



Cyber Response Analyst

Location: Camp Arifjan, Kuwait

Responsibilities:

- Cyber Response Analysts are responsible for monitoring of audit events and other data from various operating systems, databases, and applications in order to analyze and correlate event data, create situational awareness, and provide trending reports. Analysts are responsible for detection, initial investigation, and reporting. Analysts coordinate and respond to events on all of the monitored networks and the systems on those networks.
- Analysts utilize provided workflow platforms to track security events.
- Analysts work together as a team to develop skills, sources, and methods to provide the best possible cyber defense capability to protect the sponsors IT assets from all manner of cyber threats, attacks, and exploitation.
- Analysts work together with other government organization to develop relationships across industry, the Sponsor, and partners to maintain awareness and status of all relevant cyber defense initiatives, indicator lists, threat reports, incident response techniques,
- Provide technical expertise regarding the defense of military information systems and networks.
- Monitor intrusion detection and security information management systems to discover malicious activity on U.S. Army command and control networks.
- Initiate computer incident handling procedures to isolate and investigate potential network information system compromises.
- Perform malware and/or forensic analysis as part of the incident management process.
- Design and integrate custom rules and reports into military security tools and data collection architectures.
- Conduct analysis of computer security advisories, current network penetration techniques, and military intelligence threat reports in order to improve the U.S Army computer network defense posture.
- Perform penetration testing against U.S. Army networks and information systems to uncover potential security holes that could be exploited by adversarial threat actors.
- Travel to units within theater to assist in computer network defense initiatives, incident investigations, forensic evidence collection, and end-user security awareness education.
- Deploy to other countries as required in support of U.S military operations and exercises.
- Create whitepapers and briefings to highlight emerging computer security trends to U.S. Army leadership and technical personnel.



- Perform other duties as needed to fulfill requirements specified in the contract performance work statement.
- Shift work may be required.

Basic Qualifications:

- Bachelor of Science degree and 2 years of specialized experience OR; Associates Degree plus 4 years of specialized experience OR 6 years technical experience in lieu of bachelor's degree
- Applicants are required to be fully compliant with DoD 8570.1 M IA Level, Job Position, and Computing Environment certification requirements within six months of arriving on-site.
- For 8570.1 IA level requirements, all new employees will be categorized as IAT Level II, which is satisfied by obtaining one of the following certifications: GSEC, Security+, SCNP, SSCP, CISA, GSE, SCNA, CISSP, or GCIH.
- For 8570.1 Job Position requirements, all new employees will either be categorized as a CND Analyst (requires either a GCIA or CEH), a CND Incident Responder (requires either a GCIH, CSIH, or CEH), or a CND Auditor (requires either a CISA, GSNA, or CEH). Lastly, 8570.1 Computing Environment certification is also required, and can be satisfied with a platform specific certification or equivalent training (e.g. MCP, CCNA, RHCSA, A+, etc.).
- Must have an active TS/SCI

Preferred Qualifications:

- 3 years' experience using one or more of the following security applications: SNORT Intrusion Detection System, SourceFire, NetScout, McAfee Intrusion Prevention System, ArcSight SIM, HBSS, CISCO Intrusion Detection System, WireShark, BlueCoat, IronPorts, METASPLOIT, CORE Impact, ENCASE, TCPDump, Netflow, or Forensic Toolkit.
- 3 years' experience with one or more of the following operating systems: Windows7 and Windows 2003/2008/2012 SERVER, SUN-OS, LINUX, UNIX, RED HAT, CENT OS, or CISCO IOS
- 3 years' experience using and maintaining IP networks
- 2 years direct experience with U.S. military command and control or commercial LAN/WAN communication systems.
- Deployments to other countries as required in support of U.S military operations.
- Duration is a 4 year contract.



The Buffalo Group Mission statement: The Buffalo group provides innovative capabilities and extensive domain knowledge to both federal and commercial clients in order to operate more efficiently and effectively. Leveraging our team's expertise, proven industry practices, and leading edge technologies, we ensure that your return on investment is maximized. Our culture of complete commitment to customers is based upon a thorough understanding of your needs and expectations which results in flexible and agile delivery model aimed at success.