SPONSORSHIP PROSPECTUS

siberX®

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

SEPTEMBER 24, 2025.

THE WESTIN OTTAWA
11 COLONEL BY DR, OTTAWA, ON K1N 9J1

IN PERSON & DIGITAL

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 4th cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place at the beautiful The Westin Ottawa in the nations capital, Ottawa, Canada on September 24, 2025 and is designed to strengthen Canada's cybersecurity readiness and response strategies.

This event brings together Public and Private sector stakeholders along with the Canadian Cybersecurity community to discuss how their organizations would respond to such an attack.

Participants, in real-time, will deal with an active incident and breach - collaborating with leaders from across Canada, technical and operational solutions will be proposed to contain the attack.

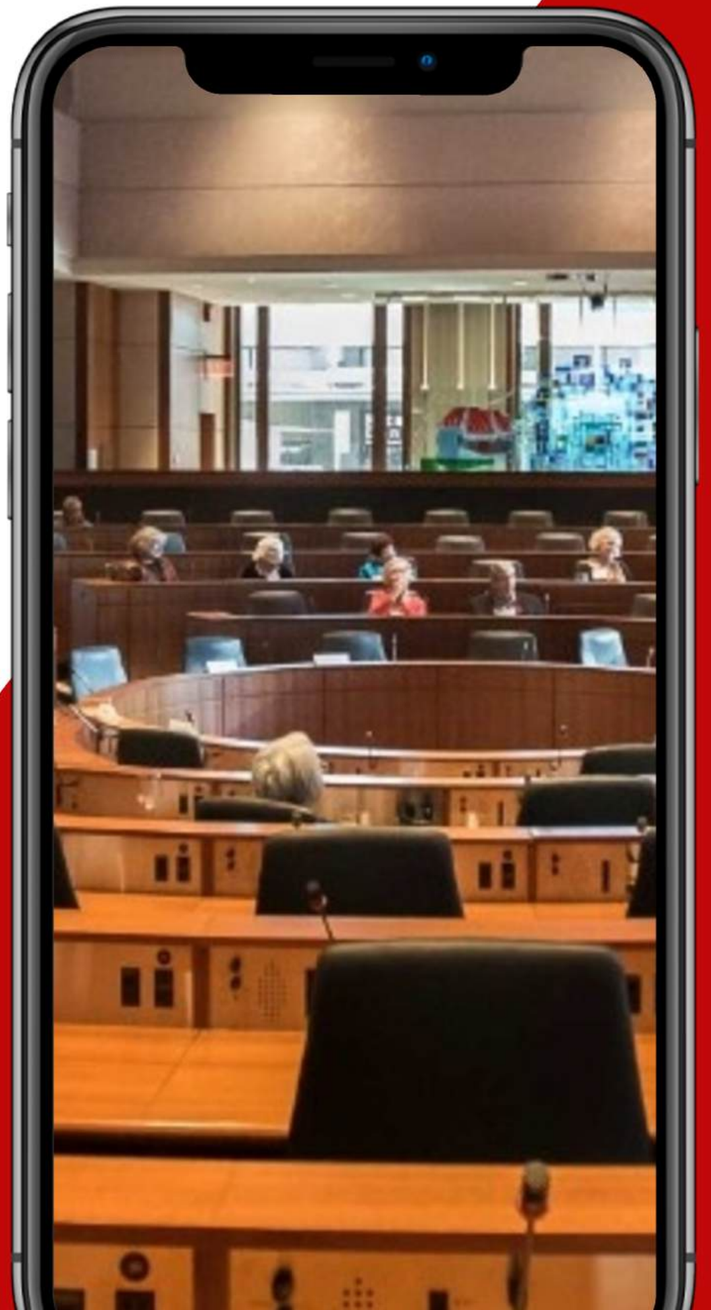
O Canada, we stand on guard for thee.
Protégera nos foyers et nos droits.

