CYBER
carrefour • hub

Contested Cyberspace:
Employing Cyber Ranges for Collective Security and Resiliency

June 16 2023

uOttawa

Guy-Vincent Jourdan

Co-Director of uOttawa-IBM Cyber Range

Full Professor, Faculty of Engineering, uOttawa

Brad Stocking

Associate Partner, Security Services
IBM Security Services, NA

Iosif-Viorel (Vio) Onut

Co-Director of uOttawa-IBM Cyber Range

Senior Manager, R&D Strategy, IBM Advanced Studies

uOttawa
Faculté de génie
Faculty of Engineering

IBM

IBM Security

Cost of a Data Breach Report 2022

Cyber risk is an expensive and time-sensitive threat

277 days

To identify and contain a data breach

-$4.35 m

Global average total cost in 2022

Canada:
2022: $5.64
2021: $5.40
2020: $4.50

Measured in US$ millions

+2.6% YtY

Global average total cost increase of a data breach

$1 Trillion

Annual cost of cybercrime on the global economy

Source: Most of the Cybersecurity experts worldwide (technology, consulting, audit)

Is expected to hit $10.5 trillion by 2025

What is a cyber range?

Military Definition of “Range” - means designated land and water areas set aside, managed, and used to conduct research on, develop, test, and evaluate military munitions and explosives, other ordnance, or weapon systems, or to train military personnel in their use and handling.

The primary purpose of a Cyber Range is to train the offensive capabilities of an organization. Typically, this lends itself to the observations of the offensive actions to study the Tactics, Techniques and Procedures (TTPs) of threat actors or adversaries.

The term “training environment” is an alternative or in addition to Cyber Range to more accurately reflect the target use cases. The military training moto “train as you fight” speaks to the requirement for a realistic training environment.

Cyber Range / Training Environment Use Cases

Use Case 1 – Cyber Operations Team Training

Use Case 2 – Security Capability Research and Development

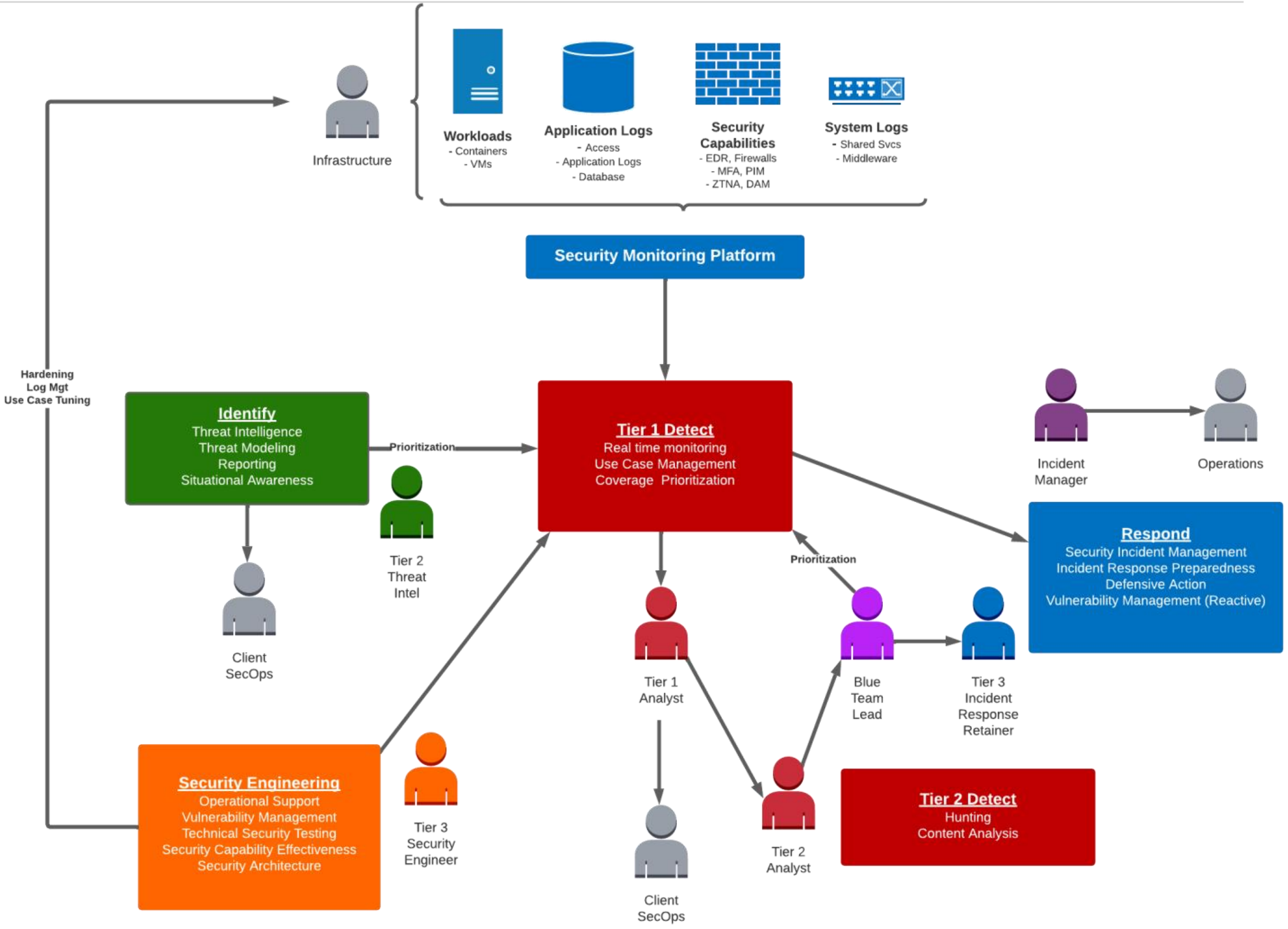
Use Case 3 – Inter-organizational Testing / Collective Training

Use Case 4 – Offensive Technique Research and Execution

Cyber Operations Enablement

Cyber Operations Enablement involves the supporting functions in the development and operations of security capabilities (technology, process, and personnel).

