SPONSORSHIP PROSPECTUS

siberX®

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

OCTOBER 15, 2026 | VANCOUVER

IN PERSON & DIGITAL

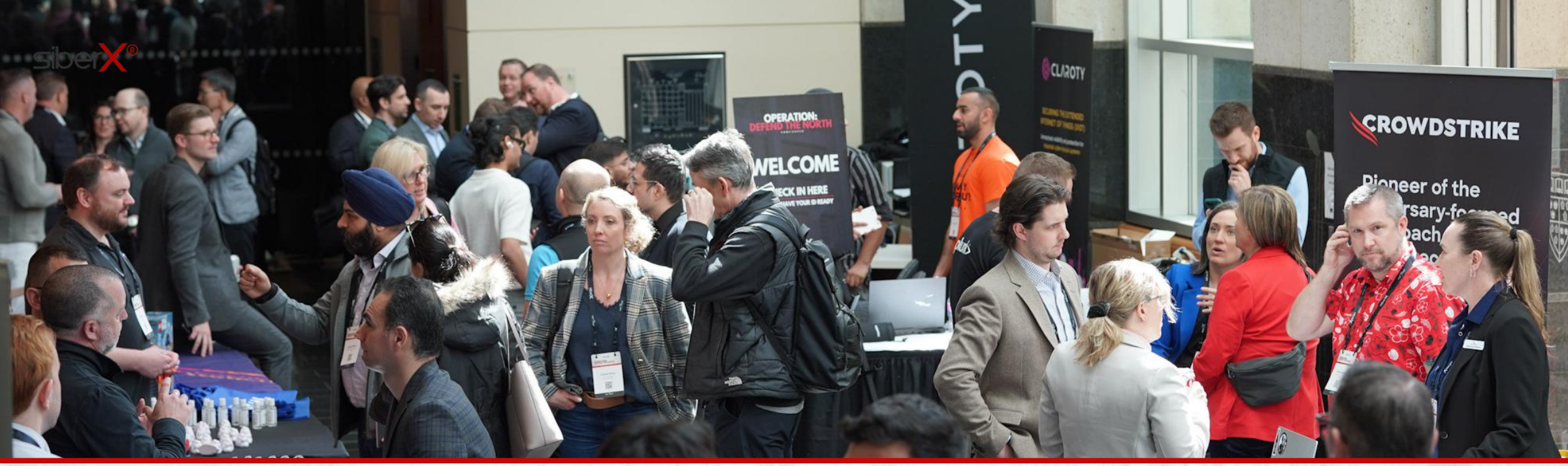
siberX®

siberX is excited to announce its **9th cybersecurity readiness tabletop exercise (TTX)**, Operation: Defend the North 2026. This next-generation, live cyber crisis simulation will take place at the beautiful **Simon Fraser University** in the beautiful, **Vancouver, Canada** on **October 15th, 2026,** designed to strengthen Canada's cybersecurity readiness, executive decision-making, and real-time response strategies.

This year, ODTN moves beyond a traditional discussion-based exercise. While the scenario remain fictitious, the leaders in the room are not. Senior executives, technical experts, and public and private sector stakeholders will step into the simulation as themselves, playing their real-world roles in real time. The experience unfolds across three integrated streams; Executive Crisis Command, a live Technical Response Stream, and Live crisis coverage reflecting how modern cyber incidents evolve simultaneously across operational, strategic, and public domains.

Participants will manage an active cyber incident and breach in real time, collaborating with leaders from across Canada as technical teams detect and contain threats, executives navigate regulatory and reputational pressure, and live news coverage shapes public perception. The result is an immersive, high-pressure national cyber crisis experience that demonstrates how executive decision-making, technical response, and public narrative collide and what it takes to lead effectively when they do.

