SAND2007-7227C

Integrated Network Security and Reliability Center (INSRC) and Cyber Enterprise Management

Todd Bruner
4318 CEM Development Project Lead
Cyber Infrastructure Development and Deployment
March 21, 2007

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

In the Beginning

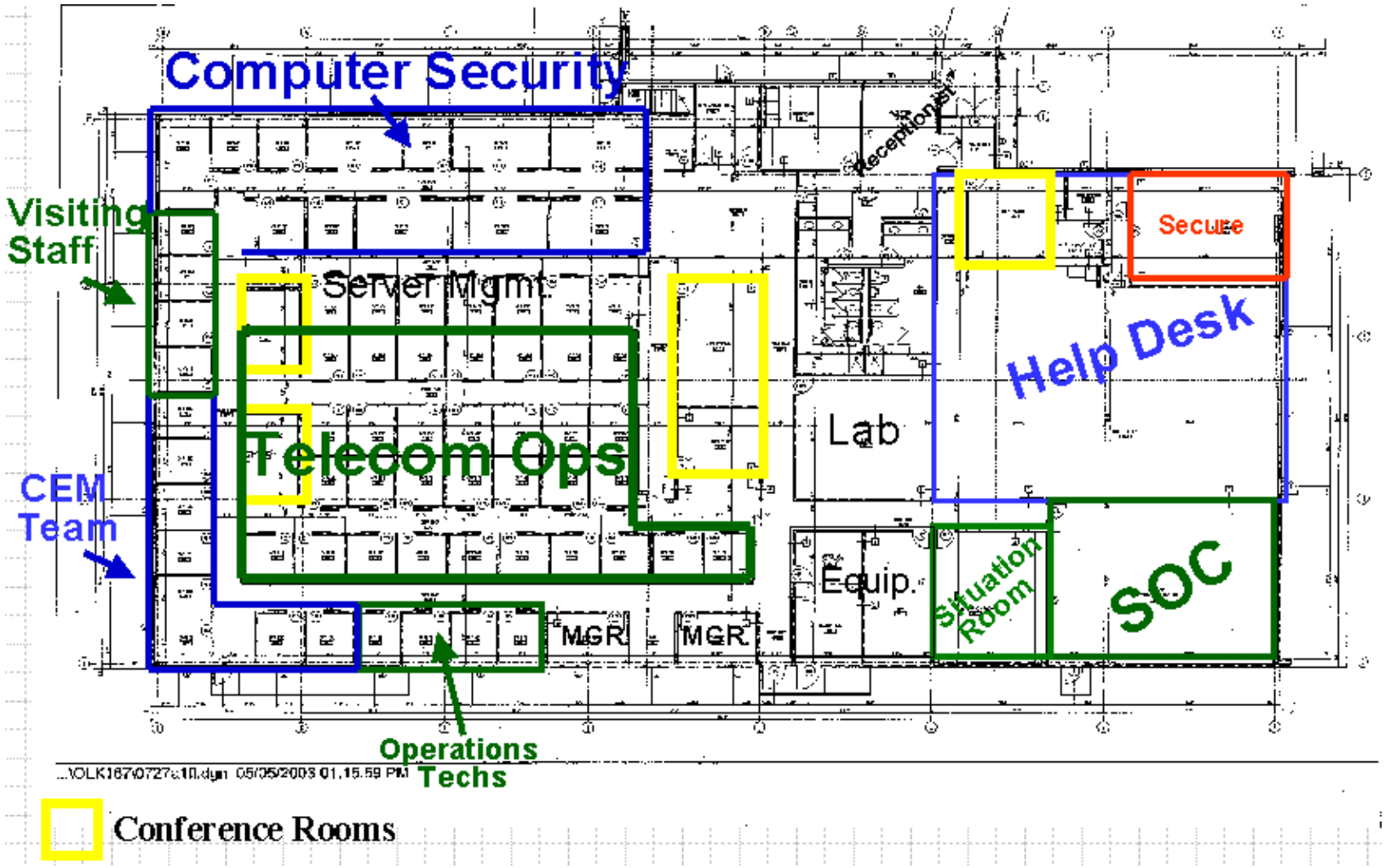
Photo Credit: Ian Blair via Flickr

- Silos of monitoring
- Independent Trouble resolution
- Then Black Thursday
- Lessons were Learned!