Understanding the operating model and current capabilities of your security organization will help drive training activities.



Cyber Resiliency vs Cyber Security

Cyber resiliency is a complimentary concept to cyber security, which is focused on reactive capabilities and continuity of operations in the face of malicious cyber threat actions.

Cyber Security

Focused on prevention and checklist control requirements

Cyber Resiliency

Focused on adapting to threats and managing their impact

Old Paradigm

- Assumes low probability of a successful attack
- Focused on attack prevention
- Employs a defense-in-depth approach driven by checklist requirements
- Security controls are mostly static
- Focused managing security risks only

New Paradigm

- Assumes high probability of a successful attack
- Focused on management, prevention, response, and exposure recovery
- Threat-driven and adaptive to the changing threat landscape
- Security controls are dynamic and aligned to threat exposure
- Aligns to enterprise risk management
- Emphasizes control validation and continuous improvement

Challenges with advanced cyber training environments

Cost of implementation and maintenance ~ often organizations underestimate the resources require to configure and maintain a cyber range/ training environment

Realistic simulation/stimulation ~ accurate assets and realistic network and user activity to support pen testing and security operations training

Motivation of the primary training audience ~ training will only get you so far. Training audience craves the real thing.

Strategic to Tactical combined training ~ scenarios are often either strategic (executive training) or tactical (operator training)

Challenge 1 ~ Maintenance

The maintenance of a training environment is not trivial. Many organizations overlook the work required to maintain a cyber range.

Infrastructure

- Workload and image maintenance (e.g. VM’s, containers/Kubernetes, registry, etc)
- Networking (e.g. nodes, routing paths, OSPF, BGP, QoS, encryption)
- Enterprise services (e.g. Outlook, ServiceNow, Web Applications)
- Security capabilities (e.g. endpoint protection, Intrusion Detection Systems (IDS), Web Application Firewalls, etc)

Training Services

- Learning Management System
- Forensic evidence/Malware creation
- Logging and monitoring (e.g. post-exercise analysis, real-time adjudication)

Challenge 2 ~ Realistic Training Environment

Depending on the use case applied to the cyber range, the realism of the environment may vary in importance.

There are few key areas that should be consider for a realistic training environment:

1) **Infrastructure and services** – if too rudimentary the networking structure, workloads and services (e.g. Active directory or exchange) will provide limited value
2) **Content**
   a) any content provided should be related to the actual scenario and services
   b) applications and any files/emails/communications require sophistication
3) **User/System Activity** – traffic generation and user activity should be considered when planning a cyber exercise

Challenge 3 ~ Motivation and Analyst Bias

A cyber range is only as fruitful as the engagement with the training audience. Maintaining the level of engagement must be considered when developing a range. Key areas of consideration include:

1) **Consequence** - Without the pressure of real-world stakes, the training value diminishes as the trainees lose interest in the fictional elements.
2) **Analyst Bias** - Analyst bias impacts regular cyber operations (analysts solving problems that and can carry over to the cyber range.
3) **Learning Style** – Each trainee will have styles of education and training that they respond to over others
4) **Gamification** – structuring the cyber range activity as a competition (either individually or collectively) can improve motivation but also leads to poor training outcomes.

Challenge 4 ~ Strategic to Tactical Combined Training

Strategic collective training involves the leadership of an organization that might form a Crisis Management Team during a major cyber incident. This training focuses on the decision-making process, communications, legal review, and inter-agency coordination. These training events may be conducted through tabletop exercises and scenario injects.

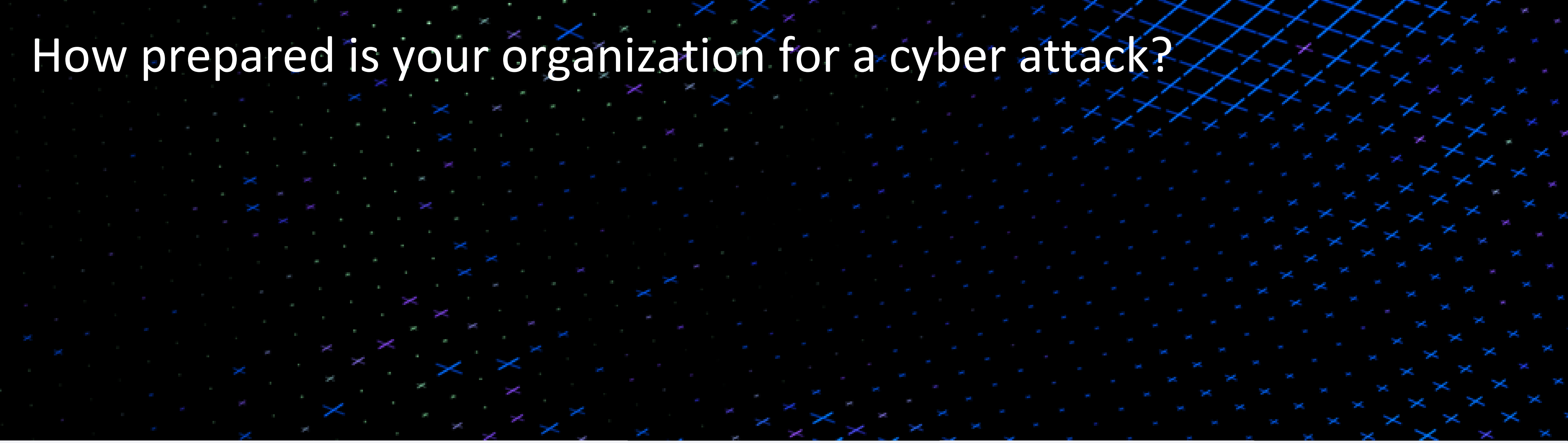
Tactical collective training involves the execution of technical activities to test the ability of the technology and security operations teams to detect, protect, and respond to simulated cyber attacks.

