NCSA Security Operations Log Review Procedures

Document Name: NCSA Security Operations Log Review Procedures
Version: 1.0
Accountable: Alex Withers
Authors: Alex Withers

Reviewed: June 24, 2021
Approved: June 24, 2020

Collection

NCSA continuously collects system logs and network data, and it utilizes automated tools to analyze and send notifications to the Security Operations and Incident Response Team.

Review

Security Operations team members review these notices during normal business hours and escalate when judge further investigation is required. Escalation follows the NCSA Incident Response procedures.
NCSA also operates a 24/7 help desk that monitors critical infrastructure. Staff can use this help desk in an emergency to reach the security team after hours using the NCSA Security Contact Process. Per the NCSA Information Security Policy all staff are required to report suspected security breaches, which are then followed up by a manual investigation of relevant logs.
System Administrators may request log reviews by the Security team by submitting a ticket or through the NCSA Help Desk.

Specific processes for review can be found in Security Log and Event Review Processes.

Tracking

Requests made directly via the ticket system or via the NCSA Help Desk are recorded and closed after an investigation completes. Findings that escalate to an incident investigation are tracked and managed per NCSA Incident Response Procedures, which include the appropriate reporting mechanisms.