BCNET 2019

SIEM Before You Buy

Cybersecurity Track

#BCNET2019

Agenda

- Introductions
- Why a Security Information and Event Management (SIEM) system?
- Use Cases: the good, the bad, the ugly.
- SIEM Governance.
- What we wish we had known before buying a SIEM?
- SIEM Future State.

Participants

- Larry Carson, Associate Director, Information Security Management
- Jill Kowalchuk, NREN Coordination Manager
- Hugh Burley, Director Information Security/Information Security Officer
- Glenn Davies, Manager, IT Services
- Alex Doradea-Cabrera, SIEM Systems Administrator, BCNET

#BCNET2019

BCNET 2019

Why a Security Information and Event Management (SIEM) system?

Some reasons for buying a SIEM

- Told it was a good idea
- The Silver Bullet solution all your security woes
- Zero Day protection
- Improve the efficiency of incident handling activities
- Compliance
- Other

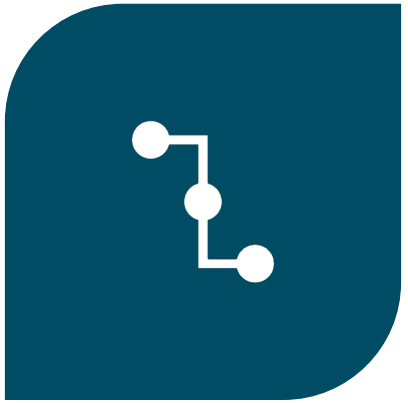
#BCNET2019

BCNET 2019

Use Cases: the good, the bad, the ugly.

Use Cases for SIEM

WHAT WERE YOUR USE CASES BEFORE YOU BOUGHT?



AFTER USING THE SIEM FOR A WHILE HOW MANY CHANGED?

DID YOU DROP ANY?

#BCNET2019

BCNET 2019

SIEM Governance

Governance Issues

Misuse of SIEM derived information.

Misuse of SIEM information by SIEM administrators.

What are you monitoring and how transparent are you about it? Should you be?

Auditing the SIEM function.

#BCNET2019

BCNET 2019

What you wish you had known before buying a SIEM?

The Things you wish you knew

LONG TERM COMMITMENT

RESOURCE INTENSIVE

RETENTION POLICY

ABILITY TO GET TRAINING ON THE SYSTEM

THE QUOTE WAS RIGHT FOR THE JOB

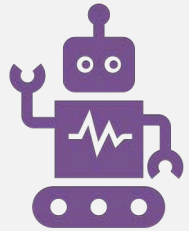
#BCNET2019

BCNET 2019

SIEM Future State

Future of SIEM

MULTI-INSTITUTIONAL COLLABORATION



ARTIFICIAL INTELLIGENCE

Questions for the Panel