Some major cyber operation exercises have attempted to combine the strategic level training with the tactical level. The complexity of preparation and execution make the multi-level combined training very costly and difficult to meet all training objectives.

IBM Security X-Force Cyber Range:

Prepare your Organization for its Worst Day

How prepared is your organization for a cyber attack?



How does your organization define various incident types, and how it would affect your organization?

How do you update and practice your incident response plan and playbooks?

Are your key stakeholders aware of their roles and responsibilities in the event of a cyber attack?

Does your organization have predefined primary and alternate communication strategies?

How do your existing plans and playbooks integrate distinct business functions beyond IT/IR and enable your organization to communicate and respond in unison?

Benefits of an X-Force Cyber Range

Test a complete business response to a cyber incident

Identify gaps in incident response teams and plans

Show how quick, practiced decisions can help mitigate risk and cost

IBM Cyber Range Experiences

Mind of a Hacker

What it is: A non-technical seminar that provides a demonstration of the types of tools adversaries are using today, a look into the scope of current attacks, and a discussion around how to best protect yourself and your organization

Who it's for: All members of your organization

Business Response Challenge

What it is: A non-technical experience that immerses your team in a simulated cyberattack to test your organization's incident response plan and expose gaps, while learning best practices in a safe environment

Who it's for: Cross-business stakeholders including legal, PR/Comms, HR, Finance, Security, Risk and Compliance - all the way up to board members

Cyber Wargame

What it is: An interactive scenario that demonstrates how technical and business teams should work together; technical participants are tasked with hands-on keyboard exercises to investigate the incident and report back to the business team

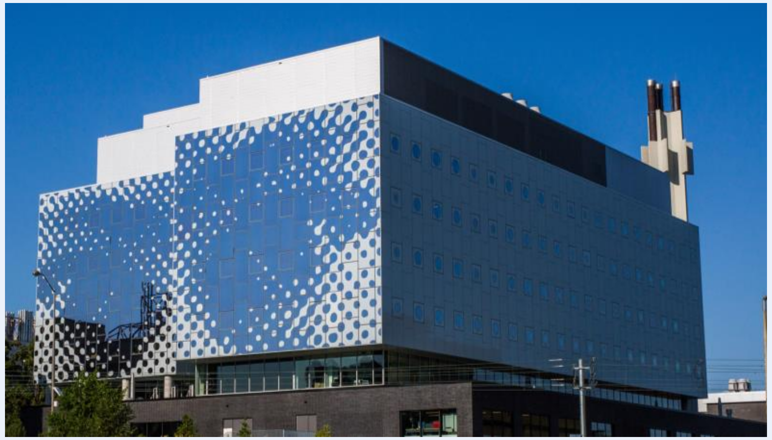
Who it's for: Cross-business stakeholders and technical participants such as SIEM analysts, incident responders, EDR specialists and CSIRT managers

uOttawa is making cybersecurity and cybersafety a priority

We are tackling the growing threat of cyber attacks and cyber crime head on.

uOttawa's Cyber Hub

CYBER carrefour • hub



CYBER carrefour • hub

uOttawa's hub for innovative cybersecurity and cyber safety training and research

Interactive
Innovative
Inclusive
Integrated
Interdisciplinary

- **Functional areas:**
  - **Academic Environment (Teaching and Training)**
  - **Individual and group work areas**
  - **Multi-purpose spaces**
  - **Areas for research and collaboration**
  - **Security operations**
  - **Cyber Range**

- **Surrounded by the highest concentration of tech talent in North America**
- **7 Faculties – disciplines**
  - **Engineering**
  - **Science**
  - **law (civil and common)**
  - **social sciences**
  - **Medicine**
  - **school of management**

uOttawa-IBM

Cyber Range

Enabling learning, training, research, and outreach

uOttawa-IBM

Cyber Range

Facility

- Cyber Range
- Data Center
- Media Room
- Briefing/Staging Room
- Observation Room
- uOttawa SOC

