UNT SYSTEM

Logging Best Practices

Overview

Logs should be stored in a central location with strong controls to maintain confidentiality, integrity, and availability. All information systems participating in log generation and management should normalize their clocks using a common network time protocol where available.

Log Categories

Operating Systems

- System Events – Operational actions performed by OS components
  - Shutting down
  - Starting or stopping a service
  - Network events
- Audit Records
  - Authentication events – successes and failures
  - File access
  - Security policy changes
  - Account changes
  - Use of privileges

Applications

- Client requests and server responses
- Account information
- Usage information
- Significant operational actions
- Major application configuration changes

Log Details

Specific log details vary depending on the log source and configuration. Below are recommended fields to capture.

- Timestamp
- Source and destination IP address
- Protocol method
- Status code
- Request details

Reference

NIST Special Publication 800-92 Guide to Computer Security Log Management

UNT System Information Security Handbook Section 12.7 Monitoring

UNT SYSTEM

Document Version Log

Version	Date	Description
1.0	6/7/2022	Initial Document Version
1.1	9/27/2022	Document approved