CyberAlberta – Who we are

Stuart Lee| CISSP, ABCP
Director, Stakeholder Engagement

Cybersecurity Division
Technology & Innovation

Government of Alberta

CYBER ALBERTA

Agenda

- The cyber threat in this highly digital world
- Reminder: Why CyberAlberta?
- Current top-3 challenges

The Cyber Threat
In this highly digital world

Increased Risk

- Organizations are committing to digital services by default
- Services are migrating to the cloud – outside of the network periphery
- Staff are increasingly leveraging mobile solutions
- Vulnerabilities in unsupported legacy products (Cobol, mainframe, etc.)
- Supply chain / 3rd party products vulnerabilities (Log4J, SolarWinds, etc.)

Increased Attacks

- Nation-state sponsored attacks from the big 4 (Russia, China, Iran, North Korea)
- The emergence of Non-Organized and Non-Sponsored Threat Actors
- Ransomware and Ransomware as a Service (RaaS)
- Data breaches cost businesses an average 4.35M in 2022
- Estimated to cost companies 10.5 Trillion USD by 2025

CYBER ALBERTA

In the news…

- Cybersecurity is omnipresent!

Reuters: RCMP Says They Were Targeted by Cyberattack (Feb 23, 2024)

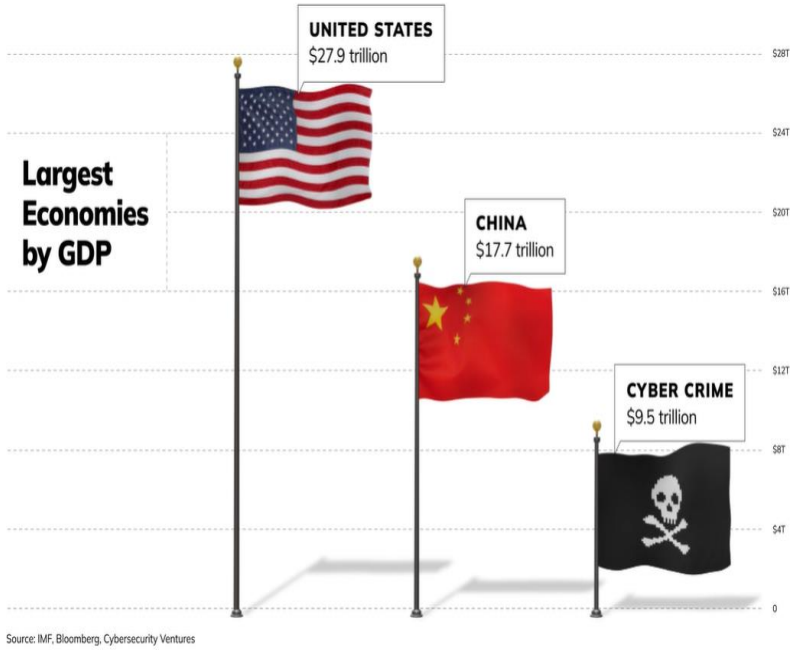
FT: North Korean Hackers Use AI For More Sophisticated Scams (Feb 21, 2024)

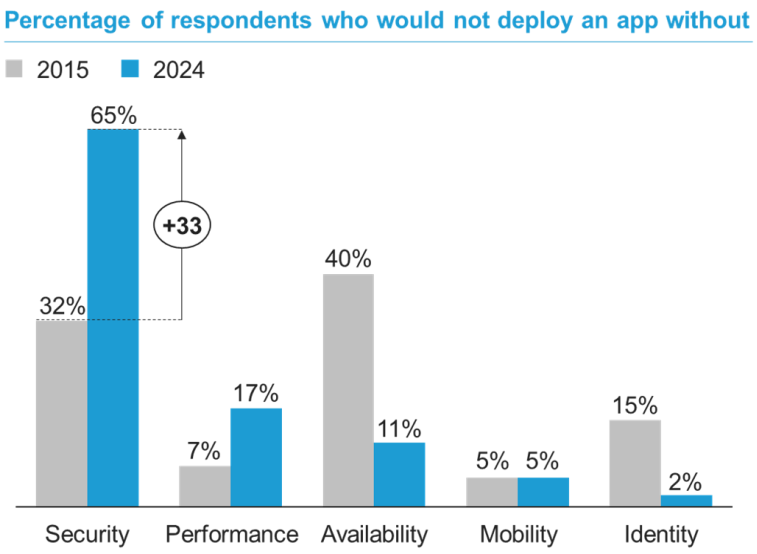
The Hill: A hacking group accessed the database of National Public Data, a background check company (Aug 12, 2024)

CBC: AutoCanada investigating cybersecurity breach , as it announces loss from previous incident (Aug 13, 2024)

WP: 'World's Most Harmful' Cybercriminal Group Disrupted in 11-Nation Operation (Feb 19, 2024)

CBC: City of Hamilton says its phone and email systems have been hit by 'cybersecurity incident' (Feb 26, 2024)





CYBER ALBERTA

The current Cyber Threat

In this highly digital world

There are reasons why attacks are increasing in number and in sophistication:

- Organizations are rapidly expanding attack surface with their commitment to digital services and mobile users
- Weak authentication systems continues to be the main vector into our digital environments
- Vulnerabilities in unsupported legacy products (Cobol, mainframe, etc.) and Supply Chain (Log4J, SolarWind, MOVEit)

The Insiders (unwitty or malicious)

Goal: Accidental or Profit

Method: We gave them access to the assets they need!!!

Nation States / Terrorists / Hacktivists

Goal: Disrupt services or shame organization

Method: Highly organized and sophisticated group hacks.

Cyber Criminals and Spies

Goal: Steal secrets and make a quick profit

Method: Social engineering and systems vulnerabilities

How they get in!

- Social engineering such as **email phishing for credentials**, website **drive by to upload malware and keyloggers.** Put you in a situation where you **don't have time to think**.
- **Legacy** systems vulnerabilities and **third party software** vulnerabilities (e.g., Log4J, TEC Java 1.7 code, MOVEit). Taking advantage of **poor computer hygiene**.
- **Brute force** of weak passwords or authentication (e.g., password crackers, digital trust established between environments). Creating **false accounts** and **increasing privileges**.
- **Application Program Interfaces (API)**. APIs facilitate communication between apps and apps components. Newer, but most effective!!! (e.g., hacking a car via OnStar)

CYBER ALBERTA

Mitigation Strategies

To counter these threats, organizations should adopt comprehensive security measures, including:

- **Robust Authentication and Access Control**: Implement multi-factor authentication and strict access controls to prevent unauthorized access.
- **Advanced Threat Detection**: Use AI-driven threat detection systems to identify and respond to unusual activities and potential intrusions.
- **Regular Security Audits and Penetration Testing**: Continuously assess and test the security of IT/OT systems to identify and mitigate vulnerabilities.
- **Employee Training and Awareness**: Train personnel on recognizing phishing attempts and social engineering tactics to reduce the risk of human error.
- **Network Segmentation**: Isolate critical/OT networks from regular IT networks to limit the spread of malware and other threats.
- **Incident Response Planning**: Develop and regularly update incident response plans to ensure quick and effective action in the event of a security breach.

REMINDER: WHY CYBERALBERTA?

The Importance of a Province-based Community of Interest

The CyberAlberta Community of Interest – led by the GoA Cybersecurity Division and formed with the cybersecurity leads of Alberta-based public and private organizations – is intended to inform and engage Alberta stakeholders and influence matters relating to cybersecurity with the goal of strengthening Alberta's overall cybersecurity resiliency.

