



Argonne
NATIONAL
LABORATORY

... for a brighter future



U.S. Department
of Energy

UChicago ►
Argonne_{LLC}



**Office of
Science**
U.S. DEPARTMENT OF ENERGY

A U.S. Department of Energy laboratory
managed by UChicago Argonne, LLC

Federated Model for Cyber Security: Sharing Intrusion Detection Analysis Results

Tami Martin

Argonne National Laboratory

DOE Network Security Monitoring Technical Summit

Jefferson Lab, Newport News, Virginia

May 9, 2008

Who Am I?

■ Tami Martin

- Intrusion Detection Systems Engineer for Argonne National Laboratory
- Three years in the Network Security section of the Core Networking group at Argonne
- Prior seven years in database design and management and web development at Argonne
- Veteran of US Air Force stationed at Los Angeles Air Force Base in California in the Computer Communications Center
- Masters Degree in Information Systems Management and Bachelors in Computer Engineering

Argonne National Laboratory



IT Environment Challenges

- Diverse population:
 - 3,000 employees
 - 10,000+ visitors annually
 - Off-site computer users
 - Foreign national employees, users, and collaborators

- Diverse funding:
 - Not every computer is a DOE computer.
 - IT is funded in many ways.

- Every program is working in an increasingly distributed computing model.

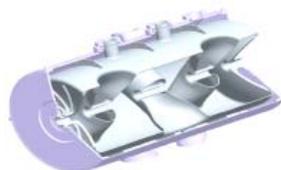
- Our goal: a consistent and comprehensively secure environment that supports the diversity of IT and requirements.

Argonne is managed by the UChicago Argonne LLC for the Department of Energy.

