

**PlaceboPharma**

**Cyber Security Team Blue Team XX**

**Recipient**:

<Recipient Name>

PlaceboPharma, Bristol

**Date**: March X, 2025

**Subject:** Response to Request <Insert Request Title/Number>

Dear <Recipient/Team>,

Thank you for reaching out to our team. Below, you will see our report regarding a recent request # made to our team, tasking us to create a comprehensive risk assessment of our infrastructure in order to identify and mitigate any potential vulnerabilities.

A list of potential high-severity vulnerabilities was compiled, as well as proposed steps to mitigate all of the issues.

Thank you,

Blue Team XX

Executive Summary

The risk assessment conducted by our team found that **a number of business critical systems contained vulnerabilities that would pose a server threat to normal business operations.** This is because… This risk assessment provided a structured understanding of our infrastructure's potential vulnerabilities and their impacts on our company and business.

Assets Affected

| Hostname | IP Address | Additional Notes |
| --- | --- | --- |
|  |  | **REMOVE IF NONE** |

Fulfilled Action Items

<Break down your tasks. What sub steps were taken>

1. Sample: We had installed [X service name] on machine 1
2. Sample: We had made changes to the firewall on machine 2 that would block the FTP port.

This should not be a step-by-step guide of what you did to complete the task. This should be a list of things broadly done to complete the task. Something like “We first SSHed into the machine and opened the PAM configuration files with VIM, and since we saw the password complexity configurations were XYZ we updated them to be ABC…” is WAY too much information and time here; You could leave it at something like “1. Analized current password configuration policies on XYZ machines, 2. Updated…” **INCLUDE SCREENSHOTS HERE BELOW THE COMPLETED ACTION**

Action Plan

1. Sample: We were not able to complete the installation of the 100GB machine onto machine 1 because of storage constraints. The system can only handle 20GB, so doing this overloads the system. If we were allocated additional time, we would have created and mounted an additional logical volume that could handle this 100GB machine so machine 1 could in fact utilize the machine. **INCLUDE SCREENSHOTS HERE BELOW THE ATTEMPTED ACTION**

This is for anything that is **IN PROGRESS or NEEDS TO BE DONE AND IS INCOMPLETE**, if something is incomplete or not started, it goes here, not anywhere else.

Vulnerability Assessment

**List common vulnerabilities here and elaborate on them.**

Machines exposed on the puublic network. Why would this be bad. Migrate the systems and configure Firewalls.

Large numbers of unknown users with sudo privileges. Implement more granular controls.

Limited Monitoring capabilities.

Etc.