CyberWave

Career Viewbook

Your first look into an exciting career in cyber security

MANITOBA INSTITUTE OF TRADES & TECHNOLOGY

RBC Foundation

CyberWave

Are you trying to figure out "what to do with your life" once you graduate high school? Or perhaps you're stuck in a boring job dreaming of a career where you can make a difference and more cash. We get it. There are so many options to choose from, some you may not even know about yet.

That's where this book comes in. Whether you've filled out dozens of applications, can't stop with the career quizzes, or drowned your indecision by scrolling TikTok, take heart. The digital world has cracked open unprecedented career opportunities for individuals looking for purpose in protecting people and data from the dark side of the web.

Which is why CyberWave at Manitoba Institute of Trades and Technology (MITT) has made this handy viewbook for you. Because the more our lives become intertwined with the internet, the more risk is involved. And the pursuit to protect ourselves from nefarious online hackers has made cyber security a compelling, well-paid, and meaningful industry to work in. Get ready to dive into 15 fascinating career profiles featuring the stories of cyber security professionals at various stages of their professional journeys.

See for yourself why these jobs matter, What's the employer demand, the range of roles available and (mythbuster!) which ones require in-depth tech know how and which ones don't. Here you'll find a compilation of careers ranging from entry and mid-senior levels all the way up to the executive suite. In cybersecurity you can dream big, work from anywhere and for anyone. Furthermore, with multiple access points, you can find the right pathway to a specialization that checks all the boxes.

Together, MITT and CyberWave – the Cybersecurity Centre of Excellence, provide diploma programs, certificate and micro-credentials as full-time and short-term learning options to set you up with the technical and interpersonal skills to make your next career step.

Use this book as a key resource to tap into a career that makes a difference and see how you can start here to get there.

Funding provided by: RBC Foundation

MANITOBA INSTITUTE OF TRADES & TECHNOLOGY

A special thank you to **RBC Future Launch** for providing the funding for this piece.

What is Cyber Security?

Technology has changed everything from the way we work and play to how we access information on topics as diverse as healthcare and climate change. Think about all the things you do on your phone, laptop, and tablet. That's a ton of data being collected each time you bank online, order takeout, or track your daily Wordle attempts.

The downside of these conveniences is that online criminals are searching for openings to steal money and identities. That's why we need cyber security. People working in this industry are in vigilant pursuit of protecting our information systems, personal data, and the services we depend on.

It's now considered mission critical for businesses and individuals to have a game plan in case of a network breach. Cyber security professionals protect us from vulnerabilities like phishing scams, where misleading messages trick users into providing personal information. They search for malware, malicious software installed unknowingly onto a user's computer and denial-of-service attacks where a hacker makes an IT system unresponsive while demanding ransom.

Cyber security is not just for techies. If you are a person who looks at weird coincidences, broken patterns and unusual circumstance and goes "hmmm..." this industry is for you. Cyber security deals with a tremendous number of unknowns so curiosity is key. Risk recognition is also a vital skill. Thinking about all the things that can go wrong and how to prepare for it is integral to cyber security. In addition, employers value candidates who are strong communicators, efficient, thorough researchers, and analytical thinkers, among a host of other qualities.

Cybersecurity careers are purposeful with real world impact that matters. Healthcare, environmental issues, education – nearly every industry is looking for defence against cyber criminals.

Make Your Mark Here

Cyber security has become fundamental in today's world, from governments and large corporations to local businesses, employees, and individuals, creating the conditions for truly compelling career opportunities.

Information and Communications Technology Council (ICTC) listed cyber security as one of the top ten digital roles identified in its 2020 Outlook Report. Labour market reports show the industry worldwide is experiencing a severe talent shortage. Canada alone expects employment demand to rise to 53,000 for cyber security practitioners. In Manitoba, it represents a significant opportunity to broaden engagement in the industry to those historically underrepresented in tech.

Hackers and cyber criminals draw from different backgrounds and experiences to formulate their attacks, so we need perspectives from all kinds of people to pursue them. Diverse teams bring more ideas, provide broader insight, and are absolutely critical to the cyber security field. The industry is evolving rapidly and seeks out those with diverse backgrounds and life experiences. This is your time to help shape the future of cyber security.

> **TECHNOLOGY WILL DISRUPT AN ESTIMATED 25 PER CENT OF CANADIAN JOBS IN THE NEXT DECADE, HOWEVER, MORE JOBS WILL BE CREATED BY TECHNOLOGY THAN LOST. (1)**

CyberWave at MITT

CyberWave is dedicated to addressing the growing labour shortage in cyber security. Created by Manitoba Institute of Trades & Technology (MITT), this new centre is a nexus for thought-leadership, work-integrated learning, and applied research.

CyberWave works closely with leading employers to identify skill-gaps and hiring needs, then rapidly develops and deploys programming to meets the sector's constantly-evolving demands. It's an ongoing process of consultation to ensure training is responsive to new cyber security practices in addressing emerging threats and types of attacks.

The results are practical certifications and micro-credentials optimized for working professionals, employers and students like you. As well, MITT offers full time academic programs including Cyber Defense & Cloud administration, Network Systems Administrator, and Software Developer.

