BROT – BREACH RESPONSE in OPERATIONS TECHNOLOGY

NIST SP 800-61+82+Experience

Further Investigation (OODA Loop)

✗

DETECTION & ANALYSIS

Is this an Incident?

- Corporate Policy Violation (SRP & CIA)
- Breach (cyber-attack, malware*, intrusion)

✓ Activate the Cyber War Room & Perform BIA (Business Impact Analysis)

- Control Eng'ng
- OT Risk Management

CONTAINMENT

Is there a BCP & DRP?

- Contingency plan
- 3211 Rule

✗ Seek approval for Containment based from BIA

✓ Activate the BCP/DRP and proceed to Containment

ERADICATION

Perform Forensics

- NIST SP 800-86

+ IOC Extractions & APT Attributions

+ Compromise Assessments & Patching

RECOVERY

Business As Usual

+ ICS/SCADA/OT

- Safety and Availability
- Reliability
- Productivity

+ Data in IoT*s

- Confidentiality
- Integrity
- Availability

POST-MORTEM

Root Cause Analysis

+ Threat Modeling (Mitre - ICS) & Risk Registry

+ Defense-in-Depth & Cyber Resilience