Sr. Arcsight Engineer/Analyst (Ashburn)
Minimum Secret Clearance TS preferred

Sr. ArcSight Engineer/ Analyst's expertise is needed to support a sophisticated enterprise management environment. The Senior Information Assurance Analyst will be responsible for requirements collection, event analysis, content development, and custom log parsing for system and security audit events in a large ArcSight deployment.
The EMS ArcSight Engineer responsibilities include:

- Meet with business users to gather requirements and make recommendations for meeting customer requirements within the ArcSight SIEM
- Identify events of interest in compliance with local audit policy for filtering, correlation and forwarding to enterprise SIEM.
- Integrate data and event feeds with ArcSight SIEM and build custom parsing/flex connectors as necessary
- Determine how best to leverage ArcSight ESM to meet the strategic goals by defining "use cases"
- Lead the content development to meet the organization's security operations goals, to include: the formation of content-specific queries, templates, reports, rules, alerts, dashboards, and workflows
- Perform installation, configuration, and technical administration of ArcSight product components
- Train personnel on the use of ArcSight solutions
- Support all aspects of Sponsor's Security Information and Event Management initiatives.
- Participate in the operation of ArcSight Security Information and Event Management systems to include ArcSight ESM, Oracle, Connector appliances/SmartConnectors, Logger appliances, Windows and Linux servers, network devices and backups
- Provide guidance to security analyst and network engineering staff
- Maintaining up to date documentation of designs/configurations
- On-call support may be required

Required Skills:

- Minimum 10 years in IT and Information Security Engineering
- Bachelors Degree in Computer Science or a related technical discipline, or the equivalent combination of education, professional training or work experience.
- 10-15 years of related experience in data security administration.

Desired Skills:

- In-depth experience in using ArcSight products, to include ArcSight Connectors, Logger, Event Security Manager (ESM), and/or Threat Response Manager (TRM).
- Hands-on developing & managing use cases and content (Dashboards, Active Channels, Reports, Rules, Filters, Trends, Active Lists, etc)
- Demonstrated ability to use problem solving techniques such as root cause analysis to resolve issues
- DoD 8570.1 Compliant Information Security Certification(s), such as CISSP, ISSEP, GSEC, GCIA, GSLC, Security+ strongly desired