WEBER STATE UNIVERSITY
Information Technology

Network Monitoring and Defense STANDARD (CIS CSC 13)

Purpose

Establish and maintain comprehensive monitoring and defense capabilities across WSU's network infrastructure and user base to detect and respond to security threats. This control aims to minimize the attack surface and potential for exploitation by actively managing network traffic, detecting malicious activity, and responding to security incidents.

Responsibility

The Information Security Office (ISO) is responsible for managing access and retention for the following log sources: Security Information and Event Management (SIEM), Network Intrusion Detection System (NIDS), Host Intrusion Detection Solution (HIDS), Network Firewall Logs, and Ingress and Identity Logs.

Centralized Security Event Alerting

Authentication and Audit logs shall be sent to the central SIEM specified in CIS CSC 8 Audit Lot Management Standard.

Intrusion Detection and Prevention

- **Deploy a Host-Based Intrusion Detection Solution**
  Deploy a host-based intrusion detection solution per CIS CSC 10 Malware Defense Standard.
- **Deploy a Network Intrusion Detection Solution**
  Network Intrusion Detection solutions are to be deployed at the Internet Border and the Data Center border.

Traffic Filtering

- **Collect Network Traffic Flow Logs**
  Border firewall logging information will be sent to the central SIEM.
- **Perform Traffic Filtering Between Network Segments**
  Filter network traffic between network segments, prioritizing segmentation of sensitive environments. This includes, but is not limited to, separating SCADA/ICS networks, critical operational technology (OT) infrastructure, user traffic, and management/monitoring networks. Use firewalls, ACLs, or other network enforcement devices to limit inter-segment communication to only essential protocols and services, thereby restricting lateral movement.

Remote Access Management

Manage Access Control for Remote Assets

Manage access control for assets remotely connecting to enterprise resources. Determine the amount of access

to enterprise resources based on: up-to-date anti-malware software installed; configuration compliance with the enterprise's secure configuration process; and ensuring the operating system and applications are up-to-date.

Revision History
Creation Date: February 24, 2026
Amended: N/A