Cybersecurity Intern

Position Summary

We are seeking an enthusiastic Cybersecurity Intern to support our team with a range of cybersecurity operations, encompassing both Security Operations Center (SOC) Level 1 tasks and broader general cybersecurity initiatives. This internship provides an excellent opportunity for ITE students to apply their cybersecurity knowledge in a real-world environment, developing practical skills in security monitoring, incident response, threat detection, and overall security posture enhancement.

Key Responsibilities

Security Monitoring & Analysis (SOC Level 1)

- Monitor security dashboards and SIEM (Security Information and Event Management) systems for potential security incidents.
- Perform initial analysis of security alerts and events to determine severity and priority.
- Conduct basic log analysis to identify suspicious activities or anomalies.
- Track and document security incidents using ticketing systems.

Incident Response Support

- Assist with Level 1 incident response procedures for various security incidents.
- Escalate security incidents to senior analysts when required.
- Follow established playbooks and standard operating procedures for incident containment and resolution.
- Maintain accurate incident documentation and case notes.

Threat Intelligence & Research

- Research emerging cybersecurity threats, vulnerabilities, and attack methodologies.
- Assist in updating threat intelligence databases and contribute to threat analysis reports.
- Support the creation of security awareness materials to educate employees.
- Help maintain cybersecurity knowledge base and documentation, including security best practices.

General Security Operations & Risk Management

- Perform routine security checks and system health monitoring across various

platforms.
- Assist with vulnerability scanning, penetration testing support, and basic security assessment tasks.
- Support security compliance reporting activities and help ensure adherence to industry standards and regulations.
- Participate in security awareness initiatives and contribute to improving the overall security culture.
- Assist in the implementation and maintenance of security controls and technologies.

Administrative Tasks

- Update security policies, procedures, and guidelines documentation.
- Assist with security training material preparation and delivery.
- Support various cybersecurity projects as assigned, contributing to their successful completion.
- Maintain organized records of security activities, assessments, and incidents.

Required Qualifications

Education & Certification

- Currently enrolled in or recently completed an ITE cybersecurity-related program.
- Basic understanding of network security principles, including perimeter defense and segmentation.
- Knowledge of common cybersecurity frameworks (e.g., NIST, ISO 27001) and their application.
- Familiarity with various operating systems (Windows, Linux, macOS) and their security configurations.

Technical Skills

- Understanding of network protocols (TCP/IP, DNS, HTTP/HTTPS) and their vulnerabilities.
- Basic knowledge of firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus, and other security tools.
- Familiarity with log analysis and event correlation concepts, including the use of SIEM platforms.
- Basic understanding of malware analysis principles and common attack vectors (e.g., phishing, ransomware).
- Knowledge of common attack vectors and security threats, including web application vulnerabilities.

Soft Skills

- Strong analytical and problem-solving abilities with an inquisitive mindset.
- Excellent attention to detail and accuracy in all tasks.

- Good written and verbal communication skills for technical and non-technical audiences.
- Ability to work effectively in a collaborative team environment and independently when required.
- Proactive attitude and strong willingness to learn and adapt to new technologies.
- Ability to handle sensitive information with discretion and maintain confidentiality.

Preferred Qualifications

- Previous internship or project experience in cybersecurity, demonstrating practical application of skills.
- Basic certifications (e.g., CompTIA Security+, SANS GIAC) are a plus.
- Experience with SIEM tools (Splunk, QRadar, ELK Stack, Wazuh, etc.) for security monitoring and analysis.
- Understanding of incident response methodologies and digital forensics principles.
- Knowledge of scripting languages (Python, PowerShell, Bash) for automation and analysis.
- Familiarity with cloud security concepts (AWS, Azure, GCP) and best practices.