

CYBERSECURITY THINK TANK

GenAI Security

May 28-29, 2025 | Four Seasons Hotel Toronto Ontario, Canada.

About The Cybersecurity Think Tank

WHERE VISION MEETS PURPOSE

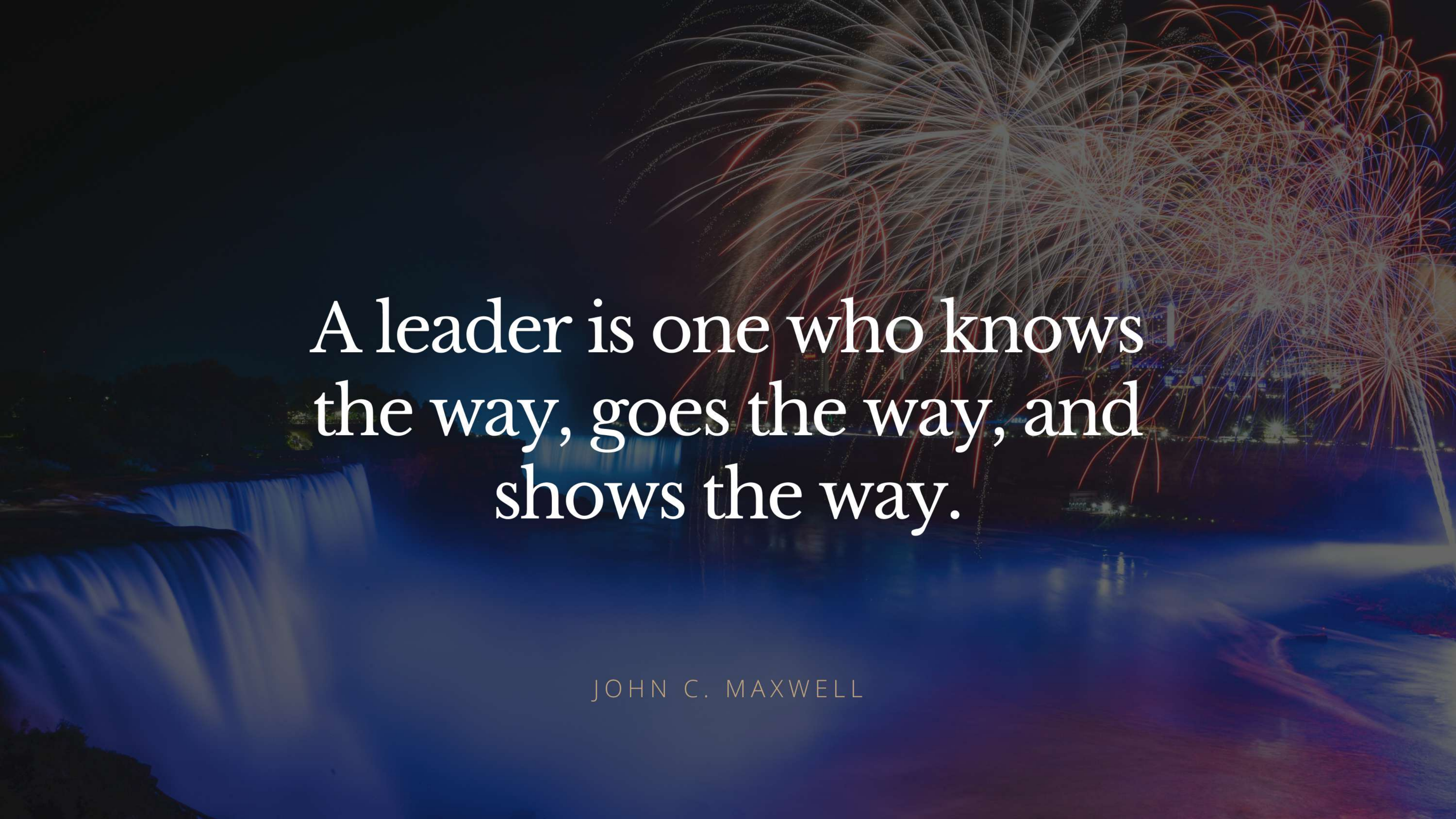
At the core of the mission is the cultivation of transformative dialogue and collaboration. We curate and host exclusive, invitation-only environment that bring together the most distinguished leaders and visionaries across industries. These specialized forums serve as a sanctuary for thought leaders to exchange insights, challenge assumptions, and foster continuous growth in an environment of trust and openness.

While our experts are regular keynote speakers at premier global conferences, they seek our forums for something unparalleled: candid, in-depth debates, innovative ideation, and the opportunity to shape the future through collective intelligence.

Our commitment is to create spaces where excellence meets opportunity, inspiring impactful conversations and equipping leaders with the knowledge and connections to drive meaningful change in their fields. This is where the art of possibility turns into action.

May 28-29, 2025 | Four Seasons Hotel Toronto Ontario, Canada.





A leader is one who knows
the way, goes the way, and
shows the way.

