BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Emergency Response for Cybersecurity, **When** You Get Attacked

BCNET CONNECT

Distributed Cyber Security Incident Response Team

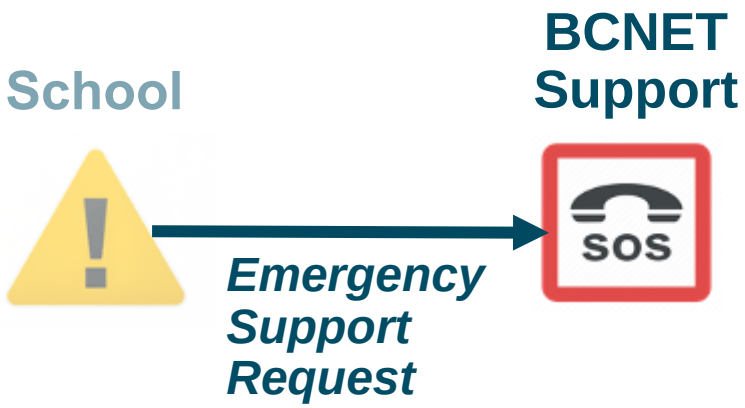
What is it?

Formation of an Incident Response Team

School

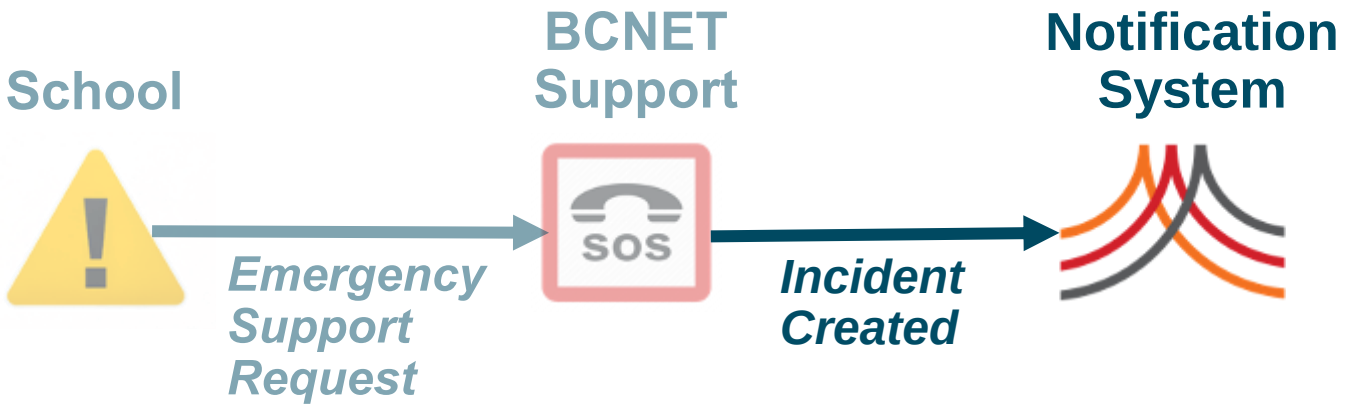
BCNET CONNECT

Formation of an Incident Response Team