- Strengthen Alberta's cybersecurity posture and stand up for Alberta against cyber threats
- Increase confidence in Alberta's critical Infrastructure and ensure the well-being of Albertans and Alberta's economic prosperity
- Create improved cybersecurity culture for Albertans
- Support job diversification and create new employment opportunities

CYBER ALBERTA

TOP-3 CHALLENGES FOR CYBERALBERTA

While CyberAlberta's objectives and scope cover more than the top-3 challenges, we cannot expect to resolve all of cybersecurity for the province overnight!

The top-3 challenges will be the main focus of the Community of Interest over the next year. As progress is achieved, focus may shift, but we recognize that these three challenges are the top ones impacting Alberta's cybersecurity posture.

1. Worldwide cybersecurity talent shortage and difficulties identifying, attracting, and retaining qualified cybersecurity personnel
2. Lack of direction and advice regarding what constitutes a secure environment
3. Inability to quickly onboard critical cybersecurity services in the most dire circumstances while under duress

CYBER ALBERTA

WORLDWIDE CYBERSECURITY TALENT SHORTAGE

Alberta to become a Centre of Excellence for the development of Cybersecurity Talent

- The worldwide cybersecurity workforce shortfall is approximately 3.5 million people, according to Cybersecurity Ventures.
- Alberta has all the ingredients – post secondary institutions, technology, expertise – to help fill the current gap.
- Working collaboratively, the Alberta public and private sector can help the province become a true Centre of Excellence in matters of Cybersecurity.

Spring 2023	Re-training for people with cybersecurity interests, including military and law enforcement professionals
Fall 2024	Work with post secondary institutions to develop a provincial Cybersecurity curriculum that will include work experience programs (coop, internship, apprenticeships, etc.)
Winter 2024	Build a K to 12 “Cyber Safe” program to provide awareness and generate interest in the cybersecurity profession

CYBER ALBERTA

GOA WORK EXPERIENCE PROGRAM

How can we maintain all services in cybersecurity?

- Think outside the box as normal recruitment and retainment was not working
- Become a pipeline where we can train entry-level cybersecurity analysts to become experienced cybersecurity professionals by creating a program that rotates graduates through all cyber domains
- While developing processes to on-board and train, opportunities to improve existing SOPs, playbooks and other processes will happen to make a better service for stakeholders

Spring 2021	Launched 2 year pilot with 4 graduates from MacEwan University (CompSci and Law Enforcement) and NAIT (BAIST program)
Spring 2023	Pilot was successful so expanded to 8 positions. 6 graduates from a recognized Post-Secondary Institution and 2 apprentices participating in SAIT's cybersecurity analyst apprenticeship-style program which is the first in North America.
2024	Participate in NAIT's Industry Immersive Program like SAIT apprenticeship-style program.
2025	Expand the Work Experience Program

CYBER ALBERTA

ESTABLISHING A COMPLIANCE BASELINE

Address the need for direction and ability to compare controls and risks with other similar organizations

- Organizations don't know, and/or cannot demonstrate, their cybersecurity program's strength or weaknesses.
- Cybersecurity teams across the province need a way to compare their programs to similar organizations and quickly identify their weaknesses and strengths to help them plan their improvements.
- A widely adopted compliance model might also assist in better understanding the level of compliance of third parties, helping secure an organization's supply chain.

Fall 2024	Draft Cybersecurity Control Compliance Model that can be evaluated by Alberta-stakeholders and improved over time
Winter 2024	Adapt compliance model based on organization size and/or criticality (e.g., Level A Compliance for a small organization versus Level C for a critical infrastructure controller)
Spring 2025	Maturity-based Cybersecurity Controls Compliance model that can be leveraged by any Alberta-based organization
Fall 2025	Ability to compare results of organizations' compliance assessments with other organizations within same category

ACCESS TO CRITICAL CYBERSECURITY SERVICES

Provide ability to bring in cybersecurity services timely in the event of critical issues

- In the event of critical cyber events such as Ransomware or disasters impacting service delivery, organization need a quick way to access critical support services.
- Alberta stakeholders will get much better agreements by combining their purchasing power, which will also result in much lower costs.
- No single organization can possibly have top-notch expertise in all aspects of cybersecurity services.

Winter 2023	Prioritized list of critical cybersecurity services the GoA could help procure on behalf of the province (pre-qualified vendor list with existing agreements)
Spring 2023	Access to Canada and Alberta specific threat intelligence warning of emergent threats and critical vulnerabilities and providing advice to resolve
Spring 2024	Access to Alberta cybersecurity awareness program including general tips and actual training material
Fall 2024	First set of critical services agreements available to the CyberAlberta Community of Interest

CYBER ALBERTA

RECAP

- Email:

Stuart.Lee@gov.ab.ca

- URL:

www.cyberalberta.ca

1. The CyberAlberta Community of Interest was established with to help strengthen Alberta's cybersecurity posture and stand up for Alberta against cyber threats

2. One of the top priorities of the Community of Interest will be to find a way to develop and attract new cybersecurity talent to fill our own staffing gaps, and create a pipeline of new talent

3. A maturity-based cybersecurity compliance model will be developed and leveraged to help organizations set their own direction to improve their cybersecurity posture

4. Alberta public and private organizations require access to similar if not common critical cybersecurity services in a timely manner – CyberAlberta will work on setting up agreements with service providers to this effect

CYBER ALBERTA

CyberAlberta Work Experience Program (WEP)

Empowering the Future of Cybersecurity Talent

Krysthel Calapardo | November 6, 2024

CYBER ALBERTA

WEP in GOA

A Government of Alberta/CyberAlberta Initiative

WEP Overview

Finding the Right Talent

Bridging the gap between academic studies and demand for professionals

Learning on the Job

Gain experience by rotating through various cybersecurity teams

GOA Tools & Support

Program Tools and Personalized Development Plans

WEP History and Timeline

Oct 2020

Inception

Launched in October 2020 in partnership with Advanced Education and Technology & Innovation

May 2021

Program Launch

Onboarded first cohort with 4 members, Creation of SharePoint, WEP Materials Mentorship Program

Oct 2022 - Apr 2023

Staff Conversion

GOA hired 3 WEP members from original cohort

June 2023

2nd Cohort

Onboarded second cohort with 8 members

Aug 2024

Program Updates

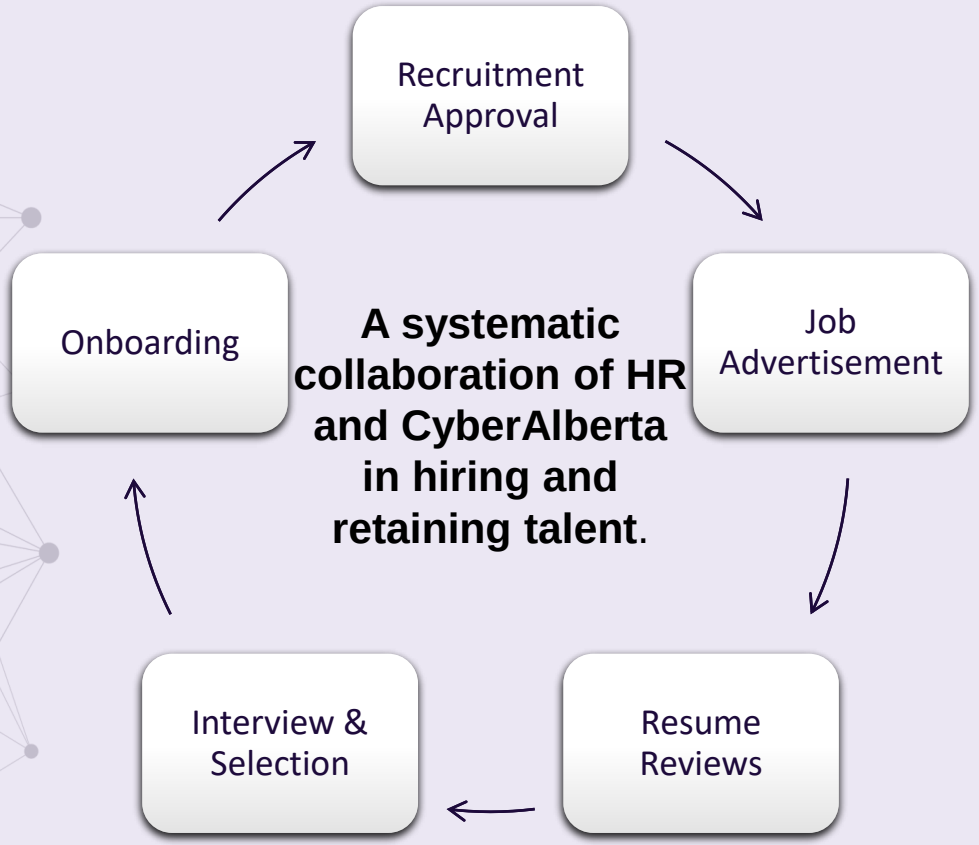
New Tools-Tracker, KPIs, SOPs; GOA hired 2 WEP members from 2nd cohort

