BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Don't Forget Your Toothbrush:

Cybersecurity Preparedness Toolkit

Speaker Corner

Antonio Brandao

SIEM Administrator

Cybersecurity professional and military veteran skilled in threat hunting with experience in risk assessment and mitigation. Combines military discipline with technical expertise to provide effective cybersecurity solutions.

Alex Doradea-Cabrera

Cybersecurity specialist

15 plus years of experience from network technician to cybersecurity specialist. My why consists of implementing cybersecurity initiatives that make a positive and lasting impact. Life learner.

Background - Antonio

- **Military**
  - prepared for the unexpected
  - remain focused
  - ready to respond at a moment's notice

- **Cyber**
  - minimizing damage
  - protecting the organization's assets
  - incident response kit
  - well-defined incident response plan
  - stay vigilant and constantly monitor the situation

Incident Response Training

- Incident Management System (IMS)

- Four basic positions
  - Incident Commander (IC)
  - Liaison Officer (LNO)
  - Scribe
  - Subject Matter Expert (SME)

CAN Report

- Communication is a critical aspect of the IMS
- CAN stands for
  - Conditions - what is happening.
  - Actions - what actions are being taken
  - Needs - what resources are needed
- Making informed decisions based on the information available.

Making the call is not about making quick decisions.
It's about making the right decision in the shortest amount of time.

Conditions

- At 0900 PST customer reported loss of a monetary discount from their mobile account.

Actions

- Business consultant to confirm if related to customer bill cycle renewal. Engineer to investigate if any patches applied in last 48 hours. Developer to Review logs from last 24 hours for errors.

Needs

- Configuration team to confirm if price plans have not changed in the customer environment in past 24 hours. The business support team to confirm if any more customers are currently impacted.

IR Strategies and Standards

- OODA Loop
  - Observe, Orient, Decide, Act
- NIST SP 800-61
  - preparation, detection and analysis, containment, eradication and recovery, and post-incident activity
- SANS
  - Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned

Situational Awareness

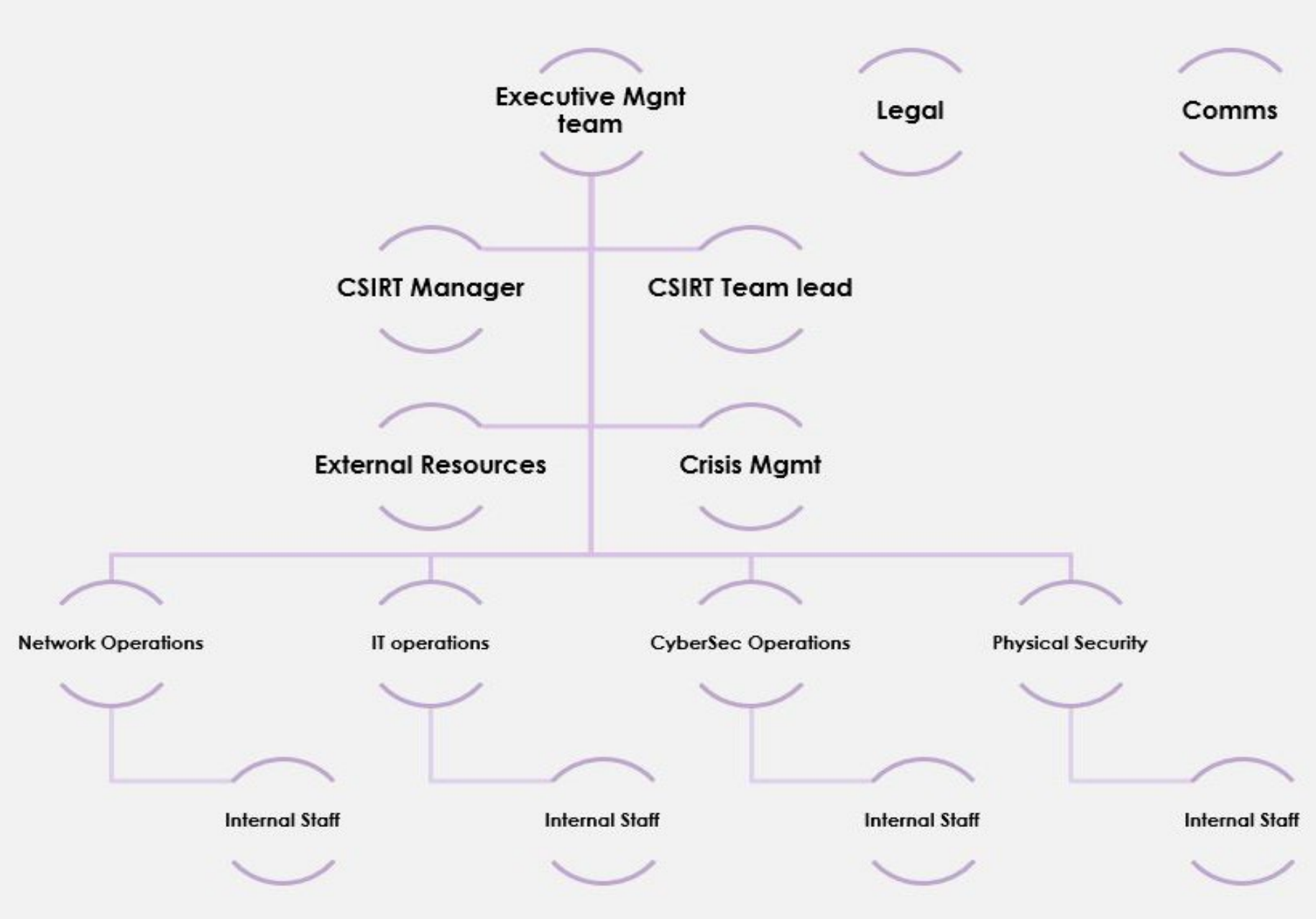
“understanding an environment, its elements, and how it changes with respect to a time vector or other factors, is critical for appropriate and optimized decision making in many environments”