PAST SPONSORS

SentinelOne, Canon, SailPoint, TELUS Business, ARMIS, CDW, aws, CROWDSTRIKE, OBSIDIAN, TANIUM

PAST PARTNERS

Cyber Security Centre of Excellence, Ontario



siberX

OPERATION: DEFEND THE NORTH

PAST ADVISORY BOARD

Rhonda Bunn
CAO
Town of Midland

Kristi Honey
CAO
Township of Uxbridge

Abdul Karim
CISO
Unity Health Toronto

Octavia Howell
VP, CISO
Equifax Canada Co.

Anshul Srivastava
CISO
TTC

George Al Koura
CISO
RUBY

Bil Harmer
Operating Partner & CISO
Craft Ventures

Cat Coode
Data /Privacy Strategist
Binary Tattoo

Ali Shahidi
Director, Information Security & Risk
TCHC/TSCHC

Jassi Kaur
Director of IT and Security
Bulk Barn

Dr. Eman Hammad
Security & Privacy Working Group Co-Chair
IEEE Future Networks Initiative

Ali Abbas Hirji
CISO
YES

Gemma Ahn
CIO
Brock University

Kush Sharma
Founder
KnightSpectre

Iain Paterson
CISO
WELL Health Technologies

John Pinard
VP, IT Operations, Infrastructure & Cybersecurity
DUCA Financial Services Credit Union

Terry T
Acting Head, Cyber Investigations Unit
CSIS

Tommaso Lorenzo
Manager, Cybersecurity
Niagara Health

Vaughn Hazen
CISO
CN

Bob Gordon
Strategic Advisor
Canadian Cyber Threat Exchange

Vivek Khindria
Former SVP Cyber Security, Network, Technology Risk
Loblaw Companies Limited

Terence Malatombee
AVP Cyber Strategy, Governance and Control
TD Bank

Emerson Rajaram
CISO
Wellington-Dufferin-Guelph Public Health

Mark Dillon
VP of IT
Enova Power

Kim Schreader
Director, Cybersecurity Professional Services
TELUS Communications

Renee Guttmann-Stark
Founder, CISO
CisoHive

Vivienne Suen
Distinguished Arcitect
TD Bank

Nilesh Shastri
CISO
Canadian Institute for Health Information (CIHI)

Roozbeh Taheri-Nia
Founder
InCloud Security

Dhanush Liyanage
Senior Manager, Cyber Security Defense Operations
Ontario Health

Daniel Pinsky
CSO
CDW Canada

Lina Dabit
Unit Commander Cybercrime Investigative Team
RCMP

Kelley Irwin
Strategic Advisor, Board Director
Descartes Systems Group

Olawumi Alofe-Babalola
Cybersecurity Leader & Advocate
Bank of Canada

Osman Saleem
ICS Cybersecurity Program Manager
GTAA

Shakeel Sagarwala
Chief Information Security Officer
Canadian Tire Bank

Rachel Babins
Co-Founder
ELCH

Shilpa Dahiya
Senior Director, Cybersecurity
CAAT Pension Plan

Sunil Chand
VP, Security Practice
Centrilogic

Shelley Wark-Martyn
Strategic Training Executive
SANS

Wes Sheppard
CISO
OrderGrid

Amit Chopra
Head of Information Systems
Lakefield College School

Kris E
RCMP

Sherry Rumbolt
Senior Cybersecurity Strategist
Treasury Board of Canada Secretariat

Mirza Baig
Director, Cyber Security
MPAC

Teodor Pana
Director, Cyber Security
SE Health

KEY HIGHLIGHTS

- **Leaders from Critical Sectors Involved in Exercise:** Energy, Financial, Healthcare, Government Services, Telecommunications and Retail.
- **Simulated Cyber Attacks:** Engage in sector-specific cyber threat scenarios
- **Expert-Led Sessions:** Technical and operational discussions with industry leaders - real-time visualizations from an active environment will be incorporated
- **Networking Opportunities:** Connect with professionals across sectors and showcase.