About MITT

MITT is your bridge from classroom to career. MITT offers 30+ certificate, diploma, and post-graduate programs that teach you the in-demand skills you need at any stage of your career. MITT campuses are welcoming and class sizes are small, offering you a safe and inviting learning environment. Our veteran instructors are industry experts who know what skills you need to get hired.

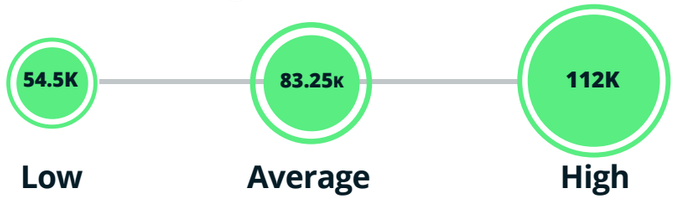
MITT is the only college in Manitoba that integrates employability skills training into every program. Beyond theory, we offer immersive learning environments where you'll practice your skills in modernized simulation labs, using state-of-the-art industry tools and equipment. Most programs also include a work-integrated learning opportunity with a local employer, giving you real-world experience that gets you ready to step into a career right after graduation.

Digital Forensics Analyst

Profiles start at entry level positions and progress to senior opportunities to give an idea of where you can start and how you can grow your cyber security career.

Type of job
Protect and Defend

Career Earning Potential



Educational pathways

MITT Programs:

Cyber Defense and Cloud Administration

CyberWave Micro-credentials:

Certified Network Defender

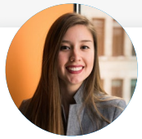
Certified Ethical Hacker

Certified Threat Intelligence Agent

Certified Incident Handler

Computer Hacking Forensic Investigator

Post-secondary education (degree or diploma in related computer science or IT field)



A day in the life

Karla works for herself as a freelance Digital Forensics Analyst. Clients come to her primarily after an information security breach, so Karla gets to put on her metaphoric trench coat each day to dig through digital trails. Organizations and individuals call her to investigate when cybercriminals steal information from a computer, web application, cell phone, network or another digital device.

Today Karla's working with a company whose network has been hacked. It's her job to uncover how the crime was accomplished. For her investigations, Karla utilizes forensic collections, intrusion correlation and tracking, and threat analysis. Once she determines the cyber criminal's process, she tries to recover and repair the stolen and damaged data files.

Karla collects and analyzes intrusive artifacts like source code, malware, and discovered data to understand these criminals. She often works with other security experts to implement processes that will prevent it from happening again. Sometimes cases take a long time to solve. However, by the afternoon, Karla solves and closes the case on the network hacker. Each day is different and she finds it thrilling to work with so many people in the pursuit of cyber defence.

Career journey

Digital Forensics Analysts are often a tier 2 and 3 position within a cyber security operations environment. They usually have two to three years in a network or operational security role like a malware analyst. This can lead to increased specialization within digital forensics or security assessment activities and red/blue team leader, penetration tester and management roles.

Why this job matters

These experts conduct digital forensics to analyze evidence from computers, networks, and other data storage devices. They are critical in minimizing any harm done from cybercrimes and reconstructing the crime to help bring criminals to justice.

Soft skills

Curious, observant, excellent analytical skills, ability to organize complex investigations and document and report findings to stakeholders

Other jobs like this

Digital Forensics Investigator (generally reserved for cybercrime environment), Digital Forensics Examiner (generally reserved for cyber audit environments)

Penetration Tester

Type of job
Protect and Defend

Career Earning Potential

Low	Average	High
49.5K	92K	134.5K

Educational pathways

MITT Programs:

Cyber Defense and Cloud Computing

Network and Systems Administrator

CyberWave Micro-credentials:

Certified Network Defender

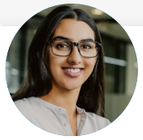
Certified Ethical Hacker

Certified Penetration Testing

Licensed Penetration Tester

Post-secondary education (degree or diploma in related computer science or IT field)

> **IN 2021, THE GLOBAL COST OF CYBERCRIME IS ESTIMATED TO BE $6 TRILLION USD. (1)**



A day in the life

Before heading into the office, Harserat starts her day with a long run. As a penetration tester, she has a lot of responsibility on her shoulders, thinking like a hacker to test the security of her company's computer systems. Although her role is high-pressure, she loves working for a global computer hardware company focused on solving some of the world's most challenging problems.

There are a lot of malicious, unethical hackers in the world, and Harserat's company relies on her to put its security to the test and measure its efficiency. When she can determine a system is sound and incapable of being compromised by terrorists or criminals, the rest of her team can assume they have done their job.

Harserat stays sharp in the ever-changing world of cyber security by regularly updating her skills, knowledge and methods for hacking systems. She loves the fast-paced energy in this new era of technology and appreciates how multi-faceted her job is. Other parts of her role include managing, technical writing and security administrator.

Career journey

Penetration testers are often a tier 2 or 3 position within a cyber security environment. They normally have 3-5 years in a cyber security operations role like Vulnerability or Malware Analysis. This is an advanced technical role that can lead to increasing technical specialization and red team leadership or management roles.

