**Name of Organization**

**Technical**

**Incident Response**

**System Requirements**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Technical Incident Response System Requirements document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute the document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. The document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc84837055)

[II. Technical Requirements 5](#_Toc84837056)

# Introduction and Purpose

For a device to be correctly analyzed during an investigation and for the investigators to be able to obtain required information to identify what has happened, and to create a remediation plan to avoid similar incidents in the future, each device needs to be configured per the standards in this document. This document shows the minimum baseline configuration and logging requirements for various devices.

# Technical Requirements

General Configuration Standard

Adhering to the measures below lays the groundwork for a robust cybersecurity program. Effective logging will enable the IT Team or Security Operations Center to analyze data and to swiftly identify possible incidents.

* **Enable Logging Throughout the Environment:** All servers, domain controllers, network devices, firewalls, applications, and workstations are logging security events and keeping them for a configurable length of time. Retaining log data for at least 45 to 60 days is a good starting point. Extending this term to six months if storage space is available is recommended.
* **Configure Robust Logging:** Many manufacturers' default logging settings simply do not fulfill modern security requirements. For instance, Windows servers by default log only successful events but not failures, however in other circumstances, they may log both successful and failure events. A logging program's effectiveness requires information about both unsuccessful and successful attempts.
* **Centralize Log Collection:** It is recommended to have the resources to implement a security information and event management (SIEM) solution.
* **Fine-tune the Logging System:** Log analysis is a time-consuming and demanding task made more difficult by the fact that the majority of settings are ‘noisy’ due to operational activity. Centralized log analysis needs to be configured according to your business practices and relevant rules to avoid false positives.

Logging Sources

* Network equipment: routers and switches
* Security equipment: firewalls, intrusion detection systems, VPNs, and intrusion prevention systems; and
* Access control: RAS, AD, and directory services.
* Operating systems (Unix, Windows, VMS, i5/OS400, and others)
* Apps: databases, email, web, and client applications
* Miscellaneous: physical access, and other non-IT technologies

Typical Logs to collect:

The following log locations should be investigated:

* The Linux operating system and key applications: /var/log
* Microsoft Windows operating system and essential applications: Windows Event Log (Security, System, Application) – servers and workstations
* Network devices: typically log via Syslog; others have their own locations and formats.
* Logs generated by security tools (e.g., anti-virus, change detection, intrusion detection/prevention system);
* Logs generated by applications (e.g., web server, database server);
* Outbound proxy logs and end-user application logs

Securing Logs

Logs should be protected from tampering or modification:

* Key theme: “Good enough” log security
* Transmission security (SSL, SSH, etc.)
* Storage security (hashing -> signing -> encryption)
* Access control – “need to know” basis
* Access and process logging - log who saw the logs! [\*\*]
* Last resort: printer + safe + armed guard

Device Configuration Standard

Linux Log Configuration Standard

|  |  |
| --- | --- |
| Successful user login | “Accepted password”, “Accepted public key”, “session opened” |
| Failed user login | “authentication failure”, “failed password” |
| User log-off | “session closed” |
| User account change or deletion | “password changed”, “new user”, “delete user” |
| Sudo actions | “sudo: … COMMAND=…” “FAILED su” |
| Service failure | “failed” or “failure” |

Network Device Configuration Standard

|  |  |
| --- | --- |
| Traffic is let through the firewall. | “Built … connection”, “access-list … permitted” |
| Firewall traffic is blocked. | “access-list … denied”, “deny inbound”; “Deny … by” |
| Bytes transferred (large files?) | “Teardown TCP connection … duration … bytes …” |
| Bandwidth consumption and protocol use | “limit … exceeded”, “CPU utilization” |
| Attack activity has been detected | “attack from” |
| Changes to the user account | “user added”, “user deleted”, “User priv level changed” |
| Administrator privileges | “AAA user …”, “User … locked out”, “login failed” |