BCNET 2019

Deploying a SIEM, but where do we start?

Cybersecurity Track

#BCNET2019

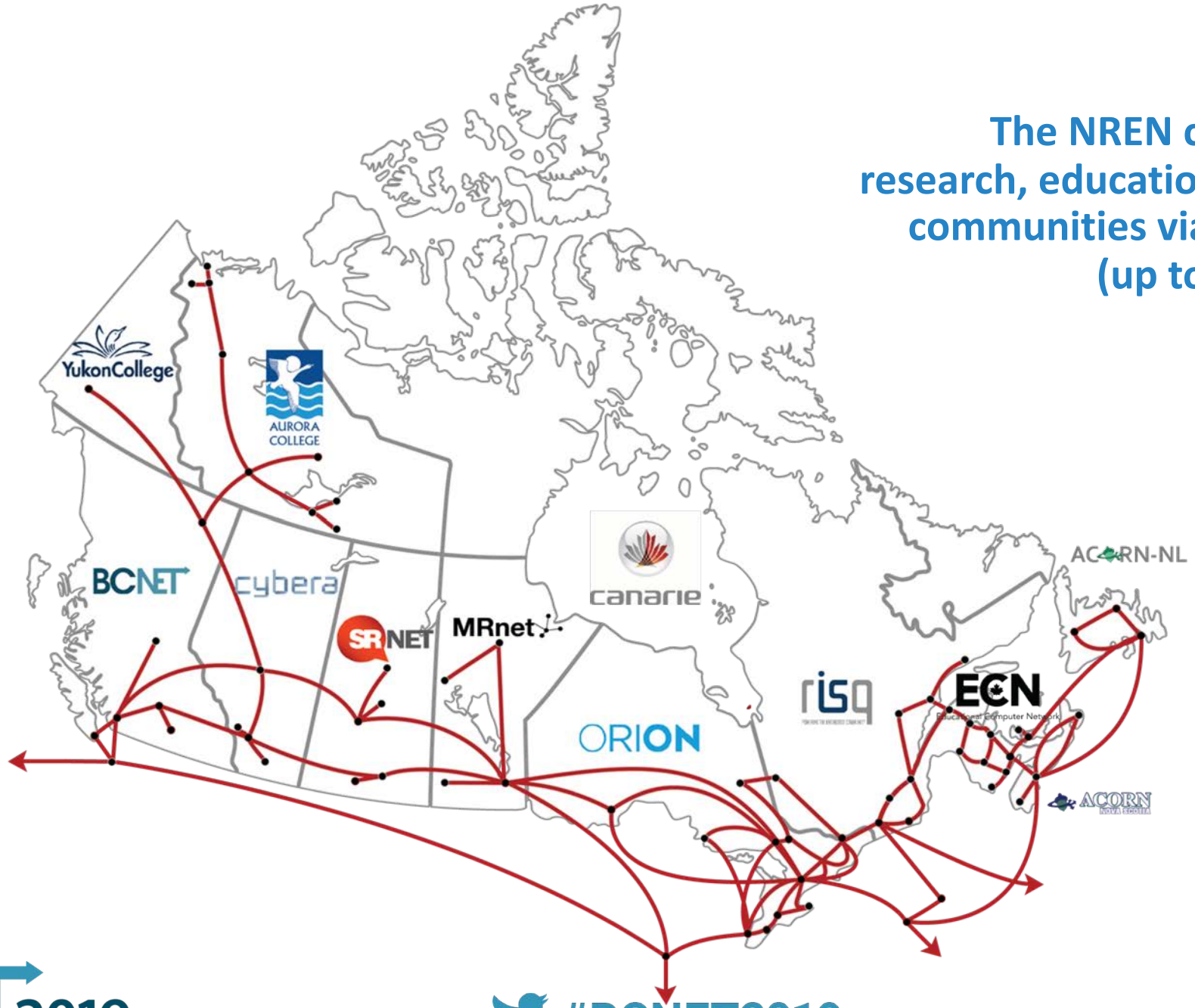
Agenda & Presenters

- NREN & SIEM Deployment Project: Jill Kowalchuk, CANARIE
- Yukon College Deployment: Blake MacIsaac
- Cybera Deployment: Andrew Klaus
- BCNET Deployment: Alex Doradea-Cabrera
- Questions

The National Research and Education Network (**NREN**)
is an **essential collective of infrastructure, tools and people** that bolsters Canadian leadership in research, education, and innovation.

CANARIE and its twelve provincial and territorial partners form Canada's NREN. **We connect Canada's researchers, educators, and innovators** to each other and to data, technology, and colleagues around the world.

The NREN connects Canada's research, education, and innovation communities via ultra high-speed (up to 100G) networks.



BCNET 2019

#BCNET2019

The NREN makes access to global research instruments and vast data stores seamless so that distance is irrelevant.

- 30 Metre Telescope
- Large Hadron Collider
- Canadian Light Source

- Genomics Databases
- Neptune 2.0
- Global sensor networks

Hackers beat university cyber-defences in two hours

By Sean Coughlan
BBC News family and education correspondent

4 April 2019 Share

The attacks were able to get through the cyber-security defences

A test of UK university defences against cyber-attacks found that in every case hackers were able to obtain "high-value" data within two hours.

CYBER ATTACK

Chinese Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds

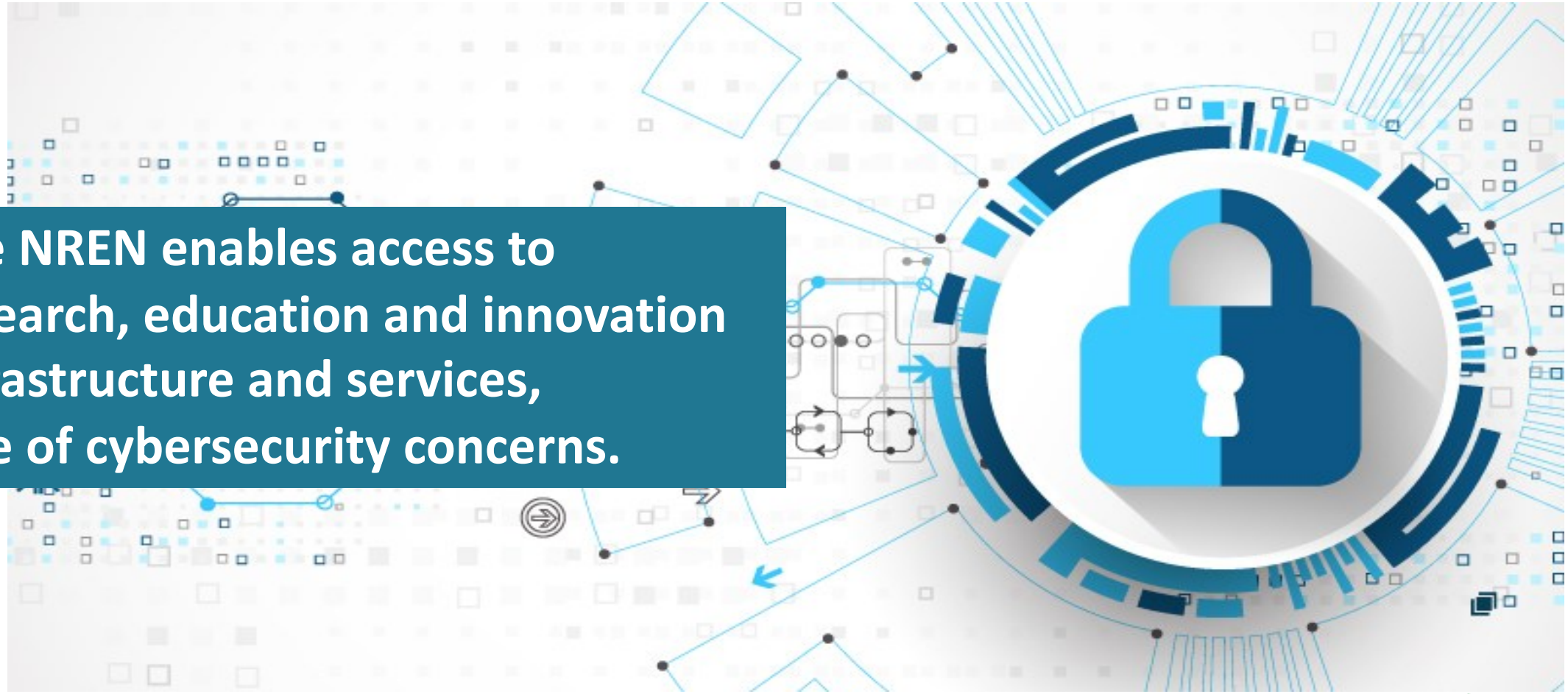
Massachusetts Institute of Technology. Yiming Chen Moment Editorial/Getty Images

By EMILY PRICE March 5, 2019

Chinese hackers have started targeting universities in an effort to uncover maritime technology that is being developed for military use, a new report finds.

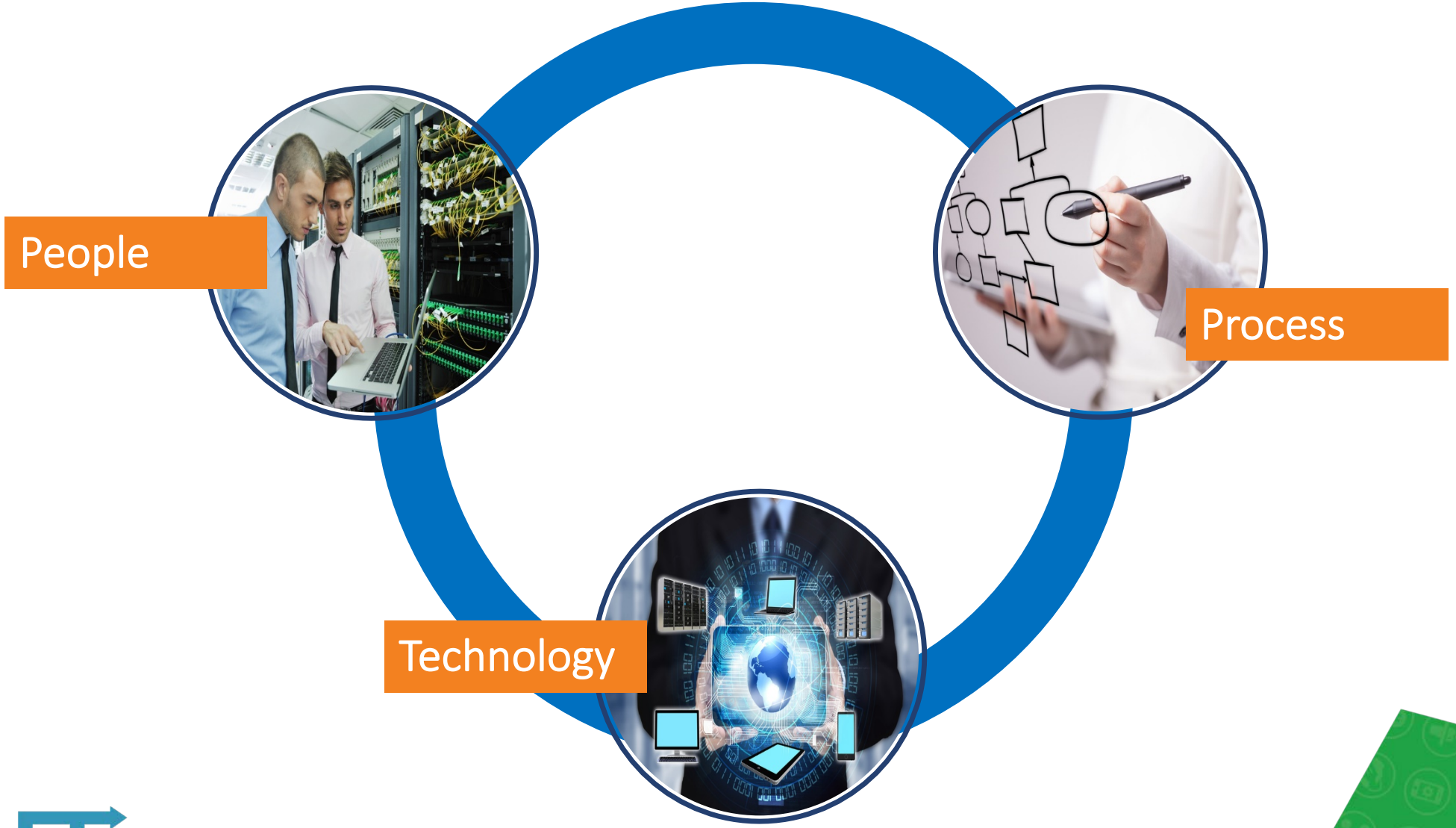
The report suggests at least 27 different universities in the United States, Canada, and Southeast Asia have been targeted by the attackers including the University of Hawaii, Massachusetts Institute of Technology (MIT) and the University of Washington.

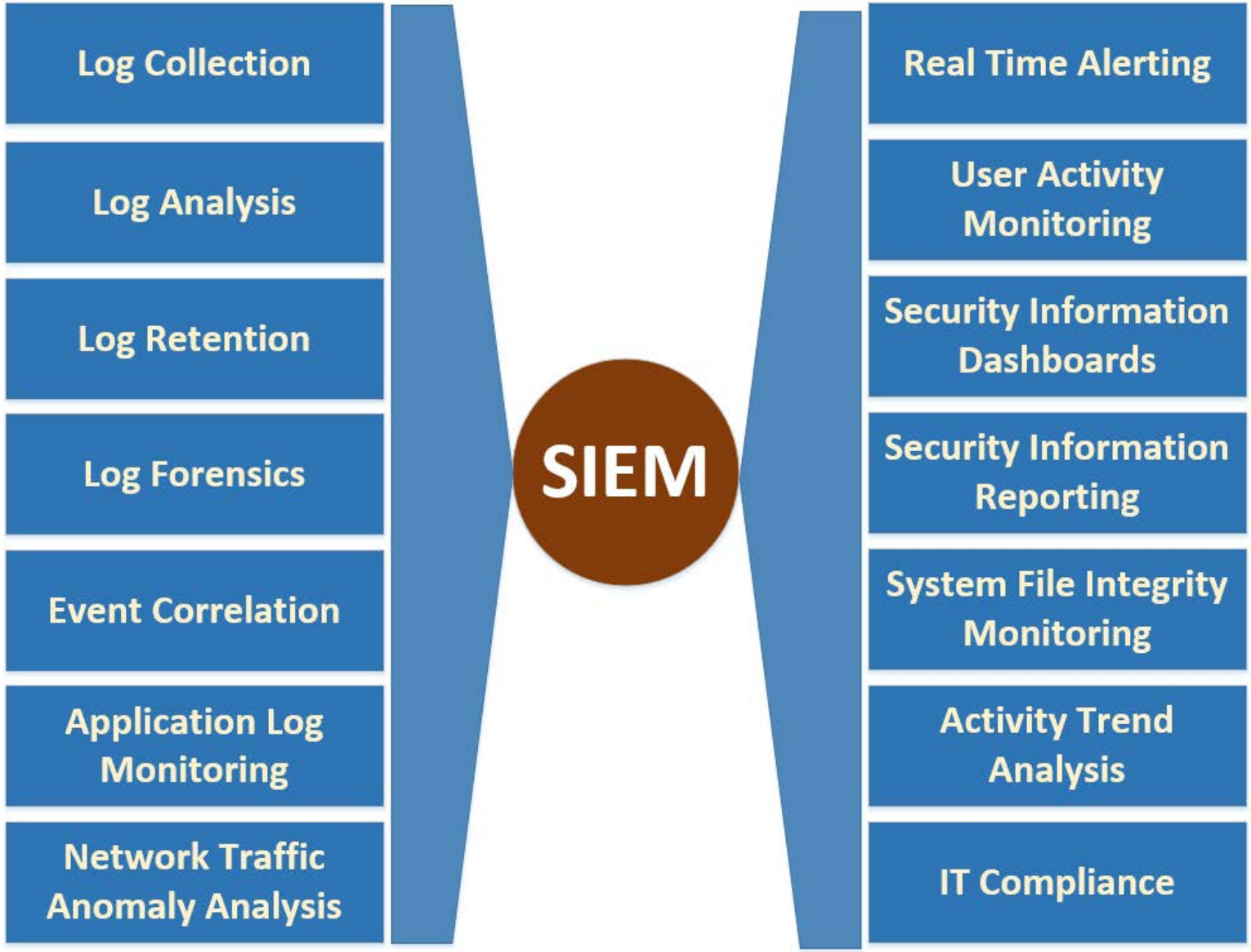
NREN Security Vision



The NREN enables access to research, education and innovation infrastructure and services, free of cybersecurity concerns.

NREN SIEM Deployment Project




Log Collection
Log Analysis
Log Retention
Log Forensics
Event Correlation
Application Log Monitoring
Network Traffic Anomaly Analysis
SIEM
Real Time Alerting
User Activity Monitoring
Security Information Dashboards
Security Information Reporting
System File Integrity Monitoring
Activity Trend Analysis
IT Compliance

#BCNET2019

BCNET 2019

Yukon College Deployment

Blake MacIssac

Yukon College

Our campuses

- Old Crow
- Dawson City
- Mayo
- Pelly Crossing
- Carmacks
- Faro
- Ross River
- Haines Junction
- Whitehorse
- Carcross
- Teslin
- Watson Lake

Yukon College SIEM Use Case

- *Tracking Internal system changes and monitoring for suspicious activity on critical systems and applications*

- *Monitoring connectivity into and out of critical network segments*

Preparing for the SIEM

- Central log collection
- Advanced audit policy configuration for Windows Servers
- Network device specific logging (i.e. tracking login success/failures, ACL Hits)
- Preparing devices to generate logs based off our Use Case
- Correlation events, rule sets and logic
- NetFlow implementation

#BCNET2019

BCNET 2019

Cybera Deployment

Andrew Klaus

RAC (Rapid Access Cloud)

- Public cloud for use within AB
- Free cloud computing resource for research
- Over 1000 active users
- Also used to host services for members

VFS (Virtual Firewall Service)

- We first hosted physical FWs for members
- This worked very well, but couldn’t scale
- VFS launched April 1, 2018
- Single, per-user instances
- First Palo-Alto, FortiGate added later
