BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Unifying the Fight Against Cyber Threats:

The Power of a Federated Security Operation Centre

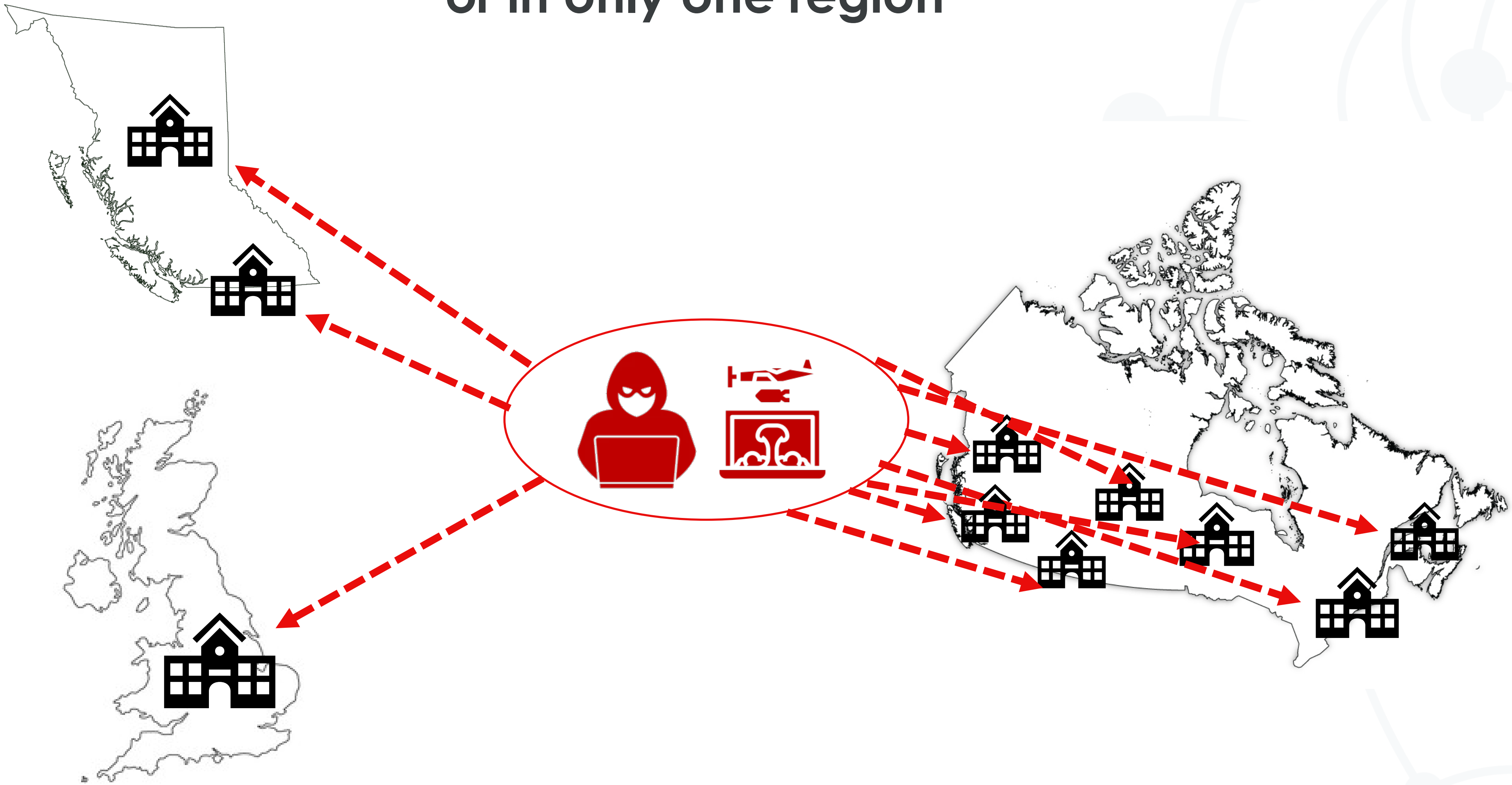
Elena Carroll | Director, Cybersecurity Services Innovation | CANARIE

Ivor MacKay | Manager, Cybersecurity | BCNET

Agenda

- ❑ Why we need a Federated SOC
- ❑ Institutions’ input
- ❑ User Story
- ❑ What is CanSSOC?
- ❑ BCNET’s SOC readiness
- ❑ Where does BCNET fit in?
- ❑ Federated SOC Capabilities
- ❑ Pilot Project and next steps

Advanced threat actors don't attack institutions in isolation or in only one region



A national approach is essential

BCNET CONNECT

Need to think and act differently

The "Old" Security Model

- Security is IT's job
- Lock it down
- Plug the holes
- A solution in search of a problem
- Security versus convenience
- "If only we had more…" Money, Time, People

End state – "We are secure"

From an IT services problem...

