NCSA Security Monitoring Policy

Document Name: NCSA Security Monitoring Policy
Version: 1.0
Accountable: Alex Withers
Authors: Adam Slagell

Reviewed: June 23, 2021
Approved: 2008 by the Office of the CIO

Scope

This policy covers all users of NCSA production systems for external customers, including Blue Waters.

Introduction & Purpose

The primary threat to the security of NCSA production systems comes from user "identity theft", often exposed as compromised user accounts and credentials. Within the existing HPC environments managed by NCSA, 25% of security incidents stem from user credentials becoming compromised and used by unauthorized persons for malicious purposes. This document details the policy covering the monitoring of user activity.

Policy Statement

The NCSA support staff (e.g. system managers, networking and security teams) monitor all NCSA production systems and related resources. This extends to monitoring all user interactions with these resources including encrypted channels such as SSH. Secure communication channels may be modified to permit this monitoring to take place.

All users where such monitoring takes place will be provided notification of this fact through user agreements, login banners or other mechanisms.

Process Details

Log Retention

The detailed SSH logs, which record most command line input and output as well as file transfers, are generally rotated out of use and discarded after approximately 4 weeks unless suspicious activities have occurred. These logs provide much of the input for the host-based intrusion detection system. For specific security incidents, relevant portions of these logs may be saved into our incident response tracking system or other areas. Higher-level logs (e.g., network flows, IDS alerts, authentication logs, process accounting, and general system logs) may be held for longer periods of time.

Host-based Intrusion Detection System (HIDS)

Our intrusion detection/protection systems (IDPS) monitors the SSH commands executed and files down[up]loaded (as part of most everything processed through STDIN/STDOUT), looking for signs of account compromise. Users will be informed as soon as possible if inappropriate activities involving their accounts are detected.