PRESENT

Program Expansion

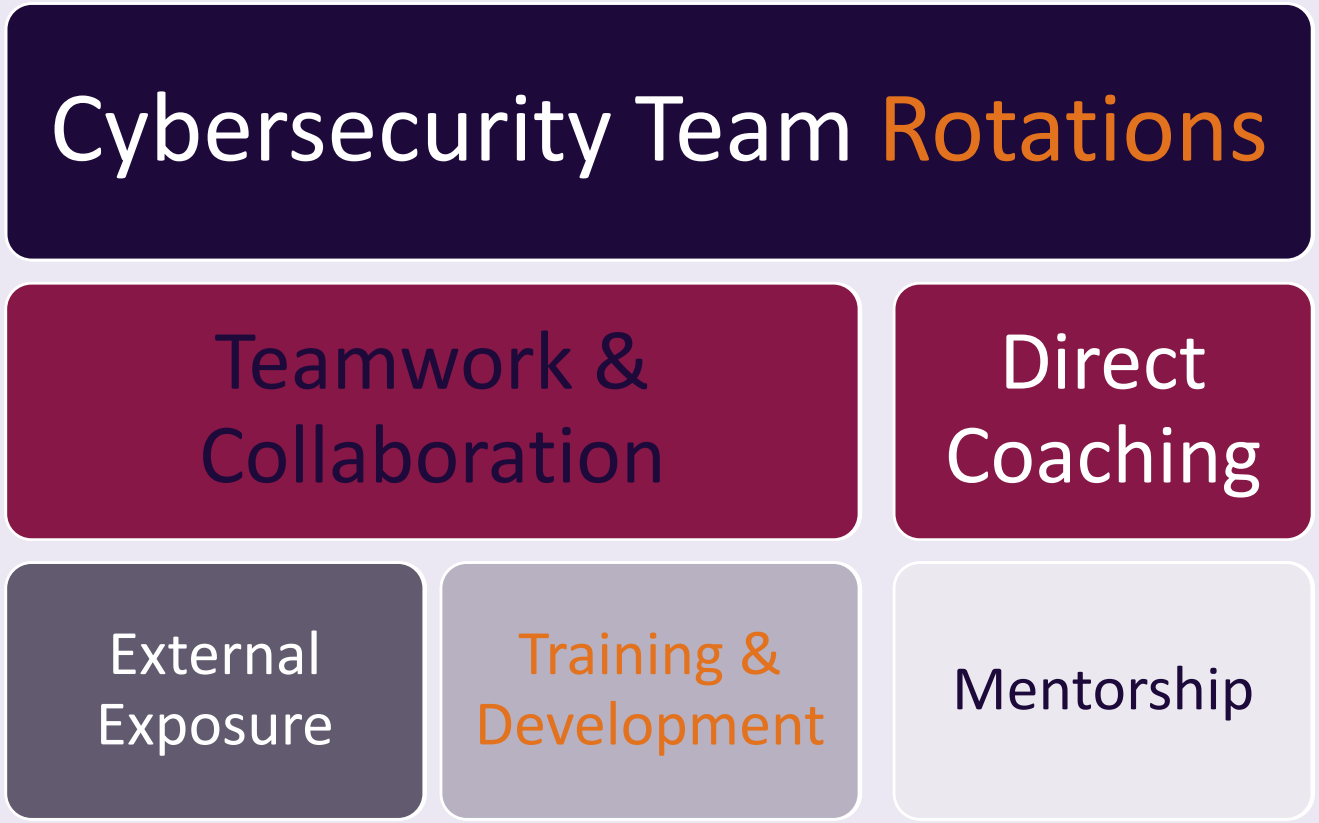
Re-hiring, External outreach

Finding the Right Talent



- Attract and recruit talent interested in hands-on experience in the cybersecurity field. Job posting details and required qualifications.
- Interview process: Panel Interview with 4 members from various teams and levels (WEP, CyberSecurity Domain, Mentorship)
- Hiring selection based on skills, cultural fit, and career goals
- Opportunity: 2 years temporary contract with same GOA benefits
- Provide a seamless transition into GOA and CyberAlberta

Learning on the Job



- Application & Product Security
- CyberAlberta Strategy & Planning
- Cybersecurity Awareness & Training
- Cybersecurity Enablement & Initiatives
- Cybersecurity Governance, Controls, & Compliance
- Cybersecurity Operations
- Digital Forensics
- IT Disaster Recovery
- Risk Management
- Threat Hunting
- Threat Intelligence & Reporting
- Vulnerability & Zero-Trust

