2025

seceon

Canada Under Digital Siege:

The 74% Ransomware Explosion Threatening National Security

With healthcare systems crippled and infrastructure breached, Canada faces a cyber crisis needing immediate, coordinated action.

Executive Summary

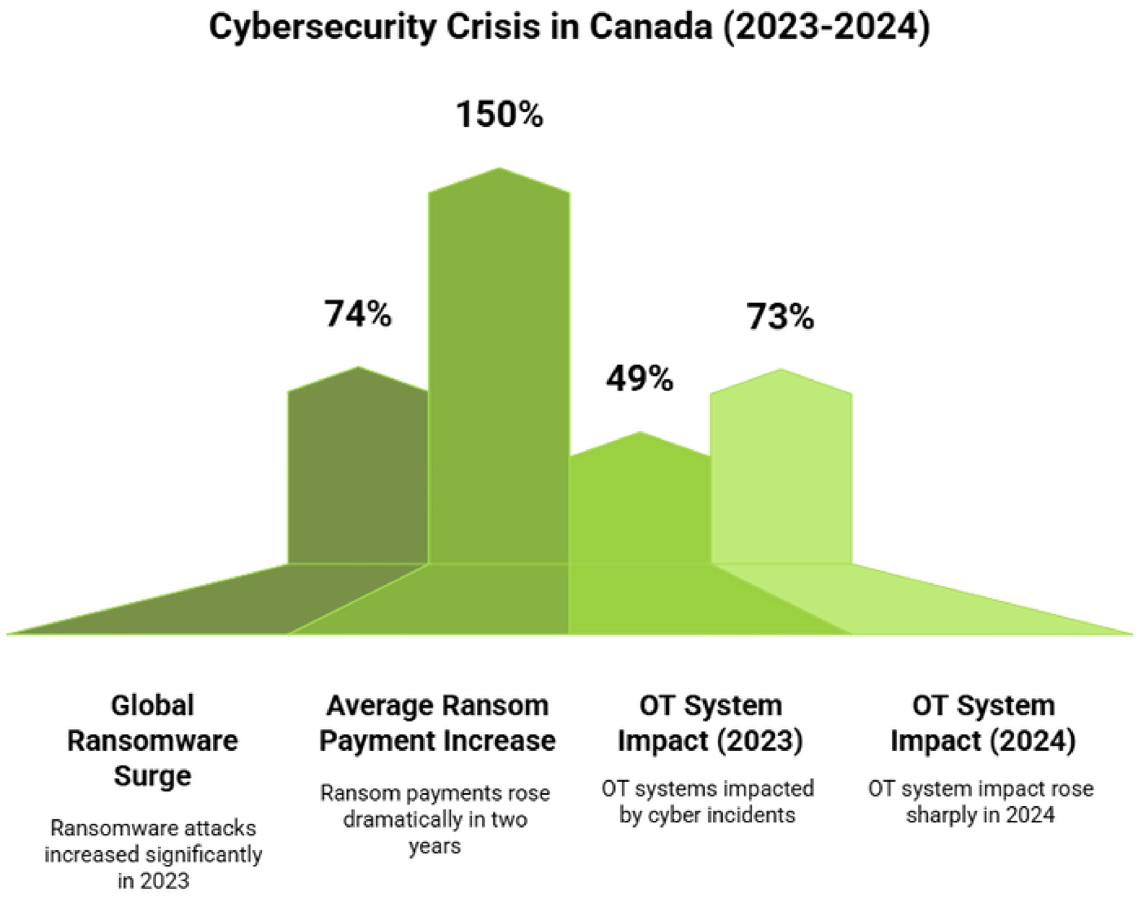
Canada is entering a critical cybersecurity era as ransomware surges 74 percent, state-sponsored attacks intensify, and OT systems become primary targets. Healthcare, energy, finance, and government networks are being compromised at an alarming scale, with 73 percent of 2024 incidents impacting OT and shifting the threat from data theft to real-world disruption. China, Russia, Iran, and North Korea are conducting increasingly sophisticated campaigns across infrastructure and supply chains, while Canadian organizations struggle with rising breach costs, talent shortages, and outdated defenses.