Located in the uOttawa Cyber Hub

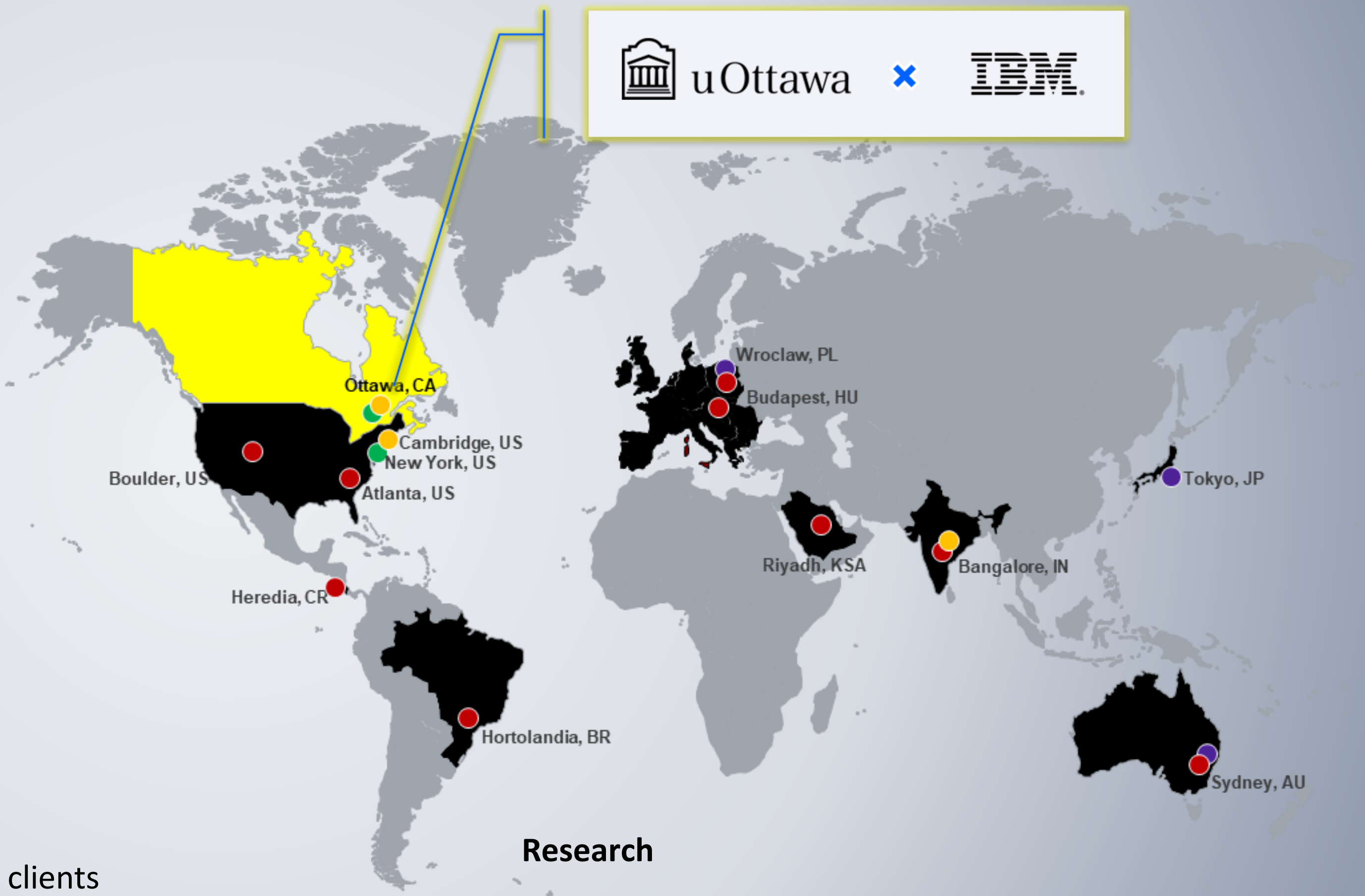
Will deliver security training, interdisciplinary research, professional development and partnering opportunities to help grow Canada's skilled cybersecurity and cybersafety workforce across government, academia and industry.

About IBM Security

Leveraging IBM extended Security & Higher Education teams as needed

Security Operations

- 12 Global and Regional SOCs (Managing Clients SOC operations) monitoring 4.7 trillion events per month from 20,000-plus devices
- Entrusted by Clients for tactical Security Incident Response
- 50 years in security business



Training

- Our Cyber Ranges train 10,500+ clients
- industry's first cyber range for commercial, government, healthcare and academia
- a first-of-its-kind training, simulation and security operations center on wheels

Research

- Threat Prevention, Detection & Investigation
- Threat Response and Recovery
- Security Technology Management & Monitoring

The Cyber Range is multi-year partnership with IBM to create a fully immersive, interactive, and experiential learning facility for research and training in cybersecurity for students, businesses, and government organizations.

IBM

uOttawa

Immersive Learning & Tailored Training

Powered by state-of-the-art technology, integrated within our curriculum and in partnership with companies and government. Real-world scenarios, advanced simulations and an immersive delivery experience.

Interdisciplinary Research

Into new areas of threat defence, analytics, AI security, cyber law, and organizational response.

Community Building

Create the next generation of experts by engaging with youth, uniting the cyber community and by attracting a diverse talent pool.

Interdisciplinary Research

Key National Cyber Research Infrastructure

AI and Cybersecurity

Malware and intrusion detection, anomaly detection, misuse or signature detection, federated learning, security of AI systems.

Cybersecurity of Firmware and IoT

Anomaly detection, cyber-persona identification, IoT security, malicious code, malware analysis, vulnerability detection

Cybercrimes Detection and Prevention

Forensics, zero-victim solutions, scalable protection, frauds and scams detection and prevention, intelligence sharing (APWG eCX, IBM X-Force, IBM Security X-Force Threat Intelligence Index)

