CANHEIT-ARC
MANITOBA 2019
Let's meet in the middle

Improved Cyber Security Through Multi-University Partnerships

The CanSSOC Proof of Concept

Welcome and Introductions

Panel

Gordie Mah
Chief Information Security Officer
University of Alberta

Paul Weber
Supervisor, IT Security
Ryerson University

Mike Wiseman
Associate Director, Information Security
University of Toronto

Moderator

Isaac Straley
Acting Director, CanSSOC / Chief Information Security Officer
University of Toronto

CANSSOC

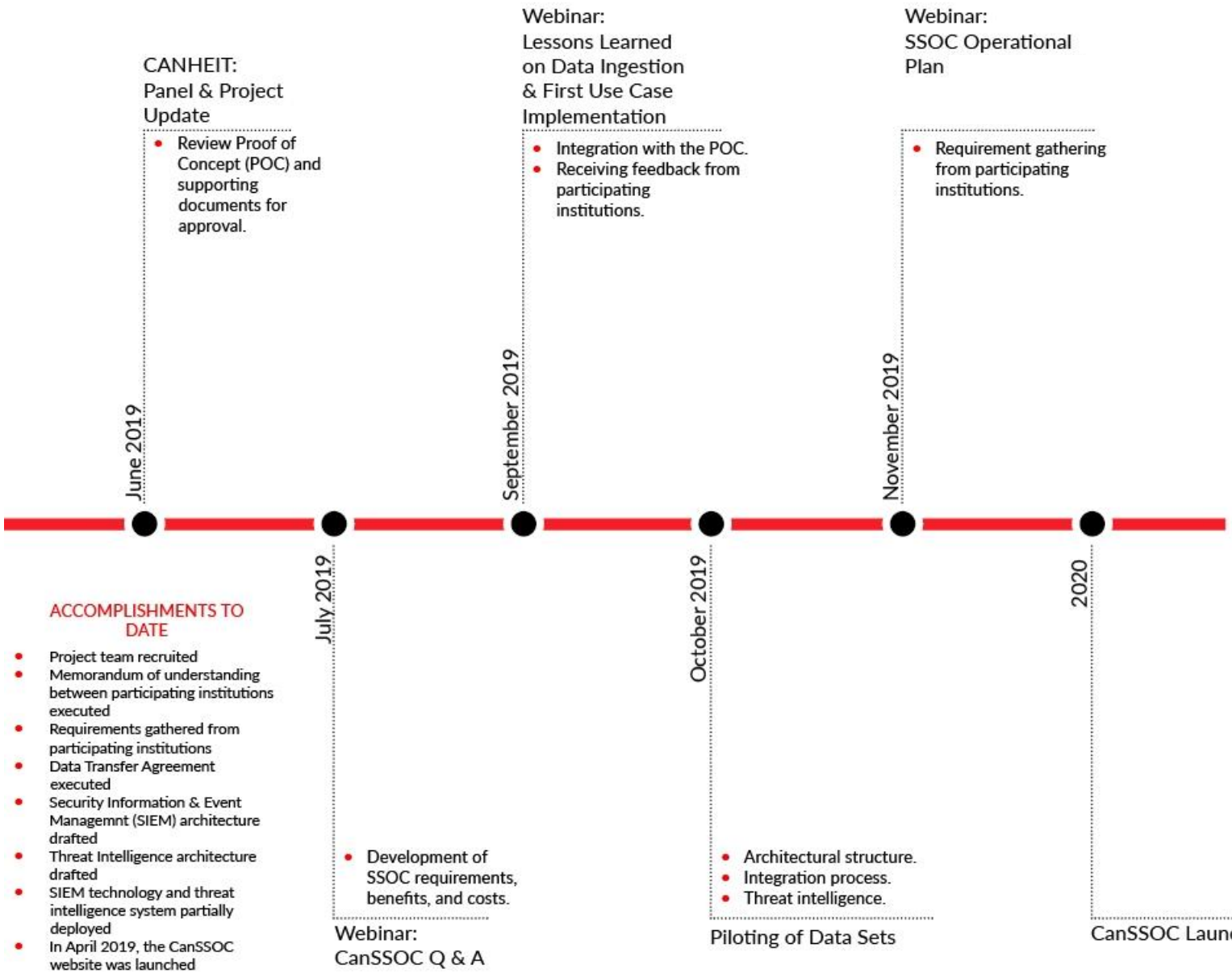
Canadian Shared Security Operations Centre (CanSSOC) is:

- A shared proof of concept project
- Based in part on a model initiated in the US higher education system
- Being pursued in partnership with six Canadian universities:
  - The University of British Columbia,
  - University of Alberta,
  - McMaster University,
  - McGill University,
  - Ryerson University,
  - University of Toronto.

