**PlaceboPharma**

**Cyber Security Team Blue Team 07**

**Recipient**: PlaceboPharma Cyber Operations Team

**Date**: 2/1/2025

**Subject:** Response to Request Inject Q01

Dear malou,

Thank you for reaching out to our team. We were asked to conduct a comprehensive network inventory to identify all active subnets, devices, and configurations. This task included distinguishing between public and private subnets along with devices in the network. The detailed report and findings are provided below.

Sincerely,

Blue Team 07

# Executive Summary

This document provides a network topology and device inventory of the network.

# Network Topology

A screenshot of a computer

Description automatically generated

# Network Device Inventory

## DMZ Subnet: 10.0.28.128/25

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **IPv4** | **Mac Address** | **Operating System/Version** | **Open Ports** | **Notes** |
| CA-01 | 10.0.2.138 | 02-6E-F2-5D-85-39 | Windows Server 2019 Datacenter | 80 – Http -IIS  135 – msrpc  139 – netbios-ssn  445 – Microsoft-ds  3389 – rdp  5989 – http – httpd  49669 – msrpc –  5985  5986 | IIS certificate web enrollment enabled |
| Nginx | 10.0.28.200 |  |  | 22 – ssh  80 – http  111 – rpcbind  443 – https |  |
| Greylog | 10.0.28.247 |  |  | 22 – ssh  9000 – greylog clistener  9200 - wap-wsp |  |
| Palo Alto | 10.0.28.254 |  |  | 22 – ssh  23 – telent  80 – http  161 – snmp  443 - https | Telnet should be closed and disabled |

### Management Subnet:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **IPv4** | **Mac Address** | **Operating System/Version** | **Open Ports** | **Notes** |
| Palo Alto | 10.0.28.10 |  |  | 22 – ssh  443 https |  |
|  |  |  |  |  |  |

## Private Subnet: 10.0.30.0/23

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hostname** | **IPv4** | **Mac Address** | **Operating System/Version** | **Open Ports** | **Notes** |
| DC-01 | 10.0.30.77 | 02-32-5E-0C-1E-A3 | Windows Server 2019 Datacenter | 53 – dns  88 – Kerberos  135 -msrpc  139 – netbios-ssn  464 – kpasswd5  593 – http-rpc-epmap  3268 – globalcatLDAP  3389 – rdp  5985 – wsman  5986 - wsmans |  |
| WIN-01 | 10.0.31.11 | 02-61-E0-A8-72-F3 |  |  |  |
| Palo Alto | 10.0.31.254 |  |  | 22 – ssh  23 – telnet  80 – http  443 – https | Telnet should be closed and disabled |
| InfluxDB | 10.0.30.192 |  |  | 22 – ssh  8086 – d-s-n |  |
| cntr-Plane | 10.0.30.255 |  |  | 22 – ssh  179 – bgp  9100 - jetdirect |  |
| node-1 | 10.0.31.0 |  |  | 22 – ssh  179 – bgp  9100 - jetdirect |  |
| node-2 | 10.0.31.77 |  |  | 22 – ssh  179 – bgp  9100 - jetdirect |  |
| node-3 | 10.00.30.5 |  |  | 22 – ssh  179 – bgp  9100 - jetdirect |  |