Emphasis on the Synergies of Multi-Program Science, Engineering & Applications



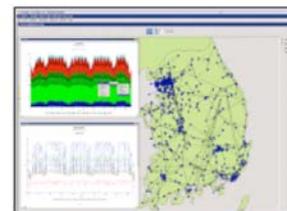
Computational Science



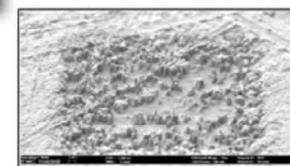
Accelerator Research



Fundamental Physics



Infrastructure Analysis



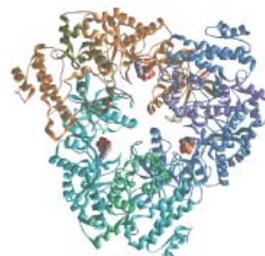
Materials Characterization



Catalysis Science



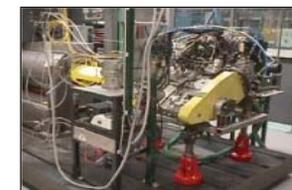
User Facilities



Structural Biology



Nuclear Fuel Cycle



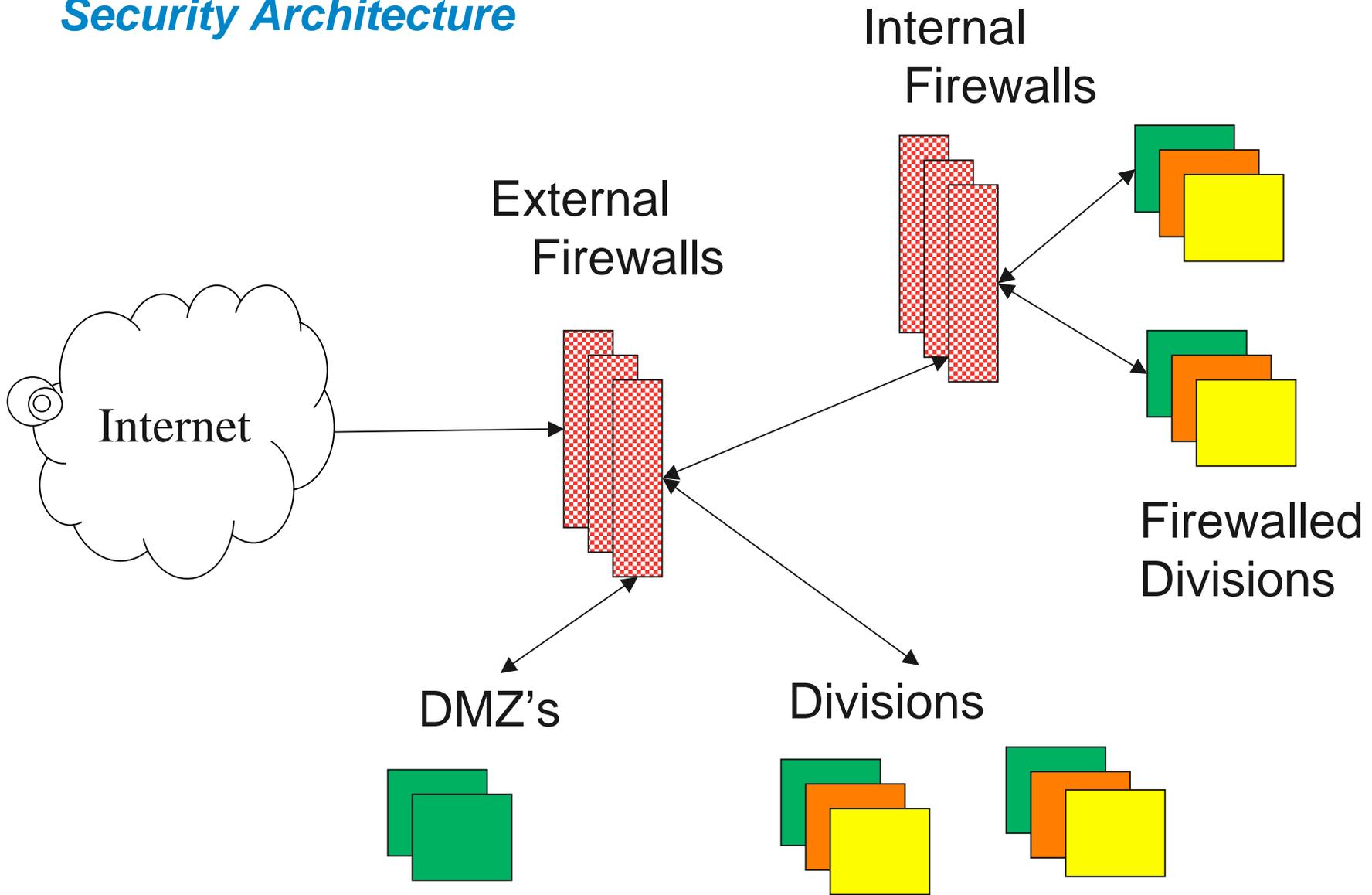
Transportation Science

.. and much more.

What is the Federated Model for Cyber Security?

- Supporting a working balance between Science and Security
- Project to share local intrusion detection analysis results across sites
 - to build a better knowledge base of addresses used in malicious network behavior
 - knowledge base can be used to automate tiered response solutions of future incidents that are detected
- Provide infrastructure to share data
- Define standards of how to share data
- Central repository of IDS analysis results
- Futures
 - Plan to build interactive query/response features
 - Move intrusion detection from local to global views and responses

Security Architecture



How the Federated Model for Cyber Security Addresses NIST controls and Best Practices?

| NIST Control | Federated Model |
|---|---|
| IR-3 Incident Response Testing IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reports | Federated model aids in supporting and background information on malicious behavior to aide in response, handling, and reporting incidents. |
| AC-17 Remote Access | Remote access to repository monitored and controlled. |
| RA-3 Risk Assessment | Information shared include severity of event. |
| RA-4 Risk Assessment Update | Information shared includes history of bad actor. |
| SI-4 Information System Monitoring Tools and Techniques | Federated model is a conglomerate of results from system monitoring tools and techniques across federated sites. |
| SI-5 Security Alerts and Advisories | Federated model designed to distribute security alerts and advisories. |

Argonne Local IDS Environment

■ IDS Commercial Tools

- Cisco IDS sensors (9 sensors strategically placed)
- Cisco Master Blocking Sensor (MBS) - to manage FW shuns
- Cisco Firewall Service Modules (FWSM) (dozens of contexts)
- Cisco trigger router to inject Null routes in core
- Arbor Networks Peakflow netflow analysis and response

■ Custom IDS Tools

- Persistent subscription to each sensor for additional processing of alerts
 - *Signature anomalies*
 - *Categories of victims to signature coordination*
- Netflow scripts (approx. one dozen routers)
 - *Scanning (port, host, internal vs. external source)*
 - *Watch lists - resource sites, CIAC defined “bad actors”*
- Log Monitoring
 - *Ssh (hundreds of servers), Active Directory (AD) (thousands of active accounts), DNS, Websense (unauthorized web use)*

