Building a CSIRT
A Mission Requirement

Michael Kyle

Los Alamos National Laboratory

LA-UR 11-03224

Topics

- Laboratory Mission
- CSIRT Goals
- Plans
- Structure
- Skills
- Mentoring Model
- Tools and data acquisition
- War room methodology
- Mitigation methodologies
- Testing
- Live fire

Laboratory Mission

Our Vision

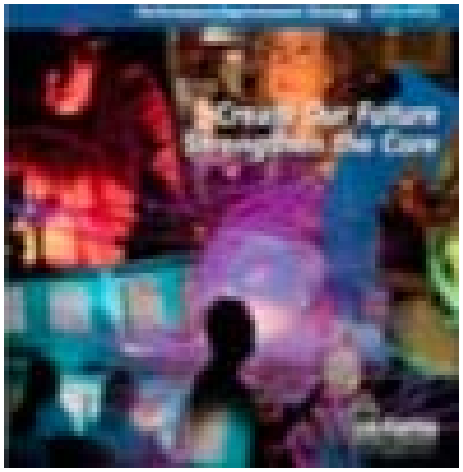
Los Alamos National Laboratory is the premier national security science laboratory.

Our Mission

We develop and apply science, technology, and engineering solutions to:

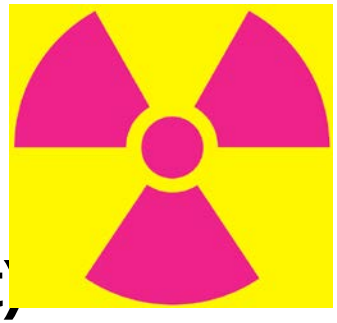
- Ensure the safety, security, and reliability of the U.S. nuclear deterrent,
- Reduce global threats, and
- Solve emerging national security challenges.

You can read more about the Laboratory's vision, mission, and values at the Performance Communication Center.



CSIRT Mission

- **Support the mission of the lab**

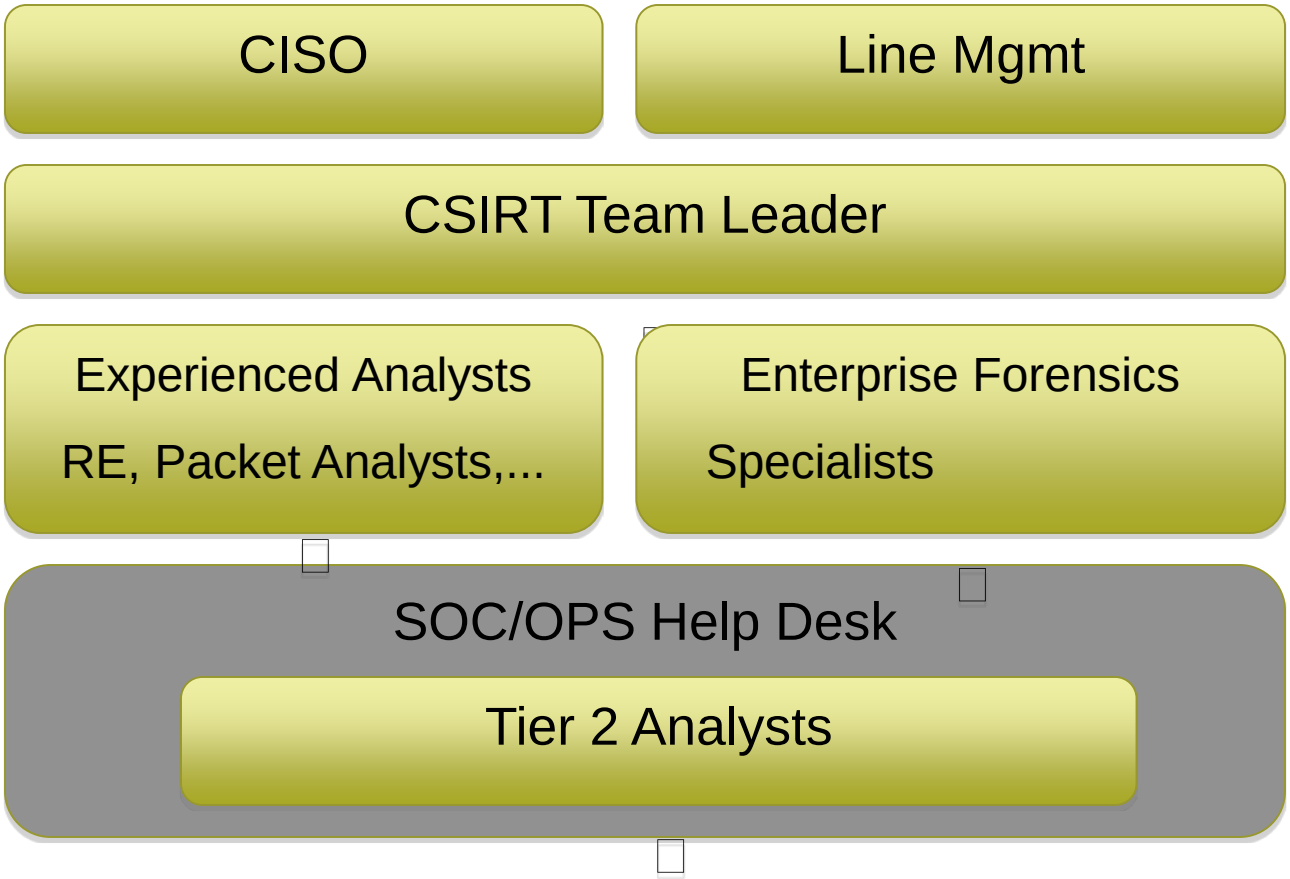


- **Nutshell (not a mission statement)**
  - Minimize likelihood that an event will affect the lab.
  - Minimize the mission impact when an incident does occur.
  - Maximize speed in which we return to normal operations.
  - Learn from events in order to (sometime antithetical)
    - Reduce costs of managing an event
    - Increase quality of response when an event occurs

