

Job Title: Information Security Engineer **Reports To:** ISET Senior Security Manager
Hours: Full Time **Direct Reports:** None
Status: Exempt **Travel:** 25%+

JOB DESCRIPTION:

The Information Security Engineer will focus on leveraging the ActiveGuard® service platform and security industry concepts for delivery of high quality managed security service to clients. Mastering and practicing continuous process improvement with implementation, escalated event resolution, troubleshooting and incident response are required areas of hands-on expertise.

JOB RESPONSIBILITIES:

- Work cooperatively with Service Delivery Managers, SOC, and other internal teams to establish and maintain a strong and supportive relationship with clients. Communicate effectively both internally and externally, and provide superior customer service throughout the lifecycle of the client.
- Proactively protect client systems and data through application of advanced security and technology knowledge, using the ActiveGuard platform and related products. Provide continuous managed security and service improvement oversight, and vigilance to possible new threats and the effects of infrastructure changes and vulnerabilities on the client's security status.
- Utilize escalated events and other tuning opportunities to optimize ActiveGuard and client configurations. Eliminate invalid events and increase the security value of the remaining events, reducing false positives and overall event volumes and assuring that events and alerts provide useful, actionable security event data to the client.
- Participate in assigned on-call and incident response activities as part of client security service delivery.
- Function in a technical QA and escalation capacity to support SOC staff and external clients on matters pertaining to Solutionary's service offerings and the digital security considerations of client systems.
- Engage in continuous tool improvement, process improvement and quality control and documentation activities to strengthen ActiveGuard and all phases of service delivery. Such activities may include participation in new hire training, rules creation and certification support, SCE mapping, helping design specifications for new reports or improved ActiveGuard functionality, etc.
- Other duties may be assigned

KNOWLEDGE, SKILLS AND ABILITIES:

- Three or more years experience in Information Security and/or technology engineering and support experience
- Demonstrated experience and expertise in one or more of the following areas: computer penetration testing, web security assessments, intrusion detection / prevention systems, firewalls, security event management.
- Ability to assess Information Security Risks, understand business needs, and apply defined information security policies and architectures in order to develop effective solutions
- Excellent interpersonal and organizational skills
- Excellent oral and written communication skills
- Strong analytical and problem solving skills
- Works well in a team environment and independently
- Certification in Information Security (GIAC, Security+, GSEC, GCIH, CEH, CISSP, etc.) a plus

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.