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, Zimperium, Telus Business, Optiv, Bitdefender, SecuredNet, corelight, splunk> a Cisco company, paloalto networks, Wiz, TrendAI, Google Cloud, kaspersky, CyberArk The Identity Security Company, Claroty

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, Bow Valley College, Operation: Defend the North

siberX®

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
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
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
TALHAH MAHMOOD Moneris
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
KIM SCHREADER Telus
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
VARUN WADHWA Deloitte
TOMMASO LORENZO Niagara Health
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
MALEENA SINGH Mirai Security Inc.
HARDEEP MEHROTARA Concert Properties
LIA SANA Fraser Health Authority
TAHER AFRIDI Marcura
FERRIS ADI Trans America Fiber System
TJ ODUGBESAN TechniRise
ANTON KAISER PaybyPhone
MICHAEL BUCKLEY Mark Anthony Group

siberX®

Event Overview:

- **Date:** October 15th, 2026.
- **Duration:** 9:00 am - 5:00 pm Exercise and Networking
- **Location:** Simon Fraser University (SFU)
- **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 participate in coverage (Globe & Mail, Toronto Star, Technology Media)
- **DIGNITARIES:** Minister of Public and Business Service Delivery, CIO & CISO Provinces, MPs Mayors, and Councillors invited to open and participate.

siberX®

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.
- **The Hands-On Technical Zone:** While Executive Crisis Command focuses on strategic leadership decisions, SiberX TechTavern brings the technical layer to life. This is applied cyber skill in motion.
- **Live Crisis Coverage:** Adding a new dimension of realism, ODTN 2026 introduces a live news desk.
- **Networking Opportunities:** Connect with professionals across sectors and showcase.

siberX®

Inside Operation Defend the North: 2026

The War Room

Live Executive Crisis Command

As the live crisis escalates, sponsors are positioned alongside senior leaders to provide insight, perspective, and strategic guidance on how incidents are contained, managed, and communicated. This is not a sales pitch — it's executive-level visibility in the moments that matter most.

In front of decision-makers, practitioners, and a national audience, sponsors demonstrate credibility, authority, and real-world expertise under pressure — elevating their brand from vendor to strategic partner.

What this Means for you:

The Executive Command Centre features high-level, scenario-driven engagement such as:

- Live executive decision-making during active incident escalation
- Board-level briefings and crisis communications moments
- Strategic trade-off discussions under regulatory and reputational pressure
- Cross-sector coordination and stakeholder management scenarios
- Sponsor-led expert commentary integrated into unfolding injects

The TechTavern

The Hands-On Technical Zone

siberX TechTavern is the practitioner-focused technical arena within Operation: Defend the North 2026. While one stream connects directly to the live simulation, the broader space allows sponsors to build and host their own interactive technical environments.

This is not a booth hall, it's a hands-on zone where cybersecurity professionals engage through applied challenges and tool-driven experiences, giving sponsors the opportunity to demonstrate real capability in action.

What this Means for you:

TechTavern features interactive challenges such as:

- Interactive technical challenge environments
- Hands-on cybersecurity labs and applied skill demonstrations
- Physical security and operational resilience simulations
- Incident response, investigation, and threat analysis scenarios

Live Crisis Coverage

Live News Desk

Insert Your Solution Into the Crisis — Live.

A parallel news desk that runs alongside the national cyber simulation, delivering real-time analysis, expert commentary, and sponsor-led insight as the incident unfolds.

Streamed directly into the Executive War Room and online audience, this is not passive coverage — it's a live insertion point where sponsors step into the broadcast to demonstrate how their solution performs under pressure, in the exact moment clarity and action matter most.

What this Means for you:

As the simulation unfolds, ODTN.NEWS delivers:

- Appear live at the ODTN.NEWS desk alongside senior advisors
- Demonstrate product capabilities during specific incident phases
- Show real dashboards, alerts, workflows, and reporting in context
- Explain what visibility your solution provides at that moment in the incident
- Walk through actions enabled for technical teams and executive leadership
- Discuss trade-offs, dependencies, and operational constraints realistically

siberX®

Module 1: Detection and Analysis

October 15th, 2026 | 9:15 AM - 10:25 AM

2 SPOTS REMAINING

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.

