Cybersecurity Analyst

Position Details

Date of issue: August, 2026
Position number: 00021561
Department and Campus: Information Security (SITIS); University Services
Workplace Location: Remote
Collective Bargaining Unit (CBU): UMPSA
Job family and Wage grade: 1 – Information Technology; Grade 5
Essential Employee: Yes
Fair Labor Standards Act (FLSA): Exempt

Primary Purpose of Position

The Cybersecurity Analyst performs professional cybersecurity analysis work focused on monitoring, triaging, investigating, and responding to cybersecurity events and alerts affecting the University of Maine System's information systems, infrastructure, and data resources. The position serves as an operational analyst within the University's cybersecurity operations function, performing threat detection and analysis, supporting incident response and vulnerability management, and maintaining continuous security monitoring in accordance with established security processes and escalation procedures.

This position works collaboratively with cybersecurity engineering, Information Technology teams, external security operations partners, and campus stakeholders to investigate potential threats, coordinate response and remediation activities, document findings, and contribute response and remediation activities, document findings, contribute to the ongoing improvement of the University's security monitoring, detection, and response capabilities.

Essential Duties

1. Monitor and analyze security alerts and events generated by enterprise security platforms, including security information and event management (SIEM), endpoint detection and response (EDR), email security, network security, identity security, and cloud security tools.
2. Perform triage and initial analysis of security alerts, determine appropriate disposition, and escalate incidents, in accordance with established procedures, severity criteria, and escalation paths.
3. Investigate suspected cybersecurity incidents, including phishing, account compromise, malware activity, unauthorized access, and anomalous system or network behavior; document findings and recommend or initiate appropriate response actions within established procedures.

4. Support cybersecurity incident response activities, including containment, evidence collection, timeline development, documentation, and coordination with affected systems and data owners.
5. Conduct log analysis and correlate security activity across systems, networks, endpoints, identity platforms, and cloud environments to identify potential threats, indicators of compromise, and unauthorized activity.
6. Perform vulnerability management activities, including vulnerability scan execution, validation and analysis of findings, remediation tracking, and coordination with responsible IT teams on corrective actions.
7. Support the development, tuning, testing, and maintenance of detection rules, alert logic, and security monitoring use cases in collaboration with cybersecurity engineering and security operations leadership.
8. Process operational cybersecurity requests, including compromised account response, device isolation and return to production, and security review requests, in accordance with established procedures and authorization requirements.
9. Maintain accurate and timely cybersecurity operations documentation, including investigation records, incident tickets, findings, and operational runbooks.
10. Develop and maintain operational cybersecurity metrics and reports to support security operations monitoring, trend analysis, and program reporting.
11. Support identity and access management security operations, including account security reviews, compromised identity response, and multifactor authentication-related security activities.
12. Coordinate with external managed detection and response (MDR) and other security operations partners on alert escalation, investigation, information sharing, and response activities.
13. Participate in incident response exercises, tabletop scenarios, post-incident reviews, and cybersecurity operations improvement initiatives.
14. Use artificial intelligence, automation, scripting, and other appropriate technologies to support cybersecurity analysis, investigation, documentation, monitoring, reporting, and workflow efficiency, consistent with institutional requirements for data protection and responsible use.
15. Identify and recommend opportunities to improve cybersecurity operations, workflows, detection capabilities, documentation, and response processes based on operational experience and analysis.

Nonessential Duties

Perform other reasonably related duties as assigned.

Supervisory Responsibilities

This position has no supervisory responsibilities. May provide guidance or coordination for student employees or interns assisting with security operations activities.

Reporting Relationship

Reports to the Director of Cybersecurity Operations.

Knowledge, Skills, and Abilities

Required:

- Knowledge of cybersecurity operations concepts and practices, including security monitoring, alert triage, incident response, threat detection, and vulnerability management.
- Knowledge of common cybersecurity threats, attack techniques, indicators of compromise, and defensive practices.
- Working knowledge of networking, operating systems, identity and access management, and cloud environments as they relate to cybersecurity analysis and incident investigation.
- Knowledge of security monitoring and analysis technologies, including SIEM, endpoint detection and response (EDR), email security, identity security, network security, and vulnerability management tools.
- Ability to analyze and correlate logs, security events, alerts, and system activity to identify potential threats, anomalous behavior, and unauthorized activity.
- Ability to investigate cybersecurity events, assess available information, determine appropriate disposition, and recommend or initiate response actions within established procedures and authority.
- Ability to prioritize operational cybersecurity work, exercise sound judgment during investigations, and appropriately escalate complex or high-risk incidents.
- Ability to document investigations, findings, response actions, and operational procedures clearly and accurately.
- Ability to develop operational cybersecurity metrics and reports and identify trends or recurring issues requiring further review.
- Ability to use artificial intelligence, automation, scripting, and related technologies to support analysis, investigation, documentation, reporting, and workflow efficiency while maintaining appropriate data protection and responsible use.
- Strong written and verbal communication skills, including the ability to communicate cybersecurity information effectively to technical and nontechnical audiences.
- Ability to collaborate effectively with cybersecurity personnel, Information Technology teams, external service providers, and stakeholders across the University.

Qualifications

Required:

- Bachelor’s degree in Cybersecurity, Computer Science, Information Systems, Information Technology, or a related field, or an equivalent combination of education and experience.
- Five years of experience in information technology, cybersecurity operations, information security, security analysis, or a related field.

- Demonstrated experience performing cybersecurity analysis using security monitoring, incident response, vulnerability management, endpoint security, identity security, or related technologies.

Preferred:

- Relevant cybersecurity certification such as CompTIA Security+, CompTIA CySA+ (Cybersecurity Analyst), System security Certified Practitioner (SSCP), Microsoft SC-200, Global Information Assurance Certification (GIAC) Security Essentials (GSEC), or a comparable credential.
- Experience supporting cybersecurity incident response or security operations in a complex enterprise environment.
- Experience with scripting, automation, or orchestration used to support cybersecurity analysis, monitoring, investigation, reporting, or workflow efficiency.
- Experience with cloud security, identity security, endpoint security, or enterprise security monitoring technologies.
- Experience working with managed detection and response (MDR), security operations center (SOC), or other external cybersecurity service providers.
- Experience working in higher education, the public sector, or a complex multi-campus environment.
- Experience using artificial intelligence or other emerging technologies to improve cybersecurity analysis, workflows, reporting, or operational efficiency.

Note: University Services reserves the right to assign reasonably related additional duties and to change or reassign job duties.

Signatures

The signatures indicate the employee and immediate supervisor have reviewed the job description and had the opportunity to edit the document.

Employee: _____ Date: _____

Immediate Supervisor: _____ Date: _____