AI-based software security testing and analysis

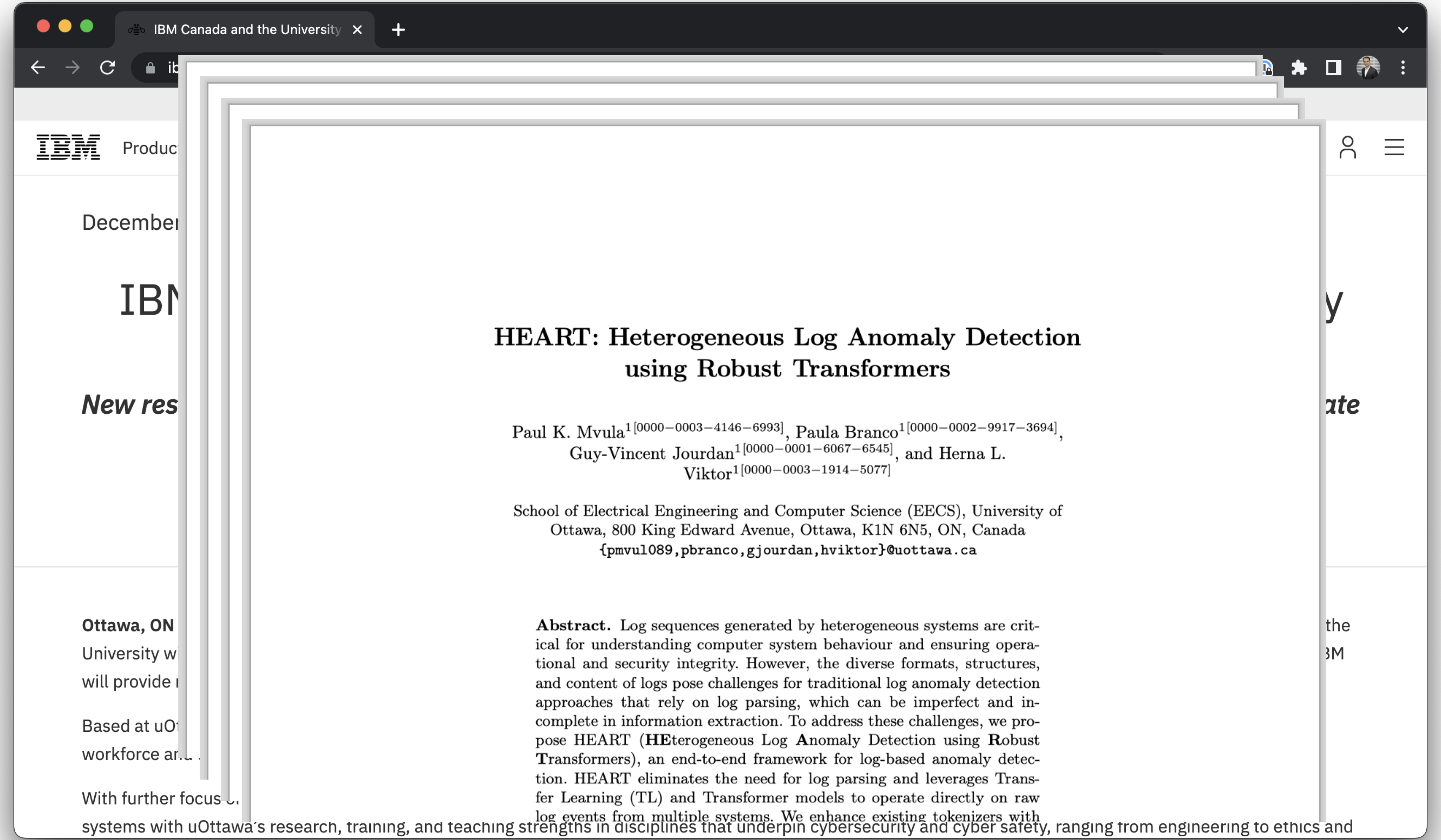
AI-based solutions for automated security testing and analysis of application software

Cryptography and Computer Security Research

Cryptography, network security, computer security, access control, and privacy

Secure Networked Systems

Safe and secure cooperative control strategies for 5G+ networks enabling anticipated and reactive architectures and algorithms for security



HEART: Heterogeneous Log Anomaly Detection using Robust Transformers

Paul K. Mvula[1] [0000−0003−4146−6993], Paula Branco[1] [0000−0002−9917−3694], Guy-Vincent Jourdan[1] [0000−0001−6067−6545], and Herna L. Viktor[1] [0000−0003−1914−5077]

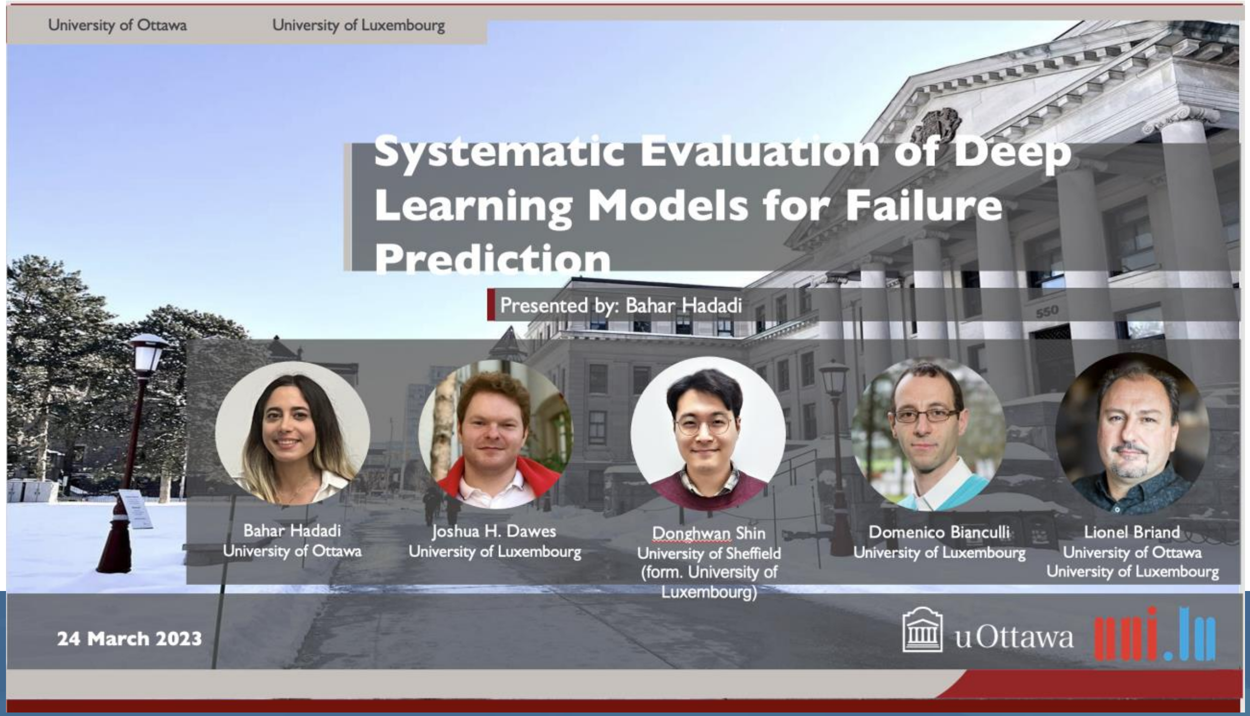
School of Electrical Engineering and Computer Science (EECS), University of Ottawa, 800 King Edward Avenue, Ottawa, K1N 6N5, ON, Canada
{pmvul089,pbranco,gjourdan,hviktor}@uottawa.ca