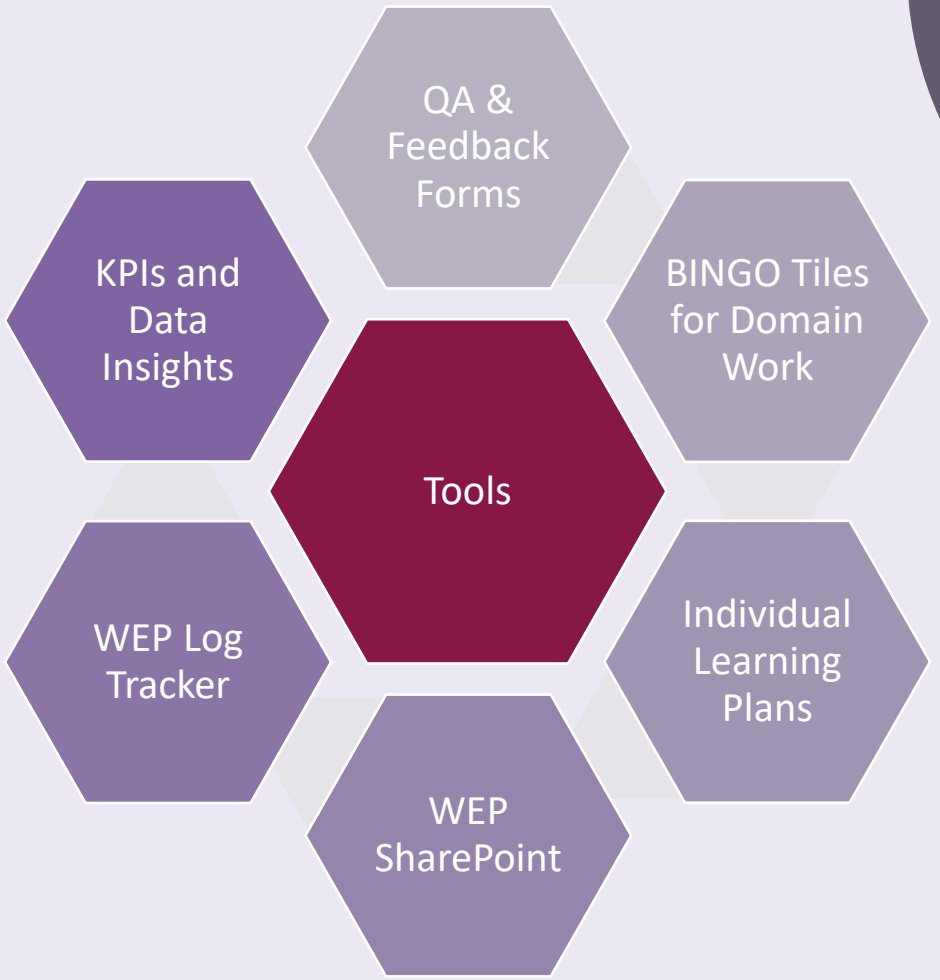
Team Rotation – 8 weeks

- Structured learning through cybersecurity team rotations for 8 weeks
- Each deployment begins with a domain onboarding/meet & greet meeting
- Discuss Bingo Cards, expectations, etc
- Setting up access
- Work Tracker
- Follow-up meetings to assess progress
- Post deployment QA Forms

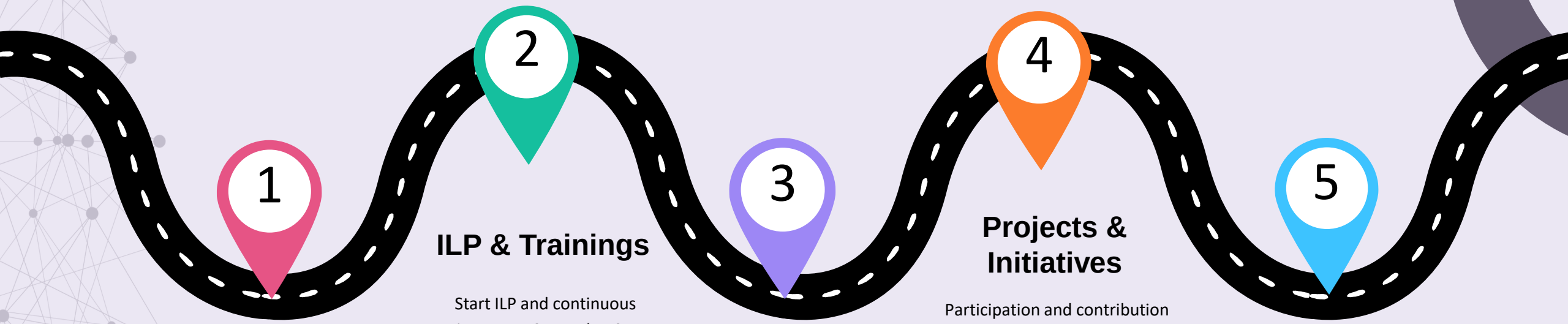
CYBER ALBERTA

GOA Tools & Support

- **Foster accountability** and data-driven insights and feedback
- **Daily tracking** of tasks and projects.
- **Use data to improve the WEP program** through available tools (eg. PowerBI and SharePoint)
- **Customizable program:**
- Vision, goals and capacity
- Program handbook
- Templates
- Workshops



Learning Journey



Meet & Mingle

Meet Supervisor, Mentor, GOA Staff; Participate in Divisional Meetings, Scrums, etc

ILP & Trainings

Start ILP and continuous review every 2 months; Cross-functional business and technical trainings.

On the job experience

Gain hands-on practical experience while being assigned to BAU tasks defined in the Bingo cards

Projects & Initiatives

Participation and contribution to available projects and initiatives when possible

Check-ins & Certifications

Work QA, Performance reviews and Feedback gathering; opportunity for subsidized or sponsored certifications

CYBER ALBERTA

Bingo Card

CYBERSECURITY WORK EXPERIENCE PROGRAM - BINGO CARD

(1) Review the learning outcomes for each Cybersecurity Division functional area. (2) Select outcomes where the learner needs to strengthen knowledge and skills.