To keep pace, institutions must modernize urgently. AI-driven platforms like Seceon deliver real-time detection of state-sponsored activity, OT-focused protection, bilingual support, and compliance with OSFI, PIPEDA, and Bill C-8. With sub-48-hour threat disruption, strong ROI, and more than 94 percent detection accuracy, organizations can move from reactive firefighting to proactive resilience. Canada’s national security now depends on unified action, zero-trust adoption, continuous monitoring, and strategic investment to protect the nation’s digital infrastructure in an evolving era of cyber warfare.

The Stark Reality: Canada's Cybersecurity Wake-Up Call

In the sterile corridors of a major Canadian healthcare network during winter 2024, an eerie silence replaced the usual bustle of medical activity. Surgeries were postponed, patient care disrupted, and sensitive data held hostage, all due to a sophisticated ransomware attack that brought one of the country's largest healthcare systems to its knees. This incident wasn't an isolated tragedy but a harbinger of a much larger crisis engulfing the nation.

According to the Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025-2026, Canada is experiencing a cybersecurity crisis of unprecedented scale. Ransomware attacks surged 74% globally in 2023, with Canadian organizations paying an average of $1.13 million CAD per incident a staggering 150% increase in just two years. Perhaps most alarming, 73% of reported cyber incidents in 2024 impacted operational technology (OT) systems, up dramatically from 49% the previous year.



"At first glance, it seems that the cyber threat environment hasn't changed much," notes the Canadian Centre for Cyber Security. "What has changed, however, is that state adversaries are getting bolder and more aggressive." This understated assessment masks a reality where 336 pre-ransomware notifications were issued to Canadian organizations in 2024 alone, spanning every level of government and critical sectors, including healthcare, energy, manufacturing, finance, and education.

The Four Horsemen: State-Sponsored Threats Targeting Canada

Canada's geographic proximity to global superpowers and its strategic importance as a G7 nation have made it a prime target for sophisticated state-sponsored cyber operations. The threat landscape is dominated by four primary adversaries, each employing distinct strategies to achieve their objectives.

China (PRC): The Persistent Infrastructure Infiltrator

The People's Republic of China poses **"the most sophisticated and active state cyber threat to Canada today,"** according to Canadian intelligence assessments. Chinese threat actors have achieved unprecedented penetration of Canadian networks, with **at least 20 Canadian government networks compromised** and politicians critical of the Chinese Communist Party specifically targeted.

The **Volt Typhoon** campaign represents a particularly concerning evolution in Chinese tactics. Unlike traditional espionage operations focused on data theft, Volt Typhoon is **pre-positioning within critical infrastructure networks** for potential disruptive or destructive attacks in the event of a major crisis. This strategic shift toward preparing for kinetic cyber warfare marks a new phase in state-sponsored cyber operations.

Chinese operations against Canada include:

- Systematic targeting of government networks at all levels
- Industrial espionage campaigns focusing on cutting-edge technologies

- **Diaspora community surveillance and intimidation**
- **Critical infrastructure reconnaissance** for future operational preparation

Russia: The Hybrid Warfare Specialist

Russia employs cyber operations as part of a comprehensive hybrid strategy designed to **"confront and destabilize Canada and our allies."** Russian threat actors combine traditional espionage with influence campaigns and destructive attacks, often using criminal proxies to obscure attribution. The **SolarWinds supply chain compromise** demonstrated Russia's capability to achieve massive scale through strategic targeting of software vendors. More recently, **Midnight Blizzard's breach of Microsoft's cloud-based enterprise email service** in January 2024 highlighted ongoing Russian capabilities against cloud infrastructure that supports numerous Canadian organizations.

Russian operations typically feature:

- **Supply chain attacks** targeting software and cloud service providers
- **Influence campaigns** designed to sow discord and undermine democratic institutions
- **Criminal proxy operations** that provide plausible deniability
- **Critical infrastructure probing** for strategic intelligence gathering

Iran: The Escalating Aggressor

Iran's cyber program has become increasingly aggressive, with the regime willing to conduct "disruptive cyber attacks beyond the Middle East" while managing escalation risks. The CyberAv3ngers group, operating as an IRGC hacktivist front, has demonstrated destructive capabilities against critical infrastructure, including water utilities and energy systems.