EVENT OVERVIEW:

- **Duration: SEPTEMBER 24, 2025.**
- **Format:** Tabletop event held at SThe Westin Ottawa, Ontario.
- 9:00 am - 6:30 pm Exercise and Networking
- **Objective:** Join professionals across sectors working towards protecting a cyber attack against Canada's critical sectors via a cybersecurity readiness exercise

---

DEMOGRAPHICS:

- **PUBLIC/PRIVATE SECTOR:** 50% public & 50% private sector viewing this online, expected attendance, 300 leaders in-person & 3,000+ online.
- **MEDIA:** Media has been invited and will partcipate in coverage (Globe & Mail, Toronto Start, Technology Media)
- **DIGNITARIES:** Minister of Public and Business Service Delivery, CIO & CISO Provinces, MPs Mayors, and Councillors invited to open each day and participate.

MODULE & SPONSORSHIP OPPORTUNITIES

A Tainted Supply:

A Cyber Attack Paralyzes Ottawa. On a crisp winter morning in Ottawa, a sophisticated cyber attack cripples the city's primary water treatment plant at 8:00 AM. Attackers infiltrate the SCADA system, compromising filtration and chlorination processes while triggering erratic valve behavior. Within minutes, the water becomes unsafe and communication channels are jammed, leaving operators blind. By 9:10 AM, hospitals report illness from contaminated water and social media spreads panic. But the attack doesn't stop there. It quickly cascades across other sectors: healthcare systems are breached, transportation faces delays and telecom networks overload, preventing effective communication.

Financial institutions struggle and phishing campaigns exploit the confusion, further compromising security. The municipal government is overwhelmed and unable to manage the chaos as misinformation spreads, paralyzing the city's response efforts. The federal government is soon involved, deploying cybersecurity experts and resources, but their efforts are hampered by the widespread nature of the attack.

This coordinated attack on Ottawa's water infrastructure causes a ripple effect across essential services. Disruptions in healthcare, transportation, finance and communications escalate as each sector faces not only operational failure but also mounting cyber threats.

The breach of one critical infrastructure provider highlights the interconnected vulnerability of the entire city, demonstrating how a cyber attack can bring a city to its knees, eroding trust in essential services and forcing federal intervention to restore control.

September 25, 2025 | 9:00 AM - 10:30 AM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 1: **Detection and Analysis** **3 SPOTS REMAINING**	A sophisticated cyber attack on Ottawa's critical water infrastructure wreaks havoc on the city's water supply. This module focuses on the initial stages of investigation as the team works to identify the attack vector, assess vulnerabilities, and establish secure communication channels. Given the magnitude of the attack, impacting the capital's core services, the team must operate under intense pressure—mitigating public panic, misinformation and ensuring that critical water supply functions are restored while investigating the breach.	• Investigating the breach: Trace signs of compromise and determine which components of the water facility's network were targeted. • Vulnerability Identification: Identify compromised systems such as water treatment controls and automated sensors to prevent further disruptions. • Secure Communication: Ensure encrypted, secure lines of communication are maintained for sharing sensitive information without risking further exposure.	CIS Control Focus: CIS Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs; CIS Control 17 - Incident Response and Management.	Sponsors providing solutions for automated threat detection, incident monitoring, and secure communications during high-stress crisis scenarios. Their technologies will help mitigate the breach's impact and improve analysis accuracy.

