

Mod 1

What you'll learn

- CISSP's eight security domain
- Security framework and controls
- Security audits
- Basic security tools
- Protect assets and data

Overview

Security domain : You will gain understanding of CISSP's eight security domains. Then, you'll learn about primary threats, risks and vulnerabilities to business operations. In addition you'll learn national institute of standards and technology Risk management framework and the steps of risk management.

Security framework and Controls : Security framework and Control.

- Core component and confidentiality integrity and availability (CIA) triad
- Open Web Application Security Project (OWASP) security principles and audit.

DATE / /
PAGE

Introduction to cybersecurity tools : Industry leading security information and event management (SIEM) tools

- How to use SIEM dashboard as part of their every day work.

Use playbook to respond to incidents : How common use of playbooks.

- Use by cybersecurity professional use playbooks identified threat, risk and vulnerability.

CISSP domains

Intro : CISSP's eight security domains

- Threat, risk and vulnerability
- Layers of web
- NIST Risk Management Framework

Security Posture : An organization's ability to manage its defense of critical assets and data, and react to change

Security and risk management (Domain)

Focused on defining security goals and objectives, risk mitigation, compliance, business continuity and legal regulation.

Risk mitigation : The process of having the right procedure and rules in place to quickly reduce the impact of a risk like a breach

Business Continuity : An organization ability to maintain their everyday productivity by establishing risk disaster recovery plan.

Asset security : Focused on securing digital and physical assets. It's also related to the storage, maintenance retention and destruction of data

Security arch and eng. : Focused on optimizing data security by ensuring effective tools, system and process are in place to protect an org. assets and data

Shared responsibility : All individual within an org. take on active role in lowering risk and maintaining both physical and virtual security

Raj
DATE / /
PAGE

Communication and network security :

Focused on managing various physical network and wireless communication

Identity and access management : Focused on access and authorization to keep data secure, by making sure users follow established policies to control and manage assets.

Components :

- Identification
- Authentication
- Authorization
- Accountability

Security Assessment and Testing : Focuses on conducting security control testing. Collecting and analyzing data and conducting security audit to monitor for risks, threat and vulnerability.

Security operation : Focused on conducting investigation and implementing preventative measures

Software development security : Focuses on using secure coding practices

Threats, risks and vulnerabilities

Threat : Any circumstance or event that can negatively impact assets

Social eng. attack : A manipulation technique that exploits human error to gain private info., access, or valuables

Risks : Anything that can impact the confidentiality, integrity or availability of an asset

Low risks assets : Information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised

Medium Risk assets : Info that is not available to public and may cause some damage to the org. finances, rep. or ongoing operation

High Risk assets : Info protected by regulation or laws which if compromised would have a severe negative impact on an organizations finances ongoing operation or reputation

Vulnerability : A weakness that can be exposed exploited by a threat

Key impact

Ransomware : A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

Layers : • Surface web
• Deep web
• Dark web

- Financial impact
- Identity theft
- Reputation

Nist

RMF (Risk Management Framework) before

- Prepare : Activity that are necessary to manage sec and privacy
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

- 1 Prepare : Activity that are necessary to manage sec and privacy risk before a breach occur.
- 2 Categorize : Used to develop risk management processes and tasks

- 3 Select: Choose, customize and capture documentation of the control that protect an organization
- 4 Implement: security and privacy plans for the organization
- 5 Assess: Determine if established controls are implemented correctly
- 6 Authorize: Being accountable for the security and privacy risks that may exist in an organization
- 7 Monitor: Be aware of how system are operating

What we Covered

- CISSP's eight security domain
- Threat, risk and vulnerability
- Layers of web
- NIST - RMF