The "New" Security Model

- Security is a shared fate
- Enable the mission and values of the institution
- Empower individuals and units
- Resources allocated based on risk
- "Assume you are breached" – do not wait for someone to say you are breached. Find intruders and kick them out!

End state – "Managed risk"

…to a corporate governance and risk problem

Community Federated SOC Workshop Oct-Dec 2022

- Inaugural series of the Community Consultation Workshops
- Objectives:
  - Communicate the high-level vision of the Federated SOC concept including value proposition, financial model, and high-level structure
  - Receive feedback and requirements from institutional participants on what is required for the Federated SOC, what will work, challenges, and concerns
  - Gather feedback on how to evolve the ongoing concept of community workshops

Workshop Attendance:

Event	**# Attendees***	**# Institutions***
BCNET	45	20
Cybera/SRNET/MRnet:	19	15
CUCCIO:	44	42
RISQ:	37	22
ORION:	13	10
Virtual:	37	24
TOTAL:	195	89**

*Preliminary numbers only includes institutional attendees only, not including NREN Partners

**Unique institutions across all sessions

Institutional Challenges Identified

1. 24x7 monitoring: after-hours monitoring to address highest risk of compromise
2. Human resources: expertise and number of positions
3. Time and prioritization: struggle to balance competing cybersecurity and IT operational priorities
4. Funding: for tools and personnel
5. Advocacy and education: frustration that the importance of cybersecurity is not understood by institutional leadership

NREN Information Security Leader (ISL) Workshop March 2023

- Workshop with ISL of Provincial NREN partners.
  17 participants from BCNET, Cybera, ORION, SRNET, MRnet, RISQ, ACORN-NL, ACORN-NS, ECN, and CANARIE.
- Objectives:
  - Align on a set of capabilities, with a focus on Detection and Response.
  - Develop a draft architecture that leverages existing detection infrastructure
  - Brainstorm principles and outcomes for a pilot consisting of a set of projects undertaken in the next 12-18 months.

Pilot Principles:

- ***Better than you can do on your own, always in partnership***
- Leverage, not replace, existing investments.
- Focus on integration.
- More actionable intelligence.
- Value for all institutions, regardless of capabilities.
- One Federated SOC providing institutions a cohesive set of services; no matter who you are or where you are.
- Continue to build a trusted network that enables sharing data and sensitive intelligence in real time.

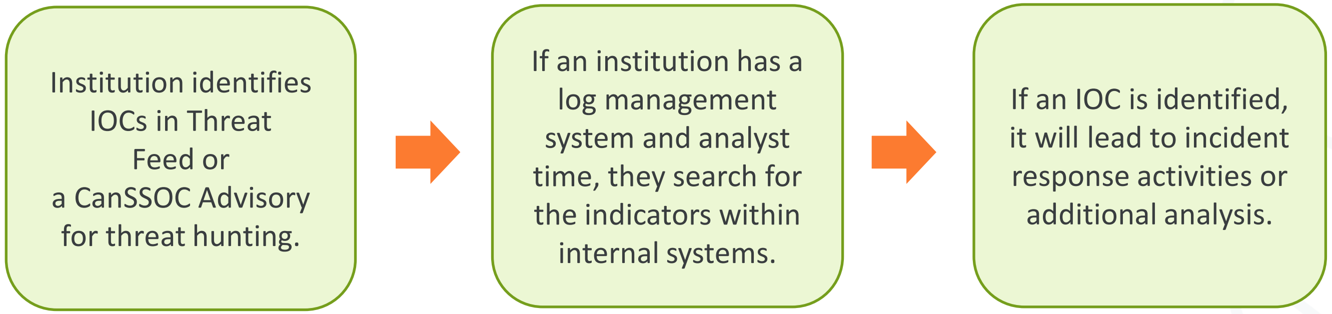
BCNET CONNECT

What is CanSSOC?

