Cyber Security Specialist 1

Job summary

We are looking for a dedicated and meticulous <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> to join our growing team. In the role, you will operate independently and as part of a team to ensure our client’s software, hardware, and related components are <a href="https://ironrangecyber.com/">protected from cyber-attacks</a> . The job description will include developing security systems, analyzing current systems for vulnerabilities, and handling any cyber-attacks efficiently and effectively. Candidates should have strong IT skills and a deep understanding of cyber hacker methodology.

Responsibilities

Develop unique, effective security strategies for software systems, networks, data centers, and hardware

Implement/build-in security systems to software, hardware, and components

Research the best ways to secure company-wide IT infrastructure

Build firewalls to protect network infrastructures

QA software and hardware for security vulnerabilities and risks

Monitor software for external intrusions, attacks, and hacks

Close off security vulnerability in the case of an attack

Identify cyber attackers, report to upper management, and cooperate with police or other legal forces to detain the perpetrator

Work independently or as part of a team as needed

Requirements

Bachelor’s degree in computer science or STEM subject preferred

Completion of an internship/apprenticeship in cyber security a plus

Strong IT skills including knowledge of hardware, software, networks, and data centers

Thorough work ethic, attention to detail

Skills of perception and QA, ability to identify vulnerabilities and overall issues

Critical thinking skills, problem-solving aptitude

Forensic approach to challenges

Ability to think like a hacker and anticipate hacker moves

Desire to self-educate on the ever-changing landscape of cyber hacking tactics

Experience in professional cyber security a plus

Cyber Security Specialist 2

Job summary

We are looking for an experienced and motivated individual for our <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> position. This individual will provide system, on-site and remote network, and cybersecurity support, operations, and monitoring services as well as some project-based involving technology implementation and documentation. The ideal candidate has excellent written and verbal communication skills, and a solid understanding of various end-user, server, network, and security technologies.

Responsibilities

Cyber Security Incident response practice responsible for the monitoring of all security events and management of all security threats, incident response, and cyber threat intelligence.

Define, identify, and classify critical information assets, assess threats and vulnerabilities regarding those assets, and implement safeguards

Highly experienced in the implementation and support of Office 365 ATP, Secure Score, and Azure environments

Network troubleshooting skills

Windows desktop and laptop

Strong written and oral communication skills, and the ability to effectively communicate with technical and non-technical audiences

Requirements

Bachelor’s degree or equivalent work experience

5+ years of experience in information security

Cyber Security working knowledge/experience

Cloud experience Azure, O365 ATP, DLP

Security Technologies, including web filtering, encryption, etc.

Cyber Security Specialist 3

Job summary

We are looking for a <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> with excellent communication skills for active collaboration with associates within the team and various external teams. It will actively participate in projects to deploy Cyber Security technologies. The successful candidate will be a self-starter and be able to work with little supervision.

Responsibilities

Responsible for security log management, archiving, and retention according to security policy.

Ensures compliance with the security controls software version, policies, and rules.

Post-deployment monitoring and testing

Support security audits, risk analysis, and assessments

Responsible for development, implementation, monitoring, and operational support of new or currently owned/managed solutions and service provider relationships

Provide and maintain consistent and accurate operational documentation, process workflows, and configurations

Participate in IS/IT Security projects as assigned

Define and implement automation and orchestration scenarios

Maintain metrics for measuring the overall health of security systems, project progress, service success, and business value

Maintains baselines for the secure configuration and operations of assets

Contributes to the IT security-related aspects of legal and regulatory compliance

Maintain and enforce adherence to corporate and SOC standards, processes, and procedures

Perform routine maintenance of Information Security infrastructure systems

Identifies vulnerabilities of networks, systems, and applications by performing regular penetration tests and assessments.

Requirements

Typically has 4+ years relevant experience

4-year degree in computer science or related field or equivalent experience

Knowledge of foundational security principles

Strong IT skills and knowledge including hardware, software, and networks

Excellent problem-solving and technical skills

Operational knowledge of system and network security engineering best practices

Hands-on experience implementing and configuring Operating Systems (Windows, Unix/Linux)

Hands-on experience in virtualization environments and backup processes.