The formal definition :

1. Perception of the elements in the environment
2. Comprehension or understanding of the situation
3. Projection of future status

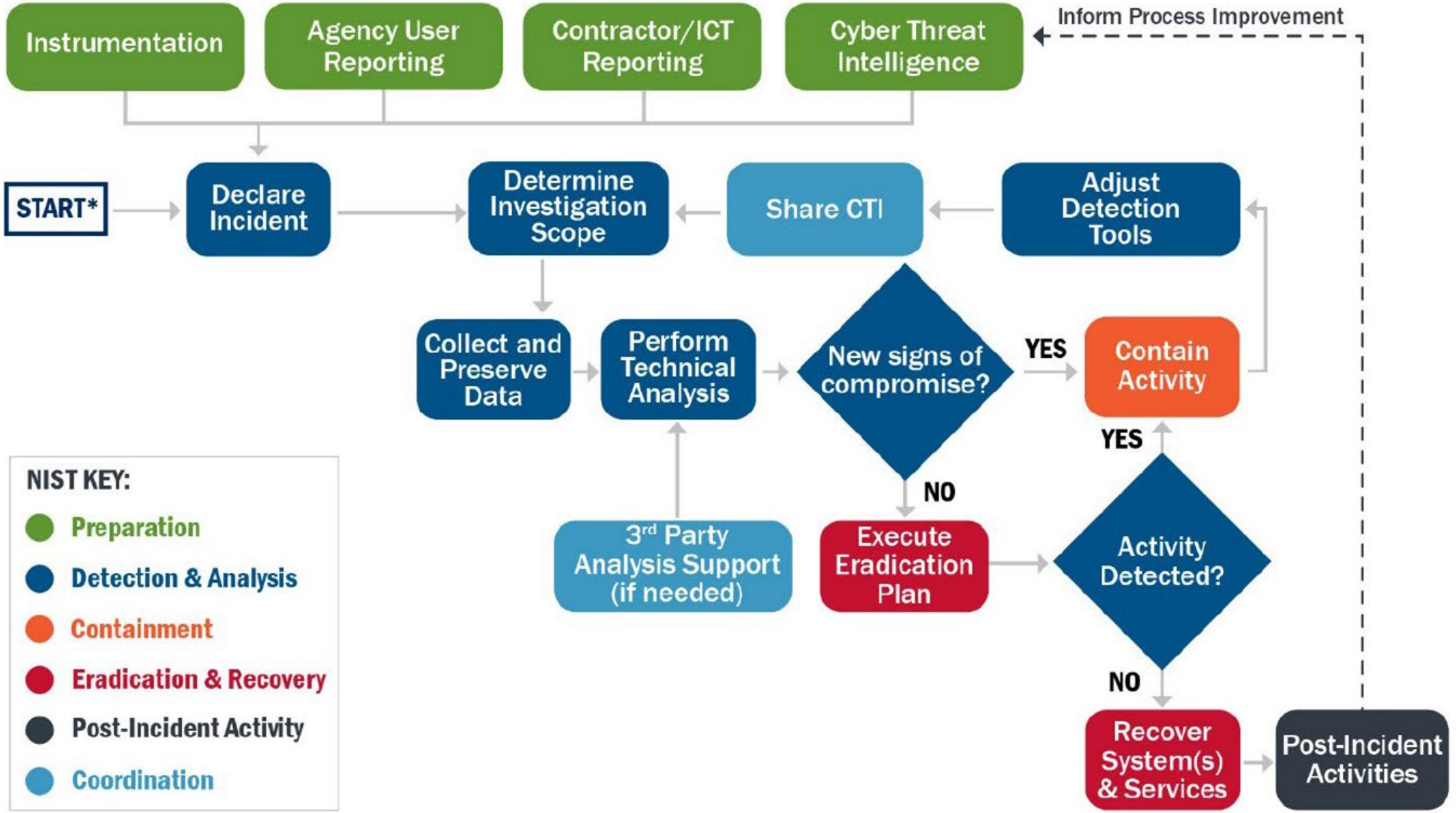
https://en.wikipedia.org/wiki/Situation_awareness

