Information Technology Senior Security Administrator

Job Code: U8831
Pay Grade: UI
Pay Scale: $109,970.12-$179,335.89 Annually
Exempt: Yes

OVERVIEW

As part of the Information Technology Security team in the Information Services Division (ISD), maintain data availability, data integrity, and data recovery on premises and in the cloud. Additionally, perform risk analysis and provide mitigation and corrective reports to assist with Sheriff's Office cybersecurity.

DUTIES & RESPONSIBILITIES

Duties may vary based on assignment.

- Architect and administer security incident and event management (SIEM) system.
- Administer and coordinate with Managed Security Services Provider (MSSP) and its security solution.
- Ensure all appropriate logs and information are ingested accurately and timely.
- Administer and architect internal network security solution.
- Administer, maintain, and support Forensic Imaging systems (FRED).
- Architect policies and administer the end point detection and response system (EDR).
- Provide technical and operational support for the security architect of cloud services selected by the Sheriff's Office.
- Administrator and implement new rules and policies for the email protection system.
- Evaluate threat intelligence received prioritizing actions for the existing environment.
- Develop, test, and deploy hardening documents and configurations to reduce configuration and vulnerability risk for servers, endpoints, software, and networks.
- Develop and document recovery strategies, processes, and tests.
- Develop and document security awareness strategies, processes, and tests.
- Develop and implement ongoing hardware and software reviews and inventory.
- Design and administer proactive monitoring of systems utilizing an enterprise monitoring solution.
- Research and introduce new technological innovations.
- Research and recommend solutions to complex issues.
- Design and perform routine security auditing and run compliance/vulnerability scans of systems as required.
- Lead or participate in project planning across ISD sections.
- Provide proactive and well qualified recommendations to purchase hardware, software, and system components to enhance confidentiality, integrity, or availability.
- Lead and perform system modeling, analysis, planning, and budgeting.
- Research and evaluate vendor products and services.
- Oversee the testing of user access reviews, system mitigation reviews, and scheduled attestations, or certificate renewals.
- Communicate effectively at all levels of the organization and with external customers and vendors.
- Proactively develop and document technical processes and procedures to enhance service levels and section efficiencies.
- Identify and proactively maintain security configuration documentation and facilitate changes

in documentation and system monitoring as devices are added and retired from the environment.
- Mentor and provide knowledge to section members and overall guidance as needed to division members.
- Remain available outside normal working hours as needed.
- Act as the IT Security Manager as necessary.
- Perform other related duties as required.

KNOWLEDGE, SKILLS & ABILITIES

- Expert level knowledge of security body of knowledge.
- Working knowledge of the Macintosh Operating System (Mac OS X) in a Windows environment to provide security standards and recommendations.
- Knowledge of Active Directory (AD) to provide mitigation recommendations for an enterprise environment to include global and group policies, organization units (OUs), and delegating authority within the environment.
- Knowledge of enterprise level storage array networks (SAN) and it associated security requirements.
- Mastery of SIEM ingestion feeds, dashboard, and management of same.
- Knowledge of cloud services and cloud security solutions and implementation.
- Demonstrated senior level skill with risk identification and mitigation.
- Skill in local area network (LAN) implementation to address security mitigation implementation.
- Ability to provide security mitigation recommendations to internetwork external entities into corporate environment.
- Ability to recommend strategies for secure and robust Identity and Access Management (IAM) solutions.
- Ability to lead projects and team members in implementation efforts of IT-related projects.
- Ability to learn, understand, and implement new technology quickly and independently.
- Ability to work independently and under minimal direction in accordance with section, division and office goals, objectives, and values.
- Demonstrated success solving complex issues, developing solutions to previously unsolved problems, and leading problem resolution at the highest escalation point.
- Demonstrated ability of continuous learning and continual self-improvement.

WORKING CONDITIONS

- Work within an office environment within a law enforcement agency.
- Stand/sit at a keyboard or workstation for prolonged periods.
- May engage in light physical exertion (e.g., lifting, carrying, pushing and/or pulling of objects and materials up to 10 pounds).
- Work standard business hours.
- May work non-standard hours including nights, weekends, and holidays.
- In the event of an emergency or disaster, may be required to respond promptly to duties and responsibilities as assigned by management chain, Division/District Commander, or the Sheriff (or their designee). Such assignments may be for before, during or after the emergency/disaster.