Proven knowledge of Cloud-based infrastructures and services.

Knowledge of Microsoft Active Directory and Group Policies

Experience with firewalls rules handling

Knowledge of TCP/IP, related network and application protocols, and their security issues

Ability to use logic and reasoning to identify the strengths and weaknesses of IT systems

Ability to multi-task, troubleshoot, and prioritize

A deep understanding of how hackers work and the ability to keep up with the fast pace of change in the criminal cyber-underworld

Detail-oriented, self-motivated, and disciplined, with excellent time management skills

Ability to seek out vulnerabilities in IT infrastructures

Previous work experience in a Security Operations Center

Understanding of database structures and centralized management solutions (SCCM, Rudder, or similar)

Experience with implementing IT security configuration standards in applying hardening procedures

Cyber Security Specialist 4

Job summary

We are currently seeking a friendly, eager, and qualified <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> to augment our service department. This position will be a part of the service team, and report directly to the Director of Services.

Responsibilities

Asses triages and prioritizes security alerts from logging and monitoring systems.

Analyze security-related data in both structured and unstructured formats from various sources.

Create, manage, and perform scheduled procedures to ensure baseline security standards across a wide variety of clients.

Conduct and assist with system audits.

Help manage remediation efforts and processes.

Requirements

Cyber security trends and technologies

Expert understanding of Cyber Security terminology, policies, and procedures.

Technical knowledge and experience working with Windows Servers, Active Directory, Networking protocols, Windows workstations, and Microsoft 365.

Security+, Network+ or equivalent experience preferred.

Cyber Security Specialist 5

Job summary

The <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> is responsible for information cyber security analysis & response with the mission of protecting the Company from data loss risks and common threat actors.

Responsibilities

Design, develop and implement solutions to IT security requirements focusing on Data Loss Prevention and related data loss risks

Prevent, detect, analyze, and respond to threat activity (internal or external), information system vulnerabilities, and cyber incidents

Provide file analysis reports, risk, and threat evaluation, after-action reports and summaries, and other situational awareness information to <a href="https://100hires.com/cio-job-description.html">CIO</a> and other stakeholders

Provide technical support, analysis, and recommendations in areas such as Perimeter Defense Efficacy; Malicious Software (Malware) Analysis; Attack vector analysis; Computer Host Based Defense; Insider Threat; Risk Analysis and Readiness; Strategic Planning Analysis

Oversee network and host-based forensics and malware analysis

Participate with the Enterprise Risk Management team to ensure proper identification of policy issues/violations

Assist in security-related incident communications and response activities

Requirements

Knowledge of Threat Vector Analysis, Intrusion Detection and Prevention, Incident Management and Response, Risk Assessment, and Mitigation methodologies, and Counter Threat Operations

Knowledge of cyber security threats, risks, vulnerabilities, and attacks, including threat actor motives, capabilities, and techniques, with the ability to analyze intelligence data and provide indicators and warnings to healthcare and financial services business functions

Knowledge of information security concepts and theory, and the application of such through technical and non-technical methods

Knowledge of current and emerging security and information technology standards and practices.

Knowledge and experience in security operations, host-based forensic analysis, malware analysis, and threat response

Ability to maintain proficiency in OS platforms, including Linux, Unix, Windows, and AIX

Ability to work under stress/pressure to meet deliverables, timetables, and deadlines

Ability to respond to multiple competing demands

Ability to continuously learn and keep abreast of technological trends

Ability to manage project activities

Bachelor's degree in Computer Science, Information Technology, or a related field and four (4) years of experience in industry experience in an information technology mission-critical area. Experience can be substituted for education.

Cyber Security Specialist 6

Job summary

We are searching for a <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> who is a positive and team-oriented professional with a desire to develop and increase their capabilities within the security industry. The identified professional will be responsible for maintaining the integrity of customer and internal systems with the use of IA principles and DoD processes/policies.