MODULE & SPONSORSHIP OPPORTUNITIES

September 25, 2025 | 11:00 AM - 12:30 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 2: **Containment & Discovery** **3 SPOTS REMAINING**	As the attack intensifies, severe disruptions to the water purification and distribution systems put public health at risk. This module focuses on isolating the compromised systems and preventing the spread of the attack to other critical infrastructure. Teams will work to identify all related vulnerabilities and take immediate action to ensure that essential services can continue, minimizing public health risks.	• System Isolation: Contain affected systems, preventing the attack from spreading to other critical infrastructure. • Risk Discovery: Identify all potential health risks, including contaminated water or failed distribution systems, and mitigate them quickly. • Mitigation Strategies: Implement immediate steps to restore water supply while safeguarding public health.	CIS Control Focus: CIS Control 4 - Controlled Use of Administrative Privileges; CIS Control 13 - Data Protection.	Sponsor Opportunity: Sponsors specializing in endpoint protection, risk management, and containment technologies for critical infrastructure. These solutions will help secure systems under threat and minimize further exposure.

September 25, 2025 | 1:30 PM - 3:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 3: **Eradication** **3 SPOTS REMAINING**	With critical systems already disrupted, the immediate focus shifts to eradicating the cyber threat and restoring operations. This module will tackle the challenge of eliminating active threats from the water facility's network, restoring essential systems, and ensuring the water supply is safe. Connectivity across key systems must be re-established to prevent cascading failures and protect public health.	• Threat Eradication: Remove all traces of malware and backdoors, ensuring the facility's network is secure. • Restoring Operations: Restore core water treatment and distribution systems, carefully monitoring for residual threats. • Re-establishing Trust: Demonstrate effective recovery efforts to regain public confidence in the city's water supply.	CIS Control Focus: CIS Control 8 - Malware Defences; CIS Control 10 - Data Recovery.	Sponsors offering malware removal tools, threat eradication solutions and recovery technologies will play a crucial role in helping the water facility restore operations and secure infrastructure for the future.

MODULE & SPONSORSHIP OPPORTUNITIES

September 25, 2025 | 3:30 PM - 5:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 4: **Response and Post Incident Activity** **3 SPOTS REMAINING**	After the immediate threat is neutralized, evaluating the incident response becomes vital. This module focuses on reviewing the actions taken during the attack and developing strategies for long-term recovery. Sponsors will showcase solutions that help improve the effectiveness of crisis management, disaster recovery, and public relations efforts to restore normalcy and trust in critical infrastructure.	• Incident Response: Analyze and refine response actions taken during the attack, assessing their effectiveness .. • Disaster Recovery: Implement long-term recovery and resilience strategies to restore the water facility to full operational capacity. • Crisis Management: Manage communications with the public and government authorities to restore normalcy and manage public trust.	CIS Control Focus: CIS Control 17 - Incident Response and Management; CIS Control 11 - Secure Configuration for Hardware and Software.	Sponsors specializing in disaster recovery, crisis management and secure communications solutions will enhance the effectiveness of response teams and help mitigate future risks.

September 25, 2025 | 5:15 PM - 6:15 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 5: **Closing Remarks and Hotwash** **3 SPOTS REMAINING**	In the final session, a thorough analysis of the cyber attack will be conducted, highlighting lessons learned and areas for improvement. Sponsors will present post-incident analysis tools and strategic insights for enhancing future resilience. Emphasizing the importance of cross-sector collaboration, the session will focus on building long-term cybersecurity strategies to prevent future attacks on critical infrastructure.	• Lessons Learned: Conduct a post-incident review, identifying key insights and areas for improvement in future responses. • Forensic Reporting: Use forensic tools to understand the full scope of the attack and implement corrective measures. • Collaboration for Future Preparedness: Encourage collaboration across sectors to enhance preparation and prevention strategies for future incidents.	CIS Control Focus: CIS Control 17 - Incident Response and Management; CIS Control 18 - Penetration Testing.	Sponsors offering solutions for post-incident analysis, forensic reporting and strategic planning tools will help strengthen future preparedness and support continuous improvement in security practices.

