



Cyber Security Systems Engineer (Full Scope Polygraph Clearance) - 1519931

Location: Herndon Virginia

Description

The Cyber Security System Engineer holding a Full Scope Polygraph clearance, will work as part of a Cyber-Security team that provides the customer with computer audit trail collection, normalization, analysis, and capability. The customer's system provides the capability to collect, integrate and organize the customers information technology audit records of system, application, and user activity. The customer's project leverages skills of a small number of engineers using commercial software, the HP ArcSight Suite, to collect and process the audit data. The system engineer will be responsible for O&M of the customer's infrastructure. The system engineer will provide remote and onsite support for the customers equipment and software, used to ingest and process audit log data.

The Cyber Security System Engineer with a computer and network background will:

- Provide O&M support for customer system components and subscriber audit feeds,
- Engage prospective system owners thru TEMS to engineer audit log collection solutions,
- Develop and deploy HP ArcSight components (SmartConnectors, FlexConnectors, Loggers, Connector Appliances), and advise system owners on how to set security audit configurations on a variety of computer and network devices.

Smart and FlexConnector development: There is a small amount of custom REGEX parsing code expected to be generated utilizing ArcSight's REGEX scripting capability(similar to Perl scripting). The Cyber Security Systems Engineer may have to use this capability to properly parse audit logs for a particular target product that ArcSight either does not parse very well, or has not developed a parser for that target product. Knowledge of network protocols is essential to understanding the data being received from target hosts. The System Engineer will design, install the audit collection/analysis system, work with target system owners on the installation and testing of the ArcSight software agents, configure other customer components, and provide Operations and Maintenance support to the customer system.

The initial focus of the System Engineer is to provide (O&M) support for the customer system. Additionally, the System Engineer will engage and engineer solutions for new subscribers to the customer's system. An important role of the System Engineer is to provide expert advice to the team and to target system owners regarding how to set up security auditing on a large variety of target devices. The developer will research and document these configurations. The System Engineer will be responsible for project scheduling, project status documentation using the customer's Project Registry, submitting and fulfilling Request for Change (RFC) documentation as well as working through O&M issues detailed in the customer Trouble Ticketing system. The customer requires each IT system to



capture a base and extended set of security logs for ingest into the customer's enterprise audit system. One of the duties of the System Engineer will be to thoroughly investigate security logging for products and technologies such as those listed below:

- Linux (RHEUScientific Linux/CentOS)
- Sun Solaris
- Unix
- VMWare ESX
- Cisco routers, switches and firewalls
- Juniper routers, switches and firewalls
- Microsoft (Windows Server 2008 R2, Windows 2003, Windows XP, Windows 7, ACS, SCOM, Active Directory, Exchange)
- NetApp
- Apache Tomcat
- BEA Weblogic
- InfoBlox NIOS
- RSA
- Oracle 11g
- MySQL

Qualifications

Required Skills:

- Experience writing basic SQL commands
- Demonstrated experience with IT development or operations
- Experience with operating system audit log review
- Detail oriented and focused
- Excellent skills in problem solving and adept at articulating solutions to customers at various technical levels
- 1 – 4 years' experience working with IT System Audit logs
- Experience with Microsoft and Unix/Linux command language

Desired Skills:

- Experience with HP ArcSight, Splunk or other SIEM a plus
- Experience using regular expression (regex) code
- Experience performing data ingestion activities
- Ability to work as part of a team
- Experience using a trouble ticket system
- Ability to document processes and communicate effectively orally and in writing



Desirable to have certifications in one of the following:

- CISSP
- Security+

Candidate must have one of the following:

- 10 Years of job related experience and a High School/GED diploma
- 8 Years of job related experience and an Associate degree
- 6 Years of job related experience and a Bachelor's degree
- 4 Years of job related experience and a Master's degree

Send Resume to Skip Rogers, skip.rogers@ableforces.org for immediate consideration