Why this job matters

Often called ***ethical hackers***, penetration testers attempt to crack into an organization's computer system to test its relative security rather than create havoc or steal information.

Soft skills

Willingness to always be learning and updating skills, writing and communication, creativity, leadership, problem-solver

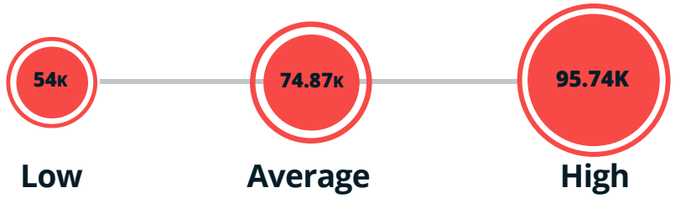
Other jobs like this

Security Testing and Evaluation Specialist, Advanced Vulnerability Assessment Analyst

Vulnerability Assessment Analyst

Type of job
Protect and Defend

Career Earning Potential



Educational pathways

MITT Programs:

Cyber Defense and Cloud Computing

Network Security Diploma

CyberWave Micro-credentials:

Certified Network Defender

Certified Ethical Hacker

Certified Penetration Tester

Post-secondary education (degree or diploma in related computer science or IT field)

A day in the life

Wing analyzes and identifies security solutions based on the latest industry best practices. She works for a media group and gets to lean into her love of movies with a company that creates, produces and distributes award-winning animated content for audiences worldwide

Today, Wing is tapping into her own creativity by using hands-on strategies to produce false vulnerabilities and discrepancies. She's looking for critical flaws in applications and systems that cyber actors could exploit, which is one of the ways Wing maintains her company's deployable cyber defense audit toolkit.

Keeping up with current IT security industry solutions is another part of her role. She's often coming up with scenarios for new attacks and threat vectors which helps her improve their security processes. Wing also has a strong understanding of cost-effective security controls and will lead a team meeting this afternoon to make recommendations to mitigate future cyber security risks.

Career journey

A Vulnerability Assessment Analyst is often a tier 2 position within a cyber security operations environment that is usually preceded by 2-3 years in a network or operational security role. This can lead to increased specialization as a vulnerability analyst, red/blue team leader, penetration tester or management roles.

Why this job matters

These analysts scan applications and operating systems to identify flaws and vulnerabilities. They conduct and present these assessments to an organization's networks and systems to have a clear understanding of where changes need to occur.

Soft skills

Proven analytical and problem-solving abilities, ability to effectively prioritize and execute tasks in a high-pressure environment, good written, oral and interpersonal skills

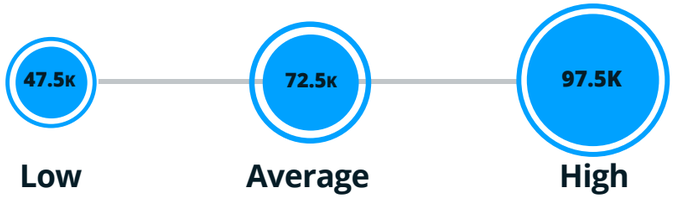
Other jobs like this

Vulnerability tester, Vulnerability assessor, Vulnerability assessment manager

Cyber Security Operations Technician

Type of job
Protect and Defend

Career Earning Potential



Educational pathways

MITT Programs:

Cyber Defense and Cloud Administration

Network Security Diploma

CyberWave Micro-credentials:

Certified Network Defender

Certified Application Security Engineer

Certified Security Analyst

Licensed Penetration Tester

Post-secondary education (degree or diploma in related computer science or IT field)

A day in the life

Irma works as part of a team to monitor and fight threats to the government's IT infrastructure. Today she's assessing security systems and measures to find weaknesses and possible improvements. Her team looks for suspicious emails, network logs, and other resources that can give them insight into an entity's network activity.

Irma is new to the role, which requires excellent attention to detail and general awareness for all things cyber. Her team's been great about showing her how to read, understand and notify cyber trends. She's like a sponge absorbing all this knowledge in areas like networking, malware analysis, cyber etiquette and incident response. It feels great.

After monitoring the security system performance all morning, her team did some troubleshooting and resolved a few software interoperability issues. In the afternoon, Irma audits, logs, and reports life-cycle management activities and conducts an incident report on the vulnerabilities they found.

Career journey

A Cyber Security Operations Technician is often the first step in a cyber security career journey. With additional training and experience there is potential for more technically or operationally focused roles and management opportunities.

Why this job matters

People in this role test, implement, deploy, maintain, and administer the security operations infrastructure hardware and software within an organization.

Soft skills

Attention to detail, organized, good communicator, problem-solver

Other jobs like this

Security Systems Technician, Security Control Analyst, Security Infrastructure Support Specialist/Technician

Cyber Security Incident Responder

Type of job
Protect and Defend

Career Earning Potential

Low	Average	High
48.5K	85.5K	122.5K

Educational pathways

MITT Programs:

Network Security Diploma

Software Developer

Cyber Defense and Cloud Administration

CyberWave Micro-credentials:

Certified Incident Handler

Certified Ethical Hacker

Disaster Recover Professional

College diploma in IT field with specialization in IT/cybersecurity, network security or similar.