In January 2024, Iranian threat actors claimed responsibility for a water storage tank overflow at facilities in Texas, posting videos of compromised control systems on public forums. Canadian officials assess that similar attacks against Canadian critical infrastructure are "likely when the opportunity arises."

Iranian cyber capabilities include:

- Critical infrastructure targeting with demonstrated destructive intent
- Water and energy system compromise through OT exploitation
- Advanced persistent espionage against government and private sector targets
- Sophisticated social engineering campaigns against key personnel

North Korea: The Financial Crime Powerhouse

While not representing a strategic threat to Canadian national security, North Korea presents a "persistent cybercrime risk across many sectors." The regime's cyber operations blend espionage with financial crime, generating funding through ransomware and cryptocurrency theft.

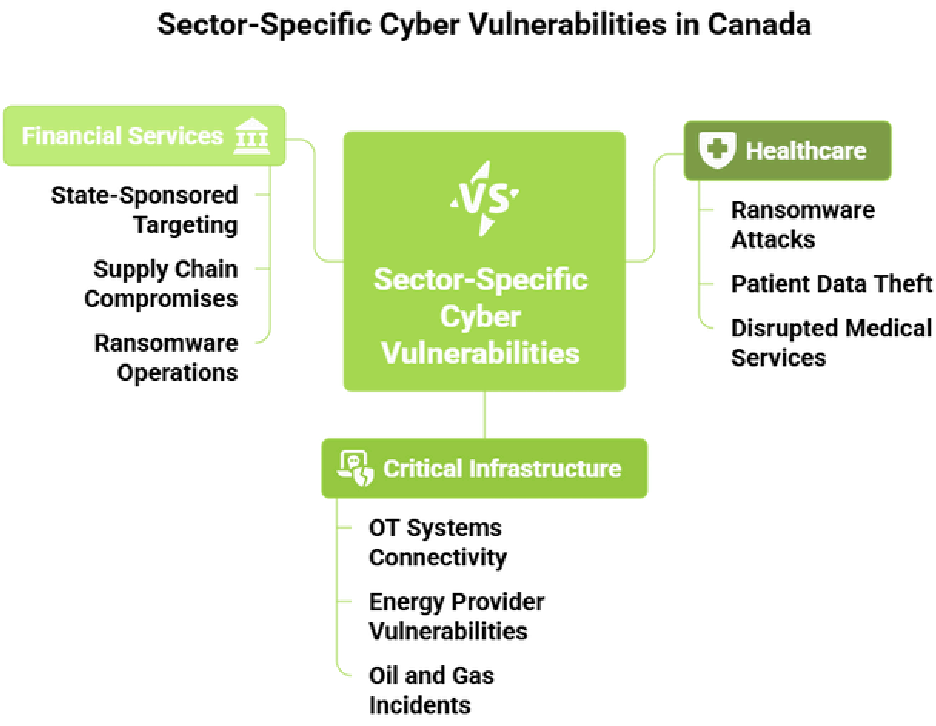
North Korean groups have pioneered sophisticated fake job recruitment campaigns as attack vectors, conducting global targeting through fraudulent employment opportunities and GitHub exploitation. These campaigns achieve high success rates through detailed research and credible professional personas that specifically target technology sector professionals.

Sector-Specific Vulnerabilities: Where Canada Hurts Most

Healthcare: Where Cyber Warfare Meets Human Lives

The healthcare sector represents the most vulnerable and consequential target in Canada's critical infrastructure landscape. **Over 400 healthcare organizations in Canada and the United States have experienced ransomware attacks since March 2020**, with incidents directly impacting patient care and safety.

The 2021 cyberattack on Newfoundland and Labrador's healthcare system serves as a stark reminder of potential consequences. The attack "paralyzed the entire Eastern Health region," forcing healthcare providers to adopt paper-based approaches for appointments and emergency procedures.



Recent healthcare targeting includes:

- **Five Southwestern Ontario hospitals** compromised through the TransForm Shared Service Organization
- **Patient data theft and public exposure** by ransomware groups
- **Wi-Fi, email, and patient information system disruption** leading to procedure postponements
- **Average breach costs of $9.77 million globally** for healthcare organizations

Critical Infrastructure: The Foundation Under Attack

Canada's critical infrastructure faces an unprecedented convergence of threats as operational technology (OT) systems become increasingly connected to enterprise networks. The expansion of Internet-connected OT increases both efficiency and vulnerability, with energy providers tracking 60 new vulnerabilities daily in grid networks.

