security Posture:
Security Posture refers to an organization's overall security readiness and resilience to cyber threats. It includes the effectiveness of security controls, policies, and procedures in mitigating risks and protecting assets.

Security Principles:
Security Principles are fundamental guidelines and best practices that govern how security measures are implemented. They include confidentiality, integrity, availability, and accountability to ensure data and resources are protected from unauthorized access.

Security Risk Assessment:
Security Risk Assessment is the process of evaluating potential threats and vulnerabilities to an organization's assets. It involves identifying risks, analyzing their impact, and implementing controls to mitigate the likelihood of security incidents.

Security Risk Management:
Security Risk Management is the process of identifying, assessing, and mitigating risks to an organization's assets. It involves prioritizing risks, implementing controls, and monitoring for threats to maintain a secure environment.

Security Threat:
A Security Threat is a potential danger or risk to an organization's assets. It can come in various forms, such as malware, phishing attacks, or data breaches, and can exploit vulnerabilities to compromise security.

Single Sign-On (SSO):
Single Sign-On (SSO) is a user authentication process that allows users to access multiple applications with a single set of credentials. It simplifies the login process, improves user experience, and enhances security by reducing the number of passwords users need to remember.

Threat Modeling:
Threat Modeling is the process of identifying potential threats to an organization's assets and assessing their likelihood and impact. It involves analyzing vulnerabilities, attack vectors, and mitigating controls to reduce risk.

Vulnerability Assessment:
Vulnerability Assessment is the process of identifying weaknesses in an organization's systems, applications, or networks. It involves scanning for vulnerabilities, analyzing their impact, and prioritizing remediation to prevent exploitation by attackers.

Zero Trust Security Model:
Zero Trust Security Model is a security approach that assumes no entity, whether inside or outside the network, can be trusted. It requires strict access controls, continuous monitoring, and least privilege to protect against insider threats and external attackers.