



www.itezz.com

Send resume to: hr@itezz.com

Splunk Engineer

Shift: Mon-Fri Dayshift, Available for after hours on-call

Customer Skill Level(s): Expert

Position Description:

- Ensure the Splunk infrastructure functions properly with PKI-based authentication, corporate authorization services, firewalls, and SSL/TLS communications.
- Contribute to development and ongoing improvement of industry best practices and standards for maintaining data analytics enterprise technologies.
- Assist with installing, testing, and deploying hotfixes/patches for Splunk app/product releases to manage enterprise vulnerabilities.
- Assist with development of knowledge articles, documentation, and work instructions used by the Splunk, server, desktop and Information System Security teams, and Tier 2/3 Help Desk technicians.

Clearance: TS/SCI

Polygraph: FS

Training:

HS or GED and 25 Years Experience

Bachelors and 20 Years Experience

DoD 8570 IA Type: IAT Level 2

DoD 8570 CE Certification Requirements: CompTIA Security+ CE

Mandatory Skills:

Experience managing user authentication within Splunk including RBAC/ABAC

Experience reviewing network, host, and firewall security logs

Strong organizational, communication, and collaboration skills

Desired Skills:

Experience with Splunk Machine Learning Toolkit (MLTK)

Experience with scripting languages such as CSS, HTML, JavaScript, and Python

Knowledge of RMF, Trellix ePO, NESSUS, SCAP, and vulnerability scanning

ServiceNow Ticketing System

Shell scripting to automate tasks and manipulate data