A day in the life

Alerial is the first responder of her organization's network in the digital world. She works at a major airline where Alerial is proactive in preventing cyberattacks in her company's security systems. She's the first one on the scene, and it's her job to fix the emergency and take the necessary actions to prevent a cyber security breach from happening again.

Alerial likes to think in worst-case scenarios and has developed a system of procedures to handle emergencies. She is vigilant in patrolling her company's network and systems to recognize errors or possible vulnerabilities and collaborates with her other cyber security team members.

At an airline, the risks are high in the event of a cyberattack. Alerial is part of the team that's developed a system for the communication trail that will take place during an emergency and how they will relay this information to law enforcement. She is always on red alert for any suspicious activity and is diligent in her role to oversee systems and applications.

Career journey

A Cyber Security Incident Responder is a common entry-level job within the security operations centre. With additional training, there is potential for more technically focused roles in cyber security operations such as vulnerability assessment & management, digital forensics, threat analytics and malware analysis and management opportunities.

Why this job matters

First responders are critical in any emergency situations and vital to keeping people safe. In cyber security, incident responders are the people who come to the rescue in times of security system trouble. They work to solve issues within a company as quickly as possible and instill measures to prevent any further problems.

Soft skills

Quick thinking, confident to make decisions in high pressure situations, patient, well-spoken, excellent writing skills, logical and rational thinker

Other jobs like this

Incident Response Engineer, Cyber Security First Responder, Operational Technology Security Incident Responder

Cyber Security Operations Analyst

Type of job
Protect and Defend

> CYBER SECURITY WAS ONE OF THE TOP TEN DIGITAL ROLES IDENTIFIED IN ICTC'S 2020 OUTLOOK REPORT. (1)

Career Earning Potential

Low	Average	High
42K	62.75K	83.5K

Educational pathways

MITT Programs:

Network Security Diploma

Cyber Defense and Cloud Administration

Software Developer

CyberWave Micro-credentials:

Certified SOC Analyst

Certified Application Security Engineer

Certified Security Analyst

Certified Threat Intelligence Analyst

College diploma in IT field.

A day in the life

Alyssa works in a hybrid remote position for a financial group. She enjoys the flexibility of going into the office two days a week alongside working from home. Her company's culture is big on idea sharing, collaboration and respect. Alyssa takes part in monthly meetings with her team to focus on inclusion and diversity conversations. This month they're talking about evolving job benefits for the 2022 workplace.

As the Cyber Security Operations Analyst, she plays the supporting role in the administration, operation and implementation of IT security solutions. Today she's responding to incident tickets and service requests from internal users and support teams.

Alyssa uses established procedures to solve her colleagues' problems, incidents, requests and change configurations. This role often requires Alyssa to rely on her common sense and sound business judgment to make decisions. She finds this has been a real boost to her confidence and is getting good at trusting herself.

Career journey

Cyber Security Operations Analyst is a common entry-level job within the security operations centre (SOC). With additional training and experience, there is potential for more technically or operationally focused roles in cybersecurity operations (e.g. digital forensics, threat analytics and malware analysis) and management opportunities.

Why this job matters

These cyber security analysts maintain and secure organizations' critical information assets and IT security devices and are often responsible for initial detection, incident response, and mitigation.

Soft skills

Analytical, inspires trust by being open and honest, sharp sense of ethics, strong interpersonal skills

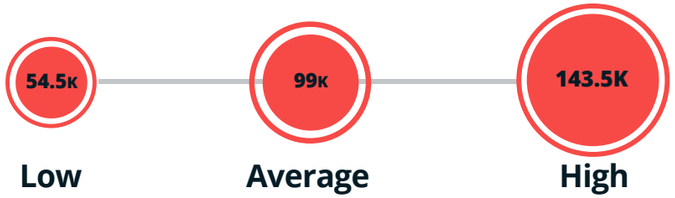
Other jobs like this

SOC Operator, Cyber Security Operator, Infrastructure Security Analyst, Network Security Administrator, Data security analyst

Information Systems Security Manager

Type of job
Protect and Defend

Career Earning Potential



Educational pathways

MITT Programs:
Software Developer
Cyber Defense and Cloud Administration
Network Security Diploma

CyberWave Micro-credentials:
Certified Network Defender
Certified Application Security Engineer
Certified Security Analyst
Certified Threat Intelligence Agent
Certified Ethical Hacker

Bachelor's degree in computer science or related discipline or College diploma in IT field.

A day in the life

Sunisa starts her day analyzing a report generated by her company's monitoring system to identify future risks in their security system. She works at a university and plays a crucial role in the university's pursuit to avoid potential cyber security disasters.

This afternoon, Sunisa is carrying out a simulated attack to test the efficiency of the university's anti-virus software, passwords, and firewalls. She loves the thrill of getting inside the mind of a hacker, and uses these opportunities to try out tactics that will keep her one step ahead.