The 2019 Statistics Canada survey found that approximately 25% of Canadian oil and gas organizations reported cyber incidents, the highest rate among all critical infrastructure sectors.

Recent incidents underscore ongoing vulnerabilities:

- **Suncor Energy's cyberattack** shut down credit and debit payments at Petro-Canada stations
- **The Trans-Northern Pipelines incident** resulted in the claimed theft of 183 GB of data
- **The International Joint Commission is targeting** confidential data stolen and encrypted

Financial Services: The Economic Battlefield

Canadian financial institutions face sophisticated targeting from both state-sponsored groups and cybercriminal organizations. **Financial sector organizations experience average breach costs of $9.28 million CAD**, making them attractive targets for profit-driven threat actors.

The establishment of the **National Security Threat Forum for Federally Regulated Financial Institutions (FRFI)** demonstrates government recognition of escalating threats. This forum brings together over 150 representatives from financial institutions, federal and provincial authorities, and national security experts to address sector-specific threats.

Key financial sector vulnerabilities include:

- **Cloud-based service targeting** by state-sponsored actors
- **Supply chain compromises** affecting financial technology vendors
- **Advanced persistent threats** focused on competitive intelligence gathering
- **Ransomware operations** targeting payment processing systems

The Operational Technology Crisis: When Digital Meets Physical

Perhaps no trend is more concerning than the surge in attacks targeting **operational technology (OT) systems**. The **73% of cyber incidents impacting OT systems in 2024** represents a fundamental shift in threat actor capabilities and intentions.

OT systems control everything from power generation and water treatment to manufacturing processes and building environmental systems.

Unlike traditional IT networks, OT system failures can have immediate physical consequences, potentially endangering human lives and causing massive economic disruption.

Critical OT vulnerabilities include:

- **Lack of network segmentation** between IT and OT systems
- **Default or hardcoded credentials** in industrial control systems
- **Unsupported legacy software** in building and industrial controllers
- **Unvetted remote access tools** installed by vendors
- **Unencrypted communication protocols** vulnerable to interception

The **2024 Black Basta ransomware attack on Ascension Health** in the United States, which disrupted care for millions of patients, demonstrates the real-world consequences of OT targeting. Similar attacks against Canadian critical infrastructure could have devastating effects on public safety and national security.

The Seceon Solution: Transforming Canadian Cyber Defense

Against this backdrop of escalating threats and vulnerabilities, Canadian organizations require security platforms specifically designed to address the unique challenges of the Canadian threat landscape. **Seceon's AI-powered cybersecurity platform** provides comprehensive capabilities tailored to Canadian regulatory, linguistic, and operational requirements.

Real-Time State-Sponsored Threat Detection

Seceon's platform excels at detecting and responding to sophisticated state-sponsored attacks that traditional security solutions often miss. The platform's AI-driven behavioral analysis can identify the subtle indicators that distinguish Chinese Volt Typhoon campaigns from conventional cybercriminal activity, enabling security teams to respond appropriately to strategic-level threats.

The platform's **sub-48-hour threat disruption capability** proved critical in a recent incident where **CSE's foreign cyber operations team and the Cyber Centre worked together** to identify victims and disrupt a ransomware group targeting Canadian critical infrastructure. The threat was **"detected and disrupted within 48 hours"** through coordinated technical operations.

Critical Infrastructure and OT Protection

Seceon's **aiSecOT360 component** provides specialized protection for the operational technology environments that are increasingly under attack. The platform supports **over 70 industrial communication protocols** commonly used in Canadian energy, manufacturing, and utilities sectors.