- In Partnership with the National Research & Education Network
  - CANARIE – federal
  - Cybera - Alberta
  - ORION - Ontario
  - RISQ – Quebec
  - BCNET – British Columbia

Value of a shared SOC

Canadian Shared Security Operations Centre Milestones

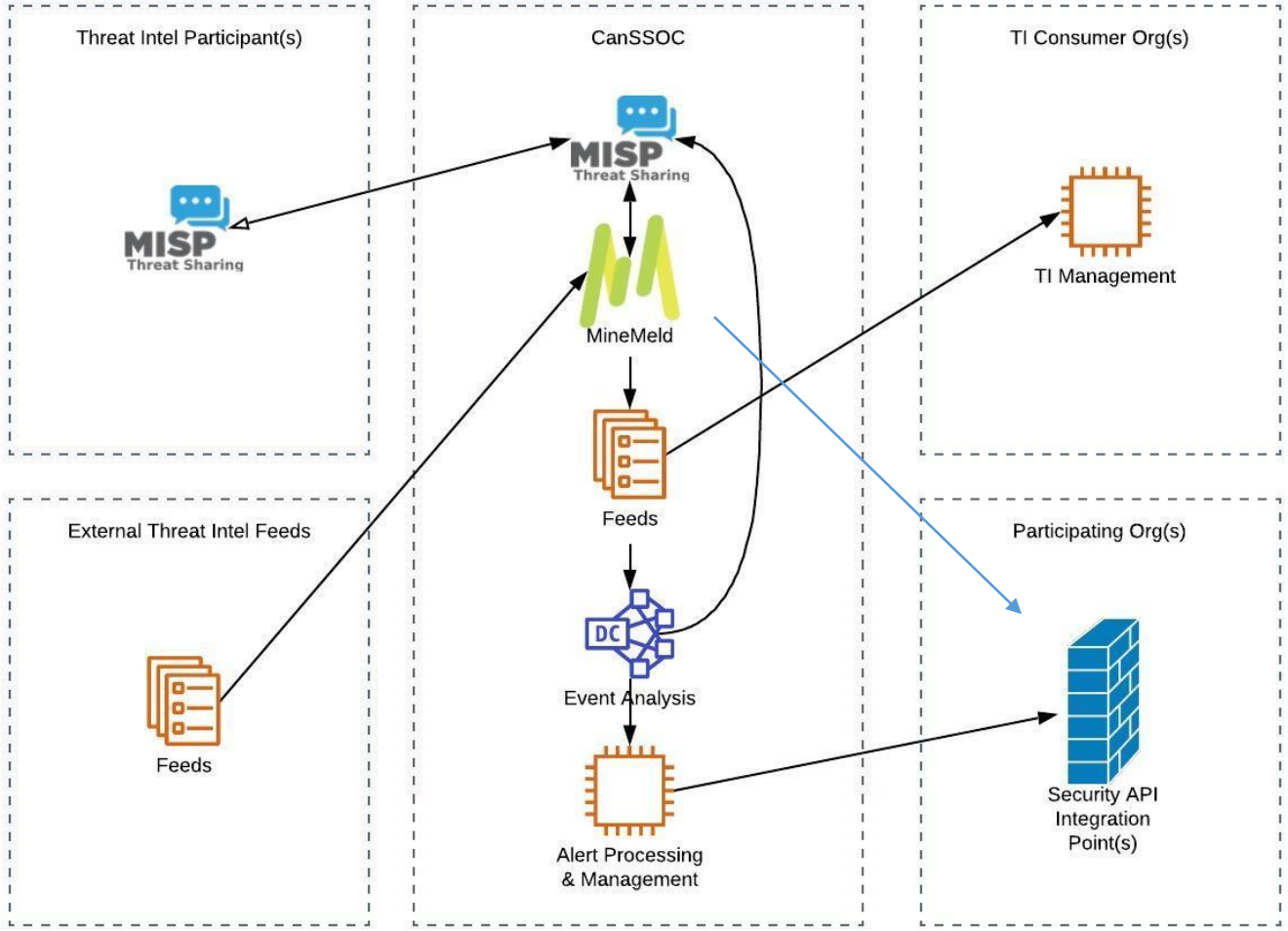


CANSSOC

POC Operational Considerations

Infrastructure	Threat Intel	Log Ingestion	Analysis	Incident Management
Hardware platform(s) On-prem vs Cloud Log collectors Events per second (“EPS”) and throughput considerations Data retention Monitoring	Identifying intel sources Curation Formatting Indicator of Compromise (“IOC”) sharing Intel back to SOCs & ISACs	Location log inventory Baseline