

**PlaceboPharma**

**Cyber Security Team Blue Team XX**

**Recipient**:

<Recipient Name>

PlaceboPharma, <Recipient Location>

**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, requesting us to submit a compliance and audit report, as well as provide some key areas in the infrastructure which are most highly at risk.  
  
Please read below to see the completed request.

Thank you,

Blue Team XX

Executive Summary

Our team performed a compliance and audit report, which can help identify infrastructure vulnerabilities and compliance risks. These will greatly improve overall security as well as enhance overall operational efficiency.

Some important compliance and audit report findings made by our team are listed below, while the full compliance and audit report can be found in the “Report” section. The tools our team used and specific steps that were taken can all be found in the “Fulfilled Action Items” section.

The following summarizes what was concluded by our team. We believe that the current security stance of the infrastructure poses a **significant** threat and business risk to PlaceboPharma.

* All of the machines across the infrastructure had a **<very high>** compliance score with **this compliance standard**
* All of the machines across the infrastructure had **<very secure>** system configurations from our audit reports and **benchmark tests**

The infrastructures “at risk areas” are as follows:

* The most at risk system on the infrastructure is the Proxy **<More here>**
* Another critical at risk system is the **<More here>**

Fulfilled Action Items

1. Both the compliance and audit reports were taken through the use of **Wazuh**, an open source SIEM (Security Information and Event Management) solution capable of providing audit and compliance reports.
2. A SCA (Security Configuration Assessment) was set up to generate an audit of all of the systems including downloaded packages, services, OS information, networking interfaces, ports, etc.
3. As part of the SCA report, a compliance report based on the CIS benchmark was generated for all of the machines.
4. Some “next steps” were compiled by our team to improve compliance scores and harden vulnerable systems (More information can be found in the “Next Steps” section.

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.

Compliance and Audit Report

This section can be omitted if there is no REPORT requested. *EACH* image must be paired with some kind of explanation and context. They should be ordered.