Integrated Network Security and Reliability Center (INSRC)

- Completed 2003
- Nerve Center
- Purpose Built
- 112 Personnel
- Central Location

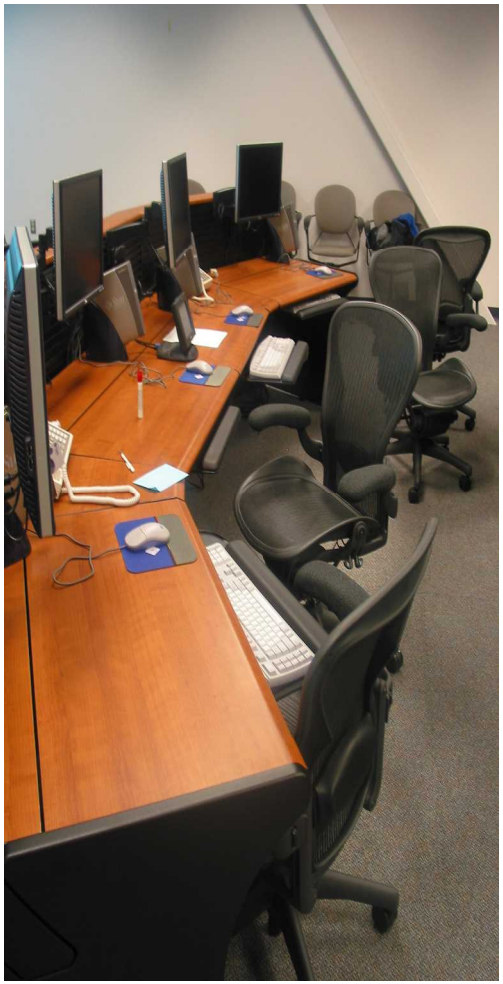
The facility provides the place for integration.