Term	Definition
Security Operations Centre (SOC)	People, process, and technology that supports information security operations activities (with a focus on detection and response).
Federated Security Operations Centre (SOC)	Describes the SOC capabilities across Canada to support Canadian higher education institutions in reducing their cybersecurity risk by offering capabilities not feasible for institutions on their own, regardless of their existing capabilities. This includes Federal SOC + Regional SOC + Institution SOC
CanSSOC	**Synonym for Federated SOC.**

Federated SOC User Story - Threat Hunting

Current State:



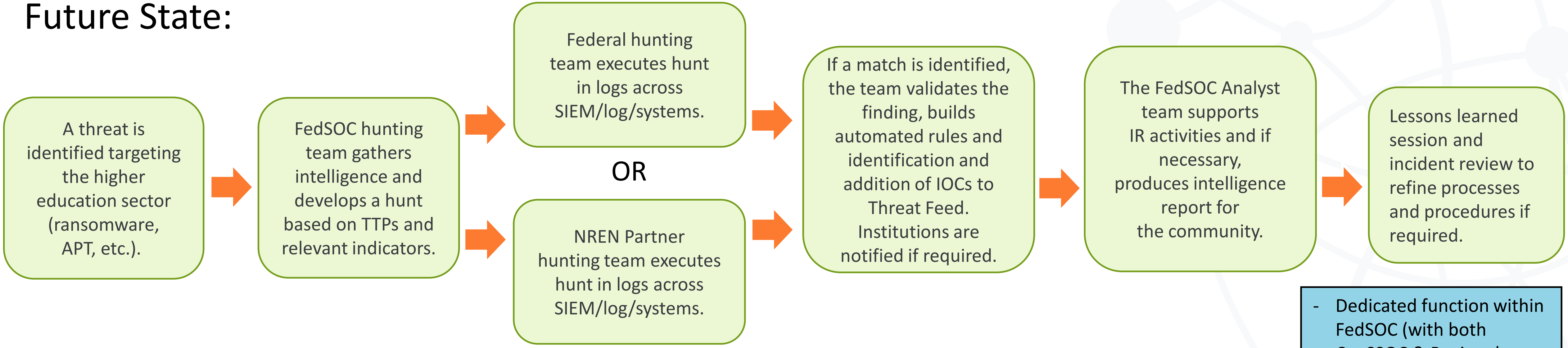
Institution identifies IOCs in Threat Feed or a CanSSOC Advisory for threat hunting.

If an institution has a log management system and analyst time, they search for the indicators within internal systems.

If an IOC is identified, it will lead to incident response activities or additional analysis.

- Lack of logs and dedicated analyst time for this function
- No national coordination or risk-assessment
- Limited use-case or automation
- Value decays over time, due to nature of IOCs .

Future State:



A threat is identified targeting the higher education sector (ransomware, APT, etc.).

FedSOC hunting team gathers intelligence and develops a hunt based on TTPs and relevant indicators.

Federal hunting team executes hunt in logs across SIEM/log/systems.

OR

NREN Partner hunting team executes hunt in logs across SIEM/log/systems.

