CIO and Cyber Security Overview

Argonne National Laboratory

Michael A. Skwarek

CIO

Matthew A. Kwiatkowski

CISO

Oct. 12, 2011

Argonne Cyber Security Overview

- **The laboratory cyber security program is mature and considered to be the "Best in Class" across the DOE Office of Science.**
- **The program focuses on a risk based approach of balancing cyber security policy and mitigating controls with the scientific mission.**
- **A technical defense in depth strategy is deployed throughout the campus network.**
- **Cultural involvement in the program and awareness of current cyber security threats is critical to success.**
  - Management support is strong and essential.
  - Employee training is provided on first day and throughout career.
  - Employees provide "field agent" eyes and ears to warn of attempts and attacks.
- **Cyber R&D capabilities have been rolled into the operational cyber program.**

Argonne Cyber Security History

Year	Examiner	Rating	Findings
2000	GAO	Ineffective	10
2000	DOE-IG		4
2000	DOE-CH	Unsatisfactory	64
2000	DOE-OA	Unsatisfactory	17
2001	DOE-OA	Unsatisfactory	7
2001	DOE-IG		3

2001: Argonne Cyber Security Project Takes Place

Year	Examiner	Rating	Findings
2002	DOE-CH	Satisfactory	1
2002	DOE-IG		1
2003	DOE-OA	Effective Performance	2
2003	DOE-IG		1
2004	DOE-CH	Satisfactory	0
2004	DOE-IG		1
2005	DOE-IG		1
2006	DOE-IG		1
2006	DOE Site Assist Visit	"Best in Class"	0
2007	DOE-IG		0
2009	DOE-IG		0
2009 DOE Cyber Security Technical Innovation Award – Federated Model			
2010	DOE-CH		0
2010 DOE Cyber Security Innovative Achievement in Collaboration – NSM			

Argonne Cyber Technical Landscape

Laboratory Cyber Environment

Population:

- 2500+ employees
- 10,000+ visitors annually
- 13,000+ systems
- Growing # Off-site computer users
- Foreign national employees, users, and collaborators

IT Management :

- Not every computer is a DOE computer.
- Hybrid approach to IT Management
- Cyber Office provides oversight

Cyber Attack Landscape

- 5 Class B networks - ~330K IPs
- Several Million probes a day
- ~400K spam messages a day - ~80%
- 2 Million hostile hosts detected last year.

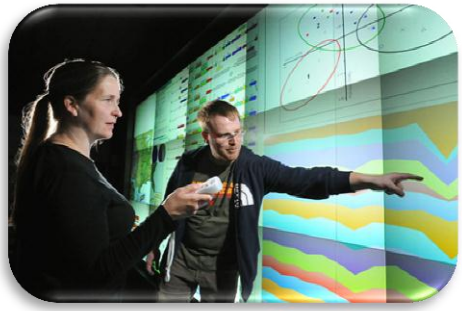
Our goal: A consistent and comprehensively secure environment that supports the diversity of IT and the requirements of the science mission.

Argonne Cyber Security Leadership

- **The cyber security program has taken a leadership role across the DOE Office of Science.**
- **The program has developed toolsets which are capable of changing the cyber landscape across DOE and beyond.**
  - Argonne is often called upon to provide technical and architectural reviews.
- **Enhanced collaboration and a willingness to share timely information is essential to the future of cyber across DOE and the Nation.**
- **Focus has been established on cyber security R&D which leverages the success of the operational program and capabilities across the laboratory.**

Argonne R&D - Cyber Security Core Competencies

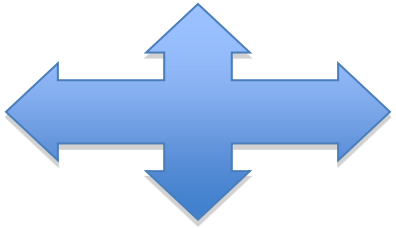
Exascale computing and storage capabilities
IBM BG/Q

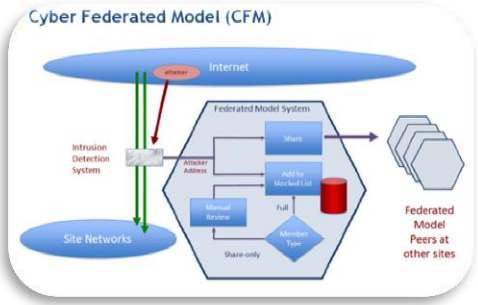


Algorithms, Analysis and Visualization

Mathematical algorithms, analysis techniques and data visualization of large and complex datasets.