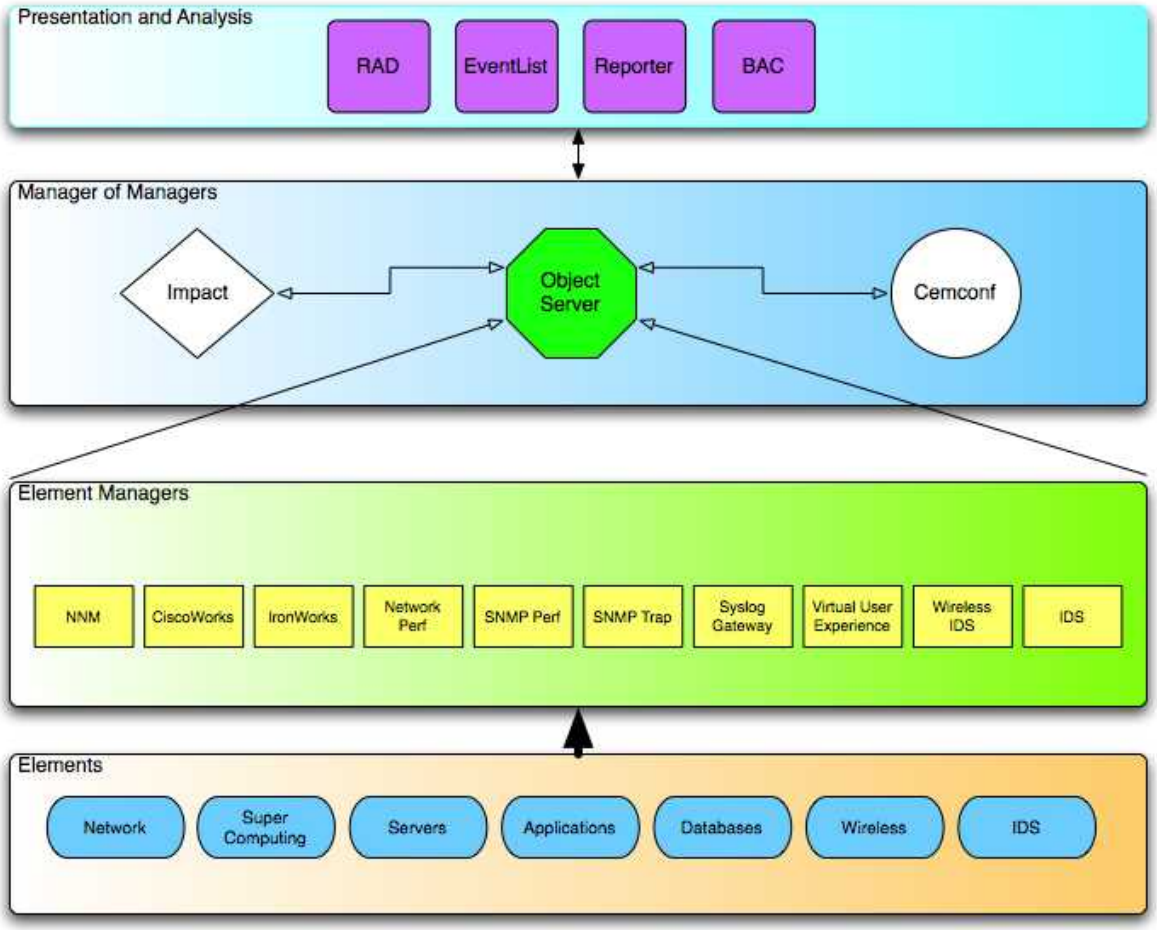
Sandia National Laboratories

Cyber Enterprise Management

- Infrastructure to detect and respond to security and service affecting events.
- Designed and implemented with mixture of COTS and custom software.
- Data analyzed and actionable information generated.

