

# Program Information

## Cybersecurity Analyst

2025/2026

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Program Overview</b>         | <p>The Cybersecurity Analyst Advanced Diploma is a comprehensive program designed to prepare students for successful careers in cybersecurity.</p> <p>The curriculum covers core topics such as computer network fundamentals, cybersecurity essentials, ethical hacking, diagnostics and repair, Python programming for ethical hackers, security governance, risk management, and Security Operations Centre (SOC) analyst training.</p> |
| <b>Area of Study</b>            | Information and Communication Technologies                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Credential</b>               | Advanced Diploma                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Program Length</b>           | <p>2 Years   Full time (20 months)</p> <p>Students in this program can expect to attend classes for 8 months, followed by a 4-month break, and then another 8 months of study. This excludes student success weeks and holidays.</p>                                                                                                                                                                                                       |
| <b>Delivery</b>                 | <p>In-classroom</p> <p>This program is primarily taught in person during full-day sessions, with less than 10% of course content delivered online.</p>                                                                                                                                                                                                                                                                                     |
| <b>Work-Integrated Learning</b> | 7-week practicum                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                                       |         |
|---------------------------------------|---------|
| <b>Open to International Students</b> | Yes     |
| <b>CIP Code</b>                       | 11.1003 |

## Career Outcomes

- Cybersecurity Analyst
- Security Operations Center (SOC) Analyst
- Penetration Tester
- Ethical Hacker
- Cybersecurity Incident Responder
- Network Security Specialist

## All Courses

| <b>Course Name</b>                           | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>Hours</b> |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Fundamentals of Computer Systems (CBRS-1000) | This course introduces students to the foundational concepts of computer systems, including hardware, software, operating systems, networking, and basic security. Students will learn how to assemble and configure computers, install and troubleshoot operating systems, and set up simple networks. The course also covers basic network security principles, secure wireless configurations, and troubleshooting common IT issues. Through hands-on activities, students will develop essential technical skills for further studies and IT careers. | 91 hours     |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Cybersecurity Essentials (CBRS-1010) | Cybersecurity Essentials teaches comprehensive cybersecurity concepts and skills at the entry-level, from threat mitigation and defence to post-incident forensics. Learners will progress from basic cybersecurity concepts to experiences in assessing vulnerabilities and risks. With video and rich interactive media support, participants learn, apply, and practice cybersecurity knowledge and skills through a series of in-depth, hands-on experiences and simulated activities that reinforce their learning.                                          | 91 hours |
| Communication Essentials (COMM-1000) | This course is designed to equip participants with the essential skills needed for effective communication within various professional settings in Canada. The course combines lectures, interactive workshops, group discussions, and practical exercises to ensure a comprehensive learning experience. Participants will engage in real-world scenarios and case studies appropriate for a range of industries to apply the concepts learned in class. Feedback from peers and instructors will refine and enhance communication skills throughout the course. | 42 hours |
| Computer Networking I (CBRS-1100)    | This course provides a comprehensive introduction to networking architectures, models, protocols, and components essential for connecting users, devices, applications, and data across modern computer networks and the internet. Students will gain hands-on experience in performing basic configurations for routers and switches to build simple local                                                                                                                                                                                                       | 91 hours |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                    |                 |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
|                                                  | <p>area networks (LANs), including the integration of IP addressing schemes and foundational network security. Additionally, the course covers configuring VLANs, Inter-VLAN routing, and applying security best practices. Students will also develop troubleshooting skills for inter-VLAN routing on Layer 3 devices, ensuring a thorough understanding of network operations and security.</p> |                 |
| <p>Cloud Fundamentals (AWS) (CBRS-1020)</p>      | <p>The Cloud Fundamentals (AWS) course is designed to provide a comprehensive understanding of cloud computing with a focus on Amazon Web Services (AWS). This course covers the essential concepts of cloud computing, the benefits of adopting AWS for business operations, and practical skills for leveraging AWS services to optimize and transform business processes.</p>                   | <p>49 hours</p> |
| <p>Windows Server Administration (CBRS-1110)</p> | <p>This course provides hands-on experience in configuring and managing Windows Server roles and services. Students will deploy Active Directory, configure DNS and DHCP, manage NTFS permissions, virtualization, and deploy Windows Server on Microsoft Azure, building foundational skills in Windows Server and cloud infrastructure.</p>                                                      | <p>91 hours</p> |
| <p>Computer Networking II (CBRS-1200)</p>        | <p>Computer Networking II builds on the foundational concepts covered in Computer Networking I, further developing students' skills in switching technologies, routing operations, and enterprise network security. Students will learn to configure and troubleshoot</p>                                                                                                                          | <p>91 hours</p> |

