Cybersecurity Analyst

Capilano University is named after Chief Joe Capilano (1854–1910), an important leader of the Skwxwú7mesh (Squamish) Nation of the Coast Salish Peoples. We respectfully acknowledge that our campuses are located on the unceded territories of the səlilwətaɬ (Tsleil-Waututh), shíshálh (Sechelt), Skwxwú7mesh (Squamish), and xʷməθkʷəy̓əm (Musqueam) Nations.

At Capilano University we are committed to supporting a campus community that is both diverse and inclusive. We believe that diversity within our workforce is essential in creating both an exceptional student and employee experience. As part of our ongoing commitment to Diversity, Equity and Inclusion (DEI), we strive to ensure that our recruitment campaigns authentically reflect the diverse community we serve. We actively encourage applications from Indigenous Peoples, Black and racialized persons, persons with disabilities, women, and members of the 2SLGBTQIA+ community, as we value the unique perspectives, lived experiences, and skillsets each individual brings to CapU.

To help us focus our efforts, we encourage all applicants to complete a short anonymous questionnaire, if they wish. The results of the questionnaire are not linked to you or your application and do not form part of the selection process. The goal of collecting this anonymous data is to gain a better understanding our organizational reach, while continuously working to improve the diversity of our applicant pool.

All qualified candidates are encouraged to apply; however, Canadians and permanent residents will be given priority. Should you require accommodations during the hiring process please reach out to jeremyorsted@capilanou.ca (faculty), or mimibuan@capilanou.ca (Ad/Ex and Staff).

Position Title: Cybersecurity Analyst

Union: MoveUP

Department: Digital Technology Services (DTS)

Position Status: Regular Full-Time

Position Number: S99194

Position Start Date: As soon as possible

Job Posting Open Date: March 9, 2026

Job Posting Close Date: Open until filled

Pay Group: 28

Salary: $6,430.00 per month (with increments to a max of $7229.00 per month)

Location: North Vancouver

Working with us

As a member of the Digital Technology Services (DTS) team here within Capilano University, you will be a vital asset in providing an exceptional experience to both our employee and student communities through invention, collaboration, and technical talent.

As we embark on our university wide digital transformation, we'll be seeking fellow trailblazers to join our teams as we integrate state of the art technologies. With a variety of projects and initiatives in the pipeline, there is no shortage of opportunity to innovate.

Within our teams, you'll be working alongside a variety of talented individuals involved in initiatives focused on cyber security, data analysis, operational analytics, quality assurance, integration, customization, and implementation.

Do you have a passion for optimization? Join us in creating a lasting impact that goes beyond routine tasks, contributing to the long-term success of our technological landscape and the university community

About the role

Reporting to the Manager, Centralized 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.

Experience, competencies & qualifications

▪ 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.
▪ 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.

For more information, please see the complete **job description**.

Benefits

At Capilano University, we understand that there is more to life than work. That is why we offer comprehensive benefits and support to help you and your family live a balanced life. Take a sneak peak to see what it is like to work at Capilano University.

Days and Hours of Work:

Our standard work week is Monday to Friday, 8:30am – 4:00pm, or dependent on the needs of the department.

How to apply

Please submit your application package to talentacquisition@capilanou.ca and be sure to included the following:

1) The position tile and position number in the subject line of your email. Ex: *Cybersecurity Analyst – Position number S99195*
2) Your resume and cover letter. We will let you know if we require any further documents for your application, such as proof of education, for example.
3) Your responses to the supplemental questions shared below. Please include both the question and your response in the body of the email:
    a. *Are you legally entitled to work in Canada?* *(i.e. valid work permit, permanent resident, Canadian citizen)*
    b. *Do you have a bachelor's degree? (Simply Yes or No)*
    c. *Do you have experience with and knowledge of security technologies, including SIEM platforms, firewalls, network and intrusion prevention / detection systems, authentication and identity management platforms, and endpoint protection solutions? (Simply Yes or No)*
    d. *Do you have 3+ years of relevant professional experience, with 1 year in a public sector environment? (Simply Yes or No)*
    e. *Have you completed courses or certificates related to cybersecurity credentials such as CISSP, CISA, CRISC, ITIL, TOGAF, Microsoft, Cisco, Palo Alto etc.? (Simply Yes or No)*

Thank you for your interest in this opportunity with us at Capilano University!