- 12 members (16 very soon)

Deployment Constraints

- Shared Data Centers (U of A + U of C)
- RAC is a publicly shared resource
- We want both in-transit and at-rest encryption
- at-rest not currently documented
- We needed to speak to FortiSIEM engineers

Netflow Collection

- Netflow is used for analyzing network traffic
- Consists of source + destination IP, ports, and protocol
- Sent in plaintext from network devices
- Netflow last hop to collector is unencrypted
  - Link and transport layer encryption not supported
- Opted for Hybrid deployment:
  - Physical collectors alongside network devices
  - Virtual collectors alongside virtualized infrastructure

#BCNET2019

BCNET 2019

BCNET Deployment

Alex Doradea-Cabrera

BCNET Network Overview

The BCNET Advanced Network directly connects 179 members in British Columbia made up of:

- Colleges
- Institutes
- Research universities
- Federal and provincial labs
- Research institution sites

The SIEM Process

Parts of a SIEM

1. SIEM governance (stakeholders, policies and guidelines)
2. Operational requirements → Security use cases
3. Data collection strategy supports detection goals
4. Define correlation rules which will perform analytics on collected data
5. Monitor, establish baselines, detect anomalies
6. Create actionable tasks → Response, or optimize SIEM

SIEM as a Tool

Our strategy, planning, and deployment

- Phases: BCNET ➡ Multi-Tenant

Challenges and opportunities

- Virtual vs hardware deployments
- Use case, scope and collection strategy
- Storage requirements
- Security framework alignment
- Security processes and operational procedures

Status Update

- Where are we now
- Next steps
- Future growth opportunities

#BCNET2019

BCNET 2019

Questions