Key OT security capabilities include:

- **Passive asset discovery** for over 10,000 OT device types
- **Deep packet inspection** for industrial protocols
- **Behavioral analysis** specifically designed for OT environments
- **Integration between IT and OT security operations**
- **Real-time threat detection** with sub-30-second response times

Bilingual Support and Canadian Compliance

Unlike generic security platforms, Seceon's solution includes comprehensive bilingual support (English/French) essential for Canadian organizations operating in both official languages. The platform also provides 100% compliance with Canadian regulatory frameworks including:

- Office of the Superintendent of Financial Institutions (OSFI) guidelines
- Personal Information Protection and Electronic Documents Act (PIPEDA) requirements
- Bill C-8 Critical Infrastructure Protection standards
- Communications Security Establishment (CSE) cyber security guidelines

Financial Sector Specialized Capabilities

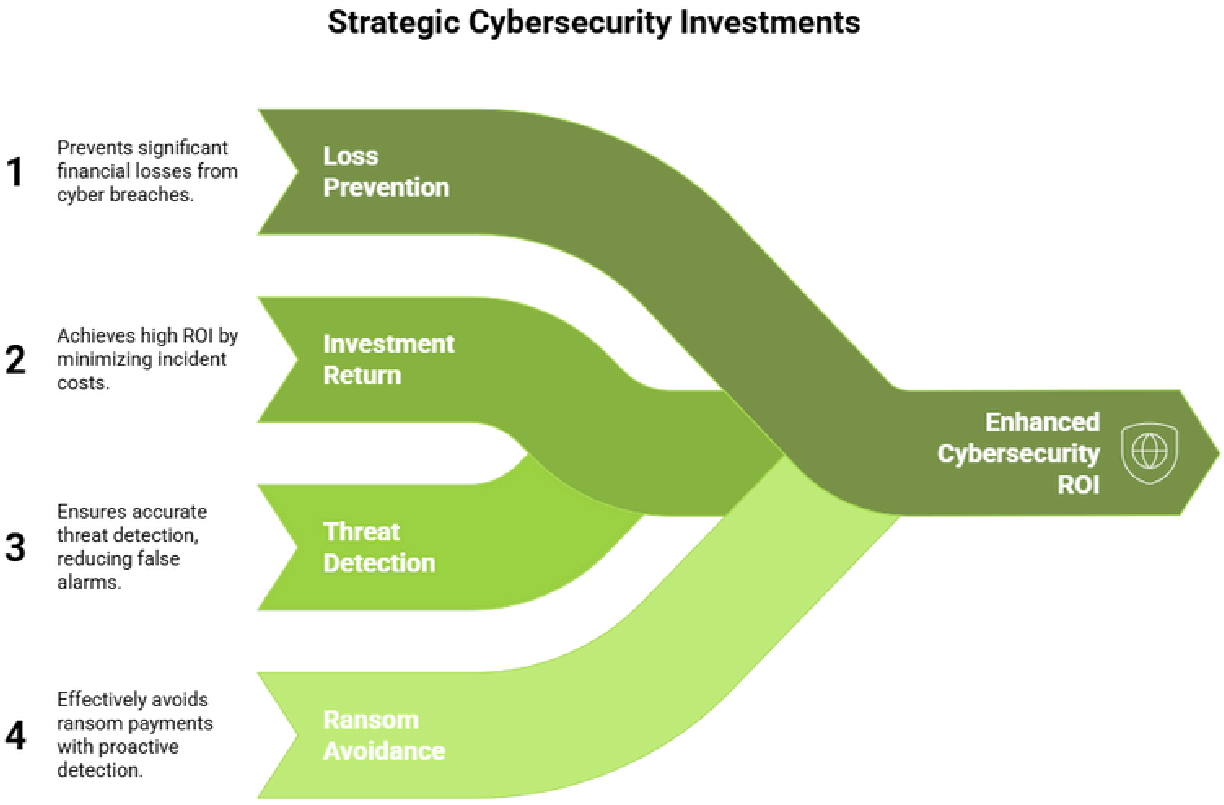
For Canadian financial institutions, Seceon provides specialized threat detection capabilities designed to identify the sophisticated targeting these organizations face.

The platform's **financial crimes detection modules** can identify patterns consistent with state-sponsored economic espionage while maintaining compliance with strict financial sector regulations.

