Bilal Ahmed Khan
20K0183
Sec:B

Date: _____

How to manage security risks and threats | Google Cyber Security Certificate

→ CISSP has 8 security domains which organisations use to establish their security posture
→ Security & risk management is focused on defining security goals & objectives, risk mitigation & compliance
→ Asset Security focuses on physical & digital assets
→ Security Architecture & engineering focuses on optimizing data security by ensuring effective use of tools & systems
→ Communication & Network Security focuses on managing & securing physical ~~cloth~~ network or wireless communications
→ Security assessment & testing focuses on security control testing & security audits
→ Security operations focuses on conducting investigations & implementing security measures
→ Software development security focuses on using secure coding practices

- Threat is any circumstance or event that can negatively impact assets
- Social engineering is an exploitative technique which targets human error to gain private information. (Mid-risk asset/high-risk asset)
- Ransomware is a kind of malware
- web layers 1) surface web 2) deep web 3) dark web
- NIST RMF framework for managing risks threats & vulnerabilities
- 1) Prepare 2) Categorize 3) Select 4) Implement 5) Assess 6) Authorize 7) monitor

Date:

→ Security frameworks provides methods to mitigate risks & improve security
→ authentication & encryption can be used to protect user data.
→ CIA triad helps organisations in mitigating risks when setting up system & security policies.
C: confidentiality I: integrity A: Authenticity
- NIST CSF (Cybersecurity Framework) is voluntary framework that consists of standards guidelines & best practices to manage cybersecurity risk
- OWASP (Open web Application Security Project) Principles are used to secure our web applications
• Minimize attack surface area • principle of least privilege
• defense in depth • separation of duties
• keep security simple • fix security issues correctly.
- Security audit is a review of an organization's security control, they may be internal or external
- An internal security audit may include establishing goals & scope + conducting risk assessment
- Logs (network, firewall & server logs) allow security analysts to analyse the security posture of an organization in a better way
- Security information & event management (SIEM) tool collects & analyses log data to monitor critical activities in an organization.

Date: _____

- SEIM tools help to minimize the no# of logs a security analyst has to manually review
- Metrics (availability, response time etc) are used to assess the performance of a software application
- SEIM tools may be • self hosted • cloud hosted or may be hybrid
- Some common SEIM tools
  • Splunk • Chronicle
- Phases of incident response playbook: Playbook is a manual that provides details about any operational actions
- Incident response is an organizations quick attempt to identify an attack & contain its damage & correct the effects
- It has the following phases 1) prepration 2) detection & analysis 3) Containment 4) eradication & recovery 5) Post incident activity

RMF steps

1) Categorize
2) Implement
3) Assess
4) Authorize
5) Select
6) Monitor