

Security Information / Event Management (SIEM) **Consultant – New York, NY**

PRINCIPALS ONLY – MUST LIVE WITHIN 30 MINUTES OF NYC

Job Description:

All candidates must have strong background in financial services and/or insurance in an enterprise level environment.

Vigilant is looking for experienced Security Consultants to join us in delivering innovative security services to our global customer base that includes some of the world's largest financial services firms.

SIEM Consultants will be responsible for the design and implementation of Security Information / Event Management (SIEM) systems (such as ArcSight, Network Intelligence, e-Security etc...) for Vigilant's customer base. Responsibilities include engineering, developing and documenting network architectures and producing detailed designs. Responsibilities also include procuring, configuring, installing and monitoring critical production and Wide Area Networks for security related incidents.

Candidate must have extensive experience with SIEM products specifically in the areas of custom rule creation, building custom listeners, applying practical logic data warehousing and management, and security transporting log data.

Additionally, the candidate should have detailed knowledge of, switches, VPNs, firewalls, content scanners and intrusion detection devices; conducting network vulnerability assessments; developing test concepts and methodologies; developing test plans, procedures and reports; leading and participating in technical meetings and design reviews; presenting proposed designs to customers and other contractors; supporting security certification and accreditation; and developing trade-off studies, proposals and cost estimates.

Requirements:

- 1-3 years experience working in Information Security
- BS degree required. BS/MS major in engineering or computer science preferred.
- Security Certification (e.g. CISSP, SANS Training) preferred.
- Excellent proven written and oral skills
- Ability to provide effective presentations

Analytical / Technical Skills:

- Extensive hands-on experience with Security Information / Event Management products (ArcSight, e-Security, Network Intelligence, etc...)
- Expert knowledge of Network Security appliances (IDS, Firewall, VPN, Intrusion Prevention)
- Expert knowledge of Network and Application Protocols (IP, TCP, UDP, FTP, HTTP, DNS, routing, etc.)
- Expert knowledge Unix/Linux/Windows Logging
- Solid understanding of IT security practices, trends and markets
- Solid understanding of Regulatory mandates such as Sarbanes-Oxley, HIPAA, and GLBA



Additional Experience in the following areas:

1-3 years in the following:

- Scripting/Programming Experience (PERL, shell scripting, C, use of Regular Expressions.
- Security data handling as it relates to security information management tools. (Correlation of disparate data types, consolidation of logs, report generation)
- Intrusion Detection (Deployment, log handling, writing signatures)
- Firewall (Deployment, management)
- Scripting/Programming Experience (C, PERL, use of RegEx, and Unix Scripting)
- Network Systems Management (Open platforms such as Tivoli and Openview)
- Business Intelligence (Product from Business Objects, Microsoft, MicroStrategy, Cognos, SAS)
- Relational Database Configuration and Design (RDBMS platforms such as Oracle and Microsoft SQL Server)

Customer Service/Communication:

- Able to build strong client relationships and be able to interact effectively at all levels of client organization
- Ability to work with Technical Partners, and 3rd party integrators
- Continuous contribution of best practices documentation and technical notes for internal and external distribution

Location/Travel:

Travel should be expected 25-50% of the time. Most travel will be domestic, but global customer base may require some international travel.

Immediate positions are available in or around the New York City Metro area. When replying to this job posting please list the area that you are interested in working in the subject line.

About Vigilant:

Vigilant is a professional services firm specialized in delivering integrated security management solutions to the fortune 1000, financial services, banking, healthcare, and large enterprise customers. The firm is headquartered in New York City with satellite offices in Boston and Chicago.

Vigilant takes pride in its focus on the people that make up the organization. We are building and will maintain an enjoyable and profitable place for talented people to work, share ideas, and grow professionally.

Position is available immediately. Please send your resume to jobs[at]thevigilant.com (replace [at] with @).

Thanks,

Vigilant's Recruiting Team

