Area of Interest: Advanced Technology

Computer Systems Technology - Security - Pathway for Computer Systems Technician

Ontario College Advanced Diploma Program Code: 0156A01FWO

3 Years

Ottawa Campus

Our Program

Further your studies to specialize your IT career in the advancing field of Security.

Graduates of the Computer Systems Technician Ontario College Diploma program may be interested in furthering their knowledge and skills with this third year of study.

This third-year Computer Systems Technology - Security Ontario College Advanced Diploma program prepares you to perform a critical role in securing the confidentiality, integrity and availability of business-critical data, transactions and network infrastructure.

In this program you develop the theoretical knowledge and hands-on skills to assess, recommend, implement, and troubleshoot various advanced security solutions and countermeasures. Throughout the program, you have access to modern computing facilities that run Windows and Linux/UNIX-based operating systems that support a variety of pre-installed software applications. Algonquin College also offers specialized networking, Cisco and hardware labs.

Learn how to deploy modern security countermeasures against threats to IT infrastructure and how to validate and evaluate security controls.

Discover common techniques used in digital forensics and investigations, and how to participate in the investigation and incident response process. Learn how to design effective corporate policies and IT forensic concepts and tools, and study the legal process and proper evidence gathering procedures.

Graduates of this program may find careers in:

- private industrial government and service sectors
- privately managed security firms
- security audit/penetration consulting firms
- law enforcement agencies and security agencies

There may also be opportunities as:

- a network security specialist
- an IT network security consultant
- a corporate information security manager and officer

SUCCESS FACTORS

This program is well-suited for students who:

- Enjoy solving problems and challenging their minds.
- Have an inquisitive, well-organized and analytical nature.

- Can work effectively independently and with others in a corporate team environment.

- Enjoy analyzing problems of a complex nature and providing solutions.

Employment

Graduates may find employment in a variety of domains in the private, industrial, governmental and service sectors such as: privately managed security firms; security audit/penetration consulting firms; law enforcement agencies (RCMP, OPP, local police forces) and associated security agencies (CSIS, CSE); information technology consulting firms; primary communications carriers and information service providers; and users of information networks, including government organizations; small, medium-sized and large business enterprises; public organizations (financial, healthcare).

Positions in the Information Technology environment may include: corporate information security or security administrator (junior to intermediate level); corporate information security manager/ officer (junior to intermediate level); network security specialist (junior to intermediate level); IT/ network security consultant (junior to intermediate level); IT/network security architect/designer (junior to intermediate level); security auditor/penetration tester (junior to intermediate level); digital forensic analyst/consultant/investigator (junior to intermediate level); IT/network security and compliance analyst/investigator (junior to intermediate level); technical support specialist - security (intermediate level); technical integration sales representative and support (intermediate level).

Learning Outcomes

The graduate has reliably demonstrated the ability to:

- Identify, analyze, design, develop, implement, verify and document the requirements for a computing environment.

- Diagnose, troubleshoot, document and monitor technical problems using appropriate methodologies and tools.

- Analyze, design, implement and maintain secure computing environments.

- Analyze, develop and maintain robust computing system solutions through validation testing and industry best practices.

- Communicate and collaborate with team members and stakeholders to ensure effective working relationship.

- Select and apply strategies for personal and professional development to enhance work performance.

- Apply project management principles and tools when responding to requirements and monitoring projects within a computing environment.

- Adhere to ethical, social media, legal, regulatory and economic requirements and/or principles in the development and management of the computing solutions and systems.

- Investigate emerging trends to respond to technical challenges.

- Analyze, plan, design, implement and administer computer systems and cloud solutions.

- Research, design, deploy, configure, troubleshoot, maintain, upgrade, and decommission computing system infrastructures.

- Select and apply scripting tools and programming languages to automate routine tasks.

- Install, monitor, optimize and administer a database management system in response to specified requirements.

- Design, implement, and administer technical support processes for computing system infrastructures that aligns with industry best practice.

- Implement defence line using security control to effectively detect and respond to various

- Implement defence line using security control to effectively detect and respond to various cyber attacks and threats.

