CYBERSECURITY ENGINEER

Department: Information Technology
Unit: 5210
Level: 7 / Exempt

Supervisor's Title: Senior Security Engineer
Supervises: No Staff

Our Information Technology (IT) Department's mission is to provide innovative, robust, and secure information and telecommunication systems for employees and members of the public who use Massport's facilities and systems. We strive to provide efficient and accessible technology to enable Massport to successfully meet its business goals and promote local and regional economic prosperity. We are a service-based organization that works collaboratively across departments to provide technological leadership, resources, technology education and tools in support of the Authority.
The Cybersecurity Team is responsible for the design, implementation, and monitoring of all technology-based security services across the enterprise environment.

ESSENTIAL TASKS OF THE JOB

As a cybersecurity engineer, you will:

1. Deploy, manage, and troubleshoot the organization's vulnerability management platform. Maintain the underlying infrastructure to ensure reliable and comprehensive vulnerability scanning and proactively identify and address any coverage gaps.
2. Implement and maintain network access control (NAC) systems, including 802.1X-based authentication. Ensure alignment with current security best practices and continuously evaluate policies to maintain secure and compliant network access.
3. Support and manage Public Key Infrastructure (PKI) and certificate services. Maintain and upgrade certificate authority infrastructure, monitor certificate lifecycles, and ensure timely renewal of root and subordinate certificates to prevent service disruptions.
4. Assist system owners and IT staff with deploying digital certificates to internal systems using the organization's internal certificate authority (CA). Provide guidance on certificate enrollment, configuration, and troubleshooting to ensure secure and efficient implementation
5. Support the organization's third-party risk management (TPRM) efforts by utilizing existing TPRM tools to assess, monitor, and document vendor security posture. Collaborate with stakeholders to ensure compliance with organizational risk standards and regulatory requirements.
6. Serve as a liaison between the organization and internal audit teams or external regulatory agencies during compliance audits. Support the development and

maintenance of compliance policies and procedures based on industry best practices and audit findings.

7. Implement and maintain system deployment, configuration, and patch management processes for both Linux and Windows environments. Ensure both platforms are regularly updated and secured through a combination of automated and manual methods. Collaborate with system administrators to develop and enforce patching policies, leveraging appropriate tools for each operating system.
8. Implement, administer, and support additional security systems as assigned, ensuring they are properly configured, maintained, and aligned with organizational security standards.
9. Create, verify, and/or maintain documentation of assigned information systems.

SECONDARY TASKS

1. Participate in the planning and execution of backup and disaster recovery strategies to ensure data integrity and business continuity.
2. Provide support for SIEM and SOAR platforms as needed, assisting with configuration, monitoring, and incident response workflows.
3. Assist with the management of the firewall infrastructure, including patching, policy configuration, and ongoing maintenance to ensure secure and efficient network operations.
4. Assist with the design, implementation, and maintenance of Identity and Access Management (IAM) solutions to enforce access controls and protect critical systems.
5. 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.
6. Participate in the research and evaluation of emerging security technologies to identify solutions that can enhance, replace, or integrate with the existing Massport IT infrastructure.
7. Participate in meetings with internal business units and external contractors to provide guidance on the implementation of new systems and ensure alignment with cybersecurity best practices.
8. Ensure the security and integrity of assigned information systems through proactive monitoring, maintenance, and adherence to cybersecurity best practices.
9. Assist with troubleshooting of all security related software and systems.
10. Assist with the physical installation of cybersecurity hardware, such as firewalls, servers and appliances.
11. Perform additional tasks and responsibilities as needed to support team objectives and organizational goals.

WHAT YOU WILL BRING

- Strong understanding of cybersecurity principles, with a focus on data protection and security best practices.
- Ability to effectively prioritize and respond to cyber alerts and security incidents.
- Hands-on experience with hardware including workstations, servers, and laptops.
- Proficiency with modern operating systems, including Windows Desktop, Windows Server, and Linux.
- Strong troubleshooting skills across hardware, software, and network environments.
- Familiarity with Next-Generation Firewall technologies.
- Experience with Microsoft 365 administration and cloud platforms such as AWS or Azure (preferred).
- Exposure to enterprise-level security monitoring and management solutions (preferred).

JOB REQUIREMENTS AND QUALIFICATIONS

Education
Degree in Cybersecurity, Computer Science, or a related field, along with relevant cybersecurity certifications (e.g., OSCP, CISSP, CEH), or equivalent professional experience in the cybersecurity required.

Experience
Professional hands-on experience with cybersecurity systems or enterprise computer systems administration.

WORK SCHEDULE

Ability to work 37.5 hours per week, occasionally after normal business hours. Ability to respond to emergency calls after normal business hours, 7 days per week, 24 hours per day and 365 days per year.