

**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. We have received the recent request #<> tasking us with the integration of our firewall (Palo Alto) logs into our monitoring (Graylog) solution.

Our team was able to accomplish this integration, creating a more efficient and responsive log monitoring environment, overall strengthening the security stance of PlaceboPharma. Please read the report below for full details.

Thank you,

Blue Team XX

Executive Summary

Our team was tasked with centralizing firewall (Palo Alto) logs into our monitoring SIEM solution (Graylog) for more efficient monitoring and logging across our infrastructure. This integration would allow for an overall more careful analysis of the infrastructure and provide a more efficient way of monitoring and responding to any active threats, since all the logging would be centralized on one monitoring machine.

Our team successfully configured the PaloAlto system to forward logs to our Graylog machine, allowing for a more secure inner infrastructure setup and allowing PlaceboPharama to effectively monitor and secure its customer and proprietary research data.

Assets Affected

| Hostname | IP Address | Additional Notes |
| --- | --- | --- |
| Graylog SIEM Machine |  | Logging machine |
| Palo Alto |  | Firewall and router |

Fulfilled Action Items

1. Palo Alto was configured to send over all event logs that it generates to the Graylog manager machine
2. The Graylog machine was configured to accept all of the logs from the Palo Alto
3. Specific Graylog search indexes were set to properly read and display all logging and event data from the Palo Alto
4. **Screenshots can be added here to maybe show the integration and final log/dashboard**

Action Plan

**Maybe mention setting up TLS encryption of all of this data…?**

Report

**Place screenshots in fulfilled action items if possible!!**