Cybersecurity Learning Outcomes

A foundation for educating Canada's cybersecurity workforce

TECHNATION CA

About

TECHNATION

TECHNATION is the industry-government nexus for technology prosperity in Canada. As a member driven, not-for-profit, TECHNATION unites Canada's technology sector, governments and communities to enable technology prosperity from coast to coast. TECHNATION champions technology prosperity by: providing advocacy, professional development and networking opportunities across industry and governments at all levels; connecting Canadian scale-ups with global tech leaders; engaging the global supply chain; and filling the technology talent pipeline. TECHNATION has served as the authoritative national voice of the $210 billion ICT industry for over 60 years. More than 43,200 Canadian ICT firms create and supply goods and services that contribute to a more productive, competitive and innovative society. The ICT sector generates more than 666,500 jobs and invests $7.5 billion annually in R&D, more than any other private sector performer.
www.technationcanada.ca

TECHNATION Future Workforce Development

Canada's prosperity relies on a digital workforce with the skills to keep our companies and our country competitive in a constantly changing global market. TECHNATION develops digital talent from both inside and outside the industry through a mix of up-skilling and re-skilling programs. As a strategic arm of TECHNATION, Future Workforce Development focuses on creating the workforce that Canada needs for leadership in the digital economy. This includes inspiring young people to pursue technology careers, advising on technical education requirements and learning outcomes, guiding those in non-technical fields or underrepresented groups to attain needed skills so that they can transition into technology careers, supporting increased diversity within the industry and helping shape public policy to support, expand and enhance Canada's tech workforce.

Acknowledgements

Academic and Industry Volunteers

The creation of these Learning Outcomes would not have been possible without the generous support, insights and guidance provided by members of the academic community and industry partners. We are very grateful for their commitment and dedication to this effort, made especially difficult during 2020 when the COVID-19 pandemic placed enormous pressures on these communities. Please see Appendix A for a full list of participants.

The Cybersecurity Talent Alliance

TECHNATION would like to commend and acknowledge the members of the Cybersecurity Talent Alliance for their leadership, oversight and insights during the Canadian Cybersecurity Skills Framework and National Occupational Standard (NOS) development process. These documents were key reference artifacts for the definition of the Learning Outcomes. To review these documents please visit **https://technationcanada.ca/en/future-workforce-development/cybersecurity/**

Cybersecurity Industry Professionals

TECHNATION also wishes to express its sincere appreciation to the cybersecurity professionals and stakeholders who directly or indirectly contributed to this standard through the interviews, surveys, consultations and informal discussions. While too numerous to individually mention, we sincerely appreciate the interest and expertise that the engaged members of the cybersecurity community have provided throughout this project. Their insights and perspectives were essential to the outcomes. We thank them for sharing their time, knowledge, research and experiences with us. We also look forward to their future contributions in the review process to keep the Learning Outcomes and NOS current and relevant.

The Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security deserves special acknowledgement for their expertise and leading the way with their Cybersecurity Curriculum Guide which helped lay the framework for the cybersecurity work in Canada and work roles used in this standard. Moreover, we will work with the Cyber Centre to ensure close alignment between our guiding documents.

The U.S. National Initiative on Cybersecurity Education (NICE)

The U.S. NICE office housed within the National Institute of Standards and Technology provided TECHNATION with support and guidance throughout this process and we appreciate their extensive work on the NICE Cybersecurity Workforce Framework upon which the Canadian Cybersecurity Skills Framework was based. As well, the U.S. NICE provided detailed and rigorous descriptions of the cybersecurity work categories, specialty areas and work roles which heavily influenced the contents of this document. We look forward to working more closely with the NICE office in defining and refining our understanding of this emerging domain of work and will continue to contribute to the NICE revision process.

Government of Canada

This project is funded in part by the Government of Canada's Sectoral Initiatives Program. The opinions and interpretations in this publication are those of the author and do not necessarily reflect those of the Government of Canada.