No.	Cybersecurity Governance, Risk and Compliance			Cybersecurity Operations			Vulnerability Management & Zero-trust	Application &Product Security	Cybersecurity Enablement	Cyber Alberta	
	IMT Governance, Controls & Compliance	IMT Risk Management	IMT Disaster Recovery & Emergency Management	Incident Management & Security Operations Support	Cyber Threat Hunting (Internal/External)	Digital Forensic Investigation				Cyber Threat Intelligence and Reporting	Cybersecurity Awareness & Training
1	Review IMT policy instruments.	Understand the basic of the Risk Management, process flow and lifecycle model.	Assist in the review and coordination of updates to IMT DR plans, procedures, activities, and tasks.	Hands-on experience with cloud-based platforms and Familiarity with industry-standard tools (e.g. Azure, Defender, Sentinel, Sandbox)	Utilizing various sources to develop threat hunting leads.	Walk through the digital forensic investigation process including acquisition, preservation, review and analysis of evidence associated with various forensic investigation	Produce vulnerabilities reports, trending analytics, and basic analytics.	Understand the concept of DevGeoOps and how it applies to the Government of Alberta. Research or assess application development tools, services, or processes for risk and recommendations.)	Work with stakeholders to understand their cybersecurity needs and advise on appropriate courses of action (i.e., consult)	Conduct research and monitor threat information coming from various sources, includes structured and unstructured data ingestion, to identify threats relevant to the GoA and the broader CyberAlberta	Assist in delivering (or presenting) information security awareness or training materials.
2	Make suggestions for improvements to IMT policy instruments and processes.	Understand the associated the key Risk Management roles and responsibilities.	Assist in the coordination and execution of IMT DR training initiatives and exercises.	Work with and provide direction to support teams (e.g. Major Incident Problmlem Management (MIPM) team) to investigate and mitigate an cybersecurity incident (e.g. Incident Response Process).	Assist in developing hypothesis regarding the threats implicit in the Government of Alberta's environment.	Participate in the creation of, and following of a plan to investigate alleged crime, violation or suspicious activity using appropriate tools necessary for the scope of the investigation.	Participate in on demand scanning and gain exposure/ knowledge of vulnerability scanning tools.	Understand the basics of application security architecture. (i.e. Involvement in application security reviews such as risk assessments e.g. STRAs or SOARs)	Assist in triaging of requests for Cybersecurity service including review and refinement of related processes.	Understand and be able to recognize the different types of cyber threat: Understand an attacker's motivations and capabilities, and the technological and human elements that adversaries require to run a successful operation.	Assist in developing and communicating phishing exercise-related material.
3	Perform and understand process steps designed to complete gap analysis.	Assist stakeholders in the classification of GoA information assets.	Assist in the deployment, coordination, and tracking of IT assets and services in support of Business Continuity and Disaster Recovery events.	Malware analysis involves analyzing malicious software to understand its behavior and how it can be prevented or mitigated.	Assist in analyzing the provided data through various programs and processes. Evaluate information related to attacks, breaches, IT in general and potential targets, and retire obsolete information.	Understand and follow the concept of chain of custody relating to digital media per jurisdictional standards.	Review current processes and procedures related to vulnerability management.	Assist with documenting the requirements, procedures, and protocols of the architecture and systems within the Government of Alberta. (i.e., Cybersecurity will be specifying requirements or controls for the product or project teams to implement. There may be a need to document these as was done for the External User Accounts for the M365 team.)	Manage audit (e.g., OAG, SOC3, PCI) requests requiring Cybersecurity involvement to ensure they are handled in a timely manner.	Intake, triage and route external intelligence for action (reviewed/addressed) by Cybersecurity teams.	Assist in developing, updating, and maintaining existing cybersecurity eCourses.
4	Understand the basics of the RACI (Responsible, Accountable, Consulted, and Informed).	Evaluate inherent and residual risks and identify the causes of these risks.	Assist in performing gap analysis on Disaster Recovery strategy, initiatives, exercise results, etc.	Communicate complex technical information to non-technical stakeholders - Understanding of privacy laws and regulations	Assist in discovering an attacker's tactics, techniques, and procedures. Review identified gaps and exposures to determine the need for additional risk analysis.	Gain an understanding of specialized software and techniques used in forensics to catalogue, document, extract, collect, and preserve digital evidence. Understand hash file analysis and how it is used in the comparison of digital evidence.	Work on ticketing systems and prioritization follow ups.	Work with various stakeholders to understand the security requirements for various projects, applications, products, etc. (i.e., Risk assessment consultation)	Support technology client procurement (e.g., RFP, NRFP, Agreements) initiatives by ensuring appropriate cybersecurity requirements are identified upfront and included in purchasing processes.	Centralize incoming intelligence to reduce duplication of effort, share information to increase visibility of relevant vulnerabilities, keep track of actioned intelligence, and increase team collaboration and communication.	Assist in developing information security articles and bulletins for distribution.
5	Review operations against legislated, regulatory compliance.	Assist in performing information security assessments of information assets.	Assist in developing reports and statistics based on IMT DR data.	Understanding of supply chain risks (e.g. Vendor Support Services)	Inform and enrich automated analytics. Work with other Cybersecurity Division areas to develop mitigations based on intelligence gathered.	Document and report incident findings to the appropriate stakeholders.	Participate in vulnerabilities resolutions meeting and related activities.	Assist with documenting the requirements, procedures, and protocols of the architecture and systems within the Government of Alberta. (i.e., Cybersecurity will be specifying requirements or controls for the product or project teams to implement. There may be a need to document these as was done for the External User Accounts for the M365 team.)	Support in managing the division project portfolio management practice.	'Produce reports for internal and external audiences that assess threats facing the GoA and broader cyber environment, and provide actionable recommendations and best practices to improve their organization's security posture.	Participate in the communication of information security-related advice to business areas.
6	Assist with inquiries, internal reviews, or internal (e.g., CIAS) and external audits (e.g., OAG, PCI, SOC).	Research and investigate risk events and contributing factors.	Assist in updating documentation related to IT Disaster Recovery (standards, best practices, plans, templates, etc.).	Knowledge of identity and access management (IAM)	Document findings to aid in further threat hunting processes.		Collaborate with other vulnerabilities teams/stakeholders on vulnerabilities activities and their resolution.		Collaborate with the Information Management and Privacy teams to understand their processes and services. Emphasize the close working relationship with Cybersecurity.	Ingest data, analyze trends, and report on operations and service metrics to internal stakeholders using clear, concise and accessible language.	Participate in the development of awareness or training material.
7		Review identified gaps and exposures to determine the need for additional risk analysis.	Assist with the testing and continuous improvement of Disaster Recovery processes and tools.		Participate in on demand penetration testing and gain exposure/knowledge of penetration testing tools.		Assist with vulnerabilities request and vulnerabilities reviews.				Assist in the response to ad hoc requests related to training or awareness.

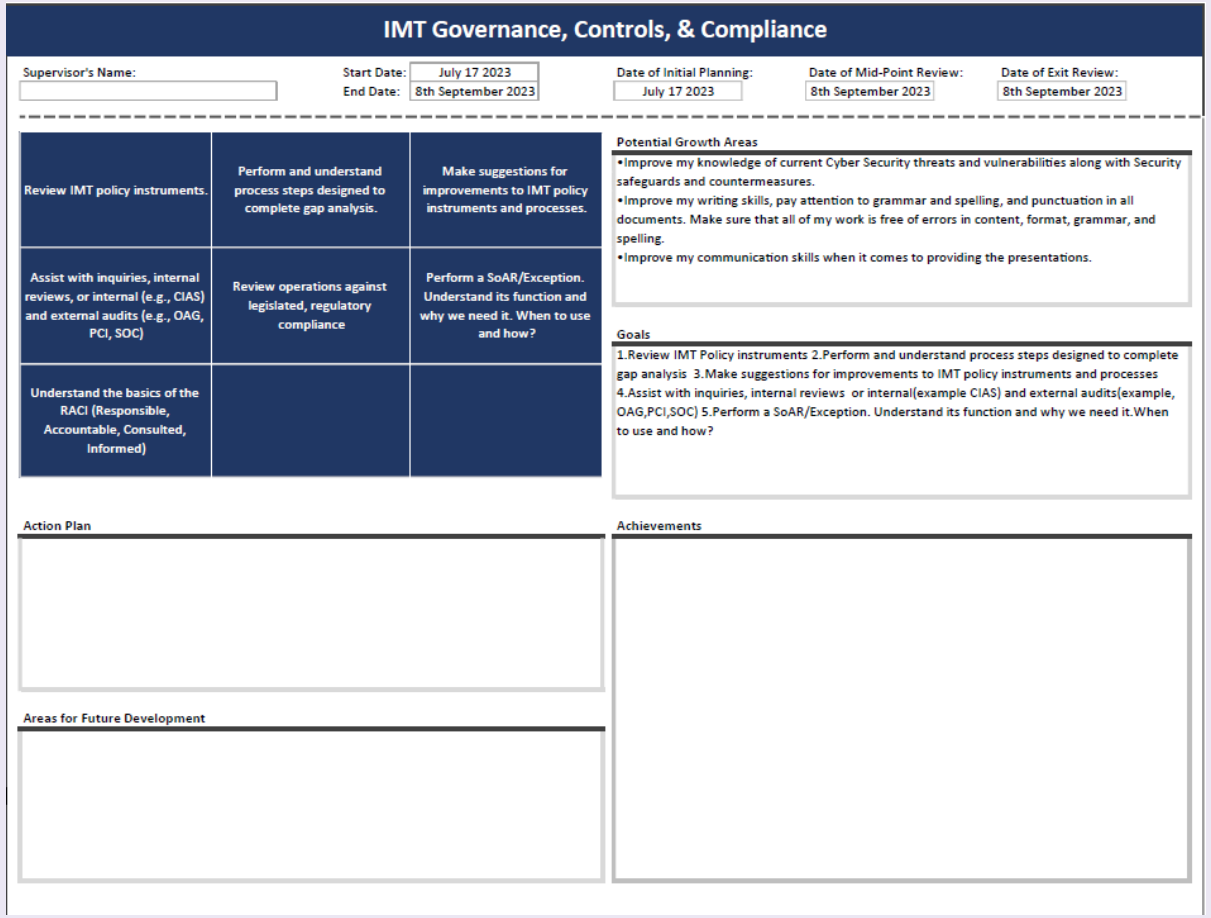
BINGO TILES

- ✓ Reviewed
- ✓ Updated
- ✓ Used for ILP

CYBER ALBERTA

Individual Learning Plan (ILP)

- Tailored development plans for each learner
- Tracked at the end of rotations
- Focus areas based on learner strengths and areas for growth
- Define action plans



IMT Governance, Controls, & Compliance

Supervisor's Name:

Start Date: July 17 2023
End Date: 8th September 2023

Date of Initial Planning: July 17 2023

Date of Mid-Point Review: 8th September 2023

Date of Exit Review: 8th September 2023

Review IMT policy instruments.	Perform and understand process steps designed to complete gap analysis.	Make suggestions for improvements to IMT policy instruments and processes.
Assist with inquiries, internal reviews, or internal (e.g., CIAS) and external audits (e.g., OAG, PCI, SOC)	Review operations against legislated, regulatory compliance	Perform a SoAR/Exception. Understand its function and why we need it. When to use and how?
Understand the basics of the RACI (Responsible, Accountable, Consulted, Informed)		

Potential Growth Areas

- Improve my knowledge of current Cyber Security threats and vulnerabilities along with Security safeguards and countermeasures.
- Improve my writing skills, pay attention to grammar and spelling, and punctuation in all documents. Make sure that all of my work is free of errors in content, format, grammar, and spelling.
- Improve my communication skills when it comes to providing the presentations.

