Open Science Best Security Practices

Alex Withers, Assistant Director Cyber Security, alexw1@illinois.edu
Jeremy Enos, System Management & Development Lead, jenos@illinois.edu
Cybersecurity Division

Current Projects
- **Blue Waters** – Securing & supporting the Blue Waters petascale machine
- **XSEDE** - Leading the distributed security team & advancing the federated IdM capabilities
- **LSST** – Security, network, and IdM design and capabilities for the Large Synoptic Survey Telescope
- **CI Logon** – Providing a platform for federated identity to access scientific resources
- **TrustedCI** – Protecting NSF resources w/ the Cyber Security Center of Excellence
- **Industry Program** – Providing expertise and value to Industry Partners
- **Advanced Intelligence Sharing** – Capabilities to securely disseminate treat intelligence data in realtime
- **Healthcare Computing** – Research computing on ePHI data within the context of HIPAA

Interest areas for collaboration/future work
Federated identity; High resolution network monitoring and analytics; High-performance networking; Software Defined Networking; Data analytics for security logs; Software assurance; Security and Big Data

Key Words: Security, networking, identity management, log analysis, data analytics, intelligence sharing.
Open Science Best Security Practices

- Security within the context of open science
  - Security is more than confidentiality!
  - **Productivity** – Ensure your systems, labs, etc. are available and operational. Your data is valuable (ransomware).
  - **Trustworthy** -- For open science, integrity of data is often most important aspect of cybersecurity.
  - **Reproducible** – Running Open Science on compromised systems?
- What are some of the best practices that NCSA uses for its open science systems?
BlueWaters Security Statistics

- No compromises in the past 10 years.
- Over 73 million attacks in the past 5 years resulting in automated action.
- Sources for security events:
  - Intrusion detection system
  - Honeypots
  - Partnered intrusion detection systems
  - Day-to-day security analysis
Key BlueWaters Security Controls

- Multi-factor authentication (MFA) required for all access to the HPC system and supporting infrastructure
  - MFA is also required to elevate privileges
- Privileges may not be elevated from user accessible systems
  - Administrator only systems are the exclusive path to elevate privileges on the HPC system
- Required integration into the identity and access management infrastructure
  - Access managed with LDAP group membership
- Network security monitoring of all traffic at NCSA’s border and into/out of BlueWaters
- Access to all systems in encrypted.
- Access is controlled with group memberships.
- All system and user activity is logged.
- Networks properly segmented and firewalled.
- Storage systems provide proper access controls
- Systems must undergo security vetting to ensure that they have properly implemented required security controls
- New and existing systems and services undergo change management review
- All systems and networks must undergo security scanning
Security In-depth

- Robust network security monitoring
- System hardening and vetting
- Identity and access management
- Security awareness and communication
Network Security Monitoring (NSM)

- NCSA’s Information Systems divided into trust zones
  - Trust zones are assigned risk levels
- Monitoring sharply tuned on higher risk trust zones
  - Including between trust zones that differ in risk level
- Security standards commiserate with risk level (more later)
- Control access into and between trust zones
  - Best practice: monitoring resources are focused on the high risk trust zones
    - Efficient use of security monitoring infrastructure
    - More meaningful security alerts, less noise
NSM Implementation

- Zeek IDS monitors traffic into NCSA’s HPC Zone and NCSA’s WAN connections
  - Open source network monitoring platform (previously known as Bro)
  - Multiple 100GB connections for WAN connections
- How do we tune and manage the “fire hose” of security alerts?
  - Manage flow of data being monitored, filter out unnecessary traffic
- How do we react to events discovered by the NSM?
- *Best practice: shunting flows and active response to security events with follow-up*
Black Hole Router (BHR) maintains block list of IPs not allowed to connect to NCSA’s networks

Network Taps passive send all WAN and Zone traffic to the tap aggregation system

Network Tap Aggregation combines, filters and divides traffic to feed into the Zeek IDS clusters
Zeek sees large network flow into Blue Waters, i.e. file transfer.
(1) Zeek records beginning of flow

(2) Zeek informs the tap aggregation to cease sending it traffic until the flow ends
(2) Zeek interfaces with BHR to block traffic from detected indicators.

(1) Zeek detects an attack, i.e. coordinated scan.
Monitoring at the system level

• Privileged access to Blue Waters controlled via bastion hosts
  • Integrated with centralized identity and access management
• Bastion hosts record all user interactivity
• All systems, including bastion hosts, send system logs to central collectors
• Logs are examined and correlated with network events (via Splunk and custom developed tools, see github.com/ncsa)
• Best practice: un-siloed monitoring of all logs in one ecosystem
System Hardening and Vetting

• NCSA policies dictate required security controls
• All systems require security vetting before being deployed
  • Vetting ensures controls have been implemented correctly
  • In practice a security engineer is given access to a system and uses automated and manual methods to vet the system before deployment
• Best practice: verify implementation of controls
  • Configuration management and change control help to make this a less time and resource intensive process
System Security After Deployment

- Vulnerability management
  - Systems are scanned externally and internally for out of date and misconfigured software
- Monitoring of changes
  - Security staff reviews change control requests
  - Active participation by security staff in system administration and project meetings
- Best practice: ensure required security controls are maintained on the system
Identity and Access Management (IaM)

- Security control: “require integration into the identity and access management infrastructure”
- All user and admin require authentication w/multi-factor and authorization to systems and services from centralized IaM
- Provide a management system for account self-service and recovery, and user and group management
- **Best practice**: centralized IaM to enable auditing, identification, and enable authorization
Security awareness and communication

- NCSA’s security team provides security awareness training for all users and staff
  - General security hygiene
  - Focused on topical threats and best practices
- Open lines of communication
  - Security staff participate in system administration and project meetings
  - Clearly documented procedures for contacting and elevating
  - Slack channel for general security discussion
Questions?

Alex Withers
alexw1@illinois.edu
https://security.ncsa.illinois.edu
Twitter: @NCSASecurity

Jeremy Enos
jenos@illinois.edu