***INJECT # - Software Audit***

***Name of Company***

**Table of Contents**

[**Executive Summary** 2](#_Toc127450182)

[**Software Audit** 3](#_Toc127450183)

[**Purpose:** 3](#_Toc127450184)

[**Scope:** 3](#_Toc127450185)

[**Risk/Threat Measurement:** 3](#_Toc127450186)

[**Software Audit:** 3](#_Toc127450187)

[**References:** 6](#_Toc127450188)

[**Document History:** 6](#_Toc127450189)

# **Executive Summary**

This document covers an outline of …

# **Software Audit**

## **Purpose:**

The purpose of this document is to identify all the devices on the network and what software is installed on each device. A risk or threat assessment can be analyzed to give the IT team a more of an understanding of what devices are at risk due to the software and identity threats that each device is facing.

## **Scope:**

The scope of this document is to identify all software on each device on the [COMPANY NAME] network.

## **Risk/Threat Measurement:**

Risk and Threat associated with a device can be determined through the measurement of two factors. The first being the probability of an attack on a system or the type of attack on a system which is laid out of the left, gray column of the diagram. The second being the severity or impact of an attack if it affected a system which is labeled on the top, gray row. With these two factors measuring the threat or risk associated with the organizations systems, a more accurate assessment can be made.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MATRIX** | **Negligible** | **Minor** | **Moderate** | **Significant** | **Severe** |
| **Very Likely** | Moderate | High | High | Critical | Critical |
| **Likely** | Moderate | Moderate | High | High | Critical |
| **Possible** | Low | Moderate | Moderate | High | High |
| **Unlikely** | Low | Low | Moderate | Moderate | High |
| **Very Unlikely** | Low | Low | Low | Moderate | Moderate |

## **Software Audit:**

Below is an software audit log organized by the type of server, server name with associated IP address, the threat level assessed, and a quick analysis of why it earned that assessment. This outline all the software on each device so that the IT team is aware of what is a risk for each device and if it is a threat that should be tended to.

|  |  |  |  |
| --- | --- | --- | --- |
| **FTP Servers** (DELETE THIS NOTE: THIS IS DEVICE TYPE SUBHEADING) | | | |
| {NAME OF DEVICE} | | {IP ADDRESS OF DEVICE} | |
| **Software** | **Threat Level** | | **Analysis** |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
|  |  | |  |
| ----------------------------------------------------------------------------------------------------------------------------------- | | | |
| {NAME OF DEVICE} | | {NAME OF DEVICE} | |
| **Software** | **Threat Level** | | **Analysis** |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
|  |  | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mail Server** (DELETE THIS NOTE: THIS IS DEVICE TYPE SUBHEADING) | | | |
| {NAME OF DEVICE} | | {NAME OF DEVICE} | |
| **Software** | **Threat Level** | | **Analysis** |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
|  |  | |  |
| ----------------------------------------------------------------------------------------------------------------------------------- | | | |
| {NAME OF DEVICE} | | {NAME OF DEVICE} | |
| **Software** | **Threat Level** | | **Analysis** |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
| {SOFTWARE NAME} | {THREAT LEVEL} | | {SHORT EXPLANATION} |
|  |  | |  |

# **References:**

EXAMPLE REFERENCE 1. (n.d.). *Scope of practice*. <https://www.nursingworld.org/practice-policy/scope-of-practice/>

EXAMPLE REFERENCE 2. (2020). *Publication manual of the American Psychological Association* (7th ed.). <https://doi.org/10.1037/0000165-000>

# **Document History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versions** | **Change Date** | **Responsible** | **Summary/Comments** |
| #-01 | 02/18/2023 | *Company Name* | This is the original version of the document set as a template. |
| #-01 | 02/18/2023 | *Company Name* |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |