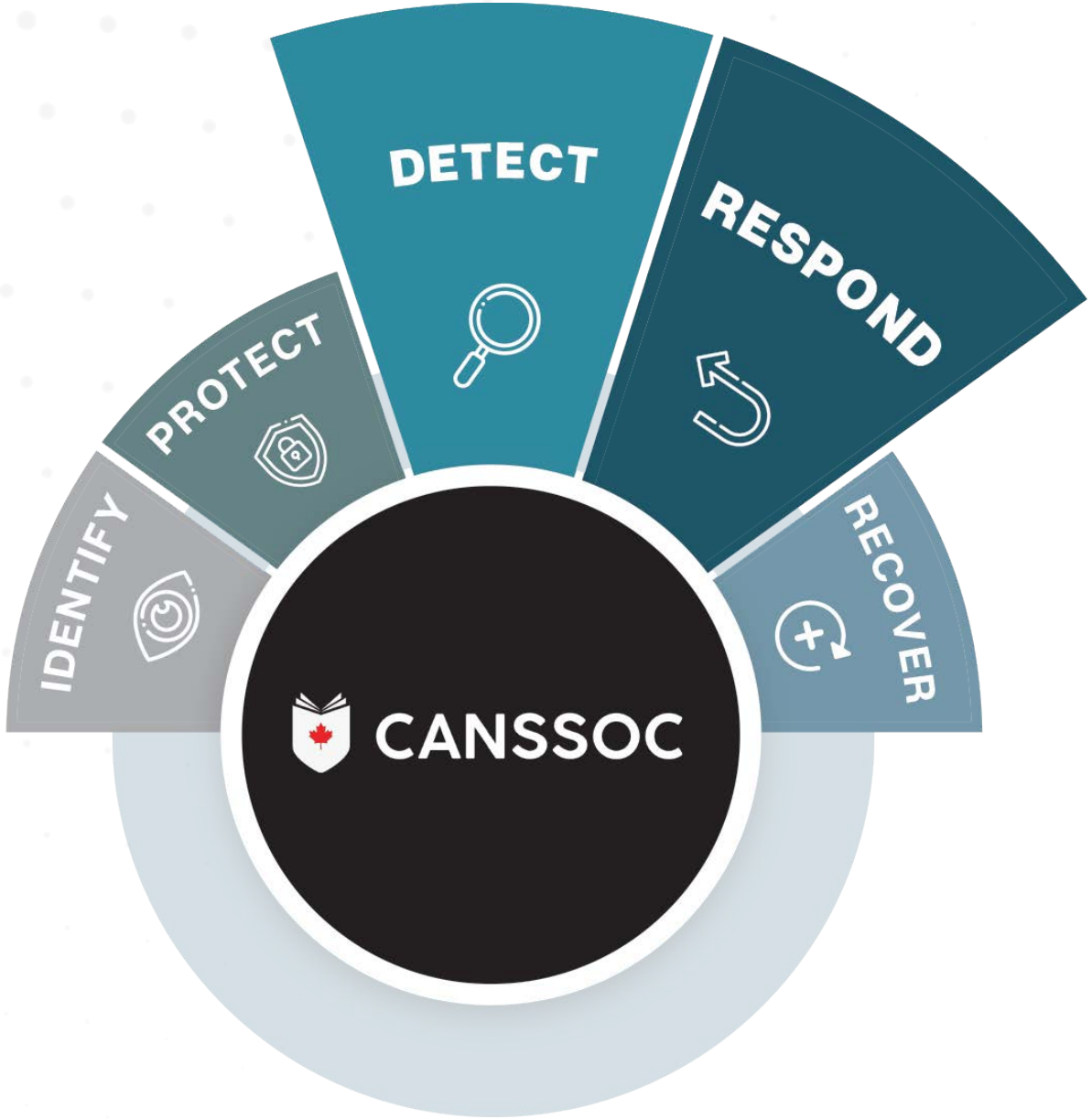
CANSSOC

The Road to Actionable Intelligence

PART OF THE **SHARED FABRIC**

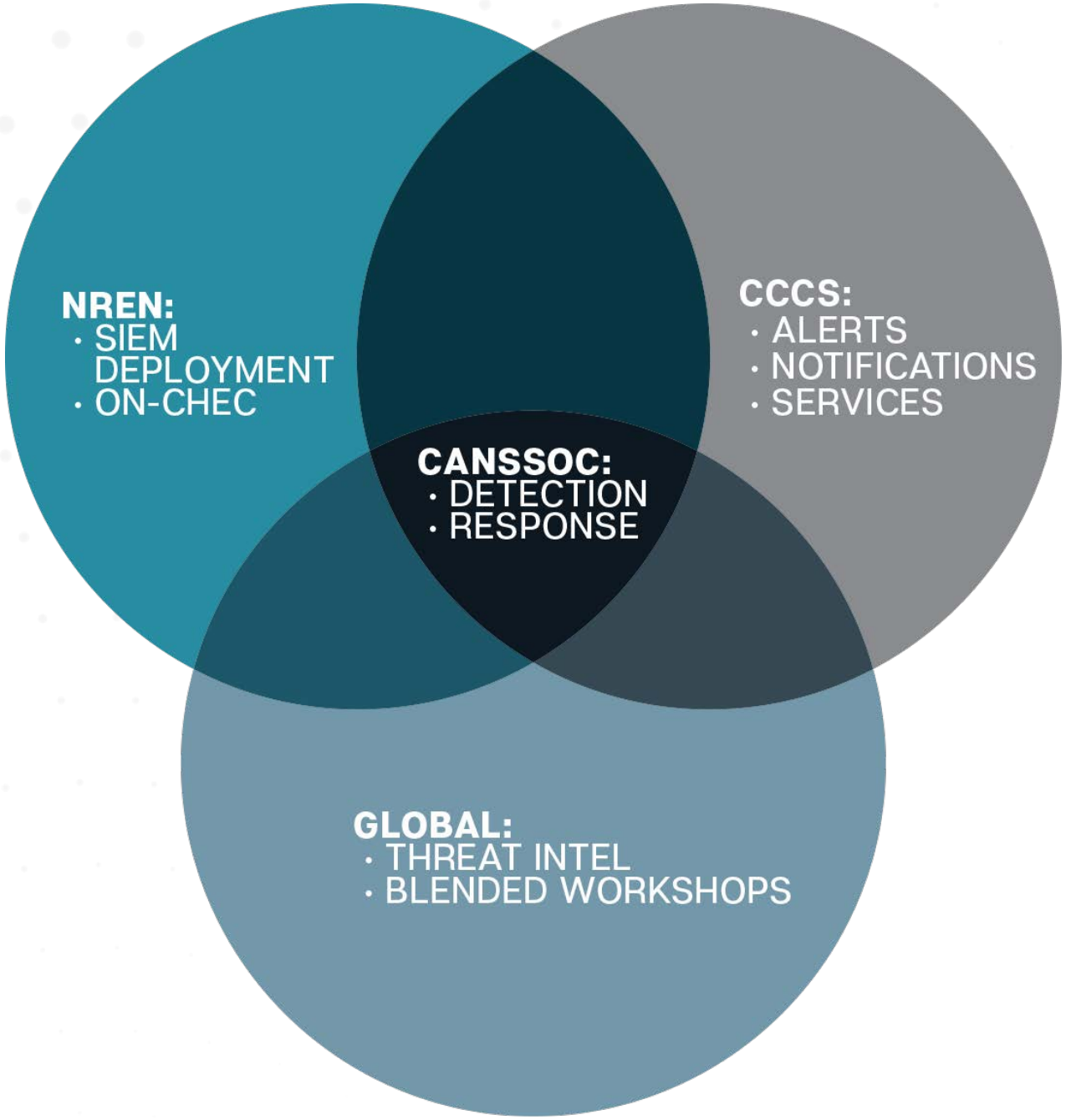
Better than we can do on our own, always in partnership

SPECIALIZING IN
DETECTION & RESPONSE



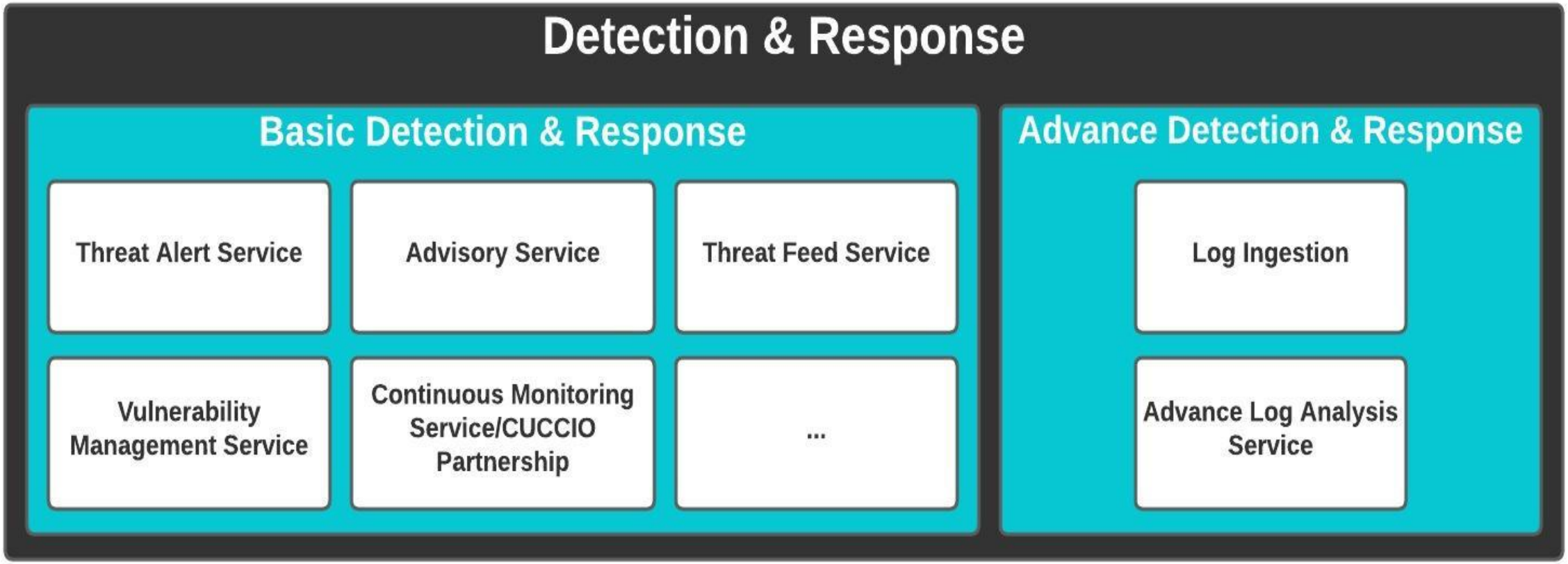
CANSSOC

DETECTION & RESPONSE **OPERATIONAL COORDINATION**



CANSSOC

CANSSOC SERVICES OVERVIEW



CANSSOC

THREAT ALERT SERVICE

Description

- **Curated alerts** sent to individual institutions which leverages intelligence detected by CanSSOC services, CCCS, REN-ISAC, CUCCIO Benchmarking, and member institutions, using contextual analysis to provide actionable alerts. **Does not require institutions to send logs.**

Objective

- Set a baseline expectation on threat alerting across the higher education sector.
- Develop skills and procedures to connect contextual data to reduce noisy security alerts.
- Test manual processes to determine automated business logic and develop shareable playbooks.

Value Proposition

- By monitoring activity from different sources and correlating those alerts enhanced with contextual data collected by CanSSOC, institutions will get actionable information about potential threats to their infrastructure and reputation better than existing institutional investments.

ADVISORY SERVICE

Description

- **Timely advisory service summarizing current sector-specific active high-risk threats** and anonymized observations from Threat Alert Service. Advisories are sent to all members and participating partners.

Objective

- Create sector-wide awareness based on issues seen by members and expert analysis.
- Improve detailed and timely trusted sharing of active high-risk threats.
- Provide a mechanism for any institution in the sector to share anonymized threats with the sector.

