CYBERSECURITY SPECIALIST

Department: Information Technology & Telecom
Unit: 5210
Level: 6, Non-Exempt

Supervisor's Title: Cybersecurity Manager
Supervises: No Staff

The Cybersecurity Specialist is responsible for protecting Massport's technology environments by implementing and managing advanced security measures that proactively detect, prevent, and respond to threats. The Specialist strengthens organizational resilience through strategic security initiatives, ensuring rapid response to incidents and continuous improvement of overall security posture. Key priorities include enhancing threat detection and response, advancing modern security principles, and enforcing access controls to minimize risk. The Specialist also supports identity security, ensures compliance with relevant industry standards and regulations, and develops processes and documentation to improve operational efficiency and readiness.

ESSENTIAL RESPONSIBILITIES OF THE JOB

Threat Detection & Response

- Deploy and administer EDR/XDR solutions for advanced endpoint protection. Deploy agents, tune detection policies, and respond to endpoint alerts.
- Assist with the deployment, configuration, and maintenance of the Security Information and Event Management (SIEM) platform, ensuring optimal performance and accurate threat detection.
- Integrate multiple data sources into the SIEM, from network devices, security appliances, servers, and other IT infrastructure components, ensuring comprehensive visibility and data accuracy.
- Regularly review and optimize log source configurations, parsers, and connectors, ensuring that data ingested into the SIEM is relevant, reliable, and actionable for security analytics and threat hunting activities.
- Assist with building and maintaining SOAR playbooks for automated incident response.
- Monitor, investigate, and troubleshoot alerts and events from all cybersecurity systems, and respond to, triage, and document all security-related incidents.
- Develop, test, and implement automation scripts and tools to streamline security operations and response tasks.
- Create, verify, and/or maintain documentation of assigned information systems.
- Manage, support, and administer additional security systems as assigned.

Identity & Access Management

- Assist with managing Identity & Access Management (IAM) systems. Audit user accounts, disable stale accounts, and enforce least privilege for on-premise and cloud applications and environments.
- Integrate cloud identity systems with enterprise SSO and MFA solutions.
- Continuously review and audit user roles, permissions, and accounts, ensuring that access is based on the principle of least privilege.
- Handle role changes, access provisions, or de-provisions efficiently, and supervise periodic access reviews.
- Administer and troubleshoot end-user remote access.
- Administer user creation and manage security access rights in Active Directory and locally where necessary.

Compliance & Risk Management

- Ensure alignment with NIST CSF, CIS Controls, TSA, USCG, and other applicable cybersecurity best practices, guidelines, and regulations.
- Support cybersecurity compliance for operational technology environments.
- Ensure the secure deployment and operation of AI systems by implementing access controls and safeguarding sensitive data used in AI models.
- Zero Trust Implementation Support. Apply micro-segmentation and identity-based access controls across environments.

Infrastructure Security & Collaboration

- Assist with the management of the organization's server & application monitoring systems.
- Assist with management of the organization's cloud infrastructure security systems.
- Participate in new product research and development of emerging security technologies that may be used to replace, augment, or layer into the existing Massport IT topology.
- Work with all other IT teams to securely implement new systems and improve security of existing systems.
- Attend meetings with business units and outside contractors to provide advice on implementation of new systems and cybersecurity best practices.

Incident Analysis

- Perform computer forensics when necessary to identify the root cause of security incidents.
- Assist with troubleshooting of all security-related software and systems.
- Assist with physical installation of cybersecurity hardware, such as firewalls, servers, and appliances.

Perform other tasks as necessary.

JOB REQUIREMENTS AND QUALIFICATIONS

Education

Degree in Computer Science, cyber certifications, or equivalent professional work experience preferred.

Experience

Hands-on experience with cybersecurity systems or enterprise computer systems administration.

SKILLS AND COMPETENCIES

- Strong understanding of security concepts and best practices.
- Ability to prioritize cyber alerts and investigations.
- Working knowledge of hardware (Workstations, Servers, Laptops, etc.).
- Working knowledge of modern operating systems (Windows Desktop, Windows Server, and Linux).
- Must be able to troubleshoot hardware, software, and network issues.
- Ability to write scripts in common scripting languages (VBScript, PowerShell, Python).
- Experience with VMware and cloud computing (AWS/Azure) preferred.
- Experience with enterprise level security monitoring and management solutions preferred.

WORK SCHEDULE AND OTHER REQUIREMENTS

- This position is based at Massport’s Logan Office Center and requires flexibility to meet the dynamic needs of the department.
- Ability to work 37.5 hours per week.
- Ability to respond to emergency calls after normal business hours, 7 days per week, 24 hours per day and 365 days per year.
- Ability to pass Massport’s pre-employment-controlled substance test and background checks.
- Current and valid driver’s license.