ESD ID: ESD-16-1010

ESD Title: Systems Engineer Level 2

Experience: 8 years, 4 years w/BS, 2 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:

8+ years experience in 1 or more of the following:

- System engineering of secure command control, communications and intelligence (C3I) systems
- Analyzing needs, deriving system-level requirements, and contributing to the design, development, implementation, and maintenance of computer networks and systems
- Microelectronics engineering, integrated circuit design and integrated circuit reverse engineering skills

Desired Requirements:

- Understanding of secure systems engineering development, including system security requirements analysis, system security requirements allocation, trade-off analysis, other systems security analyses, and secure system definition and specification development
- 2+ years experience with Firld Programmable Gate Array (FPGA) design and engineering
- 2+ years experience with Security Content Automation Protocol (SCAP) and Trusted Network Connect (TNC)
- 2+ years experience with data modeling to include the development and implementation of a data modeling methodology
- 2+ years experience with virtualization technology (e.g. VMware) implementation
- 2+ years experience in designing and developing user interface features, writing design documents, test plans and test results, and assessing architecture and current hardware limitations
- 2+ years in defining and developing comprehensive Java 2EE solutions as part of a Service Oriented Architecture (SOA) using applicable DoDAF standards
- 2+ years in system engineering for VAO Data Integration, Analysis and Reporting (IA&R) activities to include DoD and IC data standardization efforts as they relate to IA&R