These tests help her to identify weak areas that could make their information systems vulnerable. Sunisa often gets to pair her passion for cyber security with advocacy. She finishes her day training employees by explaining security risks and showing them how to better protect the data of their university's students and faculty members.

Career journey

Information Systems Security Manager typically works five to 10 years in related IT or cyber security operations. This role increasingly supports management-level responsibilities based on a solid technical foundation in cyber security.

Why this job matters

Without the proper security measures, an organization's information technology systems risk being invaded and having essential and highly confidential information lost, leading to substantial revenue loss and fines for failing to protect their data.

Soft skills

Strong leadership, good communication, efficient multi-tasker, creative problem solver, comfortable delegating

Other jobs like this

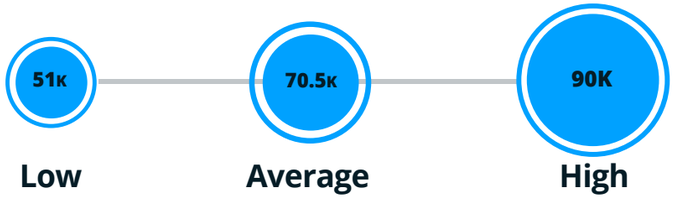
Cybersecurity Operations Manager (CSOC), Information Systems Security Manager (Cybersecurity Operations)

Data Privacy Specialist

Type of job
Operate and Maintain

DID YOU KNOW? APPROXIMATELY $6 TRILLION IS EXPECTED TO BE SPENT GLOBALLY ON CYBERSECURITY IN 2021. THERE IS A **HACKER** ATTACK **EVERY 39 SECONDS.** (1)

Career Earning Potential



Educational pathways

MITT Programs:

Cyber Defense and Cloud Administration

Network and Systems Administrator

Network Security Diploma

CyberWave Micro-credentials:

Certified Governance of Enterprise IT

Data Science Fundamentals

Post-secondary education in an applicable field (e.g.; Business Administration, Law, Political Science, Social Sciences or equivalent).

A day in the life

Evie is a data privacy specialist with a large firm that practices environmental law. She loves working with a staff dedicated to the climate crisis and environment. Today, Evie kicks her day off with the support team to advise on data protection and privacy legal matters. The group bounces good ideas off each other, and Evie leaves the meeting feeling energized.

She's responsible for supporting and implementing all aspects of her company's global data compliance strategy, so Evie spends the afternoon updating and reviewing a new process. In the world of Data Privacy, trends and best practices are constantly evolving, and Evie enjoys the methodical research she often puts in to stay on top of her industry.

Career journey

Data Privacy Specialists typically have 2-3 years of training and experience in policy analysis roles related to security or privacy. There is often the opportunity to further specialize in data security, policy analyst or senior advisor.

Why this job matters

These specialists develop, implement and advise on privacy compliance regulations and requirements to safeguard their organization's personal private information.

Soft skills

Organizational skills, collaboration, writing, problem-solving, keen to develop and use initiative

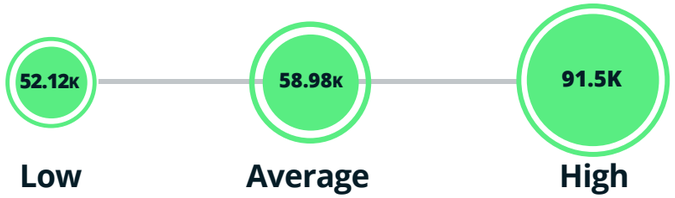
Other jobs like this

Privacy Officer, Privacy Compliance Officer/Manager

Encryption / Key Management Support Specialist

Type of job
Operate and Maintain

Career Earning Potential



Educational pathways

MITT Programs:

Software Developer

Cyber Defense and Cloud Administration

Network Security Diploma

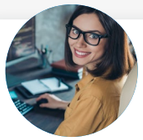
CyberWave Micro-credentials:

Certified Network Defender

Certified Ethical Hacker

Certified Threat Intelligence Agent

College diploma in IT field.



A day in the life

A data breach can cost companies millions of dollars and loss of credibility with severe consequences for their customers. Zahra works at a security firm where she mitigates the extent and severity of possible data breaches in healthcare. Encryption key management is the cornerstone of data protection and Zahra loves being at the forefront of these tools.

Essentially, she scrambles or codes data so that this information is unreadable to unauthorized users. The only way to gain access to the original data is with an encryption key. So, Zahra spends a lot of effort carefully managing the encryption key lifecycle which includes generating, deploying, and storing keys. She's also the queen of backups, which are essential in case a key is lost or deleted.

Career journey

People in this field typically have experience managing directory services and working in a security environment. This is an often an entry-level job to the security domain. With additional training and experience there is potential for more technically or operationally focused roles.

Why this job matters

Encryption / Key Management Support Specialists support the management and maintenance of virtual private networks, encryption and public key infrastructure to keep peoples' sensitive data safe.

