CYBERSECURITY ANALYST

Department: Information Technology & Telecom
Unit: 5210
Level: 5, Non-Exempt

Supervisor's Title: Cybersecurity Manager

Purpose

The Cybersecurity Analyst is responsible for safeguarding the organization's technology environment by monitoring cybersecurity systems, investigating alerts, and responding to security incidents. The role maintains and administers a wide range of cybersecurity tools, ensures compliance with security standards, and manages risk and reporting platforms to provide visibility into threats, vulnerabilities, and system integrity. The Analyst also supports awareness and prevention efforts through training initiatives, phishing simulations, DLP oversight, and vulnerability and patch management activities. Additionally, the Analyst provides user access administration, remote access support, forensic analysis, and hands-on assistance with hardware, software, and infrastructure components to strengthen the overall security posture of the organization.

ESSENTIAL JOB RESPONSIBILITIES

Security Monitoring & Incident Response

- Monitor, investigate, and troubleshoot alerts and events from all cybersecurity systems.
- Respond to, triage, and document security-related incidents, coordinating with internal teams and external partners as needed.
- Collect, analyze, and apply threat intelligence to enhance detection, response, and prevention capabilities.
- Perform computer forensics when needed to identify the root cause of security incidents.

Security Systems Administration & Maintenance

- Monitor and assist with the maintenance and configuration of cybersecurity systems, including IDS, email security, application whitelisting, AD change protection, and other security tools.
- Manage, support, and administer assigned security systems, cloud infrastructure security systems, and risk/compliance platforms.
- Patch applications and operating systems as needed and troubleshoot all security-related hardware, software, and systems.
- Assist with physical installation of cybersecurity hardware such as firewalls, servers, and appliances.

- Ensure ongoing security and system integrity of assigned information systems.

Risk, Compliance, & Reporting

- Develop and maintain dashboards and reports to track security incidents, investigations, vulnerabilities, and compliance status.
- Manage cybersecurity risk and compliance platforms, including documentation, reporting, stakeholder coordination, and vendor cybersecurity evaluations.
- Create, verify, and maintain documentation for assigned information systems.

Awareness, Training & Prevention

- Support cybersecurity awareness training programs, including designing, executing, and analyzing phishing simulations.
- Assist in the implementation, monitoring, and tuning of DLP policies and technologies to prevent unauthorized data access or exfiltration.

Vulnerability & Patch Management

- Support vulnerability and patch management programs, including platform management and hands-on patching.
- Assist with server and application monitoring system administration as part of maintaining secure operations.

Cross-Team Collaboration & Implementation Support

- Work with IT teams to securely implement new systems and enhance the security posture of existing systems.
- Attend meetings with business units and external contractors to advise on system implementation and cybersecurity best practices.
- Participate in research and development of emerging security technologies that may enhance or augment the current IT environment.

Access & Remote Support

- Administer and troubleshoot end-user remote access.
- Manage user creation and access rights across Active Directory, Entra ID, and local systems.

Performs other duties as assigned.

JOB REQUIREMENTS AND QUALIFICATIONS

Education

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

Experience

A minimum of 2 years' hands-on experience with cybersecurity systems or

enterprise computer systems administration.

SKILLS AND COMPETENCIES

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

WORK SCHEDULE AND REQUIREMENTS

- 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.
- Ability to pass Massport's controlled substance testing and background checks.