PROJECT BASED ON RISK ASSESSMENT AND THREAT MANAGEMENT

Date:

BASIL ALI KHAN
20K-0477

Video : How to Manage Security Risks and Threats | Google Cybersecurity Certificate.

The video by Ashley, customer engineering enablement lead for security operation sales at google provide a comprehensive detail of foundational principles in security operations, catering specifically to knowledge and skills required for aspiring entry level security analyst. Navigates through crucial topics aorting the CISSP's comprehensive eight security domains, offering understanding of areas such as risk assessment, asset security, security architecture, communication and network security, identity and access management, security assessment, security operations and Software development security. the course defines and explains the dynamics of threats and risk and vulnerabilities illustrating their impacts within Security frameworks. Video traverse through various scenarios explaining social engineering attacks, ransomware attacks, outdated software vulnerabilities and the human element in security compromises. Moreover it also elaborates on significant operational rectification of security incidents, also financial implications. identity theft concern and reputational damage that organization might face due to security breaches.

The video also unpacks the NIST risk management framework defining seven step approach :

prepare, categorize, select, implemat, assess, authorize, monitor

Date:

used for strategic management of security and privacy risks within organization structures. Also dissects dual component of security framework and control, explaining former as guiding principles instrumental in forming strict security plans while expounding latter as practical safeguards designed to mitigate risks. It digs deeper into examples highlighting key controls such as encryption, authentication and authorization and their role in fortifying security infrastructures. Also discusses CIA Triad as fundamentals principle in security management and their roles in data access control, data authenticity validation and ensuring authorized accessibility of data. It also covers an extensive range of cybersecurity topics It begins by explaining importance of security frameworks focusing NIST framework used worldwide The NIST Cybersecurity Framework (CSF) highlighted crucial voluntary framework comprising 5 core functions: identify, Protect, Detect, Respond, and Recover. Furthermore open wes application security principle (OWASP) emphasizing concepts like minimizing attack surface area least privileges, defence in depth, separation of duties, keeping security measure simples and addressing security issues effectively. It explain how these concepts & principles contribute to support security measure within organization complementing the use of framework and controls. Further explains on importance of these elements in identifying gaps within an organization security posture It also emphasizes value of conducting security audits

Date:

showing their role in improving security measure and their potential inclusion in professional portfolio.
Further explores security information and event management (SIEM) tools, delving into their function in collecting, analysing log data and creating dashboards. It describes how SIEM dashboards facilitate quick insights into security related data auditing analysts in monitoring, analyzing and responding to potential threats effectively. The final part focuse on different types of SEM tools such as self hosted, cloud hosted and hybrid solutions. Examples of widely used SEM tools like Splunk and chronicle are provided and their application in data analysis, log monitoring and real time security information managements
It starts by emphasizing importance of playbooks in cyber security. Playbooks are manuals that outline operational actions and are crucial for maintaining security by providing clarity on tools used in response to security incidents. They ensure urgency, efficiency and accuracy in addressing threats risk, or vulnerabilities identified within an organization. One particular type of playbook discussed is incidents playbook, fundamental in an organization quick identification, containment and resolution of security breaches. The playbook comprises six phases starting with preparation phase. Involves documenting procedures, defining roles, and educating personnel, establishing foundation for effective incident response. Second phase detection and analysis focuses on identifying and analyzing

Date:

vents. through defined process and technology
Containment, the third phase aims to prevent further
damage damage by taking immediate action to minimize
impact of incident. fourth phase eradication and recovery
~~forth A:~~ involves removing incident artifacts, eliminating
malicious code, and restoring affected system to a
secure state, ensuring a return to normal operations
Post incident activity, the fifth phase, involves documenting
informing leadership and implementing lessons learned to
fortify the organization's security posture. The final phase
coordination involves around reporting incidents and
sharing information based on established standards,
ensuring compliance and a coordination resolution process
It also stresses that incident detection can be through
SIEM tools such as which collect and analyze data
generating alerts that prompt security analysts to
use appropriate playbook. The steps involve assessing
alerts validity, containing the malware, eliminating traces
of incident and conducting post incident activities and
coordination. It's emphasized that playbooks are living
documents that evolve to address new threats,
vulnerabilities and improvement based on past incidents.
The importance of understanding playbooks and their utility
for entry level security analyst, especially in monitoring
networks and responding to incident is highlighted
Video covers CISSP security domains, security framework &
controls, CIA triad, NIST framework, security design principles
their relation to security audits, basic security tools

Date:

tools like SIEM dashboards and the protection of assets and detach through use of playbooks.

Video: Risk Management Framework (RMF) Overview

In video presented by Christian Espinosa, an expert from Alpine security, a comprehensive breakdown of Risk Management Framework (RMF) is provided focusing application within Department of defense and US Government. The RMF as explained is latest version of NIST 800-37 is presented as structured process comprising six main steps each discussed with clarity. In beginning video highlight the crucial overlooked step of preparation before going into actual RMF process. There are six essential steps of RMF, starting with the categorization of information system based fundamentals tenets of information security confidentiality, integrity and availability (CIA) emphasizing the importance of architecture description and organizational inputs this stage, it further elaborates on how these input contribute to the categorization process. underlying the role of system boundaries and the impact of law or directives in defining security categories. Furthermore it describes the selection of security controls, drawing from NIST 800-53 as foundational guide and stressing the importance of controls based on assessment and local conditions. Espinosa provides an example of a weapon system like a drone aircraft highlighting how controls may need

Date:

augmentation depending on diverse operational environments. The following steps implementing selected controls, assessing their effectiveness, and formally authorizing system operation after risk acceptance are methodically explained. Espino expressed the importance of documenting control implementation using NIST 800-53a for control assessment guidance and the necessity of a formal decision to authorize system operation based on assessed risks. It also emphasizes the role of continuous monitoring, a crucial overlooked aspect stressing dynamic nature of risk and the need to periodically reassess controls. Advocates for more frequent assessments for critical systems challenging the conventional ~~three~~ annual review cycle and support for adaptable and ongoing risks evaluation. Throughout video RMF is flexible framework rather than rigid regulation allowing decision on tailoring within the government or defense to implement it based on unique need and circumstances. ~~It~~ ~~provides~~ ~~big~~ ~~needed~~ ~~flexibility~~ Overall video emphasizes its adaptability and highlight crucial role in managing information system risk within government and defense sector.