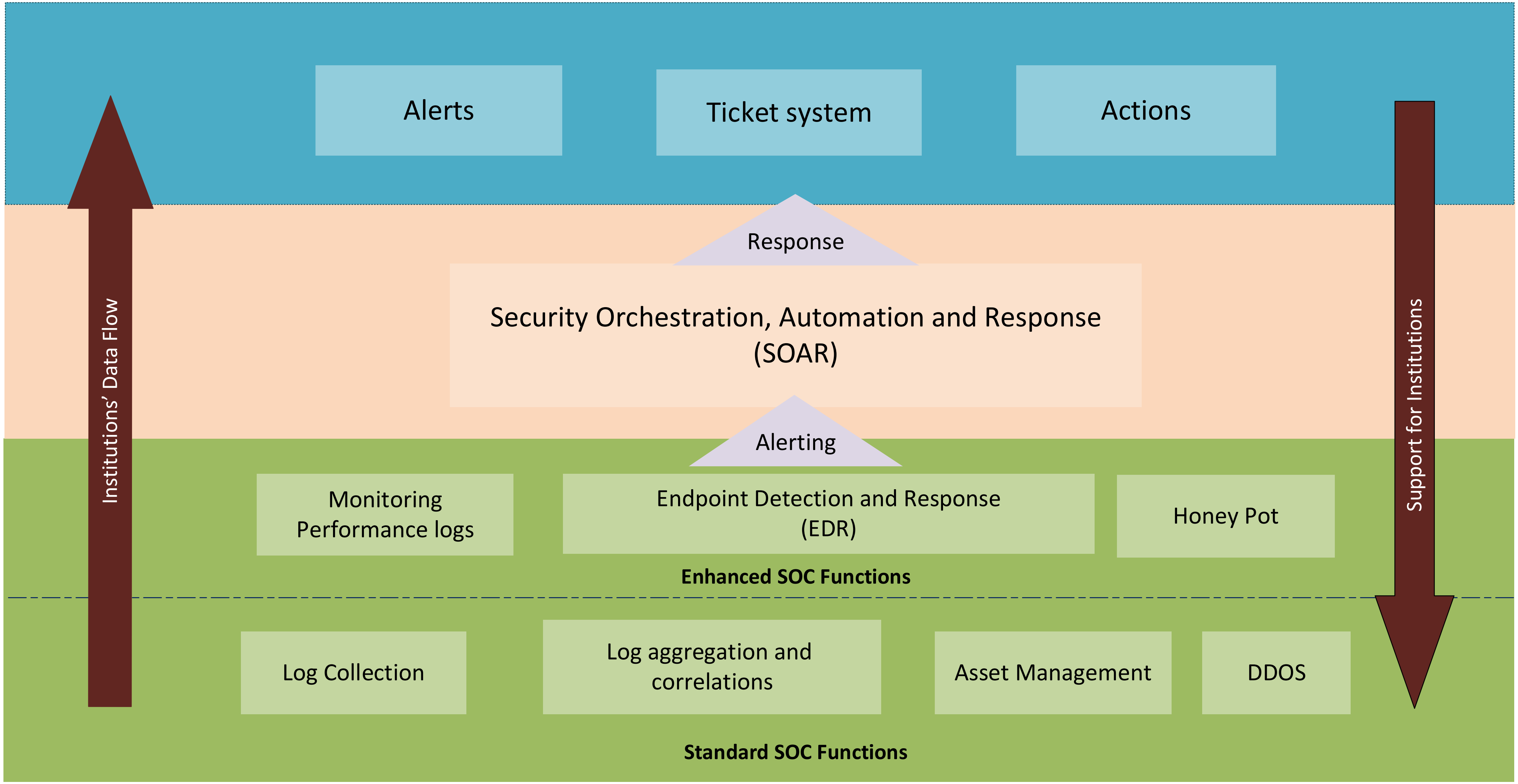
If a match is identified, the team validates the finding, builds automated rules and identification and addition of IOCs to Threat Feed. Institutions are notified if required.

The FedSOC Analyst team supports IR activities and if necessary, produces intelligence report for the community.

Lessons learned session and incident review to refine processes and procedures if required.

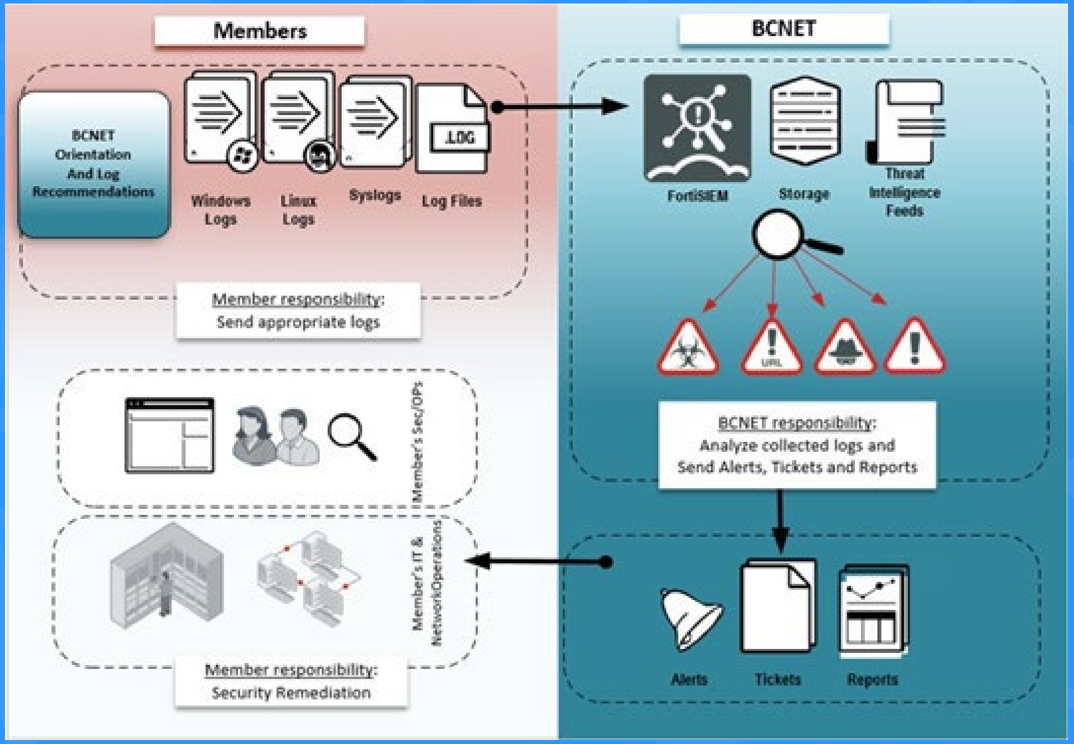
- Dedicated function within FedSOC (with both CanSSOC & Regional Analysts)
- In-depth hunting based on TTPs, IOCs, and data analytics for unusual behaviour