Abstract. Log sequences generated by heterogeneous systems are critical for understanding computer system behaviour and ensuring operational and security integrity. However, the diverse formats, structures, and content of logs pose challenges for traditional log anomaly detection approaches that rely on log parsing, which can be imperfect and incomplete in information extraction. To address these challenges, we propose HEART (**HE**terogeneous Log **A**nomaly Detection using **R**obust **T**ransformers), an end-to-end framework for log-based anomaly detection. HEART eliminates the need for log parsing and leverages Transfer Learning (TL) and Transformer models to operate directly on raw log events from multiple systems. We enhance existing tokenizers with

systems with uOttawa's research, training, and teaching strengths in disciplines that underpin cybersecurity and cyber safety, ranging from engineering to ethics and

L’Université du Luxembourg et l’Université d’Ottawa créent un programme de recherche conjoint en cybersécurité et en sécurité informatique

Axe de recherche: l'utilisation de l'intelligence artificielle pour améliorer la sécurité, la fiabilité et la disponibilité des systèmes logiciels



University of Ottawa University of Luxembourg

Systematic Evaluation of Deep Learning Models for Failure Prediction

Presented by: Bahar Hadadi

Bahar Hadadi
University of Ottawa

Joshua H. Dawes
University of Luxembourg

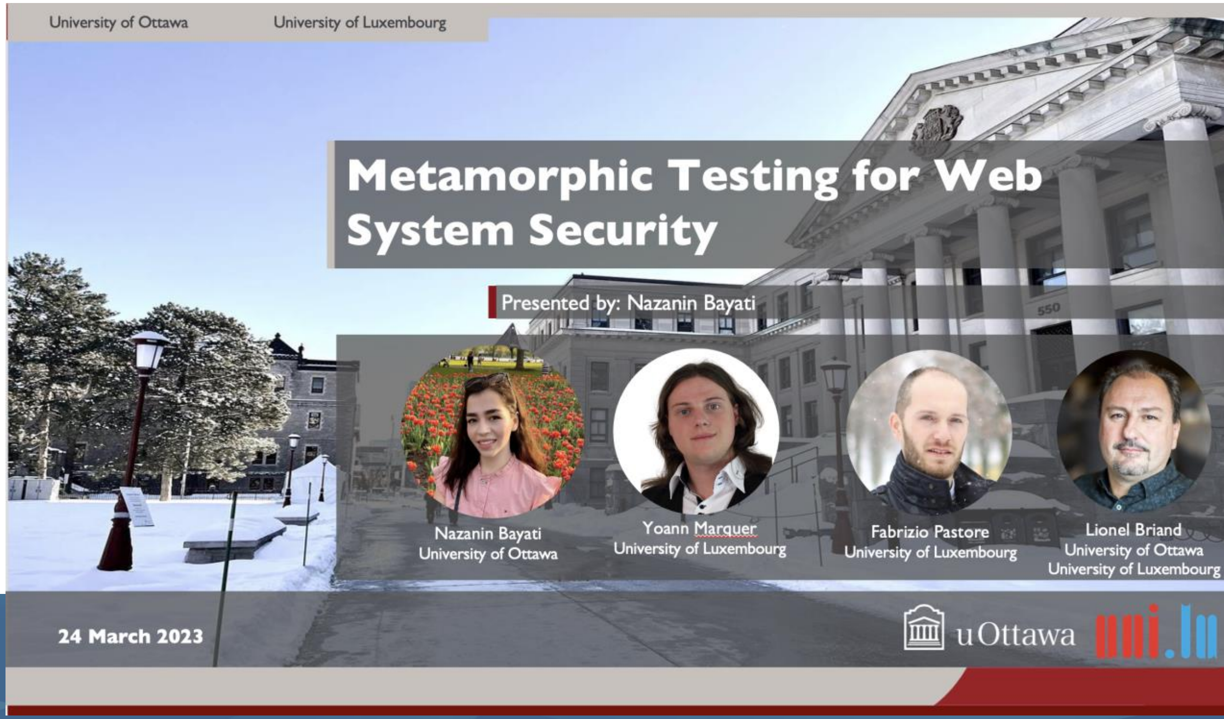
Donghwan Shin
University of Sheffield
(form. University of Luxembourg)