Canada

Contents

Forward

This document is intended to inform training and education providers on suggested learning outcomes for candidates pursuing cybersecurity careers.

These learning outcomes have been developed in consultation with industry and academic experts. The learning outcomes were designed to help ensure that candidates looking to be employed in an organizational cybersecurity team have demonstrated competent cybersecurity foundations, and the general work domain prior to pursuing specialization.

As shown in the graphic below, the learning pathway includes *initial learning requirements* that apply to all candidates entering the cybersecurity field, regardless of domain. These are considered the cybersecurity foundation's supporting cross-functional competencies for the cybersecurity occupation.

Cybersecurity foundations are followed by functional work area learning outcomes that are aligned with the Canadian Cybersecurity Skills Framework major work categories: Oversee & Govern, Design & Develop, Operate & Maintain, and Protect & Defend. These outcomes delve more deeply into the necessary cybersecurity work needed to effectively function within the domain of each work category. Once candidates have completed these learning outcomes, they should be able to fill general cybersecurity roles in an organization within that work category. This provides an important bridge between entry-level and specialized work that has not typically been available in post-secondary education programs.

Once these work category learning outcomes have been achieved, candidates may continue to build on their capabilities in that work category or progress into specialized, often more technical, cybersecurity work as shown in the graphic.

Cybersecurity Roles

Learning & Development Progression

Fundamentals for All Core Cybersecurity Roles	Work Category Fundamentals (Supports work in the domain)	Learning in Support of Specialty Roles (Degree specialization, diploma program, or vendor-based programs/courses + experience)	
Cybersecurity Foundations	**Oversee & Govern**	• Chief Information Security Officer (CISO) • Information Systems Security Officer • Information Security Auditor	Technical Specialization, Consulting or Management
	Design & Develop	• Security Architect • Secure Software Assessor • Supply Chain Security Analyst • Information Systems Security Developer • Security Automation Engineer/Analyst • Cryptanalyst/Cryptographer • Security Engineer/Security Eng. Technologist • Security Testing and Evaluation Specialist • Operational Technology Systems Analyst	
	Operate & Maintain	• Identity and Authentication Management Support Specialist • Encryption Key Management Support Specialist • Data Privacy Specialist/Privacy Officer	
	Protect & Defend	• Manager – Cybersecurity Operations • Cybersecurity Operations Analyst • Cybersecurity Incident Responder • Vulnerability Assessment Analyst • Penetration Tester • Cybersecurity Operations Infrastructure Support Specialist • Cybersecurity Operations Technician • Digital Forensics Analyst	

Learning and Development Progression →

Cybersecurity Foundations

Initial Learning Requirements

All cybersecurity professionals, regardless of role, should have a basic ability to apply the following in their functional work area (Oversee & Govern, Design & Develop, Operate & Maintain, Protect & Defend):

- **IT systems and networking**
- **Systems architecture and models**
- **Internet protocols, systems and devices**
- **Cybersecurity foundations**
    - Integrated security framework
    - Cybersecurity strategies and approaches
    - Threat landscape and common threat surfaces (personnel, physical, IT/logical, supply chain)
    - Cyber threat intelligence processes and sources

Cybersecurity Foundations

(Continued)

    - Cybersecurity analytics
    - Cybersecurity management policies, processes and best practices
    - Cybersecurity systems, tools and applications
    - Legislation and compliance (e.g. privacy, information sharing, reporting, mandatory standards, etc.)
    - National and industry standards
- **Problem-solving and complex thinking in dynamic environments**
- **Maintaining broader security situational awareness**
- **Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes**
- **Continuous learning to support currency in knowledge of emerging threats, technological innovations in security and the changing cybersecurity landscape**
- **Communications (oral and verbal) suited to organizational context including drafting and writing technical reports**
- **Strategic thinking and business acumen to include understanding the business and risk context for cybersecurity**
- **Collaborating with other in team members, including non-cybersecurity professionals**
- **Professional integrity**
- **Ethics and professional responsibilities**
- **Cybersecurity training and awareness within their domain**

Oversee & Govern

Initial Learning Requirements

Overarching responsibility for this work category is leadership and management of the cybersecurity program for the organization.

