

Job Title: SIEM Architecture Consultant
Status: Full-time Exempt
Location: Omaha

Reports to: Director Security Consulting Services
Direct Reports: None
Travel: < 50%

POSITION DESCRIPTION:

The SIEM Architecture Consultant will be responsible for customer-facing design of solutions, implementation and migration plans for Solutionary's ActiveGuard log monitoring and management platform. Paid engagements will include on-site and remote support in pre-implementation, deployment and ongoing phases.

POSITION RESPONSIBILITIES:

- Work with multiple clients to maximize security log monitoring programs utilizing ActiveGuard and other SIEM tools, including:
 - Understanding device, application and database log structures and data flow, to design and test log capture.
 - Interpret client risk and information security objectives to define effective security event types, prioritization and escalation procedures.
 - Understand, design and implement client reporting requirements.
- Assist clients in the development of information security strategies, frameworks and roadmaps.
- Interface with multiple Solutionary team members in Service Delivery Management, ActiveGuard Implementation Team, Information Security Engineering Team, Security Operations Center and Managed Device Team.
- Build multi-phase project plans and roadmaps for client and Solutionary requirements.
- Provide status reporting to client and Solutionary teams.

KNOWLEDGE, SKILLS AND ABILITIES:

- 5+ years in selection, implementation and operational experience with enterprise SIEM tools
- Previous security device installation, configuration and troubleshooting experience
- Previous multi-client consulting experience and interface with client IT management
- Knowledge of security models, industry best practices and generally accepted information security principles
- Understanding of privacy, regulatory and compliance issues and development of enterprise wide security management programs
- B.S., Information Technology or Information Security or equivalent work experience
- CISSP certification preferred
- Strong project management skills
- Excellent verbal and written communication skills
- Ability to formulate and communicate highly technical and complex security concepts to both technical and non-technical audiences in a clear and effective manner
- Ability to work well independently

WORKING ENVIRONMENT:

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this position. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

The noise level in the work environment is quiet.

PHYSICAL DEMANDS:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this position, the employee is constantly required to use hands to finger, handle or feel, talk or hear and occasionally required to stand, walk and sit. The employee may occasionally lift and/or move up to 10 pounds.

Specific vision abilities required by this job include close vision, distance vision, color vision and the ability to adjust focus.

Management retains the discretion to add or change the duties of the position at any time.