of log sources Log schema Deploying log collectors	Alerting based on known IOCs Asset identification for prioritized alerts Alert volume & risk appetite **Real time analysis**	Alerting mechanism (email, ticketing, API, etc.) Incident tracking How to get updates Incident resolution & disposition Location Portal / Dashboard

Proposed Threat Intelligence

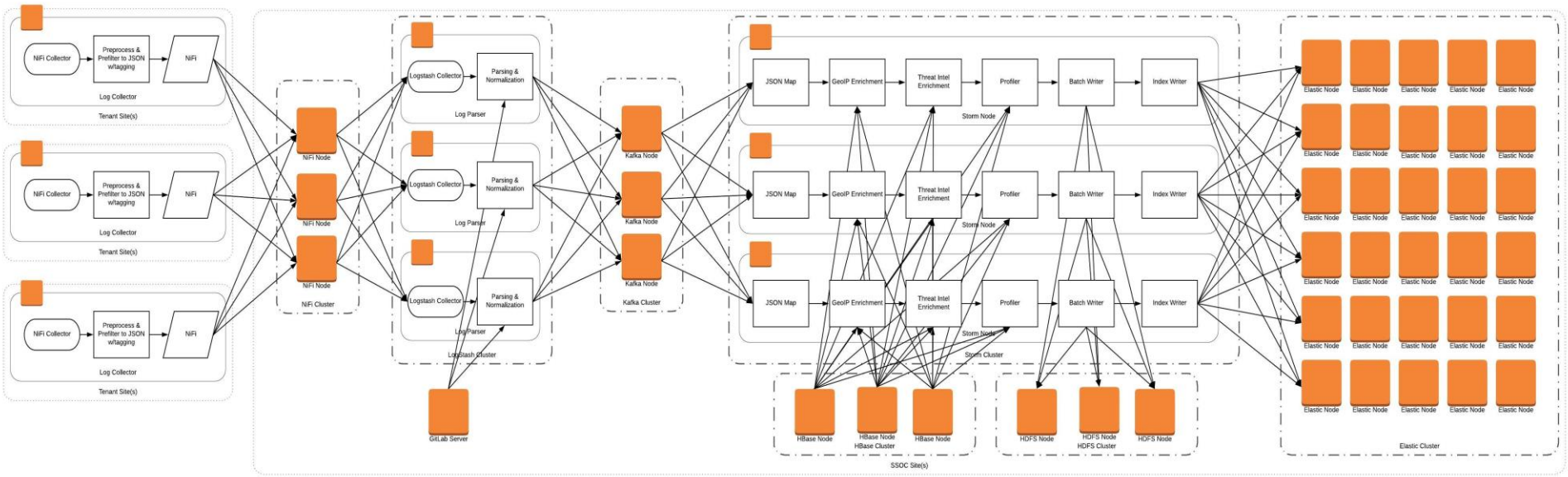


Sample Analysis Architecture

Collect

Enrich

Analyze



Normalize

Panel Discussion
and
Audience Questions

Thank you!

Stay informed and learn about the outcome of the CanSSOC Proof of Concept!

CanSSOC website: https://canssoc.ca/

Contact: CanSSOC@utoronto.ca

CANSSOC

CANHEIT-ARC 2019