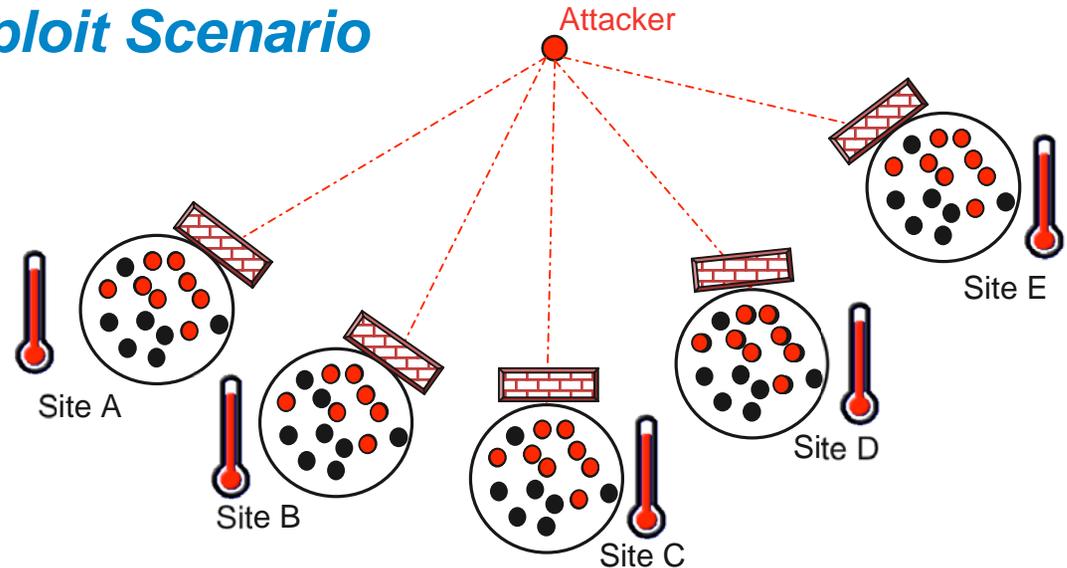
Argonne Local IDS Environment (continued)

- Automated Active Response (AR) Options
 - Firewall shuns (include manual shunning ability) (dozens/day)
 - uRPF (drop traffic as defined by trigger router)
 - Automation of dropping VPN user
 - Notification based on (include suppression measures)
 - *Who owns subnet, User involved, Cyber office, etc*
 - Differentiate between internal and external sources
- Available Authoritative Background Information
 - ARP table (15 minute polling)
 - Shun history (corporate memory)
 - Firewall conduits
 - Visitor registration (Netreg)
 - VPN user logs
 - Security contacts (HR tables)
 - Network structure (subnets)
 - Host categories and database
 - Miscellaneous databases (country of origin, vulnerabilities, etc)