Soft skills

Ability to look at the big picture, creativity, management, communication

Other jobs like this

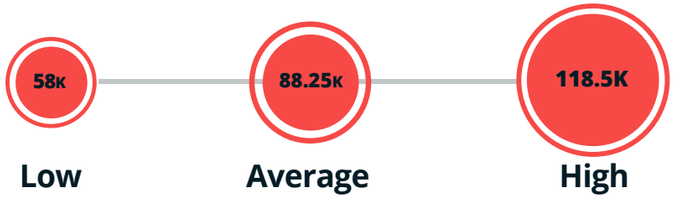
Access Management Analyst, System Analyst, Identity, Credentials and Access Management (ICAM) Specialist

> **BETANEWS SAYS CYBERCRIMINALS CAN PENETRATE 93 PER CENT OF COMPANY NETWORKS. (2)**

Identity and Authentication Management Support Specialist

Type of job
Operate and Maintain

Career Earning Potential



Educational pathways

MITT Programs:

Software Developer

Cyber Defense and Cloud Administration

Network Security Diploma

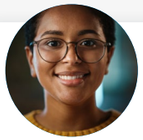
CyberWave Micro-credentials:

Software Developer

Cyber Defense and Cloud Administration

Network Security Diploma

College diploma in IT field.



A day in the life

Like many industries, insurance has gone digital increasing the need for cyber security. Destiny works at a local agency supporting identity, credential, access and authentication management. People provide incredibly sensitive information to their insurers and Destiny plays a critical role in keeping it protected.

She takes pride in pushing back on threats that would keep many insurers up at night. Today, Destiny collaborates with the organization's IT security to develop, deliver and oversee cyber security training material that will empower and educate their staff.

"CYBERSECURITY MAGAZINE LISTS MOST COMMON TYPES OF ATTACKS ON SMALL BUSINESSES AS: (2)

PHISHING/SOCIAL ENGINEERING: **57%**
COMPROMISED/STOLEN DEVICES: **33%**
CREDENTIAL THEFT: **30%**"

Career journey

Often an entry-level job, these workers have experience managing directory services and working in a security environment. With additional training, there is potential for more technical or operational-focused roles and management opportunities.

Why this job matters

Identity and Authentication Management Support Specialist's use their skills to navigate our world's increasing reliance on internet connected systems and the associated threats.

Soft skills

Communication, critical thinking, management, collaboration, strong ability to research

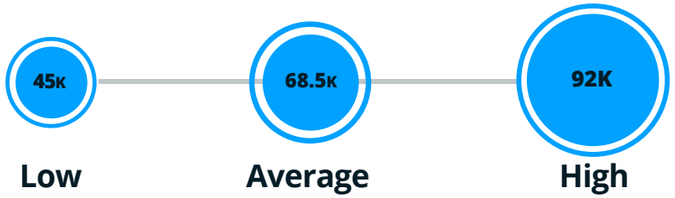
Other jobs like this

Access Management Analyst, System Analyst, Identity, Credentials and Access Management (ICAM) Specialist

Supply Chain Security Analyst

Type of job
Design and Develop

Career Earning Potential



Educational pathways

MITT Programs:

Cyber Defense and Cloud Administration

Network Security Diploma

Software Developer

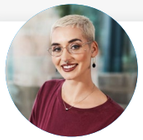
CyberWave Micro-credentials:

Certified Ethical Hacker

Certified Network Defender

Certified Threat Intelligence Agent

Post-secondary education in a cyber or IT related field (e.g.; Computer engineering, Computer Science, Information Technology, Business Technology.)



A day in the life

Supply chains are defined as a sequence of processes involved in the production and distribution of a commodity. Cleo's job is to collect and analyze data and identify cyber security flaws in her organization's operations. She's always been an avid puzzler, particularly a good 1,000 piece landscape with bright flowers or a sunny beach.

She also enjoys combing through the computer systems, searching for these vulnerabilities. When Cleo finds a threat, she works with her colleagues advising how to implement changes and mitigate risks to their supply chains.

Career journey

Typically Supply Chain Security Analysts get their start in cyber security analysis roles. This work covers a broad cross-section of professionals who assess and provide insights on potential threats such as human behaviour factors.

Why this job matters

It felt like the world ran out of everything during the pandemic. Disruptions to supply chains affect us all, and that includes cyber security flaws and vulnerabilities. Supply Chain Security Analysts collect and analyze this data, providing guidance that reduces these risks to supply chains.

Soft skills

Cyber and IT training, verbal and written communication, eye for detail, risk management, logical reasoning

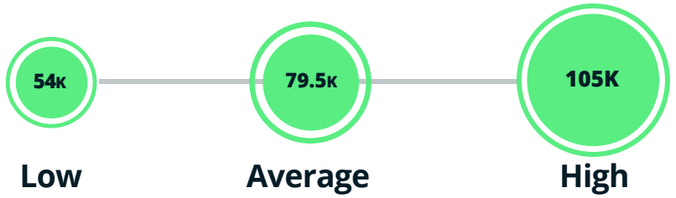
Other jobs like this

Cyber Security Analyst, Supply Chain Integrity Analyst

Secure Software Developer

Type of job
Design and Develop

Career Earning Potential



Educational pathways

MITT Programs:

Software Developer

CyberWave Micro-credentials:

Certified Network Defender

Certified Application Security Engineer

Certified Security Analyst

Licensed Penetration Tester

Relevant computer science degree or diploma related to programming, software design or software development.