Goals

1.Review IMT Policy instruments 2.Perform and understand process steps designed to complete gap analysis 3.Make suggestions for improvements to IMT policy instruments and processes 4.Assist with inquiries, internal reviews or internal(example CIAS) and external audits(example, OAG,PCI,SOC) 5.Perform a SoAR/Exception. Understand its function and why we need it.When to use and how?

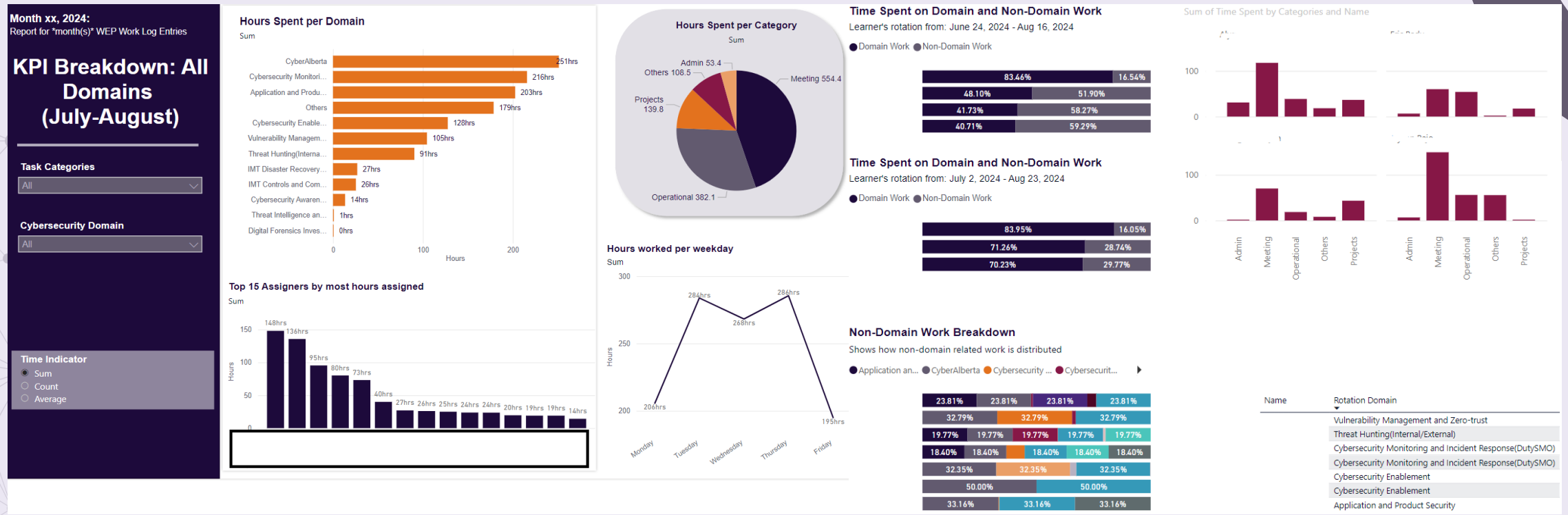
Action Plan

Achievements

Areas for Future Development

CYBER ALBERTA

KPIs and Data Insights



Automated, real-time reports from the work log tracker for learner's progress, team visibility, efficient management and decision making

Program Testimonials

““The CyberAlberta Work Experience Program is an exceptional initiative that provides participants with hands-on experience in the field of cybersecurity. The program’s structure is well-designed, offering a perfect blend of theoretical knowledge and practical application. Throughout my time in the program, I had the opportunity to work on real-world projects, collaborate with industry experts, and gain valuable insights into the latest cybersecurity trends and practices.

One of the standout features of the program is its emphasis on mentorship and guidance. The mentors are highly knowledgeable and supportive, always willing to share their expertise and provide constructive feedback. This mentorship has been instrumental in helping me refine my skills and build confidence in my abilities.”

- Sarah Hunt (Information Security Officer 2, Cyber Threat Intelligence and Reporting) – Cohort 1

“The Work Experience Program was a game changer for me as I transitioned into a new career in cybersecurity. It provided me with the chance to explore various domains within the field, helping me pinpoint my specific interests for the future. Although government and innovation don't always go hand in hand, the Cybersecurity Division of the Government of Alberta is embracing AI and automation, offering a fantastic opportunity for personal and professional growth through hands-on involvement in these exciting projects. I also had the opportunity to work with incredible people in an environment that promotes learning and pursuing passions. Breaking into cybersecurity can be tough without experience, but this program opened doors for me in ways I never thought possible. I’m truly grateful for the opportunity!”

- Jocelyn Odorizzi (Information Security Officer 2, Vulnerability Management & Zero-Trust) – Cohort 2

Lessons Learned

- **Importance of support** from leadership, groups, and team members
- **Rotation plan changes**
  - Adhoc style to structure
  - Length of team rotations based on activities and access limitation
- **Improved work plans + shadowing** (cybersecurity teams)
- **Tool creation and evolution** – e.g. Dashboard, ILP, BINGO
- **Mentorship matching** (Personality assessment's accuracy)
- **Streamlined WEP hiring** process and criteria

WEP for YOU

CyberAlberta’s collaboration with organizations to adopt the WEP Program

Benefits for Organizations

- **Talent Pipeline:** Access to a pool of trained, motivated cybersecurity professionals
- **Innovation:** Fresh perspectives and new ideas from recent graduates
- **Community Impact:** Contributing to the development of local talent and the cybersecurity industry in Alberta
- **Established Model & Framework:** CyberAlberta/GOA created the process and documents that can easily be adopted by organizations

Future Involvement

- **Partnership Opportunities:** Ways organizations can collaborate with the WEP

1. Mentorship
2. Interviews and Assessments
3. Hire from Talent Pool
4. Sponsorship

- **Adopting WEP in your Organization?**

- Contact us: cyberalberta@gov.ab.ca

Q&A

Cyber Threat Intelligence

GoA Program Overview

Krystyna Cynar
November 6, 2024

CYBER ALBERTA

> If you know the **enemy** and know **yourself**, you need not fear the result of a hundred battles.
>
> - Sun Tzu

What is Cyber Threat Intelligence?

Definition: Information about threats and threat actors that helps organizations mitigate harmful events.

Purpose: To protect against cyber attacks by understanding potential threats.

Why is Cyber Threat Intelligence Important?

Early Threat Detection

Helps in identifying and preventing cyber threats.