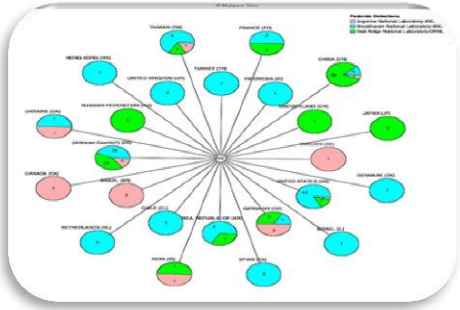
High Performance Computing





Communications
and Operational Excellence

Computational and agent based models ported to Exascale computing platforms.

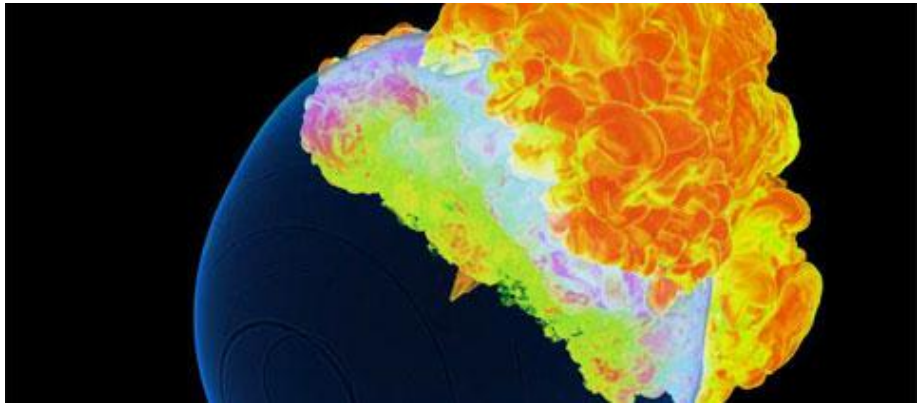


Computational and Agent Based Models

Cyber Federated Model providing timely defense information across DOE.

Technology of ANL in conjunction with the Center for Excellence in Cyber Security

- **Argonne Cyber Security Center of Excellence**
  - Opportunity to use what you've learned in a real world environment and work side by side with cyber security engineers and analysts
  - Get hands-on experience with cutting edge technology
  - Wide variety of projects to choose from
  - It's a paid internship!
  - Application: http://www.dep.anl.gov/p_shared/coop/coop.htm



Recent Accomplishments in CSCoE

- Five students were brought in last year to work in the CSCoE.
  - They focused efforts in:
    - Anomaly based intrusion detection of the lab's VPN
    - Integration of DNS into the lab's Integrated Host Warehouse (IHW)
    - Validation of vulnerability assessments with integration Pen-testing
    - Pilot of Snort and Bro IDS systems.
    - Established a network test-bed for cyber assessments.
    - Assessment of rogue wireless using smartphone detection capabilities.
      - DHS Research application submitted
  - Many of these efforts are in production today with the Cyber Office
  - ANL would like to continue the CSCoE Program.
    - Looking to bring on more students to work on challenging problems.

Question and Comments

- Contact Information:
  - Matt Kwiatkowski, MSIS
    - mattk@anl.gov
    - 630-252-6465
  - Michael Skwarek
    - mskwarek@anl.gov
    - 630-252-0572
  - To apply for the CSCoE please complete the application at the following:
    - http://www.dep.anl.gov/p_shared/coop/coop.htm