A day in the life

Hana loves the creativity it takes to be a Secure Software Developer. Today she's working on performing security testing for software vulnerabilities. Her company is a global leader in the planning, designing and manufacturing of food infrastructure around the world. She has a deep knowledge of the attack vectors used to exploit software, and she spends her day troubleshooting and debugging issues that arise.

Hana's a self-driven person who often works independently, however today she finds a tricky bug that has her stumped. She's grateful for the collaborative environment that her work promotes so Hana teams up with a colleague to find a workable solution.

She finishes her day in a meeting with their developers. Over the next few months Hana will be working with them to create a new software tool.

Career journey

Secure Software Developers typically have 3-5 years' experience in software development followed by 3-5 years in secure software development activities.

Why this job matters

Organizations rely on these workers for each phase of the software development cycle. They provide the security analysis, defences and countermeasures that make software strong and reliable.

Soft skills

Self-driven, collaborative, attention to detail, analytical, computer science foundations

Other jobs like this

Secure Software Developer, Software Testing, Evaluation Specialist, Vulnerability Analyst

Security Engineer

Type of job
Design and Develop

Career Earning Potential

Low	Average	High
58.5K	91.75K	125K

Educational pathways

MITT Programs:

Software Developer

CyberWave Micro-credentials:

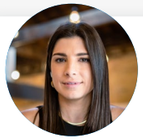
Certified Network Defender

Certified Application Security Engineer

Certified Security Analyst

Licensed Penetration Tester

Relevant engineering degree or technologist diploma (depending on organizational requirements).



A day in the life

Priya works for an engineering company focusing on transit and rail safety. She loves working for a team that believes in innovation, social responsibility and improving people's lives. Priya starts her day focused on the risk mitigation strategies and security threat analysis to identify any safety hazards for the rail including operational cyber security and emergency response planning.

Problem-solving and explaining complex concepts are a big part of Priya's job. Transit and rail line safety is a top priority at Priya's company, where lives are at stake. She is a very analytical person and is diligent in communicating the necessary protocols to keep the public safe.

Priya always purchases the latest phone and jumps on her computer updates as soon as they pop up. Now she works for a company that embraces change and new technologies and Priya finds her work incredibly exciting.

Career journey

Security Engineers typically have post-secondary education and 5-10 years' experience. In Canada, an engineer is a licensed professional, however, this role addresses cyber security occupational standards with the understanding that pure engineering tasks are out of their scope.

Why this job matters

Using tools and resources, organizational security documentation and IT guidance, security engineers research and define an organization's security to protect the people that they serve.

Soft skills

Interpersonal skills, writing, verbal communications, an analytical thinker, collaboration and teamwork

Other jobs like this

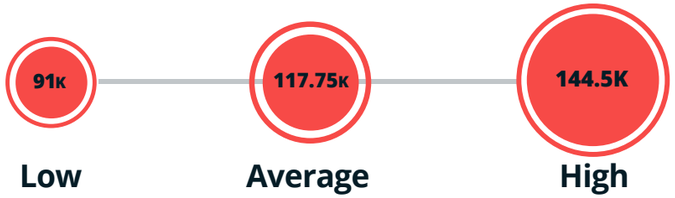
Encryption Engineer, Technologist, Operational Technology Engineer, Security Designer, Encryption Engineer

Security Architect

Type of job
Design and Develop

> IF YOUR DEVICE IS CONNECTED TO THE INTERNET, IT IS VULNERABLE TO A CYBER-ATTACK. WORLDWIDE, STRATEGY ANALYTICS ESTIMATES THERE WILL BE 38.6 BILLION DEVICES CONNECTED TO THE INTERNET BY 2025. (3)

Career Earning Potential



Educational pathways

MITT Programs:

Software Developer

CyberWave Micro-credentials:

Certified Network Defender
Certified Application Security Engineer
Certified Security Analyst
Licensed Penetration Tester
Advanced Network Defense

Post-secondary education in IT infrastructure and architecture (e.g.; computer engineering, IT systems architecture).

A day in the life

This morning, Rumi gets out of bed and does a yoga class in her living room. She strolls into her home office for 9:00 am and logs into the company system. Rumi works remotely with a flexible schedule for a technology consultant and is a person who loves IT. Google is her best friend and she serves as an expert level resource to a wide variety of clients.

Rumi enjoys the independence and self-motivation that her work requires and today she's diving into a cloud-based project. While rooting around, Rumi anticipates a complicated tech issue and is able to develop a work around before it becomes a problem for the client. The ability to be proactive is one of the reasons Rumi loves her job and why she is good at it.

The rest of her day is a mix between leading and contributing to complex security and infrastructure projects. In the afternoon, Rumi makes a green smoothie in her own kitchen and finishes the day by filling out detailed tickets to document all the activities she's completed.

Career journey

Education and previous training and experience in IT security infrastructure are the pathways to this career. It's an emerging specialist role primarily employed in large tech-enabled organizations, shared services and systems or security providers.

Why this job matters

Security architects are problem solvers who can explain complex technology to other people. They see the big picture and address security requirements in all aspects of an organization's infrastructure.