JOHN C. MAXWELL



DR. ALI DEGHANTANHA

Chair



BEN DAVIES

Steering Committee



DR. PARIYA SHIRANI

Steering Committee



DR. SAHAR RAHMANI

Steering Committee



DR. BENJAMIN FUNG

Steering Committee



DR. NATALIA STAKHANOVA

Steering Committee

Steering Committee

UNPARALLELED BRAND VISIBILITY

Position your organization prominently before senior executives and key decision-makers in a prestigious setting.

THOUGHT LEADERSHIP SPOTLIGHT

Showcase your expertise through moderated panels, exclusive workshops, or keynote sessions.

DIRECT ACCESS TO INFLUENCERS

Build relationships with top-tier leaders and potential clients in an intimate and high-value environment.

BESPOKE BRANDING OPPORTUNITIES

Tailor your presence with customized activations, speaking sessions, and branding touchpoints.

COMPREHENSIVE IMPACT REPORTS

Receive detailed analytics on attendee demographics and engagement to maximize your ROI.

FOCUSED PRODUCT SHOWCASES

Demonstrate your solutions to a receptive and targeted audience in an exclusive setting.

The Value of Participation

WHY ATTEND?

CYBERSECURITY THINK TANK

The Experience

GENAI SECURITY

May 28-29, 2025 | Four Seasons Hotel Toronto Ontario, Canada.

May 28, 2025 | Day 1

8:00 AM - 9:00 AM

Car Service Arrival & Breakfast at Four Seasons Hotel Toronto

9:00 AM - 10:30 AM

Vision Sprint 1:

Threat Intelligence for GenAI

This sprint introduces Generative AI (GenAI) and Large Language Models (LLMs), defining their current use cases and organizational impact. We will explore real-world applications of GenAI while delving into their security threats, including data poisoning and model manipulation. Utilizing the MITRE ATLAS framework, we map AI-specific adversarial tactics and identify key threat vectors. As a result, participants will be empowered to accurately identify and evaluate GenAI vulnerabilities by leveraging the MITRE ATLAS framework, establishing a robust foundation for proactive threat intelligence and enhanced security measures.

10:30 AM - 11:00 AM

Morning Tea & Networking Break

11:00 AM - 12:30 PM

Vision Sprint 2:

LLM Governance & Secure GenAI Development

Focused on establishing robust governance and secure development practices for GenAI, this sprint highlights the importance of organizational structures and AI governance. Participants will engage in managing data inventories, conducting threat modeling, and safeguarding privacy. By prioritizing responsible AI principles such as fairness and explainability, the sprint ensures that GenAI initiatives comply with regulatory requirements and maintain secure lifecycle management. The outcome is a comprehensive understanding that protects GenAI projects from ethical, reputational, and compliance-related risks.

12:30 PM - 1:30 PM

Lunch

1:30 PM - 3:00 PM

Vision Sprint 3:

Beyond Words – GenAI Threats & Deepfake Detection

Dedicated to identifying and mitigating advanced GenAI threats, this sprint focuses on deepfake detection across text, audio, and video mediums. Participants will learn to assess risks such as brand damage from synthetic statements and implement security processes to identify suspicious activities. Practical detection strategies, including anomaly detection and AI-based tools, are emphasized alongside incident response planning. The outcome enhances an organization's capability to detect and respond to deepfake threats, ensuring the integrity of digital communications.

3:00 PM - 3:30 PM

Afternoon Tea & Networking Break

3:30 PM - 4:30 PM

Industry Workshop

Workshop

6:00 PM - 8:00 PM

Fine Dining Dinner & Cocktail Reception

May 29, 2025 | Day 2

8:00 AM - 9:00 AM

Breakfast at Four Seasons Hotel

9:00 AM - 10:30 AM

Vision Sprint 4:
Red Teaming for GenAI

This sprint empowers organizations with advanced red teaming techniques and incident response strategies tailored for GenAI threats. Participants will engage in simulated attacks to identify vulnerabilities like data leakage and prompt injection, utilizing tools such as Confidential AI's DeepEval. The sprint covers response actions, including detection, containment, and recovery, ensuring swift mitigation of security incidents. The outcome strengthens organizational resilience and readiness to handle GenAI-related security challenges effectively.

10:30 AM - 11:00 AM

Morning Tea &
Networking Break

11:00 AM - 12:30 PM

Vision Sprint 5:
Shadow GenAI &
Employee Awareness

Addressing the risks of unauthorized AI usage, this sprint focuses on mitigating the risks of unauthorized AI usage by detecting and addressing Shadow GenAI within organizations. Participants will explore the risk of data breaches, regulatory noncompliance, and operational disruptions caused by unmonitored AI tools. We also explore key strategies, including developing robust governance frameworks, educating employees, and implementing AI monitoring solutions, to mitigate the risk of shadow AI. The sprint concludes with recovery plans for containment and data restoration, ensuring organizations can effectively manage and recover from Shadow GenAI incidents.

12:30 PM - 1:30 PM

Lunch

1:30 PM - 3:00 PM

GenAI Tabletop Exercise:
Morris Worm II

A self-replicating, AI-powered malware rapidly spreads across enterprise systems, manipulating communications, altering AI models, and evading detection. Participants must identify vulnerabilities, contain the threat, and decide whether to deploy AI-driven countermeasures while navigating the ethical and policy implications of AI cyberwarfare.