The majority of the work within this occupational sub-group is conducted by those within recognized occupational skill groups such as management (senior managers, middle managers) and business, finance and administrative occupations (e.g. business analysts, finance analysts, risk analysts, communications).

Consequently, many of the relevant work roles within this category are adjacent roles such as policy, communications, training and awareness professionals.

The core work roles within this activity area/work category are:

- Chief Information Security Officer (CISO)
- Information Systems Security Officer
- Information Security Auditor

For the Oversee & Govern activity area/work category, they will typically require advanced capabilities that relate to organizational planning, measurement and management of cybersecurity.

Competencies, including critical KSAs for these specializations, are included in the National Occupational Standard. The following learning outcomes are the result of an analysis of all work roles in this category and are relevant to degree, diploma or certificate programs focusing on cybersecurity management. These will also be useful to those wishing to integrate cybersecurity content into existing management programs (financial, business, health engineering, etc.). The learning outcomes are presented in suggested sequence of instruction.

COMMON TASK	SUB-CATEGORY	LO#	COMPETENCY AREA (in part derived from NICE)	KEY SKILLS	LEARNING OUTCOMES Upon completion of the program of study, learners should be able to…
Identify compliance and oversee development of compliance mechanisms	**Compliance**	1	Compliance - Legal, Government, and Jurisprudence	Interpret and Apply Laws, Regulations, Policies, Standards, or Procedures	Identify and critically review relevant compliance requirements for their organizational context
		2	Compliance - Legal, Government, and Jurisprudence - Data Privacy and Protection	Interpret and Apply Laws, Regulations, Policies, Standards, or Procedures	Critically review policies, practices and procedures related to privacy legislation, breach response, disclosure and reporting
		3	Compliance - Legal, Government, and Jurisprudence	Advise on Cybersecurity Compliance Requirements	Provide advice and guidance on laws, regulations, policies, standards, or procedures that pertain to cybersecurity to multiple audiences
		4	Compliance - Legal, Government, and Jurisprudence	Monitor and Evaluate Compliance	Establish and maintain mechanisms to monitor organizational compliance and develop consistent corrective protocols
		5	Risk Management, Data Privacy and Protection	Coordinate Impact Assessments	Critically review and help draft business and privacy impact assessments
Collaborate with key stakeholders to establish an effective cybersecurity risk management program	**Risk Management**	1	Risk Management, Requirements Analysis, Data Privacy and Protection	Analytical Thinking, Critical Thinking, Business Acumen	Identify cybersecurity risk management requirements to support organizational objectives
		2	Risk Management, Relationship Management	Communications, Interpersonal Skills	Collaborate with key stakeholders to establish an effective cybersecurity risk management program
		3	Information System and Network Security/Organizational Infrastructure, Risk Management	Analytical Thinking, Critical Thinking, Business Acumen	Identify the existing organizational security posture and risk exposure

