Job Title: Cybersecurity Engineer Job Description
Position # J-7U4SCA

Security Clearance:
- US Citizenship (Required)
- Active U.S. security clearance (Secret/Top Secret) is highly preferred

Job Description: Grit Government Solutions is looking for a qualified Cybersecurity Engineer for our customer located in Cocoa Beach, Florida (Local Remote/Hybrid Potential)

This is a contingent position based on Government contract award.

About the Role:
Grit Government Solutions are seeking a skilled Cybersecurity Engineer to join our security team, with a primary focus on leveraging Elasticsearch expertise to strengthen our cybersecurity operations. The ideal candidate will have extensive experience with Elasticsearch for security monitoring and threat detection, with familiarity in tools like Elastic Defend (also known as Endgame), Tychon, Trellix, Microsoft Defender, or Microsoft Sentinel considered secondary. Candidate will play a key role in protecting systems and data by designing, implementing, and managing Elasticsearch-based security solutions while collaborating with cross-functional teams to maintain a robust security posture.

Key Responsibilities:
- Elasticsearch Expertise: Configure, manage, and optimize Elasticsearch for security event monitoring, log ingestion, and threat detection, using tools like Elastic Security and Kibana.
- Threat Detection and Analysis: Monitor and analyze security events using Elasticsearch to identify indicators of compromise and respond to incidents.
- Security Solution Support: Assist in deploying and maintaining secondary security tools such as Elastic Defend (Endgame), Tychon, Trellix, Microsoft Defender, or Microsoft Sentinel as needed.
- Automation: Develop scripts (preferably in Python) to automate Elasticsearch queries, dashboards, and security workflows.
- Incident Investigation: Conduct investigations of security incidents using Elasticsearch telemetry and other tools, providing actionable insights.
- Security Posture Enhancement: Perform log analysis, correlation, and threat hunting using Elasticsearch to identify vulnerabilities and recommend improvements.
- Collaboration: Work with IT and security teams to integrate data sources into Elasticsearch and ensure alignment with organizational security goals.
- Compliance: Support compliance with federal regulations (e.g., NIST, FISMA) through proper log management and documentation.
- Documentation: Maintain detailed records of Elasticsearch configurations, security processes, and incident response playbooks.

Skills and Qualifications:
- **Experience**:
  - 3+ years of hands-on experience with Elasticsearch, specifically in a cybersecurity context (e.g., Elastic Security, log analysis, SIEM).
  - Familiarity with secondary security tools (e.g., Elastic Defend/Endgame, Tychon, Trellix, Microsoft Defender, Microsoft Sentinel) is a plus but not mandatory.
  - Basic proficiency in Python for scripting and automation (preferred but secondary).
- **Technical Skills**:

- Expertise in configuring and querying Elasticsearch for security monitoring and log management.
- Ability to create and optimize Kibana dashboards for visualizing security events.
- Understanding of cybersecurity principles, including threat detection, incident response, and log correlation.
- Familiarity with federal cybersecurity standards (e.g., NIST 800-53, FISMA)

- **Soft Skills**:
  - Strong analytical and problem-solving skills.
  - Ability to work independently and in a team-oriented environment.
  - Effective communication skills for documenting processes and collaborating with stakeholders.

Preferred Qualifications:

- Elastic certifications (e.g., Elastic Certified Engineer, Elastic Certified Analyst)
- Experience with Elastic Stack components (Logstash, Kibana) for advanced log management
- Familiarity with additional SIEM or EDR platforms (e.g., Splunk, CrowdStrike)
- Knowledge of cloud security (e.g., Azure, AWS) or federal IT environments
- Certifications such as CISSP, CEH, or CompTIA Security +