Draft Concept Architecture



BCNET CONNECT

BCNET Current Services and Capabilities



Member responsibility:
Send appropriate logs

BCNET responsibility:
Analyze collected logs and Send Alerts, Tickets and Reports

Member responsibility:
Security Remediation

- At this point, we do not believe we have a SOC in place yet.
- We provide SIEM services for 17 institutions 2 services, Moodle and Colleague ERP
- We support the Yukon SIEM service remotely.
- We have six people dedicated to the SIEM service.
- For the Colleague ERP, we provide close to SOC-level support in terms of monitoring all devices, EDR protections, vulnerability scanning, SIEM services, OS patching and Penetration testing.
- We are adjusting our SLAs and reviewing and updating our standard operating procedures (SOP). As we conduct this review, we are noting what process we can automate.

BCNET CONNECT

BCNET Tools & Technology

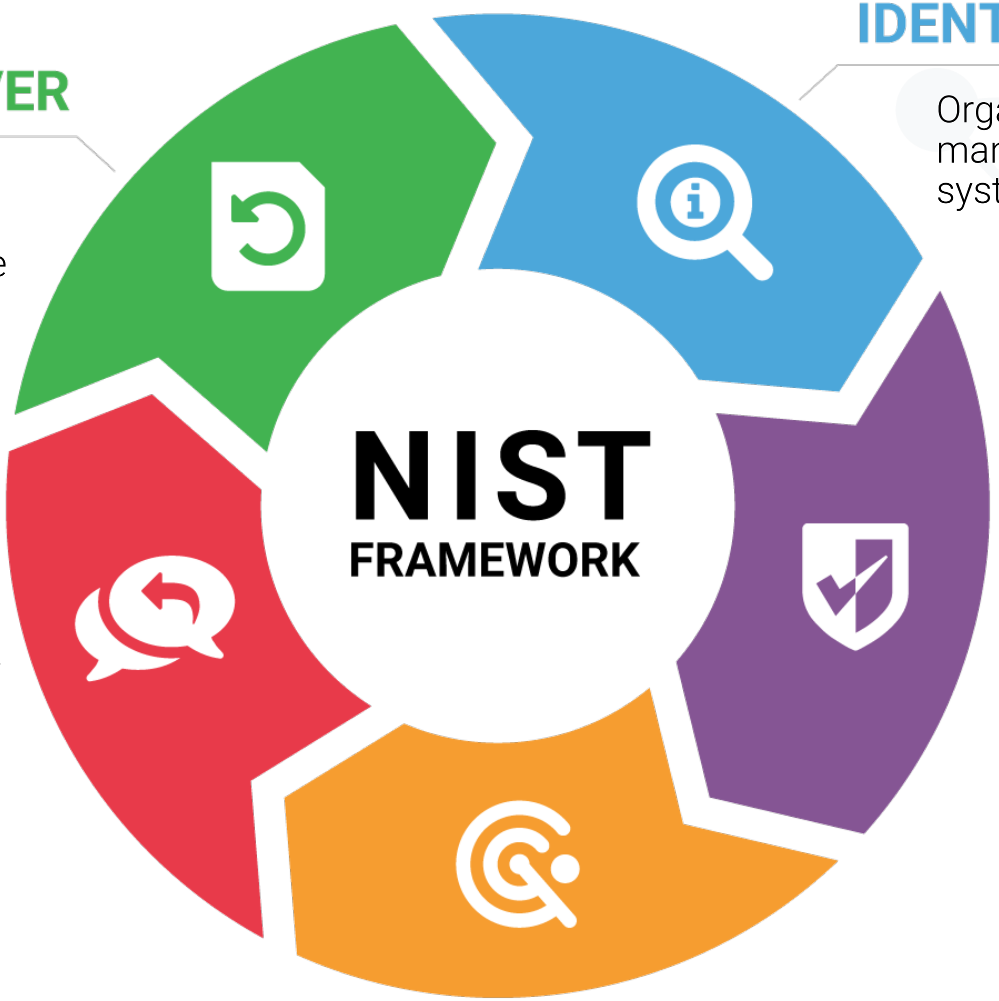
- Tenable Nessus Pro Scanning
- Zeek Bro IDS
- FortiSIEM
- Loggers: Graylog, Syslog NG
- NetScout Sightline
- MS Sentinel, MS Lighthouse
- RunZero - asset inventory platform
- Security Scorecard
- Thinkst Canary honeypots pilot

