SPONSORSHIP PROSPECTUS

siberX®

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

DECEMBER 4, 2026.

TORONTO

IN PERSON & DIGITAL

OPERATION: DEFEND THE NORTH
Arlene Worsley
Role: Lead Business Continuity & Resilience
DETECTION & ANALYSIS
CONTAINMENT

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 12th cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place at Toronto, on December 4, 2026, 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
RSM
ARCTIC WOLF
DARKTRACE
immersive
ARMIS
CDW
aws
CROWDSTRIKE
OBSIDIAN
TANIUM
LIMA CHARLIE
Abnormal
CLOUDFLARE
SOPHOS
TREND MICRO
CROWDSTRIKE
TELUS Business
OPTIV
Bitdefender
SecuredNet
corelight
splunk> a CISCO company
paloalto NETWORKS

PAST PARTNERS

CYBER SECURITY CENTRE OF EXCELLENCE
Ontario
BSIDES OTTAWA
AFCEA
CYBERSEC
ISACA Vancouver Chapter
ISC2 CHAPTER ALBERTA
Women in Cybersecurity WiCyS WESTERN CANADA AFFILIATE
ISACA Calgary Chapter

siberX

OPERATION: DEFEND THE NORTH

PAST ADVISORY BOARD

ALEX DOW
siberX

ALI ABBAS HIRJI
siberX

DR.HADIS KARIMIPOUR
University of Calgary

JAMES CAIRNS
Bow Valley College

BILL DUNNION
Mitel

ROB LABBE
MM-ISAC

ARLENE WORSLEY
Teck Resources

CHERIE BURGETT
Mining and Metals ISAC

OCTAVIA HOWELL
Equifax

RICHARD HENDERSON
Alberta Health Services

SHELLEY WARK-MARTYN
Sans

DHANUSH LIYANAGE
Ontario Health

ANTON KAISER
PaybyPhone

HARDEEP MEHROTARA
Concert Properties

VIVEK KHINDRIA
Risk Embrace INC

AMIT CHOPRA
Lakefield College School

JARETT PARENT
BSides Ottawa

GEORGE AL_KOURA
Ruby

JF PROVOST
Malvik Security

KEVIN PARENT
Orion

SHRUTI MUKHERJEE
GlobalVision

LIONEL AKAGAH

ALI SHAHIDI

EMERSON RAJARAM
Wellington-Dufferin-Guelph Public Health

BOB GORDON
Canadian Cyber Threat Exchange

SUZIE SMIBERT
Restiv

VARUN WADHWA
Deloitte

KRIS E
RCMP

KRISTI HONEY
Township of Uxbridge

MANAS KHANNA
Veryon

MICHEAL HATRICK
Town of Midland

VAUGHN HAZEN
CN Rail

MIRZA BAIG
MPAC

JASON LEAKE
Toyota

OSMAN SALEEM
Greater Toronto Airports Authority

NILESH SHASTRI
Canadian Institute of Health Information

SHAKEEL SAGARWALA
Canadian Tire Bank

SHERRY RUMBOLT
Treasury Board of Canada

JASSI KAUR
Bulk Barn

KIM SCHREADER
Telus

TOMMASO LORENZO
Niagara Health

SABINO MARQUEZ
Trustable

JAMES BAYNE
PrivacyWorks

VINAY PURI
Moneris

VIVIENNE SUEN
TD Bank

DANIEL PINSKEY
CDW Canada

GURVINDER GILL
Toronto Parking Authority

JOHN PINARD
DUCA Financial

KELLEY IRWIN
Descartes Systems Group

HANIF JESSANI
Taiga Building Products

DRAGANA PANIC
Mountain Equipment Company

SHILPA DAHIYA
CAAT Pension Plan

TAHER AFRIDI
Marcura

TALHAH MAHMOOD
Moneris

MALEENA SINGH
Mirai Security Inc.

MATTHEW GRUNERT
Bosa Properties

MANDY LIT
Global Enterprises & High-Growth Tech

NEUMANN LIM
Odlum Brown

MARY CARMICHAEL
Momentum Technology

RHONDA BUNN
Town of Midland

ROB MASSE
Lululemon

SONNY SARAI
Brockton Point Solutions

TEODOR PANA
SE Health

TODD KANE
Evolved Management

JONATHAN FRIESEN
Jane App

HUGH BURLEY

LIA SANA
Fraser Health Authority

MICHAEL BUCKLEY
Mark Anthony Group

ROB DAVIDSON
PSB Solutions

TREVOR VERBEKE
Metro Vancouver

EDER MARQUES
Bank of Montreal

PAUL SMITH
Honeywell

ROGER DERY
Rockpoint Gas Storage

KEITH DASER
Deliver Digital

EDGARD RODRIGUEZ
Rogers Communications

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:

- **Date:** December 4, 2026
- **Duration:** 9:00 am - 6:30 pm Exercise and Networking
- **Location:** Toronto
- **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

<table>
<tr><th colspan="5">December 4, 2026 | 9:15 AM - 10:25 AM</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th></tr>
<tr>
<td><b>MODULE 1:</b>
<b>Detection and Analysis</b>
<b>3 SPOTS REMAINING</b></td>
<td>The opening moments of a cyber crisis matter most. In this module, participants step into the high-stakes world of early warning, where every alert and anomaly could be the difference between swift containment and widespread disruption. Learn how leading organizations sharpen visibility, validate signals, and cut through noise to act fast when seconds count.</td>
<td>• 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.</td>
<td>CIS Control Focus:
CIS Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs;
CIS Control 17 - Incident Response and Management.</td>
<td>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.</td>
</tr>
</table>