MINIMUM EDUCATION & EXPERIENCE

- A high school diploma or possession of a GED certificate.
- One or more of the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Strategic Planning, Policy, and Leadership (GSTRT), Certified Chief Information Security Officer (CCISO).
- Nine years of paid experience providing cybersecurity support to system implementation, maintenance, troubleshooting, and evaluation of business methods and procedures within an enterprise environment to include but, not limited to virtualization, backup and disaster recovery, storage networks, messaging, cloud technology, Operating System (OS)-agnostic

systems, and intermediate networking skills.

OR

- An associate degree from an accredited institution of higher education in a technical field.
- One or more of the following certifications: CISSP, CISA, GCFA, GSTRT, CCISO.
- Eight years of paid experience providing cybersecurity support to system implementation, maintenance, troubleshooting, and evaluation of business methods and procedures within an enterprise environment to include but, not limited to virtualization, backup and disaster recovery, storage networks, messaging, cloud technology, OS-agnostic systems, and intermediate networking skills.

OR

- A bachelor's degree or higher from an accredited institution of higher education in a technical field.
- One or more of the following certifications: CISSP, CISA, GCFA, GSTRT, CCISO.
- Seven years of paid experience providing cybersecurity support to system implementation, maintenance, troubleshooting, and evaluation of business methods and procedures within an enterprise environment to include but, not limited to virtualization, backup and disaster recovery, storage networks, messaging, cloud technology, OS-agnostic systems, and intermediate networking skills.

OR

- One or more of the following certifications: CISSP, CISA, GCFA, GSTRT, CCISO.
- Five years of experience in a Hillsborough County Sheriff's Office Information Services Division position.

ADDITIONAL JOB REQUIREMENTS

- Attendance at the specified Sheriff's Office work location is required.
- Depending on assignment, employees may be required to possess a valid Florida Driver License at time of employment. Driving history will be thoroughly reviewed and may be grounds for disqualification.
- No visible tattoos on face, head, and neck. Tattoos determined to take away from the professional appearance of the Sheriff's Office must be covered with an appropriate white, black, or neutral covering.
- No illegal drug sale within lifetime.
- No illegal drug use within the past 36 months. No marijuana use within the last 12 months.
- No felony convictions within lifetime.
- No misdemeanor convictions involving perjury, false statement, or domestic violence within lifetime.
- No dishonorable discharge from any branch of the United States Armed Forces, the United States Coast Guard, National Guard, or Reserve Forces.
- Successful completion of a background investigation including criminal, reference, employment, and neighborhood checks; polygraph; medical evaluation; and drug screening.
- Live within Hillsborough County or within Citrus, Hardee, Hernando, Lake, Manatee, Pasco, Pinellas, Polk, Sarasota, or Sumter County as long as the residence is located within the 60-mile parameter of Falkenburg Road Jail at the time of appointment/employment (certified only).

The duties and responsibilities on this job description represent the essential functions that an employee must be able to satisfactorily perform with or without reasonable accommodations. Reasonable accommodations shall be made upon request to enable employees with disabilities to perform the essential functions of their job, absent undue agency hardship. The Sheriff's Office retains the right to change or assign other duties to this job as necessary.

PREFERRED QUALIFICATIONS

- Five years of security administration experience in an enterprise environment.
- Advanced scripting experience.
- Proven experience administering SIEM.
- Proven experience documenting risk mitigation.
- Demonstrated experience with cloud platform security administration.
- Demonstrated experience with policy development for EDR solutions.
- Demonstrated experience with email security solutions.
- Demonstrated experience with centralized endpoint management.
- Demonstrated experience with data center disaster recovery planning strategies.
- Demonstrated experience designing and implementing security technical implementation guide (STIG) or equivalent.
- Demonstrated experience in utilizing vulnerability management tools.
- Demonstrated experience administering antivirus/antimalware systems.
- Experience leading a multidisciplinary team.