BCNET CONNECT

BCNET Cybersecurity Roadmap

	2023/24	2024/25	2025/26	2026/27
IDENTIFY	• RunZero for SIEM Members • Cybersecurity Training Program	• Cybersecurity Assessment Road Mapping • Cybersecurity Training Program		
PROTECT	• Managed Firewall Service	• Privileged Access Management	• SASE Planning • Cloud Access Security Broker (CASB) Planning	• SASE • Cloud Access Security Broker (CASB)
DETECT	• DDoS Mitigation • Best Practice Configuration Scans (using Pentest tools)	• Suricata/Zeek Improvement • AI-enhanced UEBA Planning • Best Practice Configuration Scans (using Pentest tools)	• Suricata/Zeek Improvement • AI-enhanced UEBA Planning	
RESPOND	• Security Orchestration, Automation & Response (SOAR) Planning • Security Operations Centre Planning	• Security Orchestration, Automation & Response (SOAR) Pilot • Security Operations Centre Pilot	• Security Orchestration, Automation & Response (SOAR) Full Service • Security Operations Centre Full Service	• Security Operations Centre Full Service
RECOVER	• Retainer/Incident Coach/IRP			

NIST Framework



IDENTIFY

Organizational-wide understanding to manage cybersecurity risk for systems, assets, data and capabilities.

PROTECT

Designated safeguards to ensure continued delivery of critical infrastructure services & protection of data.

DETECT

Appropriate activities to detect the occurrence of a cybersecurity event.

