

Cyber Security Analyst

Req #: 11/2019-024

Location: International, DE - Stuttgart, Germany

Job Category: Information Technology

Minimum Clearance: TS/SCI

Job Description

Athena Technology Group (ATG) is looking for experienced, innovative and motivated IT Specialists to support enablement of EUCOM's mission objectives.

This position is in support of a Department of Defense (DoD) organization, US EUCOM located OCONUS in Stuttgart, Germany. (*This position is required to travel OCONUS.*)

The Cyber Security Analyst will provide technical expertise to support the Combatant Command (CCMD) cybersecurity program and its functions IAW current architectures which includes all hardware and software tools and sensors from perimeter to endpoint. Provides Information Security Controls and guidelines to nodes and network management systems. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Test and evaluate software security patches and security related configuration changes for compatibility with the current baseline and resolve any conflicts prior to deployment. Monitor implemented security controls and report status. Perform periodic and on-demand scans for vulnerabilities and unauthorized software on all CCMD assets using provided tools and provide results for review. Maintain scanning results and develop vulnerability trend results. Compile information and support required cyber evaluations, inspections, assessments, and reporting tasks. Perform incident response actions including, but not limited to, system isolation, data gathering, evidence handling, and reporting. Develop recommendations for counter measures or process improvement based on lessons learned from security incidents. Audit logs and provide reports as required. Other duties as assigned.

Required Qualifications:

- Currently hold an adjudicated Top Secret/SCI Clearance and be able to maintain
- BA/BS + 3 years recent specialized or AA/AS + 7 years recent specialized or a major cert + 9 years recent specialized or 11 years of recent specialized experience
- CEH, CRISC, GSEC certification
- DOD 8570 IAT 2 compliance
- Working knowledge of supporting Operating Systems: Windows Server 2008-2016 and Windows 10, VMWare vSphere, Solaris 10-11, Red Hat Enterprise Linux
- Demonstrate in-depth knowledge in network access control, intrusion prevention and detection systems, firewalls, routers, incident response, information security methods, and risk management
- In-depth experience with DoD IT security requirements
- TESA eligibility

Desired Qualifications:

- ITIL v3 – Foundation
- Experience with Bluecoat, McAfee HBSS, Splunk, CyberArk and Bitlocker, ACAS
- Automation using Microsoft PowerShell, VBScript, or batch files
- Adaptable to changing circumstances and operational needs
- Understanding of Department of Defense Military standards