Incident Response Command Structure



BCNET CONNECT

CISA IR Playbook Flow



BCNET CONNECT

Don't Forget Your Toothbrush:Cybersecurity Preparedness toolkit

https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

What to include in your Go-Bag

Key Components:

- Hardcopies of your incident response plan, policies and procedures.
- Security Team and escalation /executive contact information
- External contacts (CANSOC, OIPC,CCCS,RCMP etc)

- Laptop, mouse, roll up keyboard, varying ethernet cables
- Portable Kali (https://www.kali.org/)
- Storage drives, a few portable USB drives
- Console cables
- Mobile Wi-Fi hotspot
- Note pad, pens

Tying it all together

Responder mindset:

- Stay calm
- Maintain lines of communications
- Track and record all actions
- Ask for assistance

Preparedness :

- Contacts for vendors, critical business partners, Internal /external responders
- Evidence preservation tools for possible legal actions
- War Room for central communication and coordination
- Secure storage facility for securing evidence and other sensitive materials
- Tools and quick reference guides
- Snacks and beverages

“By failing to prepare, you are preparing to fail.”
— Benjamin Franklin

Where to start :

- Know your role in the organization
- Understand your technology stack
- Review your response plans, security policies and standards
- Coordinate with BCP, DR and emergency response
- Maintain an updated contacts and escalation list
- *Practice, Practice, Practice*

BCNET CONNECT

Raffle Time !!

Cybersecurity Go bag : Bill of Materials

- Multiple Storage (2X 1TB storage, 5 X 16G USB sticks)
- IR Software and Tools (Portable Kali instance)
- Cables and Adapters
- Mobile Wi-Fi Hotspot
- Reference Manuals (PTFM)
- Sample Incident response plan, Contacts
- Notebook, Pens
- Beverages & Snacks
- Personal Hygiene (toothbrush)

Questions ?

References

- This slide deck
- GREN Incident response template
- Sample Bills of materials

- Kali (https://www.kali.org/)
- OIPC Privacy Breach Guides
- CIS Incident response policy, Awareness
- SANS reference templates
- InfoTech reference materials
- CISA reference materials- IRP
- Canadian Center for Cyber Security