Allocate resources to support effective cybersecurity	**Resource Allocation**	1	Information System and Network Security, Organizational Infrastructure	Apply Security Concepts in the Organizational Context	Integrate information and network security into broader organizational security planning
		2	Project Management, Requirements Analysis	Project Management	Oversee and review project security requirements
		3	Resource Allocation	Business Planning and HR Planning	Identify appropriate technical, processes and people required to support organizational security objectives
		4	Security Controls	Analytical Thinking, Evaluation	Critically review and assess allocation of roles and responsibilities for security controls across the organization
Review and interpret cybersecurity information, security policies and controls	**Policy Instruments**	1	Policy Development	Communications, Analytical Thinking, Business Acumen	Critically review and provide program level input to development and implementation of organizational cybersecurity policies
		2	Policy Management	Written Communications, Editing	Critically review and evaluate organizational policies related to organizational security
Maintain current understanding of cybersecurity threat landscape for the business context	**Threat Environment**	1	Threat Assessment	Threat Analysis (High-Level)	Establish the cybersecurity threat landscape for a business context
		2	Contracting and Procurement, Project Management	Analytical Thinking, Business Acumen, Third Party Oversight	Identify and determine appropriate remediations for supply chain cybersecurity risks and risks across the SDLC
		3	Vulnerability Assessment	Vulnerability Assessment (High-Level)	Monitor and critically assess vulnerability management activities in relation to organizational risk

Advise on cybersecurity programs, policies, processes and systems	**Direction and Management**	1	Program Management	Business Planning, Analytical Thinking	Assess and contribute to the development, delivery of and improvements to the cybersecurity program
		2	Program Evaluation	Performance Measurement and Program Analytics	Identify, communicate and recommend program improvements
Schedule and oversee security assessments and audits	**Assessment and Audits**	1	Audit	Interpretation of Audit Information	Participate in internal and external information security audit processes
		2	Security Assessment	Analytical Thinking, Evaluation	Participate in security assessment activities

Design & Develop

Learning Outcomes

This work category is involved with developing secure infrastructure, systems and software.

This is a highly technical branch of cybersecurity work. The majority of this work falls within the responsibilities of computer engineers (2147), computer programmers and interactive media developers (2174), information systems testing technicians (2283) and information systems analysts and consultants (2171), in addition to the following roles within this National Occupational Standard:

- Security Architect
- Security Engineer/Security Engineering Technologist
- Secure Software Assessor
- Security Testing and Evaluation Specialist
- Operational Technology Systems Analyst
- Supply Chain Security Analyst
- Information Systems Security Developer
- Security Automation Engineer/Analyst
- Cryptanalyst/Cryptographer

Given the focus of this activity area, the emphasis is on applying deep technical understanding within a business context to better support organizational cybersecurity outcomes.

Competencies, including critical KSAs for these specializations, are included in the National Occupational Standard. The following learning outcomes are the result of an analysis of all work roles in this category and are fundamental to those in in specialized cybersecurity degree, diploma or certificate programs. These would also be of interest to those currently hosting applied technical degree, diploma or certificate programs where there is little to no cybersecurity content. The learning outcomes are presented in suggested sequence of instruction.

SUB-CATEGORY	LO#	COMPETENCY AREA (in part derived from NICE)	KEY SKILLS	LEARNING OUTCOMES Upon completion of the program of study, learners should be able to…
Risk Management	1	Risk Management, Organizational Awareness	Risk Assessment, Client Relations	Conduct organizational cyber risk assessment (IT and OT)
	2	Risk Management, Requirements Analysis	Requirements Analysis	Define organizational business needs (IT and OT)
	3	Risk Management, Relationship Management	Communications, Client Relations, Research	Coordinate security requirements research and gathering
	4	Risk Management, Requirements Analysis	Communications, Risk Assessment, Analytical Thinking	Provide basic technical advice and expertise in the development of risk management policies, requirements and practices
	5	Risk Management, Third Party Oversight	Risk Assessment	Advise on basic technical aspects of third-party risk management and supply chain risks (IT and OT)
Threat and Risk Assessment	1	Risk management, Threat Analysis	Threat Analysis, Analytical Thinking, Systems Thinking	Conduct threat and risk assessments
	2	Risk Management, Threat analysis	Threat Analysis, Critical Thinking	Identify context relevant threats
	3	Modeling and Simulation	Threat Analysis, Systems Modeling	Participate in threat modeling activities
Compliance	1	Compliance - Legal, Government, and Jurisprudence	Interpreting Legal and Regulator Documents and Standards, Critical Thinking	Interpret and identify legal, regulatory and standards compliance requirements for their business context