3:00 PM - 3:30 PM

Afternoon Tea &
Networking Break

3:30 PM - 4:30 PM

Industry Workshop
Workshop

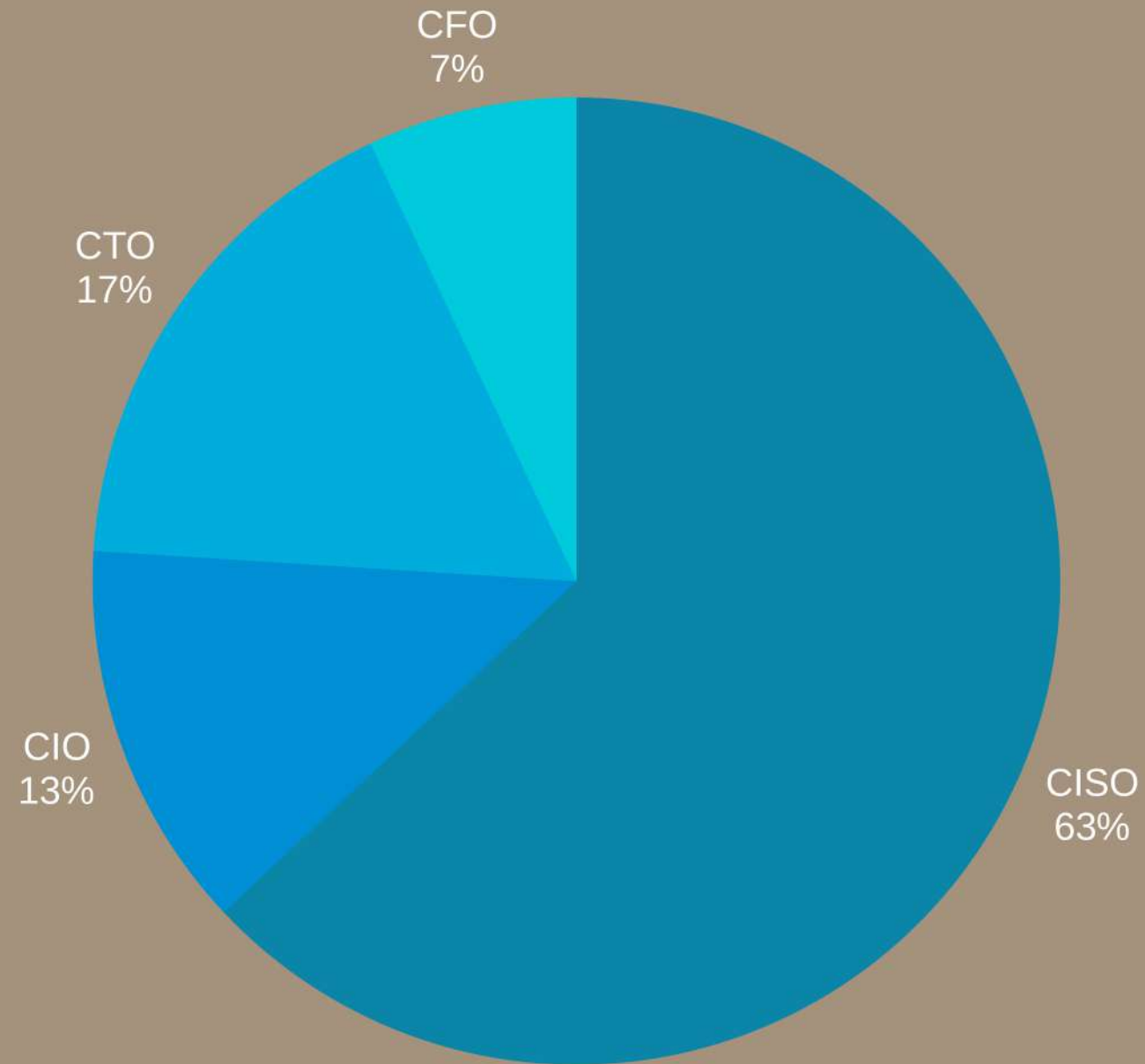
4:30 PM - 6:00 PM

**Closing Remarks & Farewell
Dinner**

6:00 PM

Car Service Pick up from Four
Seasons Hotel Toronto

ATTENDANCE (30 PEOPLE ONLY)



\$20,000

SPONSORSHIP (CAD)

- Industry Workshop hosted by your organization, seamlessly integrated into the event's learning agenda.
- Two full-access tickets to the event, including premium accommodations for your organization's representatives.
- Sponsor Branding featured prominently across all digital platforms, event signage, and marketing materials.
- Post-Event Recognition through recap content, social media, and ongoing brand exposure within our community.
- CASL-Compliant Attendee List delivered within 48 hours of the event for approved follow-up communications.

Contact Information

SIBERX

155 Commerce Valley Dr E
Thornhill, Ontario
L3T 7T2

PHONE NUMBER

416-659-6336

EMAIL ADDRESS

mahdi@siberx.org