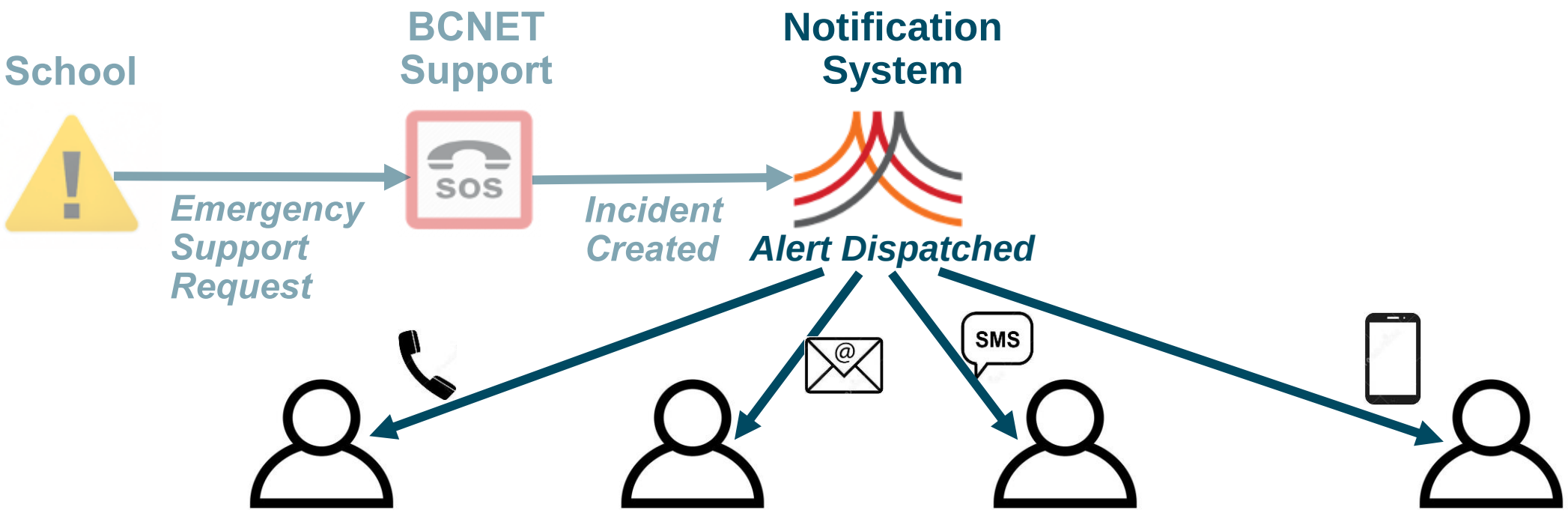
BCNET CONNECT

Formation of an Incident Response Team



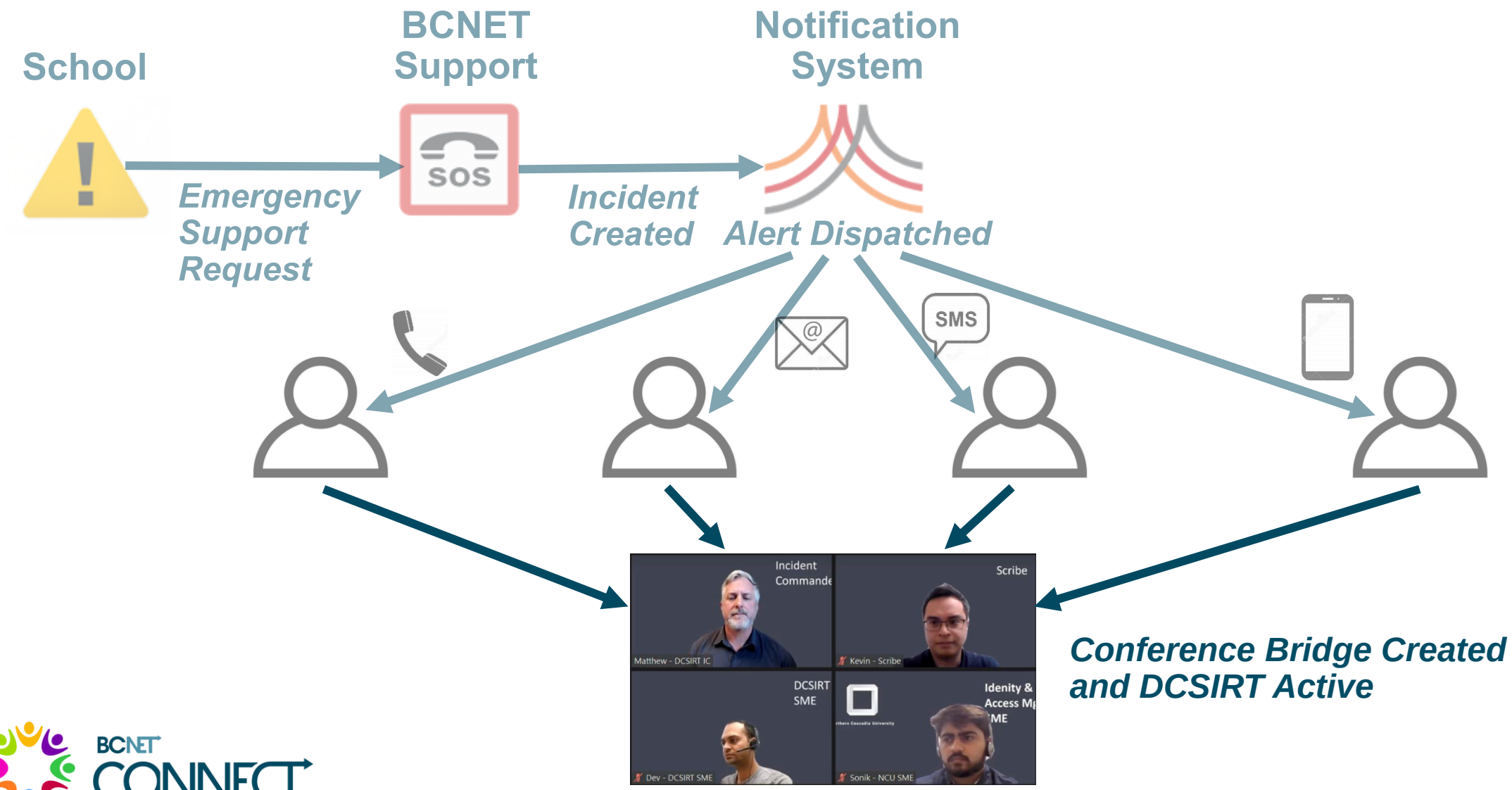
BCNET CONNECT

Formation of an Incident Response Team



BCNET CONNECT

Formation of an Incident Response Team



Conference Bridge Created and DCSIRT Active

BCNET CONNECT

BCNET CONNECT

Training

Incident Management Training

What is it:

- FEMA-based Incident Management System (IMS)
- IMS system, Practice Drills and Exercises
- Mechanics and framework for responding to emergencies
- Focusses on Interpersonal skills of leadership under adverse conditions
- **Can be applied to any incident (Cybersecurity, IT Operations, Infrastructure, EOC)**

Who delivers it:

- Blackrock 3 Partners https://www.blackrock3.com/
- Deep global experience in Incident Management and Critical Infrastructure
- Market Leader in IMS for IT

Incident Management Training

Who should attend:

- IT and Security Leadership, Managers, Team Leads
- Institutional Communications
- IT and Security Subject Matter Experts
- Risk Management
- ***Anyone*** who may be involved in an incident or crisis

Costs:

- ***Free*** for BCNET institutions !!
  - Funded by the Ministry of Advanced Education and Skills Training.

BCNET CONNECT

Incident Management Training

Incident Command Level 1 (IC1)

Over 300 participants from 25 institutions already enrolled

Practice Drills

Coming May-June!

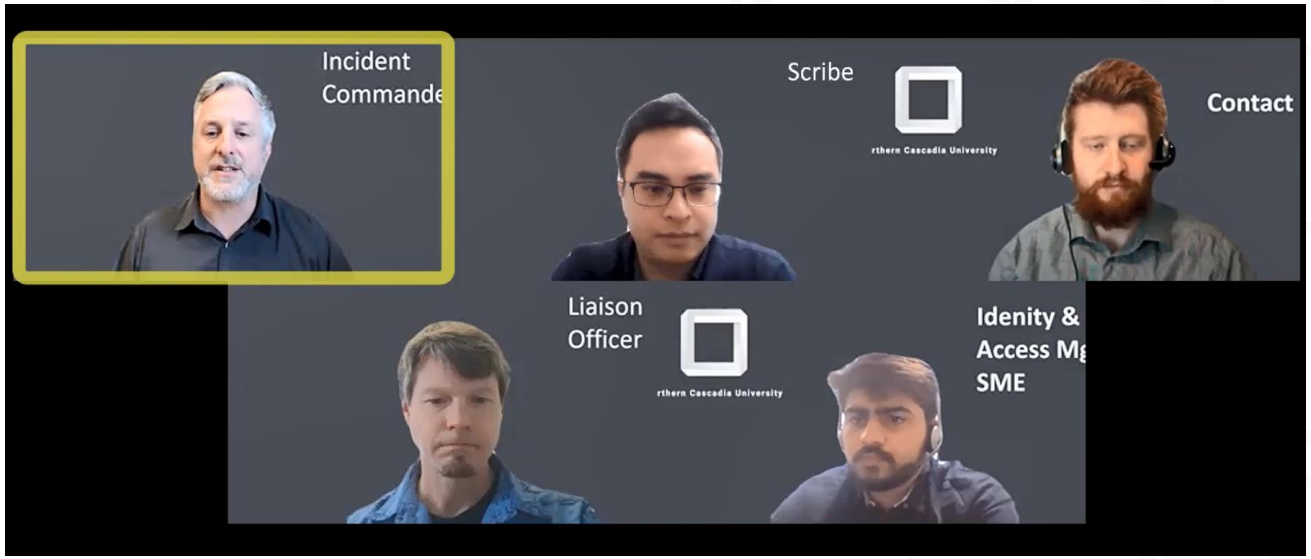
BCNET CONNECT

Example Incident: Video David

Intro: DCSIRT Log4j Incident Video

- " Under-The-Hood " view of how an incident is managed
- ~7 minutes

- Bridge
- Roles
  - IC, LNO, Scribe, SMEs
- CAN Report
  - Conditions, Actions, Needs



BCNET CONNECT

DCSIRT Incident
Log4J Vulneravility

Debrief: DCSIRT Log4j Incident Video

- Communication
  - IC Roles, not names
  - Brief, Succinct, Direct
  - Actions acknowledged for clarity
- Bridge
  - People join/leave as needed. (LNO, SME's)
- School/DCSIRT
  - DCSIRT assisting, School authorizing action
- IMS Roles vs Business Roles
  - e.g. CIO does not command the Incident Response

BCNET CONNECT

BCNET CONNECT

Q & A / Discussion