Domenico Bianculli
University of Luxembourg

Lionel Briand
University of Ottawa
University of Luxembourg

24 March 2023

uOttawa uni.lu



University of Ottawa University of Luxembourg

Metamorphic Testing for Web System Security

Presented by: Nazanin Bayati

Nazanin Bayati
University of Ottawa

Yoann Marquer
University of Luxembourg

Fabrizio Pastore
University of Luxembourg

Lionel Briand
University of Ottawa
University of Luxembourg

24 March 2023

uOttawa uni.lu

Human-Centric Cybersecurity Partnership

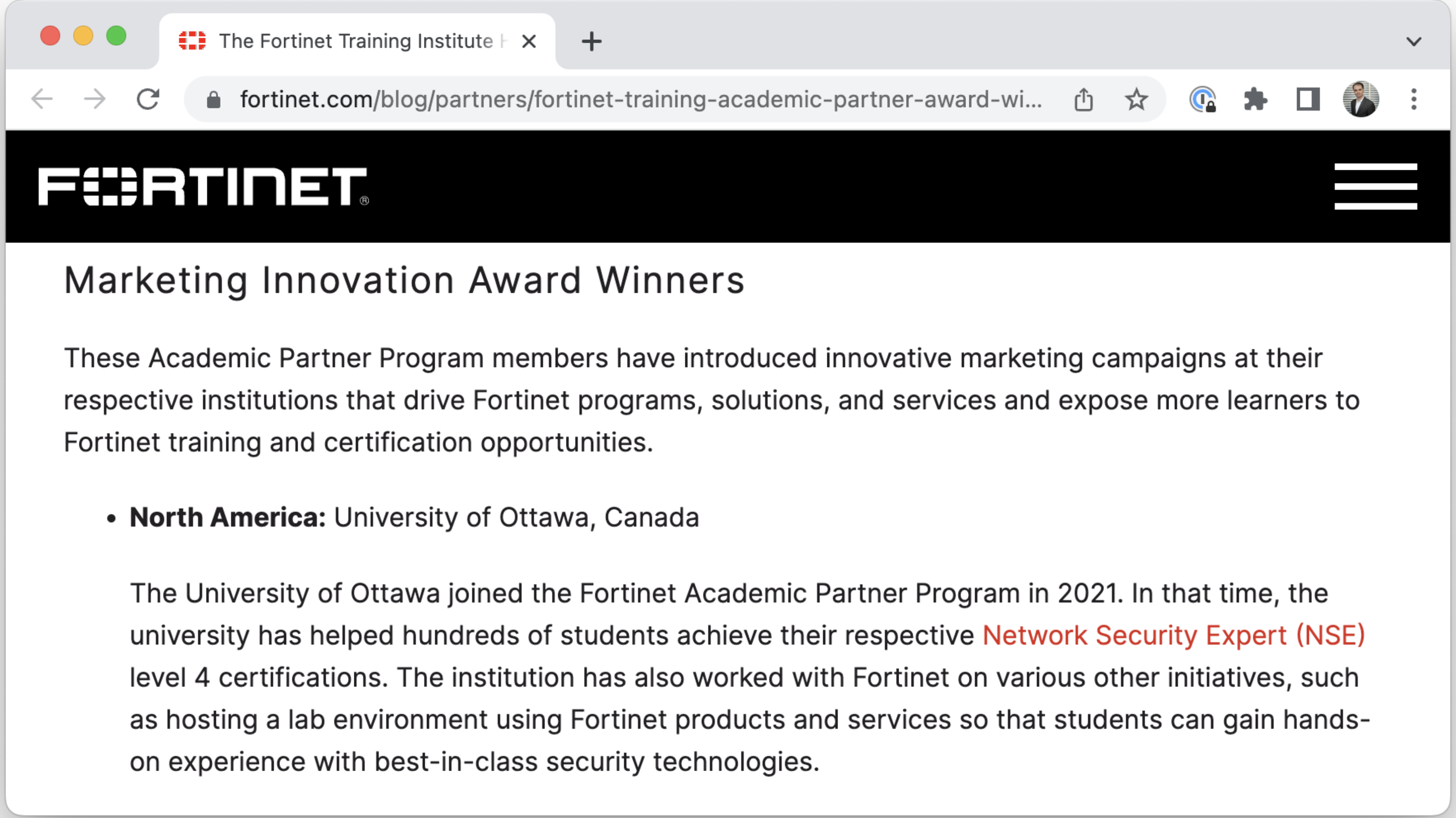
The Human-Centric Cybersecurity Partnership (HC2P) leverages a transdisciplinary group of scholars, government, industry and not-for-profit partners to generate research and mobilize knowledge that will help create a safer, more secure, more democratic and more inclusive digital society.

- 39 academics from the social sciences, law and computer science
- 8 government partners (law enforcement, intelligence, innovation, standards)
- 8 industry partners (banking, telecommunications, IT)
- 7 Not for profits (youth, economic development, information sharing)

Research themes

Society Cluster	
1. Defending democracy (the cybersecurity of elections)	How can the integrity of democratic processes be guaranteed in a context where cyber-threats, from dis-information to faulty technology, are omnipresent?
2. Enhancing cyber-resilience	How can the critical infrastructures that provide the data and energy that sustain modern societies mitigate the impact of cyber-attacks?
3. Adapting democratic institutions	How can democratic institutions adapt to the cyber-risk landscape and generate more timely and agile policies and practices?
4. Supporting evidence-based policies	How can cybersecurity and cybercrime prevention policies that are supported by a strong evidence base be developed and disseminated?
Regulatory Cluster	
5. Protecting privacy	How do the legal and normative frameworks of privacy and cybersecurity interact in the current context and how are these interactions likely to develop as new technologies, such as AI and quantum computing, evolve?
6. Increasing transparency and accountability	What new regulatory tools will be needed to improve the accountability and transparency of the public and private institutions that deliver cybersecurity while not stifling innovation?
7. Standardizing cybersecurity	What role do technical and regulatory standards play in promoting cybersecurity practices and fostering cyber-resilience?
Behavioural Cluster	
8. Disrupting cybercrime networks	How do computer-facilitated communications impact the structure of organized crime networks and what are the implications for law enforcement interventions?
9. Enabling user behaviour change	How can social and behavioural approaches be leveraged to enhance cybersecurity and how can economics and psychology principles be embedded in digital technologies to enable interventions that can be scaled?
10. Designing more usable machines and interfaces	What hardware and software features support more effective decision-making processes by users to reduce cybersecurity risks?