Value Proposition

- Any institution in the sector can learn about high confidence active threats with actionable steps even if they are not a CanSSOC member.

THREAT FEED SERVICE

Description

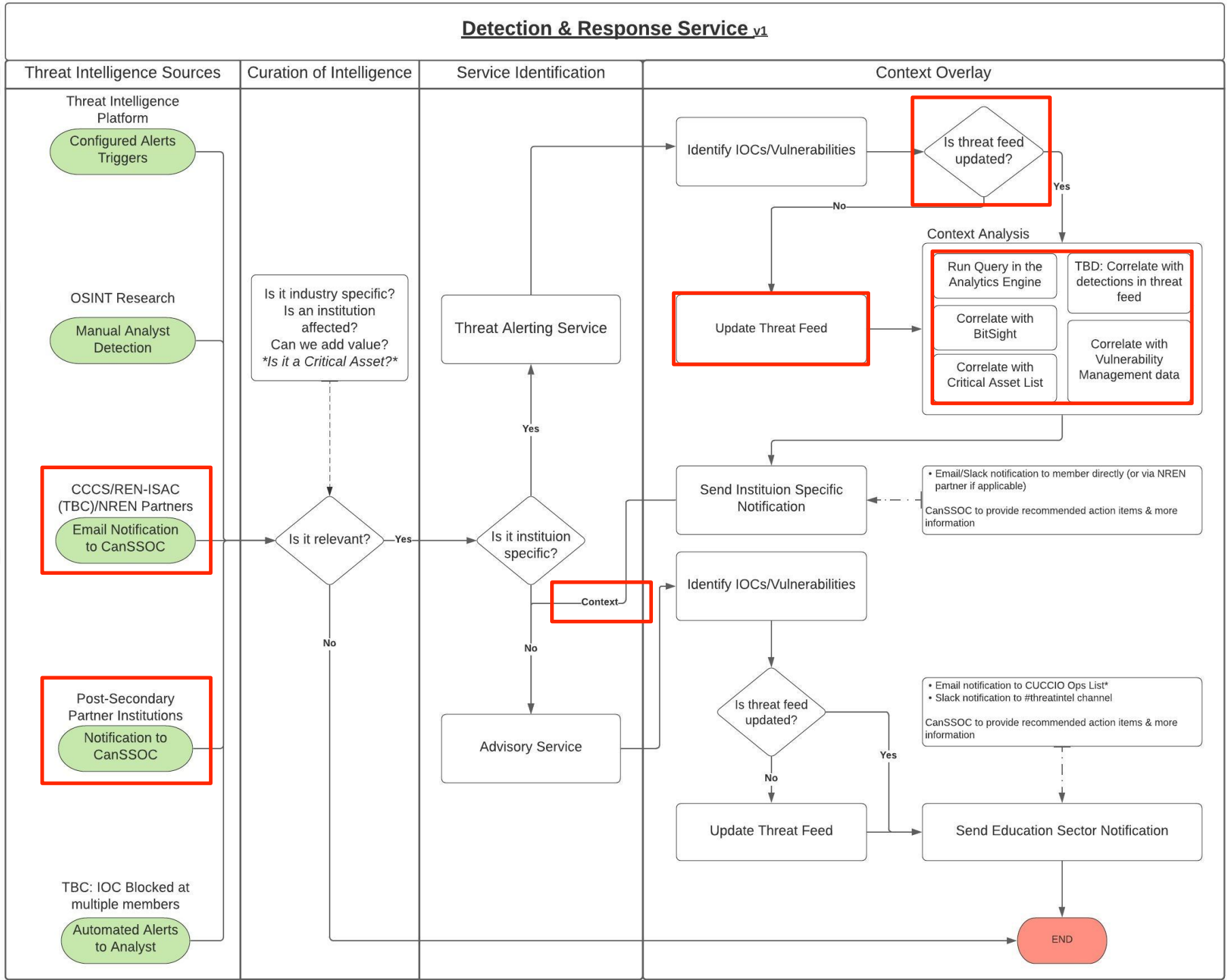
- **Current & curated stream of tagged threat data** that leverages intelligence detected by CanSSOC services, CCCS, REN-ISAC, CUCCIO Benchmarking, and member institutions.