Zero Day Vulnerability Exploit Scenario

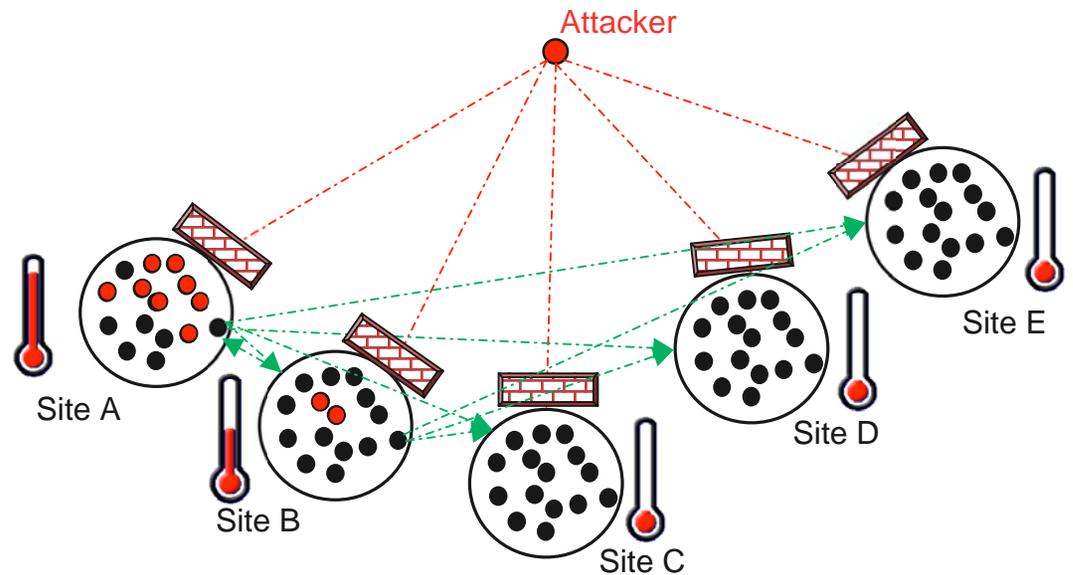
Local View

- Sites have primarily a local view of cyber security and intrusion detection
- Active response actions are reactive to attacks on local site



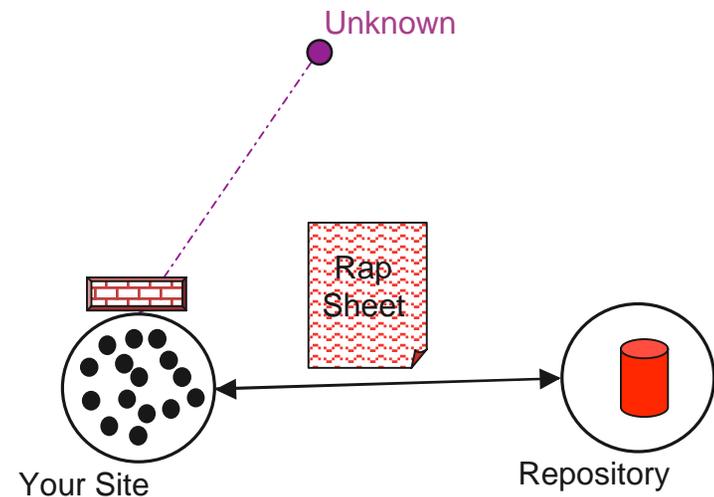
Federated Model

- Sites share actionable AR intrusion information
- Active response actions could be proactive based on activity at other Federation sites
- Works best if all share



Suspicious Behavior Scenario

- Detect behavior that is suspicious, but under thresholds for local active response
 - Analogous to Police pulling over reckless driver
- Check repository for reports from other sites
 - Analogous to Police run plates to check background
- Take active response measures if sufficient malicious activity at other sites
 - Analogous to Police making arrest



Note: Your AR actions could vary based on your sites confidence in repository and federated members with which you share

Background

- Cyber Defense continues to be a challenging problem for Federal agencies and R&E communities alike
- Security challenges
 - Threat landscape evolving rapidly - our defensive strategies and methodologies need to as well
 - Technology paradigm evolving rapidly - national networks; dynamic provisioning
- Risk based approach to cyber defense still needs to:
 - Keep the “bad guys” out
 - Let the “good guys” in, and
 - “Keep the wheels on” maintain effective operations & perform mission
- Investment in information security today is largely a cost of doing business, particularly when trust and security are expected (esp for PII)
- Propose that there is an opportunity for all of us to work smarter using a Federated Model for Cyber Security

Motivation behind a Federated Approach

- Lots of energy (\$\$) going into analysis, monitoring, tracking, and possibly blocking packets or other active response actions on the wire.
 - Each agency/site is doing this every day (in their own unique way).
 - However, there is no convenient way to interact with the each other in a near real-time automated manner, E.g.
 - Announce - this IP was hostile to us for ssh brute force attack
 - Announce - this IP was a resource site for a root kit used here
 - Query - what traffic have you seen to/from this IP ?
 - Query - is this a valid/routed IP at your site ?
 - Action Request - Suggest you add this IP to your watch list
 - Action Request - Suggest you block this IP
- (Today) We don't have an infrastructure that enables us to adapt and evolve rapidly with our threats - unacceptable risk position.
- Goal is to create a future state that enables action - more than just sending e-mails and waiting for human intervention.

