Information Assurance Technician

Linchpin Solutions, Inc – Bahrain

Job Description

This position is located in Bahrain.
The candidate shall manage risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

The candidate shall perform the following tasks:

- Maintain appropriate DoD 8570 certifications
- Install, configure and troubleshoot Information Assurance solutions in a deployed environment to include MacAfee ePolicy Orchestrator (EPO) Server, Host Based Security System, Blue Coat SG Proxy, Microsoft WSUS, Assured Compliance Assessment Solution (ACAS), ArcSight Log Management Server, McAfee and Sourcefire IDS/IPS solutions, and Firewalls (Fortigate/Sourcefire)
- Perform network vulnerability scans on operating systems software and hardware to comply with Information Assurance (IA) requirements
- Implement applicable patches including Information Assurance & Vulnerability Assessment (IAVAs), Information Assurance & Vulnerability Bulletin (IAVBs), and Technical Assessment (TAs) for their Network Environment (NE)
- Provide end user support for all IA related applications for the NE
- Perform IA related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE
- Collect data from Computer Network Defense (CND) tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environment
- Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential CND incidents within the enclave
- Track and document incidents from initial detection through final resolution
- Manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized CND applications
- Analyze site/enclave CND policies and configurations and evaluate compliance with regulations and enclave directives
- Recommend and schedule IA related repairs in the network NE

- Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats
- Write and maintain scripts for the NE
- Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence
- Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the
- Analyze system performance for potential security
- Assess the performance of IA security controls within the NE
- Investigate and analyze all response activities related to cyber incidents within the NE or Enclave.
- Identify IA vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing
- Validate network servers, hubs, routers, and switches configurations to ensure they comply with security policy, procedures, and technical requirements
- Recommend and schedule IA related repairs in the NE
- Evaluate potential IA security risks and take appropriate corrective and recovery action
- Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements
- Diagnose and resolve IA problems in response to reported incidents
- Research, evaluate, and provide feedback on problematic IA trends and patterns in customer support requirements
- Perform system audits to assess security related factors within the NE
- Develop and implement access control lists (ACLs) on routers, firewalls, and other network devices in coordination with network administrators
- Install and maintain perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic
- Apply security requirements to an operating system for the NE or Computing Environment (CE) used in their current position
- Adhere to Information System (IS) security laws and regulations to support functional operations for the NE
- Implement response actions in reaction to security incidents
- Support the design and execution of exercise scenarios
- Support Security Test and Evaluations (Part of Certification and Accreditation Process)
- Validate and manage privileged user accounts and network rights to minimize access to NE systems and equipment
- Work with other privileged users to jointly solve IA problems
- Obtain and maintain IA certification appropriate to position
- Provide appropriate IA status and information reports to higher authority as required

Qualifications

- Must have Secret Clearance
- Must have a passport
- Bachelors degree, in lieu 5 years' experience in a related field
- Must be Security + certified.
- Must be Network+ certified.
- Global Information Assurance Certification (GIAC) GIAC Security Essentials Certification (GSEC).
- Software Configuration Management Plan (SCMP) experience.
- Shall have additional CISCO and or Microsoft related certifications.
- Shall have experience performing IA related customer support functions including installation, configuration, troubleshooting, customer support, and/or training, in response to customer requirements for the NE systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
- Shall have a minimum of two (2) years' experience in a military contingency.
- Shall have knowledge of the Information System (IS) security laws and regulations to support functional operations for the NE.

Build your career with us!

Linchpin Solutions' professional services organization is committed to delivering qualified candidates that meet or exceed clients' technical and management expectations. Our growth means exciting career opportunities for talented professionals in IT, engineering, software development, logistics, project management and other key areas. We provide personnel that become valuable assets to the organizations they serve and contribute to the overall skill diversity and strength of the Linchpin Team.

Career choices

Linchpin's success comes from the talent and commitment of our professionals. As one team, we share the challenges and rewards that come from growing the company, which reinforces our culture of ownership. All of our professionals' benefit from the value we collectively create.

Benefits

Linchpin Solutions, Inc. offers paid vacation, sick time and holidays, a 401K plan with matching, health, dental, vision, and long-term disability insurance along with flexible spending accounts.