**INFOSEC ANALYST**
AlphaSixCorp, a Service Disabled Veteran owned company based in Sterling, VA, is looking for motivated, skilled individuals to join our Cyber Security Team supporting Federal Customers. At AlphaSix, we pride ourselves in providing a highly energized work environment where our employees are rewarded with competitive compensation packages and excellent benefits. Do you want the opportunity to apply your skills to solve meaningful challenges? Would you like to contribute to a team where your work will make a difference and your expertise is valued? Are you passionate about providing great customer service? If yes, then we would love to hear from you

**CLEARANCE REQUIREMENT:**

Active Secret

Ability to meet DEA suitability requirements

**LOCATION:**

Sterling, VA

All of the duties listed support one or more of the following information technology related functions; information security, incident response, cyber security, insider threat, computer forensics, certification & accreditation, vulnerability assessment and management, network data capture, intrusion detection, log management, auditing, security incident and event management (SIEM), and penetration testing.

DUTIES:
- ⊕ Prepares written reports, and provides verbal information security briefings.
- ⊕ Investigates, monitors, analyzes, and reports on information security incidents.
- ⊕ Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
- ⊕ Use mitigation, preparedness, and response and recovery approaches, as needed to maximize information security.
- ⊕ Provides incident handling support for incident detection, analysis, coordination, and response.
- ⊕ Tests, implements, deploys, maintains, and administers information system security infrastructure hardware and.
- ⊕ Monitors network to actively remediate unauthorized activities.
- ⊕ Monitors intrusion detection sensors and log collection hardware and software to ensure systems are collecting relevant data.
- ⊕ Monitors all security systems to ensure maximum performance and availability.
- ⊕ Analyze computer security threat information from multiple sources, disciplines, and agencies across.
- ⊕ Performs on-demand vulnerability scanning and compliance monitoring.
- ⊕ Performs day to day configuration and operation of production and test networks.

QUALIFICATIONS:
Documented formal training from an accredited training provider in two or more of the following disciplines: computer science, information systems analysis, science/technology, information management, computer engineering, or electrical/electronic engineering **and** two
(2) years of documented work experience performing any combination of Information System Security, Information Certification & Accreditation, Cyber Security, Computer Forensics, or Insider Threat.

EXPERIENCE:
General Experience:
Includes two (2) years of experience in developing, deploying, or supporting information systems and technology.
Information Security Specialized Experience:
Two (2) years of experience in developing or supporting information security products. Knowledge of information security hardware and software applications. Knowledge of network monitoring, and intrusion detection systems (IDS) and log management applications. Experience testing, installing, patching, and upgrading computer hardware

and operating systems (Windows, and UNIX) in an enterprise environment. Experience identifying, collecting, processing, documenting, reporting, cyber security/ incident response events.
Experience installing, patching, and upgrading various information security hardware and software applications.
Knowledge of information system security, cyber security, computer forensics, insider threat, information certification & accreditation, standards, industry best practices and guidelines.
Information Technology Experience:
Two (2) years of experience supporting, installing, patching, and upgrading computer hardware and operating systems (Windows, and UNIX) in a standalone environment.

EDUCATION SUBSTITUTION:
An associate degree in Computer Science, Information Technology, Information System Security, and Cyber Security may be considered equivalent to one (1) year
generalized and one (1) year INFOSEC specialized experience. Certificates such as Microsoft's MCSE, or Cisco's, CCNA, CCDA or CCIE, may be considered equivalent to two (2) years of general experience / information technology experience.
The CISSP certificate may be considered equivalent to two (2) years of information security experience.