The Vision - Framework

- Create an infrastructure (tools) that let agencies interact efficiently and securely
 - Close to real-time (< 10 minutes)
 - Autonomously (without human intervention)
 - Using simple underlying technology
 - Trackable, reportable, accountable
- Encourage the development of Federations
 - Multiple federations, not just one
 - Join the *ones* that make sense
 - Share appropriate info to each federation
- Define some formats for information sharing
 - XML based
 - Standards based
 - *The Intrusion Detection Message Exchange Format (IDMEF) from Intrusion Detection Exchange Format Working Group of the IETF (RFC 4765 <http://www.rfc-editor.org/rfc/rfc4765.txt>)*
 - Defined well enough to support autonomous operations
 - Flexible enough to adapt over time

What would we do with this Framework/Infrastructure ?

- Share information with each other
 - Announce malicious network behavior detected at one agency/site in an attempt to deter or prevent the spread of this behavior
 - Include history of an IP's behavior, severity, and local actions taken

- Implement a query/response mechanism that would allow a trusted agent at one site to solicit information from other sites
 - Are you seeing in-bound scanning from this IP ?
 - Are you seeing out-bound activity to this IP:port ?
 - Ideally this should be an automated lookup - each site controls what information sources from which they will share

- Implement an action request mechanism for a site to *advise* that other agencies/sites block or watch an IP address

The Strategy

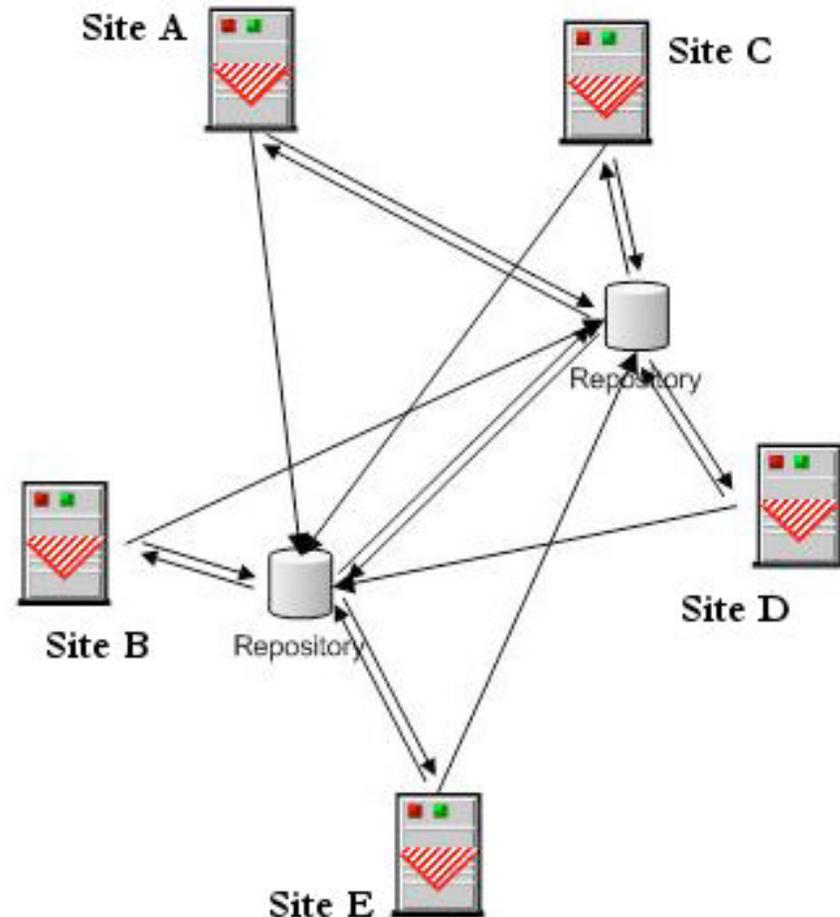
- Create an infrastructure for passing data between federation members
 - Based on limited function web service (upload and download of files)
 - RSS used to signal new data available
- Develop standards/templates on what information we should share
- Encourage the formation of federations
 - Encourage groups to think about automation points
 - Community building through grass roots effort
- Stir well and see what happens

Federated Model Features

- Grass Roots Concept
 - Provide an open list of participants and official POC
 - Allow multiple communities to leverage the infrastructure (based on a limited function web server)
- Sites directly participate
 - Sites maintain local control of what information they share
- Sites control/decide who they want to interact with
 - One federation for sharing info, one for queries, one for action
 - Via pgp key management (out of band)
- Implemented through a limited function web site
 - Goal is to implement as a near real-time automated system
 - Allows upload from registered participants only
 - Supports download to registered participants only
 - Supports RSS to allow sites to determine when new data is available