Soft skills

Problem-solver, good communicator, ability to tutor people about technology they aren't familiar with, technical aptitude

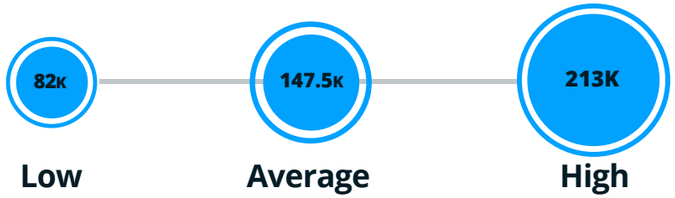
Other jobs like this

Enterprise Security Architect

Chief Information Security Officer (CISO)

Type of job
Oversee and Govern

Career Earning Potential



Educational pathways

MITT Programs:

Software Developer

CyberWave Micro-credentials:

Certified Ethical Hacker
Certified Network Defender
Certified Threat Intelligence
Disaster Recovery Professional
Advanced Network Defense

Bachelor's degree in computer science or related discipline or equivalent training and experience.

A day in the life

Freya works in a general hospital where she focuses on the privacy and safety of its patients and staff. She has a disciplined approach to the complex security programs that she plans, finalizes and executes. The hospital also has a corporate privacy program, and Freya oversees the implementation, monitoring and reporting. She collaborates with many people including administration, legal counsel, and outside parties to ensure the hospital's privacy interests are represented.

Freya likes to set her meetings in the morning and catch up on emails before lunch. She has tight deadlines and senior-level responsibilities, including ensuring her team is educated and trained on healthcare privacy issues. This includes testing incident response plans and collaborating with various leaders on business continuity and risk assessment.

Often in the afternoon, Freya blocks off time to keep up with legislation and new policies. She's always been an avid reader and appreciates setting aside time in her role to read up on material that keeps Freya informed in the everchanging cyber security landscape. Because a hospital is a 24/7 operation and breaches can happen anytime, Freya's position has an "on-call" component in case of an emergency.

Career journey

A CISO is often considered the pinnacle of a cybersecurity career. These people have extensive experience (10+ years) in IT or systems, preferably with cybersecurity management experience. Pathways to this executive-level position include competency development such as training, education and experience outside of the technical field.

Why this job matters

This role protects digital information and informs security within an organization in both the public and private sector. There's a growing number of opportunities from safeguarding people's data in healthcare to working for a global corporation.

Soft skills

Leadership, communication, project management, empathetic, persuasive, trustworthy

Other jobs like this

Chief Security Officer, Departmental Security Officer, Information Security Director

CyberWave

The Future of Cyber Security

Cyber security is a pervasive issue of our time and with that lies incredible opportunity. Manitoba is part of that evolution as opportunities for these creative, well paid and in-demand careers grow. As the global need for cyber security skills continue to rise, professionals who possess the knowledge, skills and abilities to work in these careers are enjoying major benefits.

In an industry with a nearly 0% unemployment rate, the career opportunities in cyber security are wide and expansive. Whether you're interested in working for an independent business, major corporation or as an independent contractor, every organization requires cyber security. It's always a bonus to have options, and these roles often include the ability to work in-house or remotely. There are also significant pathways for advancement, particularly for women, as the industry continues investing in growing a diverse and inclusive workforce.

MANITOBA INSTITUTE OF TRADES & TECHNOLOGY

CyberWave Micro-Credentials

CyberWave at MITT is committed to addressing the shortage of cyber security professionals in Manitoba through a variety of micro-credential programs and pathways designed to help you get started on a career path that suits you. You have the ability to pick and choose courses tailored to your personal goals and interests, while learning from the top experts in Manitoba, Canada, and the world.

If you are looking to start or jump-start your career in cyber security, visit cyberwave.mitt.ca for a full list of micro-credential courses available to you. CyberWave micro-credentials are industry recognized and certified courses that give you the knowledge, tools, and expertise you need for success in the cyber security industry, all tailored to fit your interests and schedule.

MITT Programs

MITT also offers full-time programs in multiple specialties that act as a springboard and give you a base knowledge of tech and cyber security. There are four full-time programs at MITT that all have components to help you pursue a new career in cyber security:

Cyber Defence and Cloud Administration Diploma

Network and Systems Administrator

Network Security Diploma

Software Developer

Pembina Trails Early College (PTEC)

Motivated by Manitoba's tech talent gap, PTEC is this province's only technology early college/high school dual credit program. MITT has made a long-term commitment to the success of the school model and its students working in partnership with Pembina Trails School Division and Tech Manitoba. Grade 11 and 12 students attend MITT and choose between two streams: Network and Systems Administrator or Software Developer. Upon graduating, they earn both a high school diploma, an MITT certificate plus credit towards completion of 1-year of their MITT post-secondary education.

RBC Foundation

MANITOBA INSTITUTE OF TRADES & TECHNOLOGY

CyberWave

Visit:

cyberwave.mitt.ca

and

mitt.ca/programs/post-secondary-programs

to learn more!

@CyberWave_MITT