Technical Advice - Project/Program Management	1	Information Systems and Network Security	Research, Requirements Analysis, Communications	Advise on basic technical security requirements, policies, plans and activities (IT and OT). Design with security in mind.
	2	Project Management, Contracting and Procurement	Project Management, Requirements Analysis	Identify security requirements throughout the SDLC and project lifecycle
	3	Information System and Network Security, Program Management	Performance Measurement and Program Analytics	Define basic technical security program measures and metrics
	4	Contracting and Procurement	Threat Analysis, Requirements Analysis, Communications	Review and advise on technical security requirements in procurement activities and across the supply chain
	5	Problem Solving	Complex Problem Solving	Solve problems in complex, interdisciplinary cybersecurity contexts
Technical Advice - Security Infrastructure	1	Enterprise Architecture, Information System and Network Security, Program Management	Systems Thinking, Critical Thinking, Requirements Analysis, Systems Modeling	Advise on basic security architecture and engineering principles in support of organizational objectives. Design with security in mind
	2	Information System and Network Security, Program Management	Requirements Analysis, Problem Solving, Communications	Identify and define basic technical security requirements and controls for data, systems, applications and devices for their business context (IT and OT)
	3	Cyber Defence	Analytical Thinking	Apply security concepts, reference models and standards for their business context
	4	Enterprise Architecture, Information System and Network Security, Program Management	Systems Thinking, Analytical Thinking, Problem Solving	Advise on basic functional and technical design of networks and system, and cybersecurity solutions
	5	Testing and Evaluation	Testing System Operations, Evaluation	Support security testing and evaluation processes

Technical Advice - Cybersecurity Incident Management	1	Incident Management	Planning, Communications, Client Relations	Provide technical advice during development of incident management planning. Provide technical advice and recommendations on cybersecurity threats and mitigations
	2	Risk Management, Incident Management	Performance Measurement and Program Analytics	Participate and provide technical advice on organizational risk assessments and damage assessments
	3	Business Continuity	Planning, Communications, Client Relations	Advise on business continuity and disaster response planning
Technical Advice - Security Communications	1	Communications	Technical and Business Writing	Technical communications including report writing to address cross-disciplinary technical issues
	2	Communications, Presenting	Presenting	Drafting and providing briefings and reports to different audience levels (users, managers, executives)
Security Assessment	1	Security Assessment	Analysis, Communications, Critical Thinking, Evaluation	Participate in security assessment and authorization activities
	2	Testing And Evaluation	Using and Calibrating Assessment Criteria and Testing Tools, Analytical Thinking	Collect, analyze, verify and validate test data; translate data and test results into conclusion
	3	Computer Network Defence	Evaluation of Systems and Tools in Use, Problem Solving, Communications	Assess efficacy of cybersecurity systems and software; provide recommendations to address organizational threats and support risk mitigation
Vulnerability Management	1	Vulnerability Assessment	Analytical Thinking, Systems Thinking, Threat and Risk Assessment	Participate in and provide basic advice on vulnerability management activities
	2	Vulnerability Assessment	Vulnerability Risk Assessment, Evaluation, Using and Interpreting VA Tools	Conduct vulnerability assessments
Training and Education	1	Training and Education, Organizational Awareness	Training Needs Analysis, Training Delivery Methods	Assist in development and delivery of cybersecurity training and awareness activities

Operate & Maintain

Learning Outcomes

This work category is involved in operating and maintaining system and data security as prescribed within the security architecture and design specifications.

All these functions are performed within predominantly IT occupations (NOCs 0213, 2147, 2174, 2171 and 2283) within the Canadian labour market with the exception of those identified below which have become established as occupations with the increasing reliance on internet connected systems and associated threats:

- Identity and Authentication Management Support Specialist
- Encryption/Key Management Support Specialist
- Data Privacy Specialist/Privacy Officer

For the cybersecurity specialist working in this work category, not only do they need to bring their technical expertise, they are also required to closely integrate with day-to-day organizational IT operational requirements. This typically involves enhanced client-services and communication skills in addition to the technical competencies.