Planning a CSIRT: Topics To Plan

- **Keep the business mission in mind…**
- **What services will the CSIRT be providing (beyond classic cert functions)**
- **What CSIRT structure will work best for this service model**
  - Sources: NIST 800-61, CMU, numerous trade texts
    - Most fall woefully short of an operational effort
- **Development Plan**
- **Staffing Plan**
- **Incident Response Plan**
- **Test Plan**

Structure: A Standing CSIRT



Daily SOC/OPS roles

- **Help desk (8-5)**
  - **Phone support**
  - **Email Support**
  - **General User Support Tickets**
- **Routine Intel Ingest**
  - **DOE-CIRC/CTFO (high value)**
  - **US CERT**
- **Tools**
  - **Phishing, IDS, …**
- **24x7 pager**

DOE-CIRC
CTFO

Escalation Support

- Senior personnel
- Handle escalation on issues from Tier 1-2 support personnel
- Have individual areas of expertise
- Have some generalization
- 24x7 pager

Team Leader

- **Leader and Manager**
- **Experienced both inside and outside the complex**
- **Technical background**
- **Planning**
  - Strategic goals and milestones
  - Budget
  - Supervision
  - Communication and politics
- ***Mission perspective***
- **Versed in risk methodologies**

Skills

- **T1 Help Desk/Customer Service**
- **T2 General Analyst, searching for known bad data, responding to routine events, routine intel ingest (USCERT, DOE-CIRC), tuning IDS alerts, writing log rules and IOCs, …**
- **T3 --- What we really need!**
  - Malware Analyzers
  - Reverse Engineers
  - Network Packet Analysts++
  - Enterprise Forensics engineers
  - Programmers
  - Preferably high-end system or network administration experience, too.
  - Classified Intelligence Collectors

Mentoring Model: Training from Within

- **Money for training is exceptionally slim**
- **We hired experts, let's use our experts**
  - Each senior contributor has been required to provide an outline for either 1-1 or small classroom oriented training
    - Training includes pedagogical objectives and exercises
  - Individuals match up for a required training window
  - In some instances individuals are 'certified' before granting significant accesses (e.g., encase)

Tools and Data Acquisition

- **Log Aggregation**
  - Indexed
  - Rapid searching
  - Rule writing
  - Statistical Analysis/Profiling
- **Tap Aggregation**
- **Flow Generation and Capture**
  - Indexed, …
- **Full PCAP where possible**
  - Indexed, ….
- **Enterprise Forensics**
- **Enterprise IR**

Tool Methodology at LANL

Slide intentionally left blank

A War Room Methodology

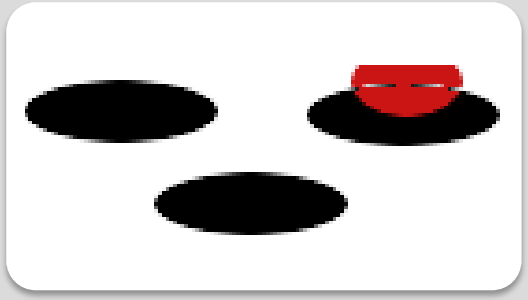
- **Virtual Servers**
  - Preconfigured Windows IR images
  - Preconfigured Unix IR images
- **Zero Client Server(s)**
- **Zero Clients**
- **IR Kit contains all pieces required to set rapidly set up war room**
  - Tested (very important)

Incident Roles

- **Out of Room**
  - CISO, Line Management
  - Incident Commander – manager in charge
- **In Room**
  - Incident Coordinator
  - Incident Communications Liason
  - Incident Responders
    - Forensics Specialists
    - Reverse Engineers
    - Malware Analysts
    - Network Packet and Traffic Analysis
    - Generalists
    - Whatever skill is needed

Incident Management Cycle

Mitigation Time



Too early and we play whack-a-mole

Strike Zone

Too late and we lose the farm

Mitigation (containment)

- **Too Early**
  - We don't know enough C2 to fully interrupt channels
  - We don't know all hosts that are internally affected
  - We will chase the problem killing individual infections for months
- **Too Late**
  - Massive exfil of sensitive data has already occurred
    - Exfil of lame information …. Who cares? Reputation, Reporting…
  - Nothing left to contain
  - Fully entrenched
- **Strike Zone**
  - Believe we have characterized the C2
  - Have found all hosts using C2 (beachheads)
  - Have found all hosts touched by beachheads
  - Block everything, C2, beachheads, tertiary hosts

Communications

- **Communications Liaison**
  - IT Groups
  - Distributed Security Personnel
  - Requisite Omitted Middle Managers
- **Briefings**
  - Once a day
  - Senior Leaders
  - By Incident Coordinator and Team Leader
- **Daily Summary Report**
  - Incident Coordinator
  - Suitable for DOE-CIRC communique
  - Emphasis on IOCs

Testing

- **Test Your War Room Setup**
  - How long does it take?
  - How many people?
  - Did all systems function to specification?
  - Lessons learned
- **Perform a NIST 800-84 Table Top Exercise**
  - Can your team verbally walk through an exercise
  - Lessons learned
- **Perform a Live Exercise**
  - Set up the war room
  - Move daily operations into the war room – appoint an Incident Coordinator
  - Do all tools and accesses function properly?