- Identify and apply discipline-specific practices that contribute to the local and global community through social responsibility, economic commitment and environmental stewardship.

Program of Study

Level: 05	Courses	Hours
CST8601	Securing Routers and Switches	84.0
CST8602	Fundamentals of Penetration Testing	84.0
CST8603	Security Law and Compliance	42.0
CST8604	Information Security Risk Management	42.0
Level: 06	**Courses**	**Hours**
CST8605	Advanced Security Appliances	70.0
CST8606	Fundamentals of Digital Forensics and Discovery	70.0
CST8607	Applied Cryptography	70.0
CST8608	Fundamentals of Cyber Incident Response	56.0
CST8609	Business Continuity and Disaster Recovery	56.0

Fees for the 2023/2024 Academic Year

Tuition and related ancillary fees for this program can be viewed by using the Tuition and Fees Estimator tool at https://www.algonquincollege.com/fee-estimator .

Further information on fees can be found by visiting the Registrar`s Office website at https://www.algonquincollege.com/ro .

Fees are subject to change.

Additional program related expenses include:

- Books and supplies cost approximately $260 in Level 05 and $150 in Level 06 and can be purchased at the campus store.

Admission Requirements for the 2024/2025 Academic Year

Program Eligibility

- Successful completion of Computer Systems Technician Ontario College Diploma, with a cumulative GPA of 2.7 or higher and completion of a pre-admission assessment with a minimum grade of 70% is required. Self-directed Cisco CCNA modules are available to assist students in preparation of the assessment. Students are required to apply through http://www.ontariocolleges.ca/ .

Admission Requirements for 2023/2024 Academic Year

Program Eligibility

Successful completion of Computer Systems Technician Ontario College Diploma, with a cumulative GPA of 2.7 or higher and completion of a pre-admission assessment with a minimum grade of 70% is required.

Self-directed Cisco CCNA modules are available to assist students in preparation of the assessment. Students are required to apply through ontariocolleges.ca.

Application Information

COMPUTER SYSTEMS TECHNOLOGY - SECURITY -
Pathway for Computer Systems Technician
Program Code 0156A01FWO

Algonquin College Computer Systems Technician - Networking students that have graduated 2 or more years ago must apply to the program through http://www.ontariocolleges.ca/ .

Computer Systems Technician students are required to apply through http://www.ontariocolleges.ca/ .

For those applicants required to apply through Ontario Colleges, applications must be submitted with official transcripts showing completion of the academic admission requirements through:

ontariocolleges.ca
60 Corporate Court
Guelph, Ontario N1G 5J3
1-888-892-2228

Applications for Fall Term and Winter Term admission received by February 1 will be given equal consideration. Applications received after February 1 will be processed on a first-come, first-served basis as long as places are available.

For further information on the admissions process, contact:

Registrar`s Office
Algonquin College
1385 Woodroffe Ave
Ottawa, ON K2G 1V8
Telephone: 613-727-0002
Toll-free: 1-800-565-4723
TTY: 613-727-7766
Fax: 613-727-7632
Contact: https://www.algonquincollege.com/ro

Additional Information

Curriculum is reviewed annually to reflect evolving industry standards in the information technology field.

Course Descriptions

CST8601 Securing Routers and Switches

Securing routers and switches along with their associated networks, how to recognize threats, and vulnerabilities to networks and how to implement basic mitigation measures are explored. Topics covered include security threats facing modern network infrastructures, securing routers, implementing basic AAA, using ACLs to mitigate router and network threats, implementing secure management and reporting, mitigating common Layer 2 attacks, implementing firewall features, IDS/IPS and VPN features. This course is based on material from the Cisco Networking Academy - Network Security course.