Competencies, including critical KSAs for these specializations, are included in the National Occupational Standard. The following learning outcomes are the result of an analysis of all work roles in this category and are intended to be used within existing IT and IT security diploma or certificate programs that support these and other roles. LOs are placed in suggested sequence of instruction.

COMMON TASK	SUB-CATEGORY	LO#	COMPETENCY AREA (in part derived from NICE)	KEY SKILLS	LEARNING OUTCOME Upon completion of the program of study, learners should be able to…
Customer Service and Technical Support	**Customers** **Help or Hot Desk**	1	System Administration, Incident Management	Triage and Prioritization	Evaluate, contextualize and organize requests and inquiries into prioritized lists for actionable outcomes
		2	Communications, Problem Solving	Communication	Compile effective responses and provide resolutions or escalation pathways
		3	Problem Solving, System Administration	People Management	Manage the aspects of customer requests and inquiries in timely manner under stressful situations
		4	Incident Response	Coordination	Provide system analyst/operator input on incident response and business continuity planning for systems that you operate.
Data Administration	**Data Systems**	1	Data Privacy and Protection, Policy Management	Communication, Reviewing and Interpreting Policies	Provide system analyst input on IT operations including design, creation, evaluation and communication of data governance policy, and data privacy policy.
		2	Data Privacy and Protection, Risk Management, Identity Management	Data Management, Information Classification, Data Analysis	Provide system analyst input on design, creation and evaluation of systems that (1) ensure that data at rest or in motion is encrypted, (2) link data governance practices (i.e. access rights, collection, retention etc.) to privacy rules, industry compliance and legislative requirements in on prem or cloud infrastructures. Identify and evaluate, for Risk Management purposes, Data system Assets, Threats, Vulnerabilities and Mitigations.
		3	Data Management, Identity Management	Process Management, Data Analysis	Provide system analyst input to the design, creation and evaluation of systems that (1) link roles and responsibility rights to HR systems to ensure that a change in role automatically adjusts access rights, (2) document data and system flows.

Knowledge Management	**Knowledge Tools** **Knowledge Services**	1	Knowledge Management	Research, Data Analysis	Classify the results of analysis
		2	Knowledge Management, Data Management	Knowledge Mapping	Demonstrate the capacity to model structured and unstructured data into diagrammatic formats that are contextually accurate and reflective of needs
		3	Knowledge Management, Data Management	Information Planning	Participate in design, creation and evaluation of system and practices documentation offering operations and maintenance perspectives.
		4	Knowledge Management	Reporting, Communications	Participate in the design, creation and evaluation of reports and reporting system to access and present stored and derived information. Demonstrate an understanding of Nielson Heuristics.
Network Services	**Networks** **Firewalls** (Hardware and Software) **Routers, Switches and Hubs** **Bridges and Multiplexers** **Servers**	1	Network Management	Technical Management	Build a system of interconnected network hardware and software components
		2	Network management	Project Management	Organize and prioritize technical requirements into tasks that can be actioned in a coordinated and timely manner
		3	Network Management, Infrastructure Design	Configuration	Provide basic technical / systems advice in the design, creation and evaluation of end-to-end computer networking.
		4	Vulnerability assessment, Information Systems/ Network Security, Systems Testing and Evaluation	Testing	Provide basic technical/ systems advice in the design, creation and evaluation of functional and non-functional requirement specifications and vulnerability testing
		5	Network management, Infrastructure Design	Maintenance	Provide basic technical/ systems advice in the design, creation, evaluation for perform maintenance procedures, schedules.