SPONSORSHIP PACKAGE

Showcase your organization, with 1 module, select from the 5 modules **$10,000**

INCLUDED	DESCRIPTION
Booth 8 x 8	A dedicated space at the event for showcasing your organization's offerings, interacting with attendees, and networking with other industry experts.
CASL Compliant List of All Attendees (72 Hours Post Event)	Access to a compliant list of attendees post-event, allowing you to follow up and engage with potential clients or partners.
30-Second Commercial Played During Break/Lunch	A 30-second commercial featuring your organization, played during event breaks or lunch periods to enhance your visibility.
Promotion on Physical Signage, Website, Social Media, and Virtual Platform	Your organization's branding and messaging will be prominently displayed across various event channels including physical signage, the event website, social media platforms, and the virtual event
Session on YouTube	Your module session will be recorded and posted on YouTube, providing ongoing exposure and content for your audience.
3 In-Person Passes & 50 Virtual Passes	3 in-person passes for your team to attend the event physically, and fifty virtual passes for remote participation.
ADDITIONAL	**DESCRIPTION**
Additional Modules	Your sponsorship comes with 1 module, for each additional module the sponsorship price is $5,000
Badge ($3,000)	Sponsorship of event badges, which are worn by all attendees. Your company's logo will be prominently displayed on the badges, providing continuous visibility throughout the event.
Lanyard ($3,000)	Sponsorship of lanyards used to hold attendee badges. Your company's branding will be featured on the lanyards, ensuring that your logo is visible throughout the event.
Breakfast ($2,000) or Lunch ($2,000)	Sponsorship of the breakfast session, providing an opportunity to have your branding featured during the morning meal.
Speakers Lounge ($3,000)	Sponsorship of the lounge area designated for speakers. This exclusive space will prominently feature your company's branding and offer a high-visibility spot to interact with industry leaders.

SPONSORSHIP OPPORTUNITY

Brand Exposure: Position your brand prominently before a diverse audience of industry leaders, cybersecurity professionals, policymakers, and tech enthusiasts via gamified purple teaming.

Thought Leadership: Showcase your expertise through expert-led sessions, workshops, panels, and discussions with industry leaders.

Branding Opportunities: Gain visibility through branding placements across event materials, website, and promotional channels.

Recognition: Acknowledgment as a key sponsor in event communications, press releases, and media coverage.

Community Engagement: Support educational institutions and emergency services personnel by contributing to their practical insights and crisis management skills.

Networking Opportunities: Connect virtually with professionals across sectors, fostering valuable relationships and potential partnerships.

WHO WILL ATTEND?

- **Government Officials:** Responsible for critical infrastructure protection, including policymakers, agencies, and representatives.
- **Cybersecurity Professionals:** Experts seeking sector-specific insights and hands-on experience in strategic cyber defence.
- **Industry Leaders:** Executives and decision-makers invested in safeguarding their respective sector.
- **Private Sector Entities:** Companies offering cybersecurity tools & solutions, to enhance national cyber resilience.
- **Tech Enthusiasts:** Individuals with a passion for technology and interest in addressing cybersecurity challenges through innovation.
- **Educational Institutions:** Students & faculty in cybersecurity programs, gaining practical insights and experience in simulated crisis scenarios.
- **Emergency Services Personnel:** Those responsible for managing crises, ensuring coordination and effective responses in the face of cyber threats.
- **International Cybersecurity Collaborators:** Professionals from allied nations, fostering cross-border cooperation and sharing insights on global cyber threats.
- **Media and Communication Professionals:** Reporters and communicators covering cybersecurity, contributing to public awareness and understanding.
- **General Public:** Engaged citizens interested in understanding the impact of cyber threats on national security and critical infrastructure.


National Economic Impact
$ 120,008,800.40
Time Since Breach 4h 18m 37s
MODULE 3
GOVERNMENT SECTOR
OPERATION:
DEFEND THE NORTH
sberX
MODULE 2
HEALTHCARE SECTOR
MODULE 1
FINANCE SECTOR

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2