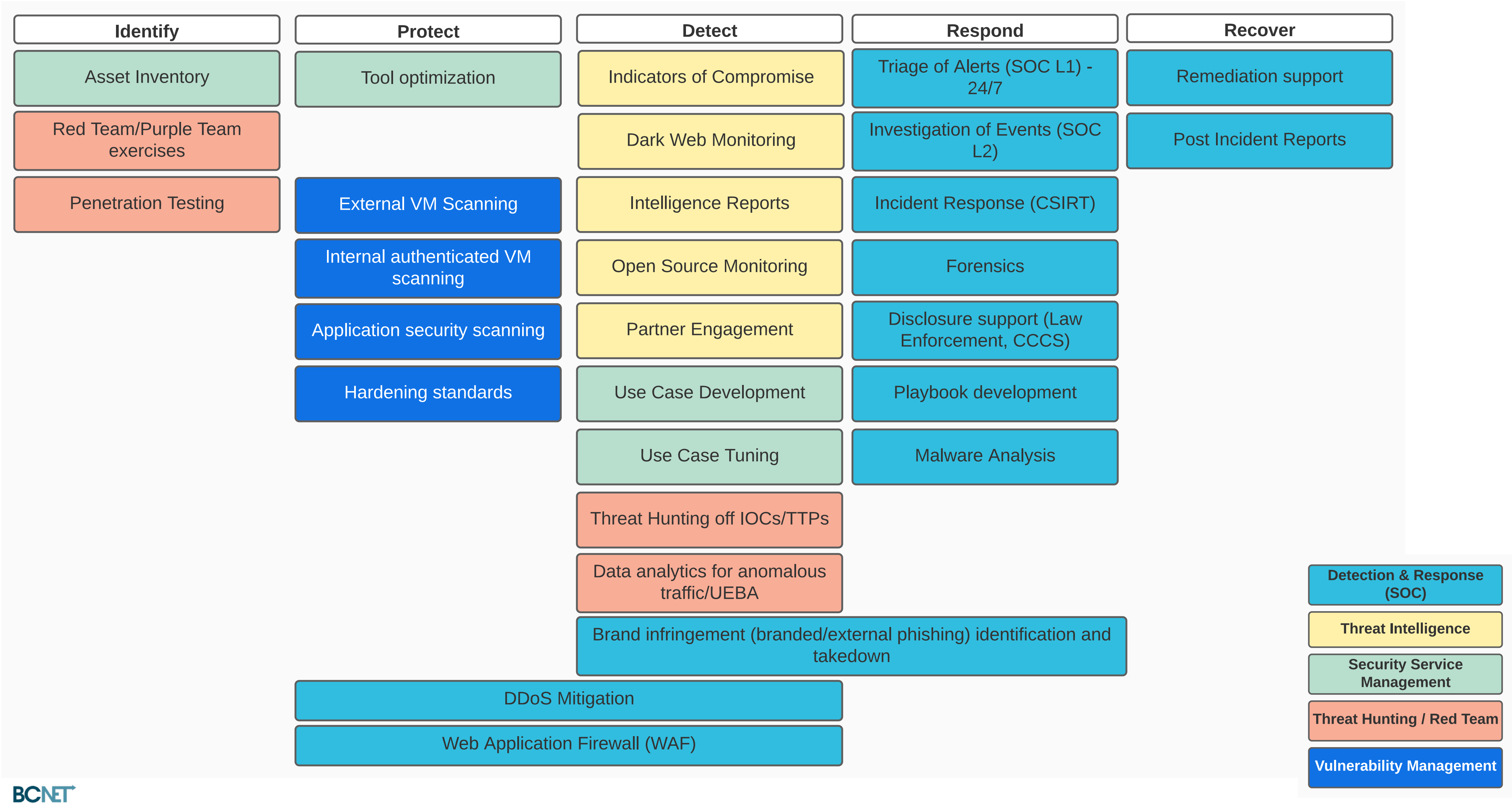
RESPOND

Activities allocated when responding to a cybersecurity event.

RECOVER

Ensure capability to recover quickly from a detected incident and restore capabilities of services impaired by the event.

Federated SOC Capabilities



Identify	Protect	Detect	Respond	Recover
Asset Inventory	Tool optimization	Indicators of Compromise	Triage of Alerts (SOC L1) - 24/7	Remediation support
Red Team/Purple Team exercises		Dark Web Monitoring	Investigation of Events (SOC L2)	Post Incident Reports
Penetration Testing	External VM Scanning	Intelligence Reports	Incident Response (CSIRT)	
	Internal authenticated VM scanning	Open Source Monitoring	Forensics	
	Application security scanning	Partner Engagement	Disclosure support (Law Enforcement, CCCS)	
	Hardening standards	Use Case Development	Playbook development	
		Use Case Tuning	Malware Analysis	
		Threat Hunting off IOCs/TTPs		
		Data analytics for anomalous traffic/UEBA		
		Brand infringement (branded/external phishing) identification and takedown		
	DDoS Mitigation			
	Web Application Firewall (WAF)			

Detection & Response (SOC)

Threat Intelligence

Security Service Management

Threat Hunting / Red Team

Vulnerability Management

Next steps

- Define pilot objectives, principles and projects.
- Develop project charter with preliminary projects, scope, timing, budget, and outcomes for internal approval.
- Refine capabilities including definitions, prioritization, and roles and responsibilities.
- Refine architecture and start engagement to get input from the institutions across Canada.
- Develop NREN Information Security Leader working group.

Questions

BCNET CONNECT

Thank-you

Suite 750 - BCIT Downtown
555 Seymour Street
Vancouver, BC
V6B 3H6

Phone: 604-822-1348
Fax: 604-822-9887
Email: info@bc.net

CANARIE & CanSSOC: Stronger Together

Where we started….