System Administration	**Hardware** **Software**	1	System Administration	Installation	Choose software applications in order to meet defined requirements
		2	System Administration, System Integration, Vulnerability Assessment	Configuration	Ensure hardware/software are optimally configured to meet security requirements and reduce vulnerabilities
		3	System Administration, Information Systems/ Network Security	Administration	Enforce administrative policies on the systems in use
		4	System Administration, Problem Solving	Troubleshooting	Investigate, analyze and initiate repair or mitigate issues with systems hardware/software
		5	System Administration, Communications	Reporting	Provide accurate, timely, concise and well targeted technical reports on systems issues.
System Analysis	**Business Requirements** **System Requirements** **Information Systems**	1	Network Management, Infrastructure Design, Communications	Technical Analysis	Translate non-technical and technical specifications into use cases
		2	Network Management, Infrastructure Design, Communications	Information Analysis	Classify requirements according to level of prioritization while remaining aligned with non-technical and technical requirements
		3	Network Management, Infrastructure Design, Communications	Communication	Draft technical systems requirements documents tailored to the target audience. Provide technical insights and perspectives to diverse target audiences. Present systems analysis findings to management.
		4	Network Management, Project Management	Project Management	Participate in project management activities as assigned.

Protect & Defend

Learning Outcomes

This work category supports cybersecurity operations that encompass active protection, event detection, incident response and recovery of organizational digital systems.

While individuals have been doing related jobs for decades, the key work roles have not been identified as occupations but rather have been typically associated with occupational groups: computer and information systems managers (NOC 0213); information systems analysts and consultants (2171); and information systems testing technicians (2283). Individuals in this work category are therefore focused on operating, maintaining and managing cybersecurity technologies, processes and personnel, that requires unique experience and distinct knowledge, skills and abilities that differentiate them from their other IT colleagues.

The following occupations have been more clearly defined as supporting cybersecurity operations:

- **Information Systems Security Manager – Cybersecurity Operations**
- **Cybersecurity Operations Analyst** (a.k.a. in the NICE framework as a Cyber Defense Analyst)
- **Cybersecurity Operations Infrastructure Support Specialist** (a.k.a. in the NICE framework as a Cyber Defense Infrastructure Support Specialist)
- **Cybersecurity Incident Responder** (a.k.a. in the NICE framework as a Cyber Defense Incident Responder)
- **Cybersecurity Operations Technician**
- **Vulnerability Assessment Analyst**
- **Penetration Tester**
- **Digital Forensics Analyst** (a.k.a. in the NICE framework as a Cyber Defense Digital Forensics Analyst)

Competencies including critical KSAs for these specializations are included in the National Occupational Standard. The following learning outcomes are the result of an analysis of all work roles in this category and are intended to support initial educational components within a specialized degree, diploma or certificate related to cybersecurity operations. The learning outcomes are presented in suggested sequence of instruction.

COMMON TASK	SUB-CATEGORY	LO#	COMPETENCY AREA (in part derived from NICE)	KEY SKILLS	LEARNING OUTCOMES Upon completion of the program of study, learners should be able to…
Monitor, analyze and identify threats and cybersecurity incidents	**Threat Analysis**	1	Security Operations	Organizational Awareness, Risk Assessment, Threat Assessment, Interpreting Legal and Regulatory Requirements, Communications, Client Relations	Conduct analyst level cybersecurity operations planning
		2	Security Operations	Threat Analysis, Traffic Analysis, Analytical Thinking, Systems Thinking, Cyber Analysis Tools, Detecting and Identifying Anomalous/Malicious Activity	Conduct basic security operations analysis activities
		3	Threat Analysis, Security Operations	Threat Analysis, Critical Thinking, Adversarial Thinking, Basic Malware Analysis and Tools	Apply threat actor knowledge and adversarial thinking across the kill chain
		4	Intelligence Analysis	Interpreting Threat Information, Cyber Threat Research, Analytical Thinking	Interpret and apply cyber threat intelligence to organizational risk
		5	Risk Management, Vulnerability Assessment	Risk Assessment, Analytical Thinking	Provide analyst level advice and input to organizational threat and vulnerability risk assessment activities, Analyze and assess security control efficacy in mitigating organizational risk and remediate problems
Install, test, maintain, monitor and manage cybersecurity systems and software	**Security Systems and Software**	1	Cybersecurity Systems and Software	Threat Analysis, Analytical Thinking, Systems Thinking	Install and configure common cybersecurity systems and tools
		2	Cybersecurity Systems and Software	Troubleshooting, Analytical Thinking, Problem Solving	Trouble shoot security systems and applications
		3	Cybersecurity Systems and Software	Evaluation of Systems and Tools in Use, Performance Measurement, Communications	Monitor, manage and report on cybersecurity systems and tool performance

