ESD ID: ESD-16-1046

ESD Title: Software Engineer Level 2

Experience: 7 years, 3 years w/BS, 1 years w/MS

Clearance: TS/SCI w/FSP

Position: Security Information and Event Management Engineer

Position Specific Requirements:

Required:

- Experience configuring and ingesting various data types in a SIEM
- Experience building SIEM dashboards
- Experience analyzing network and host-based traffic
- Splunk background and/or certification

Desired:

- Experience creating automated routines from SIEM results
- Experience writing Java or Python or Perl or Bash
- CS Bachelor's degree
- Linux understanding and comfort
- Splunk and ELK background

Minimum Requirements:

- 7+ years in software development technologies and methodology

Desired Requirements:

- Designing and developing multi-tier web applications using languages such as Java
- Writing design documents, test plans, and test results
- Designing and developing softare and/or multi-tier web applications using programming languages to include: Java/Java EE, Swing, Hibernate, Spring, Struts, JUnit, C, C++, C#, .NET, Java Script, ColdFusion, and Adobe Flex development tools
- Ability to develop and/or maintain software capabilities using C/C++ software development environment; Windows operating system internals, computer security, Win32 programming, Windows kernel programming, x86 assembly programming, COM programming, .NET programming, network programming (sockets), and software reverse engineering
- Developing applications utilizing software frameworks (e.g. Ozone Widgets, Spring, Hibernate, Struts, and JUnit)
- Working knowledge of Java APIs such as JDBC JPA, and EJB
- Experience with data base design and stored SQL procedures
- Ability to apply cost estimation techniques to software development, test, and maintenance efforts
- Working knowledge of and ability to assist others in the use of software engineering tool to support process improvement to include ClearCase/ClearQuest, MS Project/Primavera, Subversion, Doors, Mercurial and Minitab
- 2+ years in network analysis (data and protocols) and TCP/IP and UDP protocols
- 2+ years experience malware analysis and mitigation techniques
- Experience working with Scrum or other agile software development processes
- Knowledge of SOLR/Lucene, AJAX, JAXB, and JavaDB
- Knowledge of U124/U127, SOTF, Packet Capture, and Protocol Processing
- Working knowledge of and ability to implement IPv6 protocols