McGill

University of Alberta

McMaster University

University of Toronto

The University of British Columbia

Toronto Metropolitan University

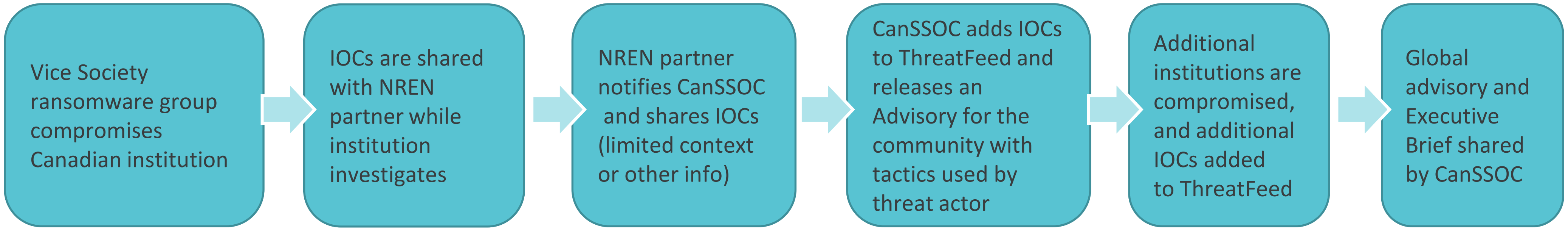
- Piloted analysis platform which generated alerts institutions were not able to detect on their own.
- Developed and piloted CanSSOC Threat Feed Service

Where we are….

- 5 CIP Initiatives: providing the foundation for an integrated set of services to build a federated Security Operations Centre
- CanSSOC: The Federated SOC – People, process and technology at CANARIE, NREN Partners, and across Canada

Federated SOC User Story: Vice Society

Current State:



Vice Society ransomware group compromises Canadian institution

IOCs are shared with NREN partner while institution investigates

NREN partner notifies CanSSOC and shares IOCs (limited context or other info)

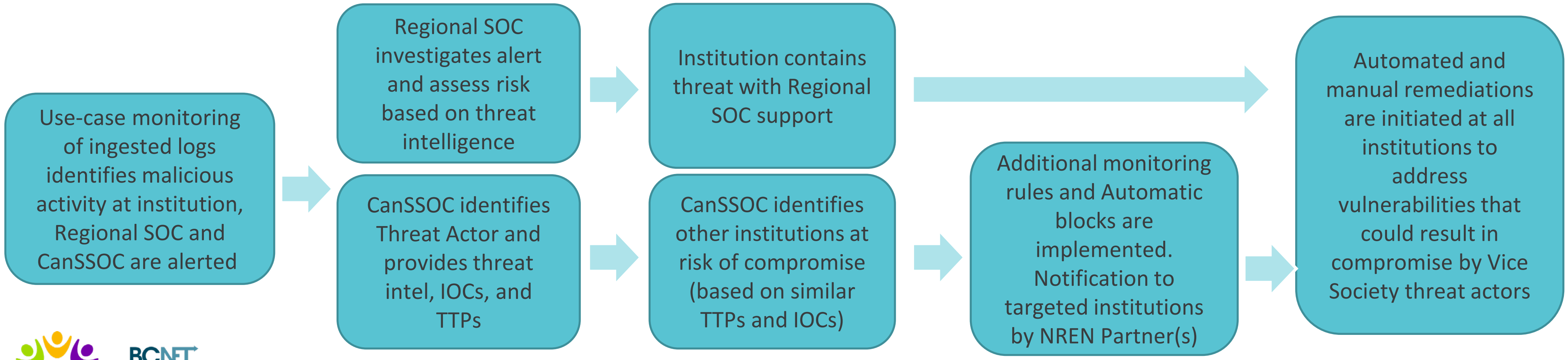
CanSSOC adds IOCs to ThreatFeed and releases an Advisory for the community with tactics used by threat actor

Additional institutions are compromised, and additional IOCs added to ThreatFeed

Global advisory and Executive Brief shared by CanSSOC

- Less effective
- Occupies information security resources
- Risk is not mitigated on time for the sector
- Information is shared across multiple systems
- Manual processes (lack of integrations)
- Information channels are interrupted/broken

Future State:



Use-case monitoring of ingested logs identifies malicious activity at institution, Regional SOC and CanSSOC are alerted

Regional SOC investigates alert and assess risk based on threat intelligence

Institution contains threat with Regional SOC support

CanSSOC identifies Threat Actor and provides threat intel, IOCs, and TTPs

CanSSOC identifies other institutions at risk of compromise (based on similar TTPs and IOCs)

Additional monitoring rules and Automatic blocks are implemented. Notification to targeted institutions by NREN Partner(s)

Automated and manual remediations are initiated at all institutions to address vulnerabilities that could result in compromise by Vice Society threat actors

- Automated detection
- Faster containment mitigates risk
- TTP's are used to update security controls
- Fewer institutions impacted

BCNET CONNECT