Strength in Numbers, Exploring the Viability of a Shared SOC

CANSSOC

Gayleen Gray – AVP and CTO McMaster University
Jill Kowalchuk – Director CanSSOC and NREN Coordination Manager, CANARIE
Brian Stewart – Deputy CIO, University of Alberta
Bo Wandschneider - CIO, University of Toronto

October 16, 2019
Shared Threats

cyber-attack universities

About 15,400 results (0.26 seconds)

Cyberattacks Mar Start of Academic Year
Inside Higher Ed - Aug. 27, 2019
Two universities suffered devastating cyberattacks just before students returned to campus. Is the timing a coincidence?

Colleges and Universities at Risk for Cyber-Attacks as School Year ...
The National Law Review - Aug. 29, 2019
It's a busy time for colleges and universities as the fall semester starts and campuses are bustling with activity. It's also the perfect time for cyber...

Just in Time for Fall Term, a Cyberattack Forces an Entire College's ...
The Chronicle of Higher Education - Aug. 16, 2019
Experts warn that cyberattacks are a mounting threat to colleges, whose...
"Colleges and universities have some challenges that maybe don't....

Cyberattacks targeting students on the rise: Here's how to protect your ...
CTV News - Aug. 17, 2019
Cyberattacks targeting post-secondary students are becoming... The University of Calgary was forced to hand over $20,000 to hackers after...
Do you have a Security Operations Center?

42 institutions surveyed and definitions of SOC varied in those that responded yes.
Opportunity

"Together we see more"

- Higher Ed focus
- Global profile
- Economies of scale
- Attracting talent

#EDU19
Governance and Team

Institutional Participants

STEERING COMMITTEE

DIRECTOR
CISO
Analysis Engine Project Team

McGill
Project Manager
Threat Intelligence Project Team

PROJECT TEAM
Timelines

2018
Early discussions

June 2019
Data sharing agreements signed

2019
SOC requirements and use cases

July - Sep. 2019
Threat intel and site data flowing

Oct. 2019

Early 2020
Proof of Concept Milestones

- Services
- Data, resources & staff
- Cost model
- Process for integration
- Metrics
- Delivery mechanism
- Structure
- Evaluation

#EDU19
Core Components

- Shared Security Operations Center
- Analysis Engine
- Threat Intelligence
  - Threat hunting
  - Vulnerability management
  - Red Team intrusion testing
Analysis Engine Architecture
Threat Hunting Architecture
The IT Security landscape

• Many complimentary projects happening across the Research and Higher Ed community:

**Canada**
- CUCCIO Leadership in Higher Ed IT Security
- CUCCIO Security Benchmarking
- CANARIE Joint Security Project (JSP)
- NREN SIEM project
- ORION OnCHEC (Shared CISO)

**International**
- OmniSOC
- AARNET
- JISC

#EDU19
CanSSOC Vision
CanSSOC
- AWARENESS
- THREAT INTELLIGENCE
- VULNERABILITIES
- BENCHMARKING
- USE CASES
- ANALYSTS

NREN
- MEMBER SERVICES
- SIEMS
- ANALYSTS
- ALERTING TO ORGANIZATIONS

JSP
- VISUALIZATION
- ZEEK
- ANALYSTS

CONSUMING UNIVERSITIES
ONE WAY

UNIVERSITIES W MATURE SECURITY
CAPABILITIES – TWO WAY

#EDUCASE
EDUCASE
ANNUAL CONFERENCE 2019
CAMSSOC - "Better Times"

Awareness
ThreatIntel
Vuln/Benchmarking
Use Case

Member Services

Visualization
Seek

Analyst
Analysis/Egde
Attacking

Mature Site

JSP

NRG

CanSSOC Outcomes

• a clear understanding of the best way to develop a shared national higher education SOC
• participants will have had the opportunity to explore, develop and test ways to bring together a wide range of needs, partners, technology and data
• a robust Shared Security Operations Center service model, leveraging strengths within and across Canada.
Contact Info

- CanSSOC website: https://canssoc.ca/
- Contact: CanSSOC@utoronto.ca

NOTE: This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution 4.0 International (CC BY 4.0), which grants usage to the general public, with appropriate credit to the author.

#EDU19
Session Evaluations
There are two ways to access the session and presenter evaluations:

1. In the online agenda, click on the “Evaluate Session” link.

2. From the mobile app, click on the session you want from the schedule > then scroll down or click on the associated resources > and the evaluation will pop up in the list.