Enhanced Security Posture

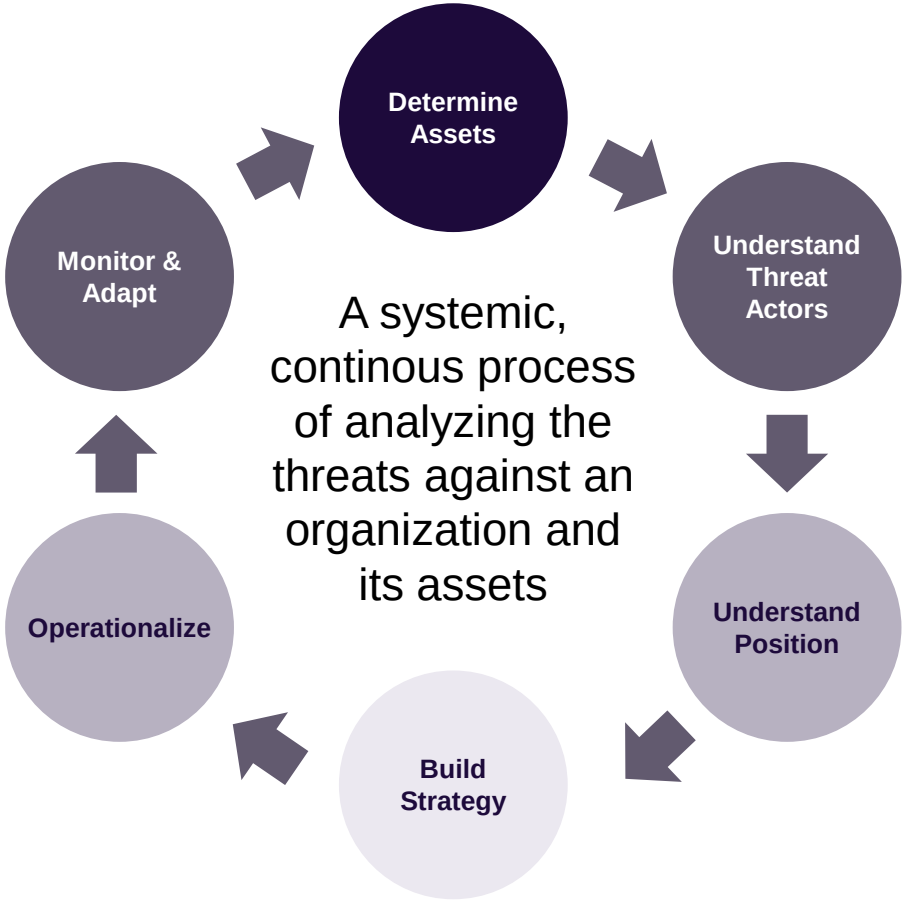
Allows GoA to stay ahead of potential attacks.

Decision-Making Support

Informs security strategies and policies.

The CTI Framework

- What is it we are trying to protect?
- Who are we trying to protect from?
- How do we protect it from who wants it?
- What was missed?
- What controls can be created?
- What change(s) can we enact?



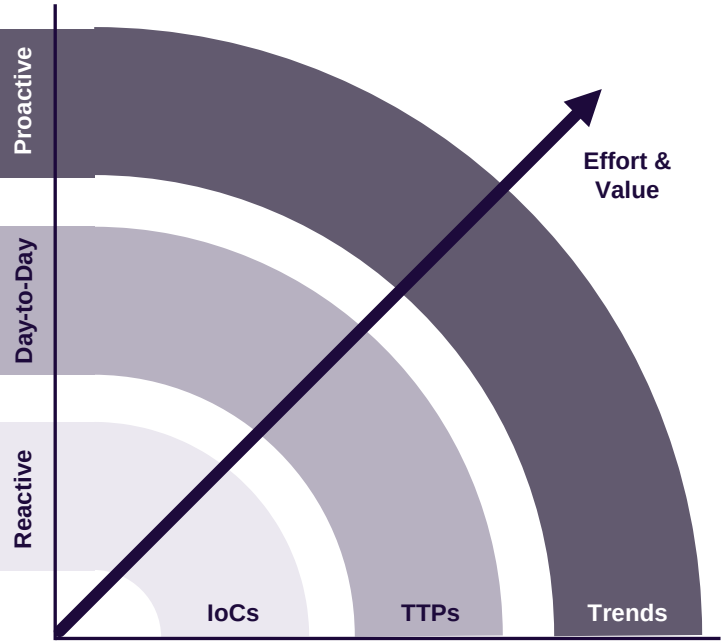
CYBER ALBERTA

Types of Intelligence

Strategic: High-level information influencing long-term decision-making.

Operational: Insights into specific attacks, techniques, and actors.

Tactical: Immediate, short-term threats like IP addresses or URLs.



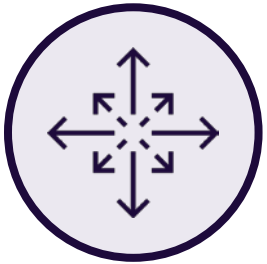
CYBER ALBERTA

Evolving Threat Landscape

Overview of Current Threats

The Growing Threat Landscape

Increasing Number and Sophistication of Attacks



Expanding Attack Surface

Weak Authentication Systems

Vulnerabilities in Legacy Systems and Supply Chain

Critical Importance of Supply Chain Management

Types of Cyber Threats

Malware

Viruses, worms, ransomware.

Phishing

Fraudulent attempts to obtain sensitive information.

DDoS Attacks

Overwhelming a system with traffic.

Insider Threats

Threats from within the organization.

Is Your Business Immune?

No one is…

Is Your Business Immune?

Attackers preferred methods include:

Phishing Scams

Identity Theft

Online Fraud

Malware & Viruses

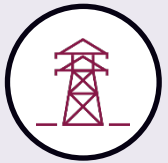
Those targets with weaknesses are selected:

Finance

Healthcare

Government

Retail & E-Commerce



Energy & Utilities

Manufacturing & Industrial

CYBER ALBERTA

Cybercrime Statistics

Canadian Cybercrime Statistics

KPMG 2023 Survey: Cybercrime Incidents

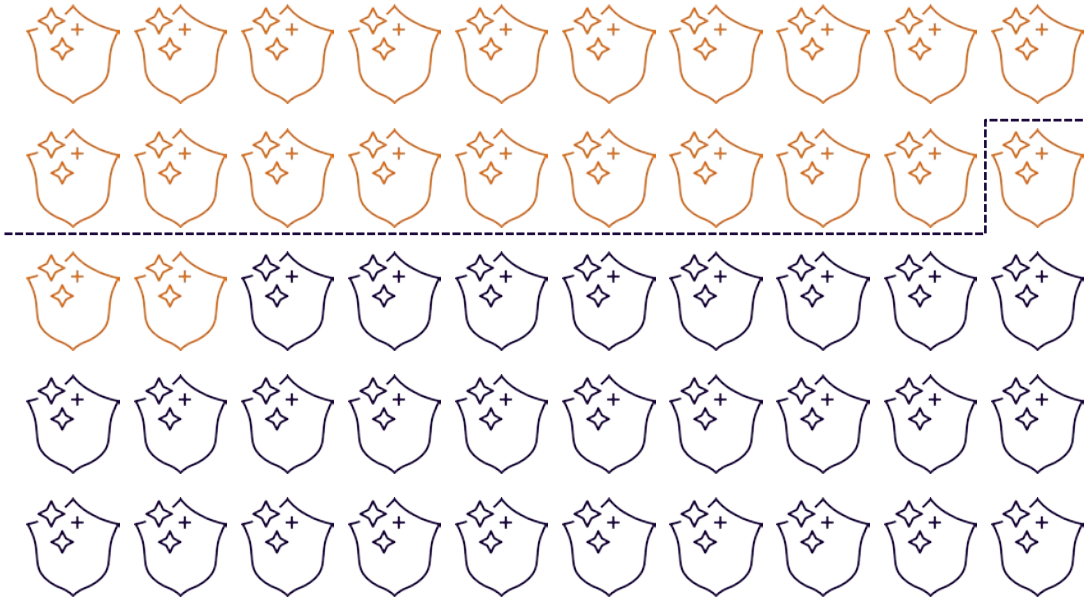
Over half (**51%**) of small and medium-sized businesses (SMBs) in Alberta reported being attacked by cybercriminals in the past year. This is slightly lower than the national average of **63%**.