The Economic Imperative: ROI in the Age of Cyber Warfare

The business case for comprehensive cybersecurity platforms in Canada extends far beyond compliance requirements. Organizations implementing platforms like Seceon report significant measurable benefits:

- **$6.32 - $9.28 million CAD annual loss prevention** based on average Canadian breach costs
- **380% return on investment within 18 months** through reduced incident response costs and downtime prevention
- **94% threat detection accuracy** reducing false positives and security team workload
- **88% ransom avoidance rate** among organizations with pre-ransomware detection capabilities


Strategic Cybersecurity Investments
1
Prevents significant financial losses from cyber breaches.
Loss Prevention
2
Achieves high ROI by minimizing incident costs.
Investment Return
3
Ensures accurate threat detection, reducing false alarms.
Threat Detection
4
Effectively avoids ransom payments with proactive detection.
Ransom Avoidance
Enhanced Cybersecurity ROI

These metrics demonstrate that cybersecurity represents a strategic business enabler rather than merely a cost center. In an environment where 42% of Canadian organizations that pay ransoms fail to completely recover their data, prevention-focused security investments provide both financial and operational advantages.

The Workforce Crisis: Skills Shortage in Critical Times

Canada's cybersecurity crisis is exacerbated by a **dangerous gap in services and expertise**. The Canadian Centre for Cyber Security warns that the cybersecurity industry "**lacks sufficient professionals, solution providers, and vendors with the expertise to deliver OT-specific security at scale.**"

Current workforce challenges include:

- **Insufficient cybersecurity professionals** across all sectors
- **Lack of OT-specific security expertise** in critical infrastructure protection
- **Skills gaps in state-sponsored threat detection** and response
- **Limited bilingual cybersecurity capabilities** for Canadian organizations

The federal government has implemented several initiatives to address these challenges, including programs that created **over 1,000 student work placements in cybersecurity** between 2018 and 2021. However, these efforts remain insufficient to meet the scale of current and projected threats.

Regulatory Evolution: From Guidelines to Requirements

Canada's regulatory landscape is evolving rapidly in response to escalating cyber threats. **Bill C-8** and similar measures are driving **mandatory risk programs** that include building systems and operational technology.

For owners of commercial, healthcare, financial, and public sector facilities, **compliance frameworks are no longer optional**.

Key regulatory developments include:

- **Mandatory cyber risk assessments** for critical infrastructure
- **Incident reporting requirements** to federal authorities
- **Supply chain security standards** for technology vendors
- **Data localization requirements** for sensitive government and financial data

Cyber insurance providers are also adapting to new realities, with underwriters beginning to view OT systems as **uninsurable without proper visibility and controls**. Insurance renewals are now contingent on demonstrating comprehensive security controls across both IT and OT environments.

Looking Forward: The Next Phase of Cyber Warfare

Several trends will shape Canada's cybersecurity landscape through 2026 and beyond:

AI-Driven Attacks and Defenses

The integration of artificial intelligence into both attack and defense capabilities will fundamentally alter the cybersecurity landscape. **AI-enhanced social engineering campaigns** and **automated vulnerability exploitation** will require equally sophisticated defensive AI systems.

Quantum Computing Threats

As quantum computing capabilities advance, current cryptographic standards will become vulnerable. Canadian organizations must begin **planning for post-quantum cryptography** implementation to maintain data protection in the quantum era.

5G and IoT Proliferation

Canada's **5G infrastructure rollout** and widespread IoT adoption will create exponentially more attack vectors. The **global smart OT market** is expected to grow from $280 billion CAD in 2020 to over **$1 trillion CAD in the early 2030s**, dramatically expanding the attack surface for critical infrastructure.

Geopolitical Cyber Warfare Escalation

The integration of cyber operations with conventional geopolitical strategies means that **cyber defense is increasingly a matter of national security**. The Canadian government's **$917.4 million Budget 2024 allocation** for enhanced intelligence and cyber operations programs reflects this reality.

Strategic Recommendations: Building Cyber Resilience

For Canadian organizations navigating this threat landscape:

Immediate Actions

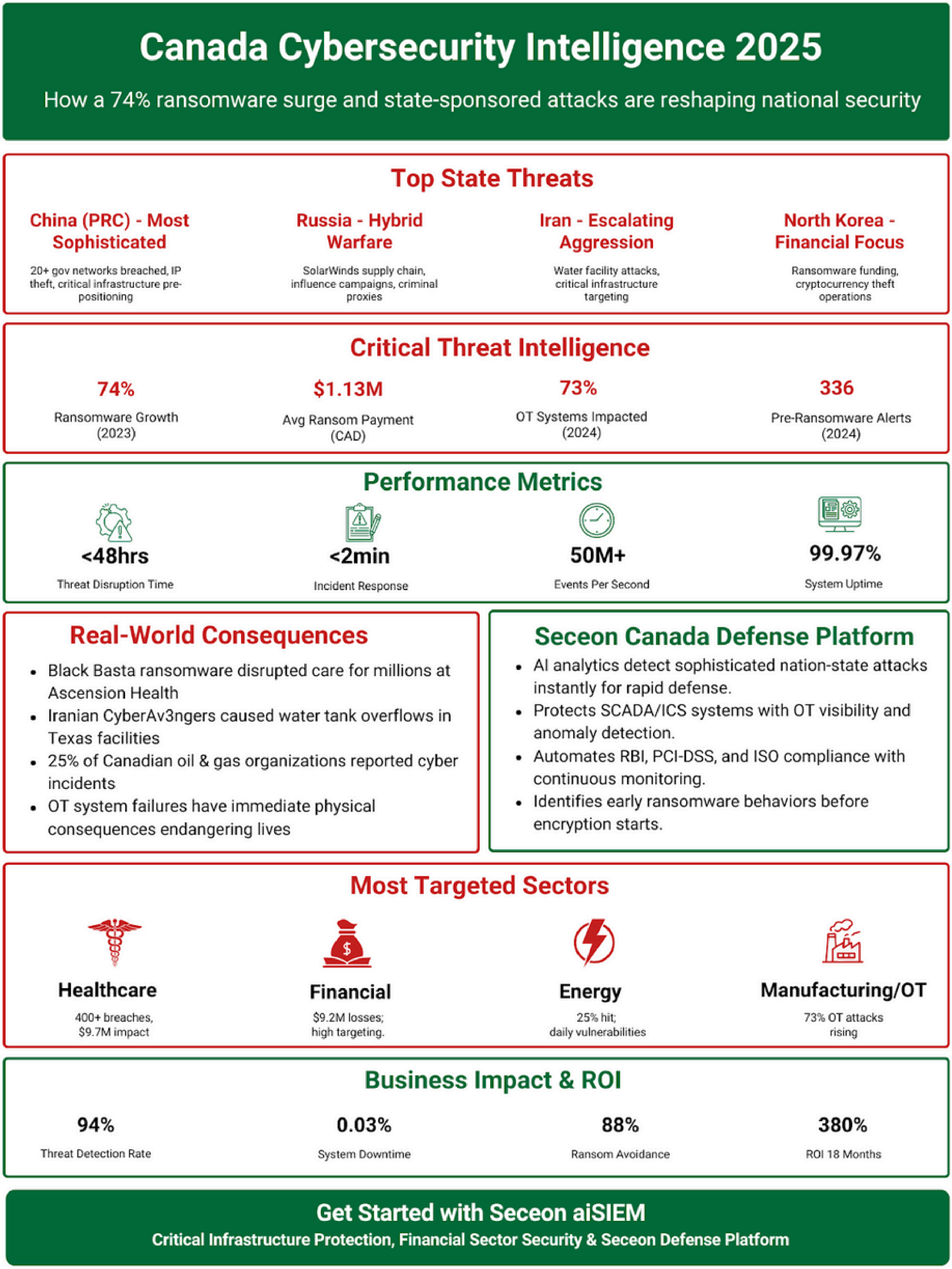
- **Implement comprehensive OT security** covering all industrial control systems
- **Deploy AI-driven behavioral analysis** to detect state-sponsored activities
- **Establish 24/7 security operations** center capabilities with bilingual support
- **Conduct regular vulnerability assessments** focusing on IT/OT convergence points

Strategic Investments

- **Adopt zero-trust architecture** principles across all network environments
- **Implement automated compliance** frameworks for Canadian regulatory requirements
- **Invest in cybersecurity workforce development** with OT-specific training
- **Develop quantum-resistant security architectures** for long-term protection

Collaboration and Intelligence Sharing

- **Participate in sector-specific threat intelligence sharing** through CSE programs
- **Establish public-private partnerships** for critical infrastructure protection



Canada Cybersecurity Intelligence 2025

How a 74% ransomware surge and state-sponsored attacks are reshaping national security