Objective

- Improve detailed and timely trusted sharing of active high-risk threats in an automation process to assist organization detect threats and protect the environment.
- Provide contextual data for the partners leveraging the Advance Detection & Response services.

Value Proposition

- By providing curated and updated stream of tagged indicators of compromise, CanSSOC can assist the members with detecting threats and protecting their infrastructure in an automated process without the members augmenting the existing institutional investments.


Detection & Response Service v1
Threat Intelligence Sources
Curation of Intelligence
Service Identification
Context Overlay
Threat Intelligence Platform
Configured Alerts Triggers
OSINT Research
Manual Analyst Detection
CCCS/REN-ISAC (TBC)/NREN Partners
Email Notification to CanSSOC
Post-Secondary Partner Institutions
Notification to CanSSOC
TBC: IOC Blocked at multiple members
Automated Alerts to Analyst
Is it industry specific? Is an institution affected? Can we add value? *Is it a Critical Asset?*
Is it relevant?
Yes
No
Threat Alerting Service
Is it instituion specific?
Yes
No
Context
Advisory Service
Identify IOCs/Vulnerabilities
Is threat feed updated?
Yes
No
Update Threat Feed
Context Analysis
Run Query in the Analytics Engine
TBD: Correlate with detections in threat feed
Correlate with BitSight
Correlate with Vulnerability Management data
Correlate with Critical Asset List
Send Instituion Specific Notification
• Email/Slack notification to member directly (or via NREN partner if applicable)
CanSSOC to provide recommended action items & more information
Identify IOCs/Vulnerabilities
Is threat feed updated?
Yes
No
Update Threat Feed
• Email notification to CUCCIO Ops List*
• Slack notification to #threatintel channel
CanSSOC to provide recommended action items & more information
Send Education Sector Notification
END

THREAT FEED METRICS

		Count
Post-Secondary Institutions	Institutions Onboarded	33
	Users Onboarded	104
Partners	Partners Onboarded	6
	Users Onboarded	13
CanSSOC Team	Analyst Contributed Events	38
	Total Attributes (IOCs)	75,939
CanSSOC Partners	Analyst Contributed Events	539
	Total Attributes (IOCs)	247,243
Total (All Partners/CanSSOC Team/Open Source)	Total Events	74,986
	Total Attributes (IOCs)	4,120,674

CANSSOC

- Event is a container that includes contextually related information described as Attributes.
- Attribute is any indicator that is part of an Event, example: IP address, Hashes, etc.

VULNERABILITY MANAGEMENT SERVICE

Description

- **External scanning to identify vulnerabilities** detected within member public facing infrastructure.

Objective

- Leverage vulnerability management information to enrich and contextualize detection & response.
- Consolidate vulnerability data from multiple complementary sources in one dashboard.
- Track member vulnerability posture over time and compare it to peers.
- Correlate information into meaningful partner views.

Value Proposition

- By using real and current vulnerability information, detection and response services can provide more accurate alerts and information. By providing a holistic view of vulnerabilities using curated dashboards, members can minimize time to review institutional posture and prioritize their remediation efforts based on effective risks.

VULNERABILITY MANAGEMENT SERVICE TIMELINE

	Discovery Release	Data Expansion Release	Data Enrichment Release
Description	• Limited data sources: mass scan, Nessus, Shodan • Authentication to interactive dashboard • Based on webinar demo	• Add additional data sources: Bitsight, Security Scorecard, Recorded Future, CCCS NCTNS, etc. • Additional dashboard enhancements	• Enhancement to provide deeper dive into key vulnerabilities • Pre-pilot internal scanning capabilities
Target Release	Q1 2021	Q2-Q3 2021	Q4 2021

CANSSOC

QUESTIONS / CONTACT US

info@canssoc.ca

@CanSSOC

https://tinyurl.com/canssoc-youtube

CANSSOC