On the

RV Sikuliaq

Cyber Training Cruise


OmniSOC
The Higher Education & Research
Security Operations Center

Mike Simpson

- **CISO for ARF**
- Senior Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - Cybersecurity Program Development & Strategy
  - Network Security
  - Digital Forensics
  - Network Penetration Testing
  - Physical Security

Mikeal Jones

- **Leads CRMP / Compliance Documentation initiative**
- Security Analyst at OmniSOC
- 20+ years of experience in IT / Cybersecurity
- Areas of expertise:
  - IT Operational Strategy
  - Cybersecurity
  - Systems Architect + Admin

UAF - R/V Sikuliaq Cruise of Opportunity - April 2024

Definitions:

- Security Exercises:
  - An exercise or drill designed to test or discover information about how policies, procedures, systems and resources function under simulated real-world circumstances.
    - Tabletop Exercise
      - Walk through of a hypothetical real-world situation for testing policies, procedures and resources.
    - Live Exercise
      - Exercise conducted using real systems and resources. Higher risk, but proves procedures work as intended.

Definitions:

- Our definition of Cyber-Incident drill:
  - A tabletop exercise with key live elements
  - Recommended live elements:
    - Initial discovery
    - Communications between key stakeholders
    - Others depending on the exercise’s focus or goals

Benefits of conducting Cyber-Incident Drills:

- High ROI - time required to run exercises is a great investment towards good responses to real incidents.
- Decisions are made on assumptions; exercises test those assumptions revealing how much truth or falseness is behind them.
- Find gaps or inaccuracies in policies and procedures.
- Build 'muscle memory' with IR procedures

Want to learn more? Want to learn how these work?

Come to our training this Friday afternoon!

Cyber Incident Drill on R/V Sikuliaq

Exercising and Improving Incident Response Plan

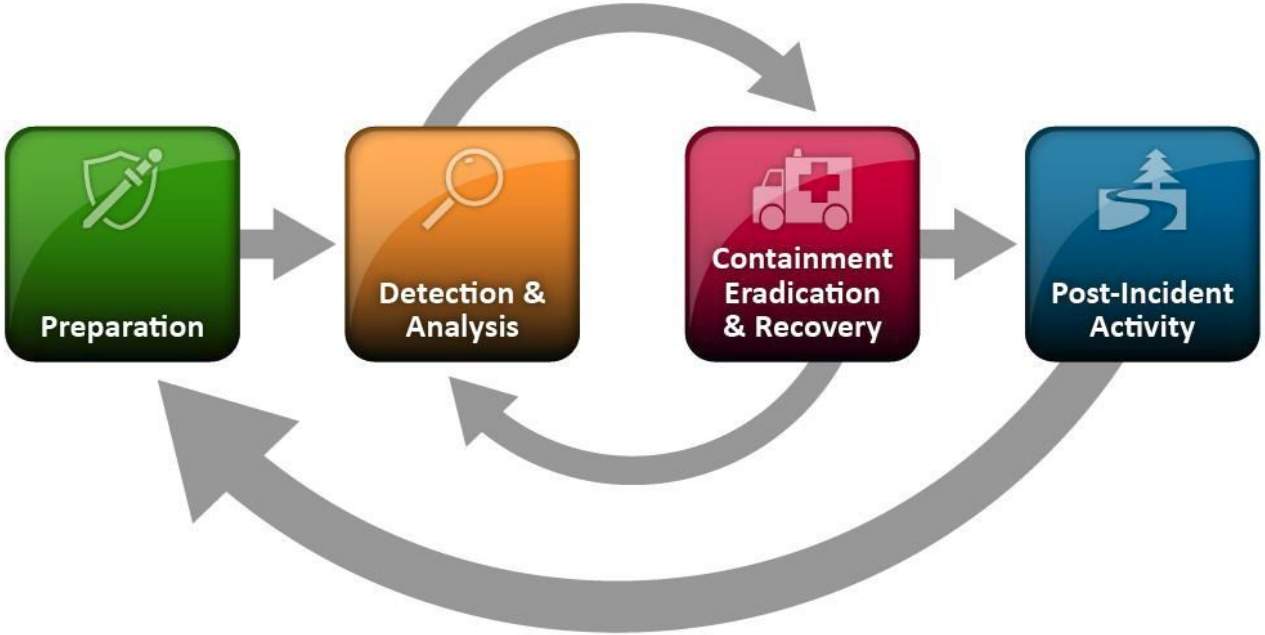


Image: NIST

Cyber Incident Drill on R/V Sikuliaq

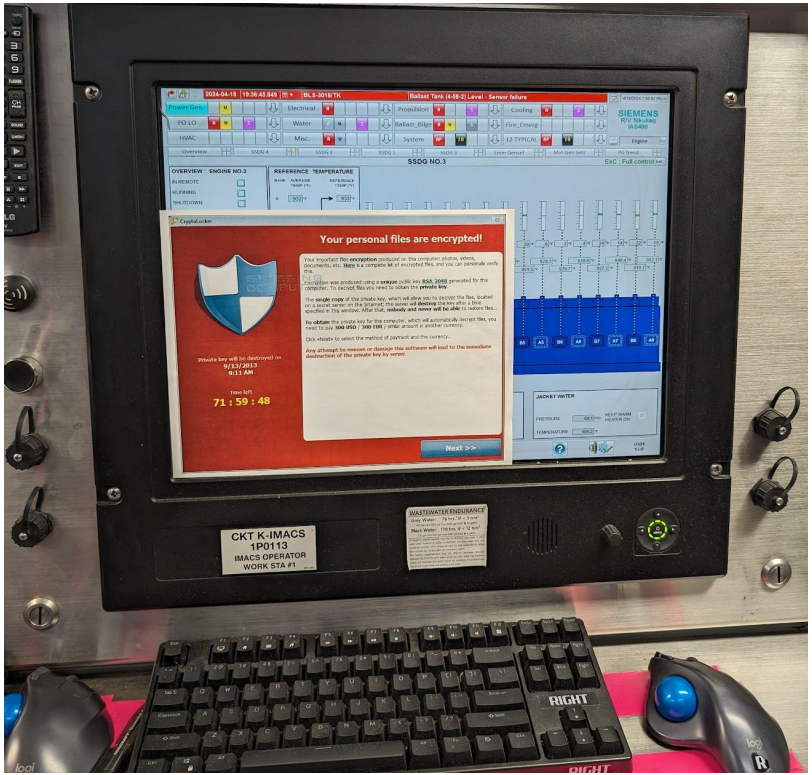
Simulated Issue to Exercise an Organization’s Incident Response

- Impact
- Roles & Responsibilities
- Incident Response Plan
- Communication Strategies

Cyber Incident Drill on R/V Sikuliaq

Scenario:

Infected PC in Engine Control Room



Cyber Incident Drill on R/V Sikuliaq

Post-Exercise Debrief, Report, Improvement Plan

- Review the Simulated Incident
- Identify What Went Well
- Identify Areas for Improvement
- Incident Drill Report
- Plan and Implement Improvements
- Repeat

Open Discussion