Top State Threats

China (PRC) - Most Sophisticated	Russia - Hybrid Warfare	Iran - Escalating Aggression	North Korea - Financial Focus
20+ gov networks breached, IP theft, critical infrastructure pre-positioning	SolarWinds supply chain, influence campaigns, criminal proxies	Water facility attacks, critical infrastructure targeting	Ransomware funding, cryptocurrency theft operations

Critical Threat Intelligence

74%	$1.13M	73%	336
Ransomware Growth (2023)	Avg Ransom Payment (CAD)	OT Systems Impacted (2024)	Pre-Ransomware Alerts (2024)

Performance Metrics

<48hrs	<2min	50M+	99.97%
Threat Disruption Time	Incident Response	Events Per Second	System Uptime

Real-World Consequences

- Black Basta ransomware disrupted care for millions at Ascension Health
- Iranian CyberAv3ngers caused water tank overflows in Texas facilities
- 25% of Canadian oil & gas organizations reported cyber incidents
- OT system failures have immediate physical consequences endangering lives

Seceon Canada Defense Platform

- AI analytics detect sophisticated nation-state attacks instantly for rapid defense.
- Protects SCADA/ICS systems with OT visibility and anomaly detection.
- Automates RBI, PCI-DSS, and ISO compliance with continuous monitoring.
- Identifies early ransomware behaviors before encryption starts.

Most Targeted Sectors

Healthcare	Financial	Energy	Manufacturing/OT
400+ breaches, $9.7M impact	$9.2M losses; high targeting.	25% hit; daily vulnerabilities	73% OT attacks rising

Business Impact & ROI

94%	0.03%	88%	380%
Threat Detection Rate	System Downtime	Ransom Avoidance	ROI 18 Months

Get Started with Seceon aiSIEM

Critical Infrastructure Protection, Financial Sector Security & Seceon Defense Platform

- **Engage with international allies** through Five Eyes and other security partnerships
- **Support national cybersecurity research** and development initiatives

Conclusion: From Crisis to National Security Imperative

Canada's cybersecurity crisis represents both an urgent threat and a strategic opportunity. The escalating sophistication of state-sponsored attacks, the surge in ransomware incidents, and the targeting of critical infrastructure demand immediate, coordinated action across all sectors.

Organizations that invest in comprehensive, AI-driven security platforms like Seceon's solution will not only protect themselves but also contribute to national resilience against cyber warfare.

The choice facing Canadian leaders is stark: adapt quickly to the new reality of persistent, sophisticated cyber threats, or risk becoming casualties in an escalating digital conflict that threatens both economic prosperity and national security.

As Canada navigates this critical juncture, the organizations that will emerge stronger are those that view cybersecurity not as a compliance requirement, but as a fundamental enabler of digital sovereignty and national security. In this context, platforms like Seceon represent more than security tools, they are the foundation for Canada's secure digital future in an increasingly dangerous cyber environment.

The winter 2024 healthcare ransomware attack was a warning. The question now is whether Canada will heed that warning and take the bold action necessary to protect its digital infrastructure, economic interests, and national security in the cyber warfare era that has already begun.

About Seceon

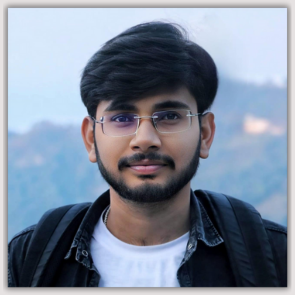
Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

References and Citations:

This whitepaper is based on research and data from:

- Canadian Centre for Cyber Security – National Cyber Threat Assessment
- Communications Security Establishment (CSE) – Cyber Alerts & Reports
- Statistics Canada – Cybersecurity and Critical Infrastructure Data
- Public Safety Canada – Infrastructure Protection Framework
- Documented incidents and intelligence from Canadian healthcare, energy, finance, and government sectors

About the Author



Anand Prasad

AI/ML Cybersecurity Engineer, Seceon Inc.

Anand with expertise in SOC operations, SIEM & XDR platforms, threat intelligence, and incident response. He strengthens enterprise cyber defense, streamlines security workflows, and ensures compliance across IT, OT, IoT, and cloud environments. Passionate about AI/ML-driven security, Anand focuses on reducing risk exposure and delivering measurable ROI.