



Example of Information Security Senior Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is looking to fill the role of information security senior. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for information security senior

- Understand security policies and procedures and assist in enforcing them
- Knowledge of moderately complex information system engineering concepts, practices, and procedures for the solution of technical system problems
- Determine security violations and inefficiencies by conducting periodic audits on accounts and workspaces
- Assist in the development and application of security patterns that would be applied to network, host, application, and data resources
- Work with business units in the implementation of security components and controls into the systems development lifecycle
- Implement Role Based Access Control to ensure compliance to internal policy and current regulatory laws
- Integrate existing access control mechanisms into enterprise authentication and access management toolsets
- Proven experience managing numerous projects and activities simultaneously ensuring the correct priorities are assigned and completed within the constraints of resources
- Proven ability to make decisions based on the given data in a timely fashion
- Configuration, management, and support of various network and host security systems and programs such as Data Loss Prevention (DLP) systems, network Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), Host Intrusion Prevention (H-IPS), Application Control, other associated security systems/environments

-
- Must have strong familiarity with various security solutions including SIEMs, firewalls, web proxies, anti-virus, and DLP working experience with an enterprise SIEM solution
 - Must possess a thorough understanding of network protocols, TCP/IP fundamentals
 - Must have working experience with packet capture and analysis
 - Must have experience working in a SOC and a knowledge of all related SOC processes, including incident response and digital forensics
 - Specialist in cyber threats including malware and advanced threats, with in-depth understanding of exploit and attack mechanisms at network and system level
 - Deep knowledge of information security principles, techniques and methodologies such as the SANS Top 20 Critical Security Controls and the OWASP Top 10