Southern Alberta Institute of Technology
1301 16th Avenue NW
Calgary, Alberta T2M 0L4
Canada
Toll-free: 1.877.284.7248
sait.ca

EDGE UP – Cybersecurity for Today's World

SAIT offers a 17-week full-time program in Cybersecurity for Today's World in association with Calgary Economic Development, with support from Future Skills Centre. Graduates of this program will develop skills to identify and interpret information security threats and risks in a business context. They will learn to review, analyze and evaluate incoming cybersecurity threats that impact strategy and operations. Graduates of this program will receive a SAIT Certificate of Achievement.

The ideal candidate for the Cybersecurity for Today's World program has a previous post-secondary diploma or degree. You recognize the critical nature of cybersecurity and are intrigued by the ever-changing ways that both corporate and personal information continue to be compromised. You have a strong ethical standard and a curious mind. A previous technical discipline or basic literacies in python programming and 'C' language programming is an asset.

Learning Objectives

- Develop skills to identify and interpret information security threats and risks in a business context.
- Adapt industry-standard frameworks to propose practical solutions to mitigate risks.
- Learn to investigate cybersecurity events or crimes related to IT systems, networks and digital assets.
- Learn the strategies and tools to prepare you to manage cybersecurity threats that can occur in the ever-changing cybersecurity threat landscape.
- Explore current cyber security environment, security laws and ethical practices.

Topics of Instruction

- Network Security Protocols
- Programming Foundations for Cybersecurity
- Security Tools
- Enterprise Network Security
- Cybersecurity Frameworks
- Risk Identification and Management
- Vulnerability, Threats and Attacks
- Cyberspace and Cyber Domain

Southern Alberta Institute of Technology
1301 16th Avenue NW
Calgary, Alberta T2M 0L4
Canada
Toll-free: 1.877.284.7248
sait.ca

Program Timeline:

- Foundations of Digital Transformation Course: March 29 - April 1, 2022 (8:30am – noon)
- Cybersecurity Training Program: April 4 – July 29, 2022 (8:00am – 3:00pm)

Program Details:

- Program schedule is 8:00am-3:00pm Monday to Friday (except for stat holidays)
- Time commitment (instructional and assignment/project work): 40-50 hours per week
- Virtual delivery via Zoom or MS Teams
- Online learning expectations for success in the program
- All students will require a computer or laptop for their program with the following recommended specifications:

Standards	**Hardware**	***Software***
Processor	i7	Windows 10 Pro 64-bit (MacOSX is not supported) Antivirus/malware protection
RAM (memory)	16 GB RAM or greater	
Hard drive storage	512 GB SSD or greater	
Video card	On-board integrated	
Screen size	15" or greater	
Screen resolution	1920 x 1080 or greater	

Is this program the right fit for me?

- This program requires a commitment of both time and energy. Students who experience success are those who make their education a priority throughout the program and are open to new learning experiences and working with others. We find there is a direct correlation between the time and energy invested to the amount of success achieved. Learners with strong time-management, adaptability, and discipline have a greater propensity to succeed. Remaining focused and diligent with course work is important for success in completing the program.

Southern Alberta Institute of Technology
1301 16th Avenue NW
Calgary, Alberta T2M 0L4
Canada
Toll-free: 1.877.284.7248
sait.ca

Topic Descriptions:

Programming Foundations for Cybersecurity

- This introductory course provides students the basic principles of programming applicable to program design and exploitation. Principles are illustrated using an intermediate, compiled language such as C. The examination of program data structures and execution flow is emphasized in the lab using debuggers; as well as how basic program instructions are implemented in assembler.

Network Security Protocols

- This introductory course provides students a grounding in basic switching, routing and general protocols. These are analyzed and implemented from both a functionality and vulnerability viewpoint. The configuration of defensive and offensive tools is practiced in the lab environment.

Cybersecurity Frameworks

- Students will learn current industry security control frameworks and apply accepted practices to function within various security environments.

Enterprise Network Security

- This course teaches students the skills needed to obtain entry-level positions as security specialists. It provides a hands-on introduction to network security. This course introduces the core security concepts and skills needed to monitor, detect, analyze, and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. Students will gain practical, hands-on skills needed to maintain and ensure security operational readiness of secure networked systems.

Cybersecurity Risk Management

- Students will classify security risks and threats to assess the impact on business operations. Exploration of current cyber threats will assist the students in identifying potential impacts of security breaches.

Southern Alberta Institute of Technology
1301 16th Avenue NW
Calgary, Alberta T2M 0L4
Canada
Toll-free: 1.877.284.7248
sait.ca

Cybersecurity Tools

- In this course, you will learn the strategies and tools to prepare you to manage cybersecurity threats that can occur in the ever-changing cybersecurity threat landscape. You will explore all phases of ethical hacking, including reconnaissance, scanning, gaining and maintaining access, and clearing tracks. You will learn about vulnerability scanning, wireless and web attacks, malware and system exploits. Finally, you will explore how to discover and remediate security vulnerabilities, provide measures to defend systems, respond to security incidents, and design and implement security controls for system hardening.

Cyberspace and the Cyber Domain

- As global cyber security evolves, it is important for industry professionals to understand current developments. In this course, students will explore the current cyber security environment, security laws and ethical practices. Students will analyze the use of cyber capabilities as the fifth domain of warfare, learn how to make an organization's cyber assets resilient, and implement incident response plans. Focus is also placed on communicating security-related issues to an organization's senior management.

Cyber Threats, Vulnerability and Attacks

- This course examines the concepts used in the threat and vulnerability management of industrial control systems. You will consider the real-life examples in managing threats, vulnerabilities of ICS systems and attacks aimed at ICS systems. You will also learn how to leverage cyber intelligence including darkweb based cyber intelligence in improving the cyber maturity of an industrial control system.

Cybersecurity Capstone Project

- The capstone course provides students with the opportunity to explore a problem or issue presented by an organization and address it through applied research. Students should have a command of skills and knowledge in cybersecurity principles including:
    - identifying and interpreting information security threats and risks in a business context
    - reviewing, analyzing and evaluating incoming cybersecurity threats that impact strategy and operations.
- The capstone allows students to demonstrate an integration of technical skill and knowledge, professional competencies and development/execution strategies.