ΣΟΦΙΑ™
SOFIA INFORMATION TECHNOLOGY CONSULTING
'MISSION CRITICAL' I.T. SOLUTIONS

Contact:
info@sofiaitc.com

Information Systems Security Engineer

Job Description:

The Information Security Engineer will be a key member of the security team providing policies and solutions in the following environments: CISCO, Juniper, and Palo Alto Networks, Cloud solutions such as Microsoft Azure/O365 and Amazon Web Services (AWS), Virtualization solutions such as VMWare and Hyper-V, and Active Directory/Exchange within Data Centers.

This individual will be responsible for working effectively with numerous cross-functional stakeholders across the company (Finance, IT, HR, Security, Operations teams, Product Groups, etc.) to engage on all aspects of control and process design, testing, implementation, execution, monitoring, documentation, and remediation activities as needed.

The ideal candidate should be organized and extremely detail oriented with broad knowledge of controls, compliance activities, security tools, and related best practice standards and methodologies.

Roles/Responsibilities:

The Information Security Engineer will serve as a key member of the company's Information Security Program by supporting ongoing compliance activities, security engineering and monitoring efforts across different regulations and standards (ISO, PCI, FedRAMP, HIPAA, NIST RMF, SOX, EU Data Privacy Directives, and Security of Network and Information Security Directives, etc.) as applicable.

They will provide leadership and input for the design, engineering, and implementation of security solutions in all aspects of Information Assurance and Information Security. This includes being able to assess and mitigate system security threats and risks, validate system security requirements, establish system security designs, implement security designs in hardware, software, data, and procedures, verify compliance with system security requirements, and perform system certification, testing, validation planning, and act as liaison with other departments and business units to supporting ongoing system security operations and maintenance.

Specific Roles and Responsibilities include:

- Ability to design and develop information security architectures that support control implementation within existing architectures
- Capable of independent management of projects from design through implementation and ongoing monitoring.
- Apply an enterprise-wide set of disciplines for the planning, analysis, design, and construction of Information Assurance solutions based on relevant (and

various) information security regulations and standards, including ISO27001 requirements, FedRAMP, HIPAA, NIST RMF, PCI, SOX, EU Data Privacy Directives, and Security of Network and Information Security Directives.
- Develop analytical and computational techniques and methodologies for problem solutions
- Perform enterprise wide strategic systems planning, business information planning, and business impact analysis on a scheduled or ad-hoc basis to ensure ongoing Information Security activities within the enterprise. This includes performing process and data modeling in support of the planning and analysis efforts using both manual and automated tools.
- Provide technical guidance in software engineering techniques and automated support tools.
- Implement, test, document, and maintain enterprise-wide Information Security solutions
- Establish functional and technical specifications and standards, solve hardware/ software problems, define input/output parameters, and ensures interoperability of proposed solution
- Perform analysis at all system levels to include: concept, design, test, installation, operation, and validation.
- Analyze and identify all or part of a customer's existing or new peripheral, network, and systems architectures
- Coordinate, facilitate, and maintain ongoing Information Security programs including the remediation of identified vulnerabilities, security alerts, and applicable reporting metrics.

Requirements:

- BA or BS degree in IS or related field required (Computer Science, Computer Engineering, or related Engineering) or equivalent.
- CISSP certification or equivalent (CAP; GSLC; CISM)
- System administration experience
- Network engineering experience
- Must have a minimum of seven to ten years work experience in Information Security including network and system security, and Compliance or Audit experience including working with Industry regulations and standards (ISO27k1, PCI, SOX, FedRAMP, HIPAA, NIST RMF and data privacy directives)
- Must have experience in Security Risk Assessment/Analysis support.
- Must have excellent communication and customer interface skills.
- Must have experience working within a large enterprise
- Strong knowledge of Windows, Linux and OSX operating systems and environments including knowledge regarding active directory and group policy, networking architecture design and implementation, virtual environments, and data-center design (Windows Server 2012R2 and Microsoft SQL a plus)
- Strong information security domain knowledge and experience.
- Expert level knowledge regarding the implementation, deployment, and usage of security tools and programs, including:

- Intrusion detection/prevention software, such as AlienVault, qRadar, Log Rhythm, ArcSight ESM, etc.
- Vulnerability scanners, such as Qualys, Nessus, and Nexpose
- AD audit tools, such as NetWrix
- Web Application scanners, such as Acunetix
- Log Aggregation/management tools, such as Log Insight and Splunk
- Ticketing systems and integration with the above through ServiceDesk Plus, Service Now and ZenDesk

Other desired skills and experience:

- CISA, PMP, CRISC, Security + and/or other relevant designations
- Experience in large scale compliance or auditing environments
- Systems Engineering, Integration, and Technical Support within environments containing various levels of technical acumen.
- Experience with SOCII and/or audit criteria definition
- Experience performing vulnerability assessments, QA testing, Implementations & Validations.
- Scripting experience in the area of vulnerability testing.
- User account management experience and IAM.

Contact:

Send resume to info@sofiaitc.com