CYBER SECURITY ANALYST IN FORT MEADE, MD

Job Description

Client: Enterprise Government Integrator

Location: Fort Meade, MD

Compensation: Competitive based on years of relevant experience

Clearance: Able to maintain an active TS/SCI Clearance with the DOD

Job Description

The Cyber Security Analyst will enable Command and Control (C2) of the Department of Defense Information Network (DODIN) by ensuring its overall health through 24/7 monitoring, directing, controlling, coordination, de-conflicting, synchronizing, and reporting the current status to proper military personnel.

- Execute in real time, in accordance with mission requirements:
  - Incident handling
  - Triage of events
  - Network analysis and threat detection
  - Trend analysis
  - Metric development
  - Vulnerability information dissemination
  - DoD CSSP methodology
- Coordinate Computer Network Defense (CND) operations with DoD Component Commands/Services/Agencies/Field Activities (CC/S/A/FA) and monitor and report effect of DCO-IDM operations on CC/S/A/FA missions.
- Have knowledge of DoD Computer Network Defense with an understanding of the lifecycle of the network threats, attack vectors, and network vulnerability exploitation.
- Candidate to work as part of a team, however, the candidate must be able to work independently (where required) to achieve day-to-day objectives with significant impact on operational results or project deliverables
- This position is a shift work position and could require you to work Day shift, Afternoons, OR Overnight, as well as potentially weekend days.
  - Schedule will be a 9/80, and shifts will **NOT** be rotational.
  - **First 4 weeks will be day shift** while selected candidate is read on, trained, given access to the systems, and selects their permanent schedule.

Basic Qualifications:

- Active TS/SCI security clearance
- Bachelor's degree in a relevant technical discipline and 6+ years of overall related experience. 4+ years of additional related years of experience is accepted in lieu of a degree.
- Extensive hand's on SIEM Tool Experience (ArcSight, Splunk, Wireshark, etc) to identify current & potential network threats
    - Must be able to speak to the findings these tools provide insight into, and then present those findings; as well as explain potential threat impact & remediation tactics.
- Hands on experience OR Strong Familiarity with POA&M's
- Experience with various Microsoft technologies such as MS Office 2013 and Sharepoint
- Good oral and written communication skills

Preferred Qualifications

- Familiarization with STIGs process and structure
- Knowledge of the DoD orders process
- Currently possess DoD 8750 certification at IAT level II, Security+ce.
- ITIL V3
- Experience briefing Senior Leaders

Send Resume to info@intellectualpoint.com job.