Prerequisite(s): CST8249
Corerequisite(s):none

CST8602 Fundamentals of Penetration Testing

Students are exposed to applied skills and practical techniques required for penetration testing when used to evaluate corporate security processes and procedures. Students gain concrete

knowledge of penetration testing concepts, ethics and ground rules; planning for penetration testing projects; applicable Security Audit standards (e.g. OSSTMM); requirements for successful penetration testing; how to conduct effective vulnerability audits using Threat / Risk Assessment; researching exploits and associated security solutions for identified vulnerabilities; and preparing Penetration Testing / Vulnerability Assessment reports. Common security audit tools and exploitation frameworks are used in practical penetration testing exercises to help reinforce the theory. The course borrows from EC-Council Certified Ethical Hacker (CEH), SANS' GIAC Certified Penetration Tester (GPEN) and ISC2 Certified Information System Security Professional (CISSP) certification materials.

Prerequisite(s): none
Corerequisite(s):none

CST8603 Security Law and Compliance

Students gain insight into legal and regulatory issues related to information technology and security by discussing and contrasting the Criminal Code of Canada, selected federal statutes, privacy laws, and international trends in cyber law all with a focus on electronically stored and transmitted information. Issues of compliance to laws and regulations are also explored. Students are also guided through the process of and encouraged to complete a police background check and a confidential security clearance.

Prerequisite(s): none
Corerequisite(s):none

CST8604 Information Security Risk Management

Students acquire the skills necessary to develop processes for protecting against economic loss owing to disruptions of business activities due to natural disasters or cyber-attacks. Topics include roles and responsibilities of IT Security professionals in relation to risk management; the importance of making concurrent business and security decisions; managing risks in order to minimize impacts to business; risk assessment tools; cost-benefit analysis for security solutions; quantifying risks vs. threats; and using effective and enforceable policies as a tool to effect change in an organization.

Prerequisite(s): none
Corerequisite(s):none

CST8605 Advanced Security Appliances

The proper design and implementation of common security appliances in the overall security solution are examined. Topics include advanced firewall/IDS/IPS rules and management, integrating IPS and firewall capabilities, centralized logging and analysis, active alert systems, smart security appliances, along with NAC and 802.1x mechanisms. Industry standard appliances are explored through the hands-on portion of the course.

Prerequisite(s): CST8601
Corerequisite(s):none

CST8606 Fundamentals of Digital Forensics and Discovery

Students develop skills in digital forensic techniques and tools for investigations of cyber-crimes or corporate policy violations. Topics include file system structures of O/S, hash database comparisons, full and partial file recovery and analysis, forensic methodology and techniques, evidence acquisition and handling, interacting with law enforcement and forensic best practices. Forensic lab environments, tools and equipment are also explored.

Prerequisite(s): CST8602
Corerequisite(s):none

CST8607 Applied Cryptography

Students explore concepts and tools related to data security and integrity using mechanisms, such

as authentication, access control, cryptographic systems and secure communications. Topics include cryptographic algorithms and protocols, security protocols, encryption technologies (e.g. IPSec, VPNs, SSL, Digital Signatures), Public Key Infrastructure (PKI), Trusted Computing concepts, authentication and non-repudiation mechanisms, steganography data and transaction integrity.

Prerequisite(s): none
Corerequisite(s):none

CST8608 Fundamentals of Cyber Incident Response

Students are introduced to incident handling tasks and critical-thinking skills required for Incident Responders, allowing insight into the typical work that incident responders may perform. Also provided is an overview of the incident handling arena; Computer Security Incident Response Team (CSIRT) services and their inter-relationships with other departments, agencies and organizations; and the nature of incident response activities. Interactive instruction, in-class practical exercises using case studies and mock events and role playing are integrated. The course also relies on having basic knowledge and skills related to Penetration Testing, Security Audits and Digital Forensics.

Prerequisite(s): CST8603 and CST8604
Corerequisite(s):none

CST8609 Business Continuity and Disaster Recovery

Students participate in the planning and implementation of mechanisms designed to safeguard enterprises from serious disruption to normal business activities, whether it is due to a disaster or other disruption to essential services. Topics include Business Recovery Planning vs. Disaster Recovery Planning; operational risk / vulnerability assessment and analysis; disaster recovery; business continuity planning strategies and techniques; implementation of plans and policies to support for recovery; and cost-benefit analysis of security safeguards.

Prerequisite(s): CST8603 and CST8604
Corerequisite(s):none