Support cybersecurity incident management	**Incident Management**	1	Incident Management	Planning, Analytical Thinking, Communications, Organizational Awareness, Crisis Management Protocols, Client Relations	Provide analyst level advice and input to incident management planning
		2	Incident Management	Intrusion Analysis, Root Cause Analysis, Risk Analysis, Tool Use and Interpretation, Logging and Reporting	Conduct triage and initiate incident response protocols
		3	Risk Management, Incident Management	Performance Measurement and Program Analytics	Provide analyst level advice and input to organizational risk assessment and damage assessments
		4	Cybersecurity Incident Investigation	Assess Evidence, Maintain Chain of Custody, Use Evidence Gathering Tools, Communications	Conduct evidence collection and investigation in support of law enforcement digital evidence collection
		5	Bcp/ Drp, Recovery	Analysis, Testing and Evaluation Tools, Vulnerability Assessment	Provide analyst level advice and input to recovery activities
Provide technical advice and recommendations on operational cybersecurity threats and mitigations	**Technical Advice**	1	Computer Network Defence	Evaluation of Systems and Tools in Use, Problem Solving, Communications	Assess efficacy of cybersecurity operations systems and software and provide recommendations to address organizational threats
		2	Cyber Defence	Threat Analysis, Analytical Thinking, Systems Thinking, Organizational Awareness	Provide analyst level advice and input to advise on cybersecurity threats and mitigations
Develop, deliver and support cybersecurity training and educational efforts	**Training and Education**	1	Training and Education, Organizational Awareness	Training Needs Analysis, Training Delivery Methods	Assist in the development and delivery of cybersecurity training and awareness activities

Appendix A

Content Contributors

George Al-Koura, ADGA

Peter Aruja, AGDA

Joel Black, ADGA

David Cramb, Ryerson University

Kevin Deveau, Centennial College

Dillon Donahue, CyberNB

Rushmi Dua Hasham, Rogers Cybersecure Catalyst, Ryerson University

Ed Dubrovsky, York University

Anthony Elton, Amazon Web Services (AWS)

Isabelle Hertanto, ADGA

Nicholas Johnston, Sheridan College

Tahmeed Khan, ADGA

Kathy Knight, Manitoba Institute of Trades and Technology (MITT)

David Knox, University of Ottawa

Murray Lee, BulletProof

Sophia Leong, University of Ottawa

Heather MacLean, EC-Council Canada

Angela McAllister, Canadian Centre for Cyber Security

Alan McCafferty, Strategic Consulting Group, myscg

Ron McLeod, Nova Scotia Community College

Karen Murkar, Consultant

Jeff Musson, Dynamite Network Solutions

John Olaonipekun, ADGA

Krishna Raj Kumar, CGI's Atlantic Cybersecurity & Privacy Practice

Rob Samuel, Amazon Web Services (AWS)

Juliana Scharrer, Rogers Cybersecure Catalyst, Ryerson University

Sumbal Syed, TriOS College

Ramy Taraboulsi, Vertiablesoft Innovations

TECHNATION^CA

Funded in part by
the Government
of Canada

Canada