KPMG 2023 Survey: Ransom Payments

55% of Alberta-based businesses that experienced a cyberattack paid a ransom within the past three years, compared to **60%** nationally.

KPMG 2023 Survey: Cybercrime Priority

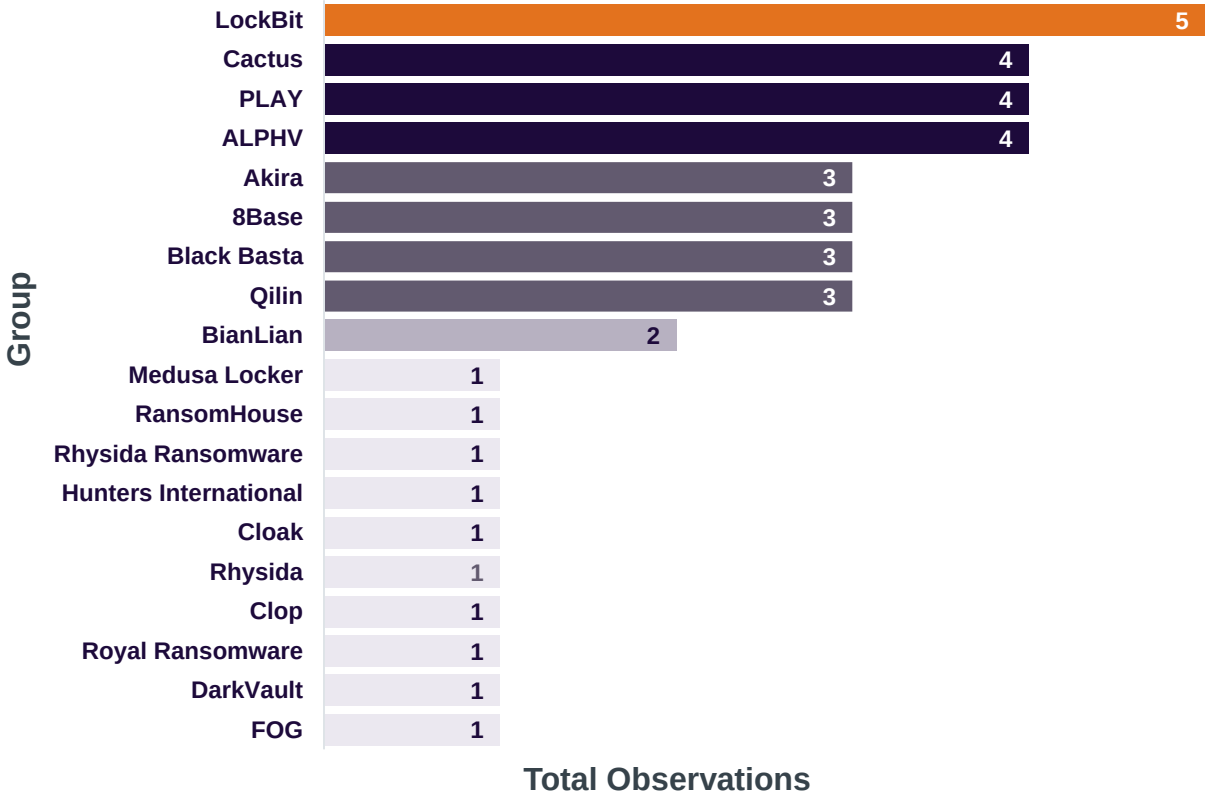
Only **44%** of businesses in Alberta consider cybersecurity a business priority, which is higher than the national average of **38%**.



Cybercrime Statistics

Alberta Ransomware Activity in 23/24

Ransomware Group Activity in Alberta 23/24

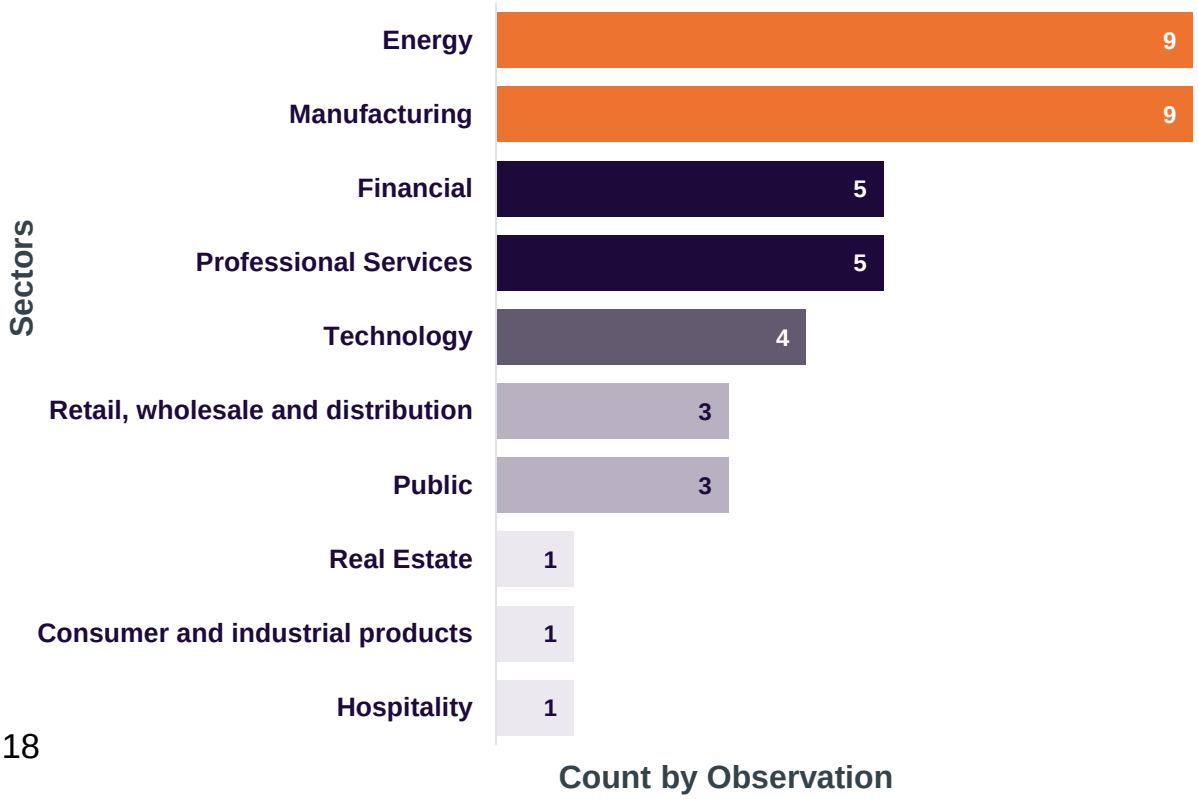


Since January 2023, CyberAlberta has observed **41** ransomware attacks on **Alberta** based organizations since January 2023.

Organizations of all sizes have been targeted in **Alberta**. SMBs are often perceived as a softer target.

CYBER ALBERTA

Ransomware Targeting in Alberta by Sector 23/24



The top three targeted sectors in Alberta are:

Energy Manufacturing Finance

Ransomware organizations are financially motivated and opportunistic in nature.

Targeting can be cyclical. Attacks often increase in-line with a sectors busy periods.

CYBER ALBERTA

Q&A