Repository Design

- Only accept PGP encrypted files for security
- Central collection for scalability
- Duplicate repositories for continuity
- Only accept downloads and uploads from authorized sites based on IP
- Controlled access
- Each site sets own upload and download schedules



Reasons for Participating

- To be successful in the future - need to speed up our OODA loop for cyber defense !!!
- Improve the data glut, information famine problem
- Assumption: malicious attackers prey on related sites (government, defense, financial, research & education, etc)
- Creating an IP profile enables better suited response actions
 - Know what to watch for
 - Quicker and possibly more severe response to known “bad guys”
- Valuable resource for incident response
 - We saw “x”, wonder if anyone else did ?
- Valuable resource for US CERT, CIAC, or other trusted agencies
 - Automated method for CIAC to push an IP address to all the sites with the suggestion of blocking it (fully automated)
- Valuable tool for interacting with “Internet Service Providers”
 - DISA, ESnet, etc

Information being Disseminated Falls into 3 Categories

- Announcements from a site
 - This IP was bad for the following reasons ...
 - Extends the “corporate memory” of anti-host (bad guy) knowledge
 - Maintains situational awareness, recidivism
- Query to a site
 - We are interested in the following IP address
 - Can you send us flow data from your site over time range ... ?
 - Have your IDS logs seen this IP before ... ?
 - Is this a valid IP address at your site
 - Network currently being routed at the site ?
 - Is that IP address in use ?
 - Did that IP address send e-mail over time range ... ?
- Action Request (strongly suggested)
 - The following IP address is actively involved in an exploit at our site, suggest you block it
 - US CERT/CIAC advisory that we block (or watch list) an IP address

What Information is Shared ?

- Strictly unclassified information

- Information on (usually external) IP addresses that was malicious enough to warrant a site response (blocking or other)
 - IP address:tcp/udp port #
 - Time of attack
 - Type of attack
 - Exploit attempted
 - Severity of attack
 - Previous history of offending IP at that site (corporate memory)

 - We could periodically share watch lists

- Information presented in a standardized exchange format
 - Small XML file
 - Using IETF standards for cyber data exchange

Project Growth

- Version One (1)
 - Build infrastructure, automate data transfer
 - *Push and pull of data based on each sites schedule*

- Version Two (2)
 - Implement automatic query/response capability
 - *Two-way communications*
 - *Auto response to standard queries*

- Version Three (3)
 - Look beyond Federations to involve ISPs in fight to find sources and stop malicious traffic
 - *Backscatter detection*
 - *Path to real source (not spoofed)*
 - Expand data shared to URLs, DNS, Email addresses, etc.

Wait - Does This Really Work? (Case Study)

- From May 2007 to May 2008
- Number of unique IPs determined to be actionable per site and contributed to the Federated Model Project - limited site participation.
 - National Center for Supercomputing Applications (NCSA) at University of Illinois ~10,000
 - Argonne National Laboratory, Illinois ~13,000
- Commonalities between two sites:
 - Geographically close
 - Both research and high level computing (edu vs gov)
- Number of IPs appearing in both sites (i.e. one site gave forewarning to the other)
 - ~1,300, from Argonne perspective - that's 13% of IPs that NCSA shared or 6% of all addresses shared
 - With dozens of IPs having response action taken daily, everyday 2 responses could be faster or pre-empted based on information from one other site
 - Does not include under radar activity that may be escalated to actionable based on reports from other site

DOE HQ/CIAC notification (Case Study)

- Timeline of events
- April 9 - HQ detected malicious activity (event)
- April 11 - HQ issued digital (pdf) report on event
- April 20 - Traffic from Argonne to malicious site
- April 23 - CIAC posted malicious site
 - Argonne downloaded email
 - Read and decipher email to find malicious site
 - Implement block action against malicious site manually
- April 25 - CIAC notified Argonne of traffic on April 20



Can I Play, too? How to Get Involved.

- Think about how you would like to speed up your OODA loop
 - Observe, orient, decide, act
 - Automate OODA where possible
- Create a federation - even if it is with just another single organization
 - Start with already trusted friends
- Think about what you have automated to date
 - What can you/should you automate in the future
- Get involved
 - Come as you are, using your already defined IDS analysis methodologies
 - To inquire or join send email to federated-admin@anl.gov
- For additional info:
 - <https://www.anl.gov/it/federated>
 - Argonne Contact: Tami Martin, tamim@anl.gov