Investigating the breach

Analyze indicators of compromise and determine which systems, networks, or operational components have been targeted or affected.

Vulnerability Identification

Identify compromised systems, controls, or automated components to prevent further disruption and limit the spread of impact.

Secure Communication

Establish and maintain encrypted, trusted communication channels to share sensitive information without increasing exposure or operational risk.

CIS Control Focus:
CIS Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs.
CIS Control 17 - Incident Response and Management.

Sponsor Opportunity: 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.

siberX®

Module 2: Containment

October 15th, 2026 | 10:55 AM - 12:05 PM

2 SPOTS REMAINING

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.

System Isolation

Contain affected systems, preventing the attack from spreading to other critical infrastructure.

Risk Discovery

Identify potential operational, safety, and organizational risks resulting from the incident and prioritize rapid mitigation to reduce impact.

Mitigation Strategies

Implement immediate recovery actions to restore essential services while safeguarding operational stability and public safety.

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.

siberX®

Module 3: Eradication

October 15th, 2026 | 1:05 PM - 2:15 PM

2 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

Eliminate malicious code, unauthorized access mechanisms, and persistence methods to restore system integrity and ensure the environment is secure.

Restoring Operations

Restore critical systems and operational processes while continuously monitoring for residual threats or signs of reinfection.

Re-establishing Trust

Demonstrate transparent and effective recovery efforts to rebuild stakeholder confidence and reinforce trust in essential services.

CIS Control Focus:

CIS Control 8 - Malware Defences.

CIS Control 10 - Data Recovery.

Sponsor Opportunity: Sponsors providing threat eradication, remediation, and recovery technologies play a critical role in restoring operations, strengthening infrastructure resilience, and helping organizations securely move from containment to long-term stability.

siberX®

Module 4: Recovery

October 15th, 2026 | 2:45 PM - 3:55 PM

2 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 full operational capacity and strengthen defences against future incidents.

Crisis Management

Coordinate clear, timely communications with stakeholders and authorities to support stabilization efforts and reinforce public trust.

CIS Control Focus:

CIS Control 17 - Incident Response and Management.

CIS Control 11 - Secure Configuration for Hardware and Software.

Sponsor Opportunity: Sponsors specializing in disaster recovery, crisis management and secure communications solutions will enhance the effectiveness of response teams and help mitigate future risks.

siberX®

Module 5: Lessons Learned

October 15th, 2026 | 4:10 PM - 5:00 PM

2 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.

Sponsor Opportunity: 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.

siberX®

Sponsorship Package

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

Included

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.

siberX®

Additional Sponsorship Opportunities

Breakfast ($1,000) or Lunch ($1,000)

Sponsorship of the breakfast session, providing an opportunity to have your branding featured during the morning/afternoon meal.

Badge ($2,000)

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 ($2,000)

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.

Live News Coverage on Product ($5,000)

Advertise your tool/product on the stage during our live news broadcasts. Swoop in as the saviour of a module.

Included:
CASL Compliance List of all Attendees
Session Recording

Speakers Lounge ($2,000)

Sponsorship of the lounge area designated for executive speakers. This exclusive space will prominently feature your company's branding and offer a high-visibility spot to interact with industry leaders.

The Tech Tavern ($5,000)

Sponsorship of the siberX TechTavern Zone provides a high-visibility technical presence, allowing your organization to host hands-on experiences, demonstrate real capability, and engage directly with cybersecurity practitioners.

Included:
CASL Compliance List of all Attendees

Why Sponsor?

- **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.

Alex Dow
Chair
Operation Defend The North

Rob Lahlar
Chief Operating Officer

Octavia Howell
Communications Manager

Rajul Khurab
Director of Cyber Resilience & Business Continuity

OPERATION:
DEFEND THE NORTH
WELCOME

Global Leader
Cybersecurity

siberX®

Will YOU Defend the North?

Visit **siberx.org/defendthenorth**

Contact Us

SALES@SIBERX.ORG

1-888-742-3798

Location

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2

OPERATION:
DEFEND THE NORTH