Fortinet Training Institute Honors its 2023 Academic Partner Awards Winners


The Fortinet Training Institute H
fortinet.com/blog/partners/fortinet-training-academic-partner-award-wi...
FORTINET

Marketing Innovation Award Winners

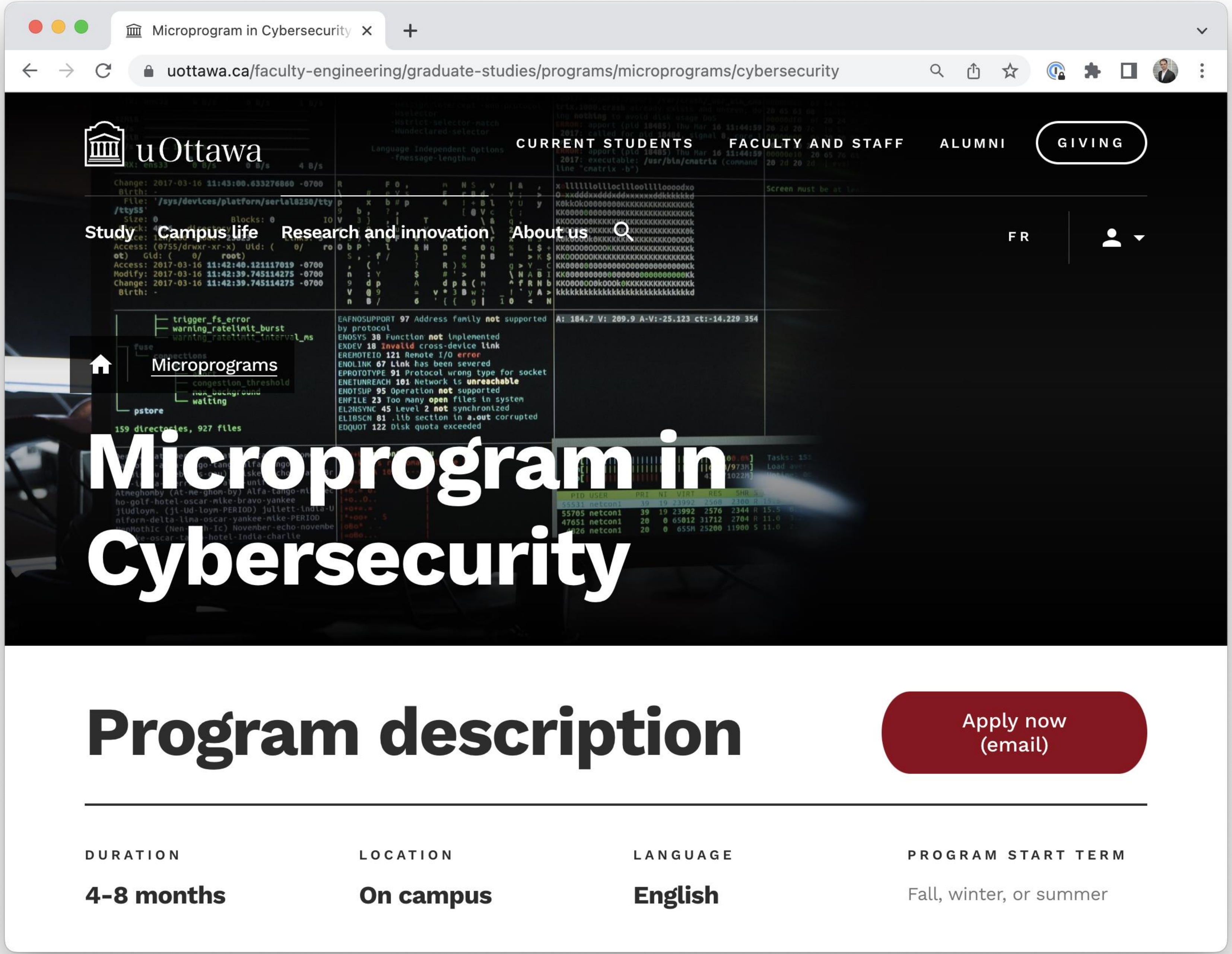
These Academic Partner Program members have introduced innovative marketing campaigns at their respective institutions that drive Fortinet programs, solutions, and services and expose more learners to Fortinet training and certification opportunities.

- **North America:** University of Ottawa, Canada

  The University of Ottawa joined the Fortinet Academic Partner Program in 2021. In that time, the university has helped hundreds of students achieve their respective Network Security Expert (NSE) level 4 certifications. The institution has also worked with Fortinet on various other initiatives, such as hosting a lab environment using Fortinet products and services so that students can gain hands-on experience with best-in-class security technologies.

https://www.fortinet.com/blog/partners/fortinet-training-academic-partner-award-winners

CYBER
carrefour • hub



Microprogram in Cybersecurity

Program description

DURATION	LOCATION	LANGUAGE	PROGRAM START TERM
4-8 months	On campus	English	Fall, winter, or summer

Community Building

- Host events, conferences, seminars, and hackathons to bring together the cyber community.
- Support youth in their journey to build cybersecurity literacy with local outreach programs for kids and teens such as workshops, summer camps, enrichment programs, demos, and more.
- Build international collaborations with other educational institutions to expand the talent pool.
- Support historically underrepresented students with programming, scholarships, and grants to incentivize greater diversity in this field.

Thank You