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                 |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
|                                                      | <p>small-to-medium business networks, including wireless local area networks (WLANs), while identifying and mitigating LAN security threats. The course also explores enterprise network architectures, security considerations, and network management tools. Additionally, students will gain hands-on experience in protecting networks against cybersecurity threats, preparing them for more advanced networking roles.</p>                                                                                                                                                                                                                                                           |                 |
| <p>Technical Writing and Documentation (NSA-590)</p> | <p>This course is designed for IT professionals seeking to enhance their technical writing skills, with a focus on language use within the IT and cyber-security industries. Participants will explore the linguistic aspects of creating high-quality technical documents, such as proposals, manuals, process guides, and cyber-security-related materials. Through hands-on practice, students will learn the structure and format of these specialized documents and gain practical experience by crafting them. This approach equips participants with the skills to effectively and precisely communicate complex information tailored to technical and cyber-security contexts.</p> | <p>42 hours</p> |
| <p>Linux for Cybersecurity (CBRS-1160)</p>           | <p>This course provides a practical introduction to essential Linux system administration skills. Students will gain proficiency in Linux command-line navigation, managing files and users, setting permissions, and monitoring processes. They will delve into Linux networking, software management, task scheduling, and bash scripting. The</p>                                                                                                                                                                                                                                                                                                                                       | <p>91 hours</p> |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                 |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
|                                          | <p>course also covers system security, storage solutions, and the basics of web services, databases, and containerization. Through practical exercises, students will develop the skills needed to effectively manage and troubleshoot Linux systems.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                 |
| <p>Database Fundamentals (CBRS-1130)</p> | <p>Database Fundamentals covers essential topics in database administration, including understanding database types and structures, recognizing standards and commands, and running scripts for data systems. You will learn about the impact of programming on database operations, database planning and design, and the implementation, testing, and deployment of databases. Additionally, the course includes monitoring and reporting on database performance, data maintenance processes, governance, and regulatory compliance, and securing data, data access, and the database server. It also addresses classifying types of attacks and planning for disaster recovery, as well as best practices for backup and restore operations. The course will integrate video, interactive media support, lectures, hands-on activities, discussions, group activities, and scenario simulations to reinforce learning.</p> | <p>63 hours</p> |
| <p>Firewall Applications (CBRS-1220)</p> | <p>This course provides students with the knowledge and hands-on experience needed to configure, manage, and monitor Next-Generation Firewalls. Through practical in-class activities, students will develop the skills necessary to implement firewall security policies, configure Network Address Translation (NAT), and</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>63 hours</p> |

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                      | enforce Threat Prevention strategies to safeguard networks from known and emerging threats. Additionally, students will learn to monitor network traffic using the firewall's interactive web interface and reporting tools. By the end of the course, students will be proficient in deploying and managing essential firewall features to enhance network security.                                                                                                                                                                                                                              |          |
| Fundamentals of Web Development (CBRS-1140)          | The Fundamentals of Web Development course introduces essential web development skills for future cybersecurity professionals. Students will learn the basics of HTML, CSS, and JavaScript to build simple web pages and gain a foundational understanding of how web applications function. Alongside development skills, the course introduces key security concepts, enabling students to recognize common vulnerabilities in web applications. Through hands-on practice, students will learn how to apply basic security measures, preparing them for more advanced studies in cybersecurity. | 56 hours |
| Introduction to Programming Using Python (CBRS-1150) | Students will learn the basics of programming using the Python Programming Language. Students will solve problems, explore real-world software development challenges, and create practical and contemporary applications.                                                                                                                                                                                                                                                                                                                                                                         | 56 hours |
| Ethical Hacking I (CBRS-2100)                        | This course offers a thorough introduction to ethical hacking, encompassing core principles, methodologies, and legal considerations. Students will delve into                                                                                                                                                                                                                                                                                                                                                                                                                                     | 91 hours |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                      | various techniques including information gathering, vulnerability assessment, system exploitation, and defense tactics against cyber threats such as malware, social engineering, and denial-of-service attacks. Hands-on exercises and real-world scenarios deepen proficiency in cybersecurity, equipping students for roles in penetration testing and defensive security strategies.                                                                                                                                                                                                          |          |
| Ethical Hacking II<br>(CBRS-2200)    | This course covers advanced ethical hacking techniques across diverse digital environments. Students will learn session hijacking, evasion of IDS, firewalls, and honeypots, and how to exploit vulnerabilities in web servers, applications, and databases. The course also covers wireless network hacking, securing mobile platforms, IoT, OT systems, cloud environments, and applying cryptography to protect data and communications.                                                                                                                                                       | 91 hours |
| IT Project Management<br>(CBRS-1050) | This course equips cybersecurity professionals with the skills and knowledge to successfully manage projects from initiation to completion. Participants will learn how organizational factors influence project success, develop essential initiation documents, and build project teams. The course covers key project management processes, including planning, scheduling, resource allocation, risk management, communication, and change management. Participants will also gain practical experience in executing projects, addressing challenges, and ensuring successful project closure | 49 hours |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                            | through reviews and lessons learned. By the end, learners will have the tools to effectively lead and contribute to projects in cybersecurity environments.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          |
| Applied Penetration Testing I (CBRS-2300)  | This course provides an in-depth exploration of the foundational skills required for effective penetration testing, focusing on the red team role. Students will master the penetration testing process, from reconnaissance and enumeration to exploitation and lateral movement. Key topics include network enumeration, vulnerability assessment, password attacks, and Active Directory exploitation. By the end of the course, students will be equipped with the skills necessary to identify, exploit, and pivot within target systems, laying the groundwork for advanced offensive security techniques. | 91 hours |
| Applied Penetration Testing II (CBRS-2400) | Building on the skills from Applied Penetration Testing I, this course focuses on web application exploitation, post-exploitation techniques, and enterprise network attacks. Students will explore SQL injection, XSS, file upload vulnerabilities, and privilege escalation on both Linux and Windows systems. The course concludes with a capstone project where students conduct simulated attacks on enterprise networks, followed by comprehensive documentation and reporting to simulate real-world red team engagements.                                                                                | 91 hours |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Python for Ethical Hackers (CBRS-2010) | This course is tailored for students who have completed an introductory course in Python programming. The course delves into the practical applications of Python in the field of ethical hacking and cybersecurity, focusing on automating security assessments, developing hacking tools, and enhancing network security.                                                                                                                                                                                                                                                                                                               | 49 hours |
| SOC Analyst I (CBRS-2110)              | This course equips students with the foundational skills to monitor, detect, and respond to security incidents as a SOC Analyst. It focuses on real-time security monitoring, log analysis, and threat detection, providing hands-on experience with SIEM tools like Splunk and Elastic. Students will learn to analyze event logs from different sources, investigate threats, and examine network traffic to identify malicious activity. Through practical labs and in-class activities, they will strengthen their ability to recognize attack patterns, implement defensive measures, and effectively respond to security incidents. | 91 hours |
| SOC Analyst II (CBRS-2210)             | This advanced course builds on SOC Analyst I, focusing on malware analysis, digital forensics, and advanced threat detection techniques. Students will gain hands-on experience with tools like YARA and Sigma for rule-based detection, investigate Windows attacks using Splunk, and conduct in-depth forensic analysis. The course also covers proactive threat hunting, security incident reporting, and effective communication of incidents. Through practical exercises, in-class activities, and an applied project,                                                                                                              | 91 hours |