Responsibilities

Provides engineering security aspects into subsystems network designs (e.g., Cross Domain Solutions, Firewalls, Guards, Intrusion Detection Systems, Data Classifications, User authentication access, and Virus Detection) and security certification accreditation of subsystems network according to DITSCAP DIACAP process

Provides technical network design, design testing, administration, configuration management, and troubleshooting services

Research, identify, evaluate, and provide the status of information assurance controls

Analyze security incidents and document response procedures and report actions

Conducts technical vulnerability assessments, assists system administrators apply security patches, and validates changes

Assists in the creation and/or validation of certification and accreditation documentation

Evaluates potential IA security risks and recommends corrective action

Work with government representatives and personnel to maintain Cross Domain accreditation for the transfer and collection of data between various secure and nonsecure domains

Interact with development and test teams to coordinate systems upgrades and test cycles

Provide support over system configuration and ensure compliance with operation procedures

Support users of information technology systems through understanding and resolving problems to minimize service disruptions

Requirements

5 years experience in an Information Assurance Specialist capacity

Comprehensive knowledge of IA principles and DoD process and policies

Knowledge of DoD certification and accreditation procedures (RMF aka NIST 800-53r4 in reference from DoDD 8510.01)

Able to identify and understand security vulnerabilities

Ability to read, comprehend and interpret security audit logs

Must have demonstrated general experience in information operations

Excellent verbal and written communication skills

Ability to obtain a government security clearance

Ability to read, write and speak English

Ability to travel roughly 20%

Active Secret government clearance or the ability to obtain

Cyber Security Specialist 7

Job summary

The <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> develops and maintains information security programs; analyzes, designs, and develops enhancements to the security system; coordinates and implements disaster recovery strategies. Assists in day-to-day security and audit compliance operations for the IT Security Services group, primarily focusing on technology issues.

Responsibilities

Implements and monitors network security mechanisms in compliance with established security policies.

Provides consulting support regarding secure connectivity, network services, and protocols.

Provides consultation regarding various security controls and processes and policies.

Ensures protection and secure implementation of the IT infrastructure.

Provides support to the Computer Incident Response Team as requested.

Assists with periodic reviews, audits, troubleshooting, and investigations.

Provides support during site security reviews as requested.

Requirements

2 plus years experience in the cyber security field.

Certified Information <a href="https://100hires.com/security-manager-job-description.html">Security Manager</a>

(CISM) or Certified Information Systems Security Professional (CISSP)

Bachelor's degree in Computer Science or related field preferred with specific expertise and certification in IT Security.

BS/BA in Cyber Security or related discipline.

2-5 years of experience in cyber security.

CompTIA Security+ Base-Level Certification.

CISSP certification is preferred or MS/MA in Cyber Security and generally 2-4 years of experience in the cyber security field.

Cyber Security Specialist 8

Job summary

The <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> is responsible for supporting, creating, and implementing of security architectures and secure application designs for information systems. This includes assisting application developers/support teams with secure application design, planning, and integration. Conduct security architecture reviews, provides secure application/infrastructure solutions, designing/implement mechanisms & programs that restrict access to malicious intent or other unauthorized users. Introducing new security methods/technologies for integration with existing technical architectures, frameworks, implementation planning, documentation of standard methodologies, and templates. Assessing security threats/risks and recommending/assisting in the delivery of solutions to mitigate risks.

Responsibilities

Participating in the creation and administration of data security policies, procedures, and standards.

Participating in access audits and conducting computing forensics.

Participate in the creation and maintenance of data and network security policies and procedures.

Provide system assurance and security oversight in the EIS change control process; review and evaluate risks of submitted changes and impact on the security of CSMC network and systems.

Review logs from intrusion detection and monitoring systems; conduct correlation analysis and take action accordingly.

Facilitate external third-party assurance reviews to assess networks (internal, external, wireless, etc.).