<table>
<tr><th colspan="5">December 4, 2026 | 10:55 AM - 12:05 PM</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th></tr>
<tr>
<td><b>MODULE 2:</b>
<b>Containment</b>
<b>3 SPOTS REMAINING</b></td>
<td>Once a threat is identified, the real challenge begins: keeping it from spreading. This module explores the strategies, decision-making, and collaboration required to draw effective boundaries under pressure. Participants will experience how coordinated containment buys time, protects critical assets, and sets the stage for a successful response.</td>
<td>• 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.</td>
<td>CIS Control Focus:
CIS Control 4 - Controlled Use of Administrative Privileges;
CIS Control 13 - Data Protection.</td>
<td>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.</td>
</tr>
</table>

MODULE & SPONSORSHIP OPPORTUNITIES

December 4, 2026 | 1:05 PM - 2:15 PM				
MODULE 3: **Eradication** **3 SPOTS REMAINING**	Cyber threats don't vanish on their own — they have to be driven out. Eradication is where technical precision meets organizational resolve. In this module, attendees see how organizations isolate root causes, eliminate malicious footholds, and neutralize adversaries without losing focus on business continuity.	• 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.

December 4, 2026 | 2:45 PM - 3:55 PM				
MODULE 4: **Recovery** **3 SPOTS REMAINING**	Every crisis eventually shifts from survival to restoration. Recovery is where resilience is proven. This module highlights the pathways organizations take to restore operations, rebuild confidence, and return stronger than before. Attendees will discover how effective recovery isn't just about systems — it's about trust, reputation, and continuity.	• 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.

MODULE & SPONSORSHIP OPPORTUNITIES

December 4, 2026 | 4:10 PM - 5:10 PM				
MODULE 5: **Lesson Learned** **3 SPOTS REMAINING**	A cyber incident doesn't end when systems are back online — it ends when the lessons are captured. This final module closes the loop, showing how organizations transform crisis experience into lasting advantage. From refining playbooks to building culture, participants will leave with practical insights they can bring back to their teams immediately.	• 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.

```
                 drop systemd[1078]: Reached target Exit the Session.
Dec  3 13:22:02 filedrop systemd[1]: Started Session 6 of User ubuntu.
Dec  3 13:22:19 filedrop systemd[1]: Started Session 8 of User ubuntu.
Dec  3 13:22:23 filedrop systemd[1]: Started Session 9 of User root.
Dec  3 13:22:30 filedrop systemd[1173]: Finished Exit the Session.
Dec  3 13:22:30 filedrop systemd[1173]: Reached target Exit the Session.
Dec  3 13:22:40 filedrop systemd[1366]: Finished Exit the Session.
Dec  3 13:22:40 filedrop systemd[1366]: Reached target Exit the Session.
Dec  3 13:22:46 filedrop systemd[1]: Started Session 11 of User ubuntu.
Dec  3 17:50:33 filedrop systemd[1]: Started Session 17 of User root.
Dec  3 17:50:34 filedrop systemd[1434]: Finished Exit the Session.
Dec  3 17:50:34 filedrop systemd[1434]: Reached target Exit the Session.
Dec  3 17:50:35 filedrop systemd[1]: Started Session 19 of User root.
Dec  3 17:50:37 filedrop systemd[1]: Started Session 20 of User root.
Dec  3 17:50:39 filedrop systemd[1]: Started Session 21 of User root.
Dec  3 17:50:40 filedrop systemd[1]: Started Session 22 of User root.
Dec  3 17:50:43 filedrop systemd[1]: Started Session 23 of User ubuntu.
Dec  3 17:50:51 filedrop systemd[1661]: Finished Exit the Session.
Dec  3 17:50:51 filedrop systemd[1661]: Reached target Exit the Session.
ubuntu@filedrop: $
```

MODULE 3
GOVERNMENT SECTOR
n across Canada gather to simulate and defend against a large-scale cyber attack. - Participants are engaging in real-time decision-making and response strateg
OPERATION: DEFEND THE NORTH
siberX
LIVE CALGARY
Arlene Worsley
experts from across Canada gather to simulate and defend
DETECTION & ANALYSIS
CONTAINMENT
MODULE 3
GOVERNMENT SEC
k scenarios and cross-sec
siberX
OPERATION: DEFEND THE NORTH
siberX
OPERATION: DEFEND THE NORTH
siberX
OPERATION: DEFEND THE NORTH
OPERATION: DEFEND THE NORTH
$1,203,656,926.26
LEAD ENGINEER - SIBERX
LIVE CALGARY
siberX
OPERATION: DEFEND THE NORTH
llaboration.
Follow live updates and insights at live.siberx.org or download
ERADICATION
RECOVERY
LESSONS LEARNED

Adam Singh

I need to get my father's medications - I do not have cash, ATMs are down & my father is very ill. I need help! I don't have cash - I WILL PAY. CHARGE ME WHEN YOUR SYSTEMS ARE WORKING. KEEP MY CARD! OH MY GOD! #dobetter #dogood #peopleoverprofit #help #trudeau

11:31 AM · Dec 04, 2024 · 0 Views

10 Retweets 0 Quotes 25 Likes 0 Bookmarks

MODULE 2
HEALTHCARE SECTOR
g and response strategies to mitigate a simulated breach
CTOR
ess potential threats to infrastructure
OPERATION: DEFEND THE NORTH
siberX
OPERATION: DEFEND THE NORTH
OPERATION: DEFEND THE NORTH

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG
1-888-742-3798
155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2