Position Title:

Security Operations Center (SOC) Analyst (Senior)

Job Description:

The SOC Analyst analyzes and manages information system security controls, protecting the network against unauthorized access, modification, destruction, or disclosure of data.

Company Description:

Example Aquariums Inc. is revolutionizing the world of luxury aquariums. We design, install, and maintain breathtaking underwater environments for high-end homes, businesses, and public spaces. Our team of marine biologists, engineers, and artists creates unique ecosystems that are both beautiful and technologically advanced.

	Traditional	Skills-first (Senior Analyst)	Skills-first (Entry-Level Analyst)
Required Certifications	CySA+ (Cybersecurity Analyst)	N/A *(Does not require certifications unless mandated by regulation or contract)*	N/A *(Does not require certifications unless mandated by regulation or contract)*
Required Years of Experience	5+ years of related experience in Cyber Security	N/A *(Does not list years of experience)*	N/A *(Does not list years of experience)*
Required Skills	Experience in security monitoring and incident detection Experience in SIEM tool configuration Experience in project management Ability to effectively communicate Ability to manage time effectively Excellent problem solving and negotiation skills	Use SIEM tools to perform detailed log analysis of network traffic for threat detection Perform light coding to create custom integrations between security tools (no formal developer training required) Organize, plan, and implement compliance-focused security events (e.g., tabletop exercises, phishing campaigns) Effectively document and communicate SOC data and areas of progress to non-technical and technical audiences. Troubleshoot and resolve operational issues during critical incidents, strictly following established timelines Reconcile competing priorities between internal and external teams during incident response or when implementing new security controls.	Use SIEM tools to analyze network traffic logs and detect potential security concerns, with guidance from senior analysts. Use basic scripting or coding knowledge to enhance security tool functionality, leveraging resources and templates provided by the team. Assist in the planning and execution of compliance-related security events, contributing to team efforts under supervision. Clearly document technical findings and security updates, collaborating with the team on how to best communicate this information to various audiences. Follow established procedures to troubleshoot and resolve basic operational issues during incidents, escalating complex problems to senior analysts. Support communication and coordination between internal and external teams during incidents or security control implementation, guided by senior analysts.
Preferred Certifications	CCSP (Certified Cloud Security Professional)	N/A *(Does not list certifications)*	N/A *(Does not list certifications)*
Preferred Skills	Experience in cloud architecture and security	Implement security controls (e.g., Identity and Access Management), encryption, and network segmentation within cloud platforms.	Assist in configuring and maintaining security controls (e.g., identity and access management, encryption, and network segmentation) within cloud platforms, under the supervision of senior team members.