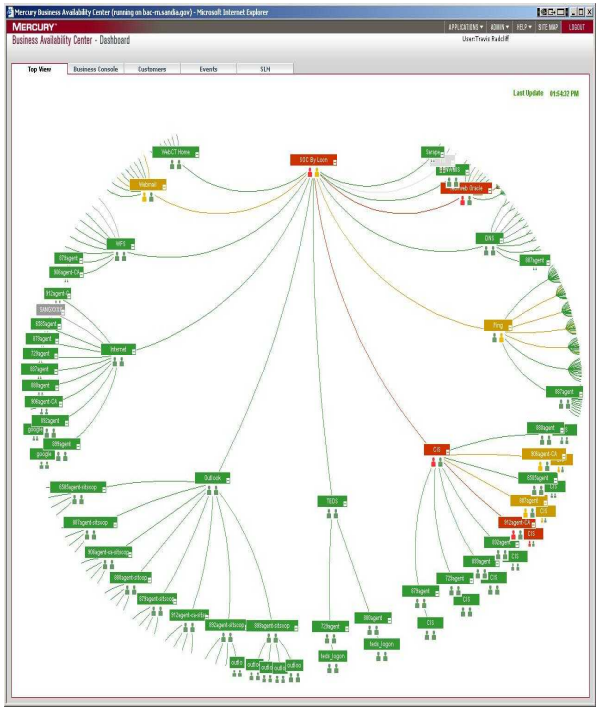


CEM System Architecture



CEM's Security Focus

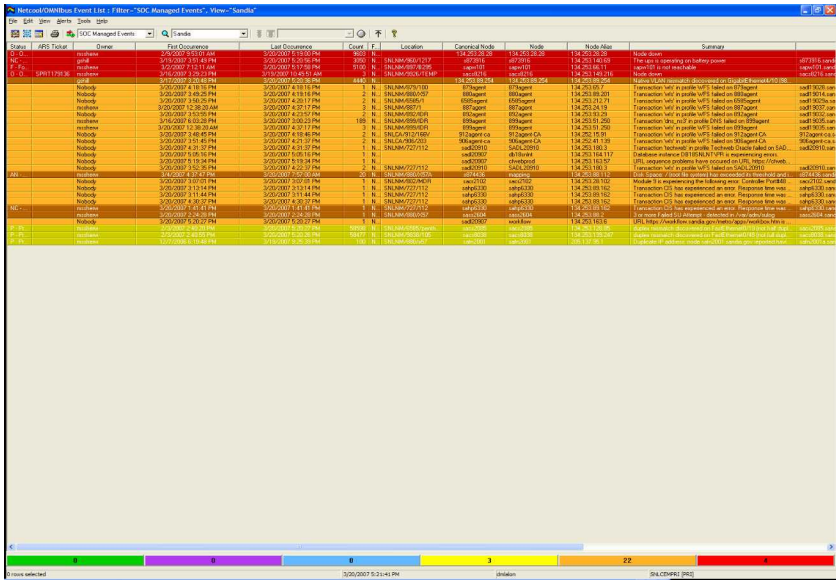
- Analyze IDS logs and generate daily IARC report for NNSA/DOE.
- Monitor and Detect Security Events reported from servers, applications, and network equipment.
- CID
- Wireless IDS
- Reliability and Availability of Security Infrastructure



Sandia National Laboratories

Scenario

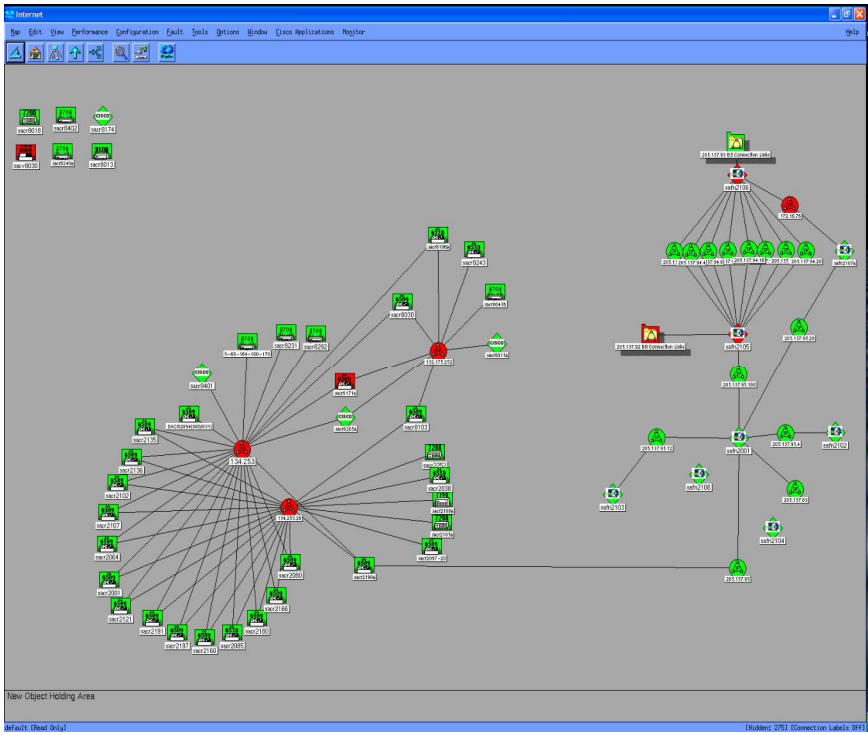
- Analysts detect suspicious traffic in IDS logs.
- Servers start reporting multiple failed logins from various locations.
- Network traffic spiking on normally unsaturated links.



Sandia National Laboratories

Scenario continued

- Analysts place call to Cyber Security and relate salient details.
- Cyber Security initiates Rapid Response Team.
- RRT assembles in Situation Room and coordinates response to threat.



Fun Stats

- Approx 1500 monitored entities (SRN)
  - 460 Network devices
  - 440 Unix and NT servers
  - 15 Applications
- ~ 4 tests per monitored entity
- Average of 100 actionable events per 9.5 hour SOC shift across 3 networks
- Response Time Average ~ 2.9 minutes (90% of events handled under 1 minute)
- CEM System processes averages approximately 30k events per day.
- Correlation, de-duplication, and filtering reduces the event stream by 90%.

Questions?

Todd Bruner
tbruner@sandia.gov

Sandia National Laboratories