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |          |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                     | students will reinforce real-world SOC operations, enhancing their ability to investigate, respond to, and mitigate cyber threats.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |          |
| Security Governance and Risk Management (CBRS-2500) | This course is a cornerstone of the Cybersecurity program, designed to equip students with the strategic insights necessary to manage and govern security within an organization. This course explores the critical aspects of security governance, including policy development, risk assessment methodologies, compliance obligations, and the alignment of security strategy with organizational goals.                                                                                                                                                                                                                                                                                                                                                                                                  | 49 hours |
| Global Citizenship (GLOB-1000)                      | Inspired by the United Nations' Sustainable Development Goals, this course introduces students to global challenges and issues to broaden their knowledge, skills, and perspectives on the world today. Through discussions, readings, and online and in-class activities, students will explore diverse cultural perspectives, critically examine systems of oppression and discrimination, and engage with the stories and experiences of global citizens who have fought for social justice, human rights, and environmental sustainability around the world. Students will emerge from this course with greater cultural competence, improved intercultural communication skills, and a deepened commitment to promoting diversity, equity, and inclusion at work, at school, and in their communities. | 42 hours |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <p>Cybersecurity Analyst Practicum (CBRS-3900)</p>       | <p>This seven-week practicum provides students with the opportunity to gain real-world experience by working with industry employers in professional settings. Students will apply their knowledge and skills in diverse roles, adapting to the specific needs and operations of their host organizations. This practical experience enhances their readiness for the workforce, offering valuable insights into professional environments. The practicum serves as a capstone experience, bridging academic learning with real-world application.</p>                                                                                                                                                                                                                                                                                                                                   | <p>217 hours</p> |
| <p>Cybersecurity Analyst Applied Project (CBRS-3500)</p> | <p>This seven-week course offers students the opportunity to apply the skills and knowledge gained throughout their program to complete a comprehensive, real-world project. Working individually or in teams, students will address a cybersecurity challenge by designing, implementing, and documenting a solution in areas such as threat detection, vulnerability assessment, penetration testing, or security operations. Through this hands-on experience, students will strengthen their problem-solving, research, and technical skills, preparing them for professional roles in the field. The course culminates in a tangible deliverable, such as a security tool, a proof-of-concept implementation, or a detailed assessment report. This project-based alternative is ideal for students seeking to further develop their expertise and showcase their capabilities.</p> | <p>217 hours</p> |