Work with technical teams to facilitate & promote security incident response procedures, address monitoring concerns, and identification of criteria for audit reporting.

Conduct on-demand forensics analysis and review of compromised systems and/or systems used in a potentially un-secure and un-trusted manner.

Conduct periodic review and scanning of DMZ assets, critical servers, internal/external, and wireless networks.

Develop security metrics and report on security monitoring efforts.

Use security monitoring tools to evaluate and improve the security of organization systems and networks.

Maintain and support the security tools suite to ensure logged data fidelity and integrity.

Requirements

2+ years as a security specialist with experience in solution design, deployment, and operations in desktop, server, network, and server technologies.

Demonstrated understanding of computer/network security, operating systems (UNIX/LINUX, Windows, and NT) LAN/WAN networking protocols such as TCP/IP, routing, firewalls, IDS/IPS, PKI, and encryption.

Solid grasp of Information Classification, Network security protocols, methods and technologies, Application and Web Layer Security (Web 2.0, Secure Messaging, Secure Protocols), Continuity of operations planning and disaster recovery strategies and architectures, and Identity Access Management and Access Control.

Experience with regulatory and compliance information security frameworks, standards, and best practices (NIST, ITIL, HIPAA, PCI-DSS, ISO 27000 series, etc.).

Cyber Security Specialist 9

Job summary

We are seeking to hire a <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> to support our team.

Responsibilities

Manage all day-to-day cybersecurity operations including administrative functions, assessing risks, and identifying unstated assumptions

Knowledge of Defense Information and Accreditation Risk Management Framework (RMF) and process for system and application controls

Determines applicable enterprise cyber and security standards

Develops and implements defined cyber/security standards and procedures

Coordinates develops and evaluates security programs for an organization

Recommends cyber/security solutions to support customer requirements

Identifies, reports, and resolves security violations

Establishes and satisfies cyber and security requirements based upon the analysis of user, policy, regulatory, and resource demands

Requirements

Bachelor's Degree from an accredited college or university in computer science, computer engineering, advanced analytics, applied mathematics, physics, or a related field

Minimum 8 years relevant experience

Certified Information System Security Professional (CISSP) required

Obtain an IT-II clearance (Non-Critical Sensitive)

Degree in computer science, computer engineering, advanced analytics, applied mathematics, or physics

Cyber Security Specialist 10

Job summary

We are seeking a <a href="https://100hires.com/cyber-security-specialist-job-description.html">Cyber Security Specialist</a> for our headquarters office.

Responsibilities

Implement and audit security controls to preserve confidentiality, integrity, and availability of information systems

Integrate security configuration procedures and tools on Windows and Linux platforms

Evaluate requirements, select/implement security controls, create and/or review installation procedures, conduct verification and validation of test procedures and script changes, tailor and configure security controls for specific product use, tailor platform hardening, implement application software and/or Operating System vulnerability patches, draft overall security assessment plans, prepare test procedures, perform security tests, and perform security vulnerability assessments using Assured Compliance Assessment Solution (ACAS)

Participate in certification and accreditation activities with various government authorities and certification agents to obtain and maintain official system Authorization to Operate (ATO)

Completing security and Information Assurance (IA) training as required, achieving a minimum of 40 hrs/yr of continuing education per DOD IA workforce improvement program

Travel to receive training or to complete system installations at customer sites

Requirements

Associates degree in an Information Technology or Cyber Security related field or two years’ equivalent Information Technology experience

Proficiency with Windows Operating System Configuration

Must have, or be able to obtain, Security+ or equivalent certifications

Must be a U.S. citizen, eligible for a U.S. Department of Defense (DoD) security clearance

Experience in obtaining system ATO

Working Knowledge of Mac OS X and Linux

Proficient in Active Directory and Event Viewer

Proficient in Windows 7, Windows 10, and Windows Server

Possessing an active U.S. Department of Defense (DoD) security clearance

Current Security+ or equivalent certification