Classification	
Original Date:	April 2024
Revision Date:	September 2024
Pay Group:	28

CLASS SPECIFICATION

CYBERSECURITY ANALYST

NATURE AND SCOPE OF WORK

Reporting to the Manager, Centralised Security Services, (DTS) the cybersecurity analyst will perform technical work in support of the university cybersecurity operations and strategy. An incumbent in this position is primarily responsible for implementing and maintaining cybersecurity measures processes and controls, monitoring the digital ecosystem for security breaches, analysing and responding to complex cybersecurity-related alerts and incidents, monitoring network and system logs, network traffic for cybersecurity incidents, implementing technical projects relating to cybersecurity, and participating in the development and implementation of the university's cybersecurity strategy and programs.

ILLUSTRATIVE EXAMPLES OF DUTIES

- Implements, and maintains cybersecurity measures, processes and controls as guided by developed cybersecurity frameworks, critical security controls and the National Cybersecurity Assessment (NCA) framework.
- Uses established processes to complete work outlined in cybersecurity programs such as digital security services, identity and access management and cybersecurity to ensure all digital solutions are cybersecurity compliant.
- Proactively monitors the digital ecosystem using industry standard tools to detect malware, suspicious activity, and breaches across all levels of the digital ecosystem, including network, services, cloud infrastructure, software, and systems.
- Monitors infrastructure components related to cybersecurity including security information and event management (SIEM) platform, firewalls, endpoint protection, intrusion detection/intrusion prevention system (IDS/IPS), active directory, Azure security tools, Office 365 advanced threat protection and others.
- Maintains the enterprise security architecture; contributing to the development of operational and tactical plans related to cybersecurity.
- Collaborate with DTS teams to identify security gaps and implement approved solutions.

- Implements and monitors a server and endpoint patch management strategy.
- Provides recommendations and guidance to the central cybersecurity services management team on maintaining an appropriate level of cybersecurity maturity. Implements approved recommendations.
- Participates and provides the appropriate level of response to security breaches including incident response as required by the centralized security services management team.
- Perform security audits to assess the effectiveness of policies, procedures and security measures to ensure continued risk mitigation, protection of assets, and maintain compliance with industry standards, regulations, and laws.
- Prepare audit plans, document all reviews, present recommendations for DTS policy revisions, data analysis, reporting, and follow up and monitoring.
- Investigates and responds to cybersecurity alerts and incidents, including troubleshooting, researching, and implementing technical solutions.
- Participates in technical assessments, performs security threat risk assessments (STRA) and follows up with DTS teams for risk mitigation on any identified risks.
- Prepares reports for the technical assessments and STRAs.
- Develops and delivers cybersecurity training materials, participates in the annual refresher cycle ensuring that the university community is cybersecurity training compliant.
- Coordinate and develop prioritized action plans for vulnerability and penetration tests as directed by the central cybersecurity services management team.
- Performs other duties related to the requirements and qualifications of the position.

REQUIRED KNOWLEDGE, ABILITIES AND SKILLS

- Experience and knowledge of security technologies, including SIEM platforms, firewalls, network and intrusion prevention / detection systems, authentication and identity management platforms, and endpoint protection solutions.
- Experience and knowledge of cybersecurity best practices, including incident response processes and procedures.
- Experience and knowledge of Microsoft Office 365 and Azure environments, including security capabilities and technologies.
- Experience in problem solving, performing investigations, data analytics and strong ability to make meaning from large volumes of data to inform decision making.
- Ability to exercise tact, diplomacy, discretion, and sensitivity when dealing with university community members.

- Understands the context of issues to exercise initiative and judgement regarding action required.
- Ability to multitask, maintain attention to detail, apply organization skills to meet deadlines, and work with minimal supervision.
- Ability to understand and follow complex verbal and written instructions, and communicate information effectively, both verbally and in writing.
- Ability to present complex ideas and information in a creative and visual way for different levels of the university community,
- Experience in delivering cybersecurity training.
- Ability to adapt to changing situations, anticipate needs, and reprioritize tasks efficiently.
- Strong collaboration and coordination skills to maintain effective working relationships with other DTS teams and within the university community.

REQUIRED TRAINING AND EXPERIENCE

- 3+ years of relevant professional experience, with 1 year in a public sector environment.
- Experience with cybersecurity processes, procedures, and tools.
- Experience in conducing audits, assessments and writing STRA reports.
- Experience in performing investigations related to cybersecurity in one or more of the following areas: Network, server, endpoint, Azure cloud, Active Directory, Office 365
- Direct related experience assuming progressively more technology and systems related duties, including experience with security technologies, IT infrastructure, identity management, and cybersecurity platforms
- A bachelor's degree.
- Completion of courses or certificates related to cybersecurity credentials such as CISSP, CISA, CRISC, ITIL, TOGAF, Microsoft, Cisco, Palo Alto etc.
- Experience with the ITIL framework and ITSM best practices, tools, and techniques; ITIL certification is an asset.
- Experience in effectively communicating and preparing cybersecurity information.
- Completion of a criminal record check.