



Example of Security Service Engineer Job Description

Powered by www.VelvetJobs.com

Our growing company is looking to fill the role of security service engineer. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for security service engineer

- Although this is not an incident response position, we are a service delivery team
 - Partner with engineering, program management and operations personnel within the WDG Online Services community to suggest and implement security improvements to processes and technologies Although this is not an incident response position, we are a service delivery team
 - Manage risk to preserve and build revenue, brand, and shareholder value by identifying and assessing the security health of online services
 - Protect the confidentiality, integrity, and availability of online services by ensuring that hosting environments, services, and applications are secure
 - Protect, detect, and respond to malicious and criminal activity which threatens the trusted experience of our customers
 - Optimize policy and regulatory compliance management through the design, deployment, and testing of a control framework for audit control objectives and activities
 - Develop next generation operational security management tools which scale efficiently to support online services
 - Designing and producing software to meet the goals of the business expressed through requirements
 - Maintaining high standards for quality and security of software
 - Keeping our build automation pipeline fit for purpose
-

- Data dynamo - You are a data sleuth
- Pathfinder - You are a highly skilled and specialized tactician that can be inserted into any area of operation (development project)
- Customer focused - everyone is a customer, either current, or potential
- Hand-on experience with vulnerability management tools and devices
- 7+ years of proven expertise in common security monitoring technologies/platforms including Intrusion Detection Systems (IDS), Security Incident Event Management systems (SIEM), anti-virus log collection systems, data loss prevention (DLP) systems, host based integrity validation platforms, cloud scale forensic platforms for the purposes of comprehensive artifact collection and analysis
- Provide both architecture and project management ownership for the initial program the long term service