

**<Company Name>**

**Cyber Security Team Blue Team XX**

**Recipient**:

<Recipient Name>

<Organization> , <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 # made 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, documenting critical jump points, and categorizing key devices. Below, you will find our report detailing our findings.

Thank you,

Blue Team XX

Executive Summary

Our team conducted a comprehensive network inventory to identify all active subnets, devices, and their configurations. As part of this assessment, we distinguished between public and private subnets, documented critical jump points, and categorized key devices. This analysis revealed several network misconfigurations that could significantly impact security and business continuity.

Notably, we observed **[Placeholder: network segmentation to isolate critical systems]** , which results in critical resources being unnecessarily exposed to public networks. Additionally, **[Placeholder: open ports on sensitive systems]** and **[Placeholder: firewall rules]** increase the attack surface available to threat actors. These misconfigurations leave infrastructure-critical resources vulnerable to exploitation. This increases the likelihood that a minor incident could escalate into a severe breach, potentially exposing sensitive customer and business information.

To address these risks, we recommend implementing **[Placeholder: network segmentation to isolate critical systems]**, hardening public-facing systems by **[Placeholder: restricting unnecessary open ports]**, and continuously monitoring traffic to detect unauthorized access attempts. These changes are critical for reducing exposure and ensuring a secure environment for both customer and business operations. Our team has started to triage and implement some of our suggested changes with the current approvals that we have.

**Key Accomplishments:**

* **Private Subnet Range Identified:** **[Subnet 1 Range Placeholder]**
* **Public Subnet Identified:** **[Subnet 2 Range Placeholder]**
* **DMZ Zone Identified:** **[Subnet 3 Range Placeholder]**

Findings

#### **Management interface: [Subnet 1 Range Placeholder]**

* Internal services
* **Devices Identified:**

| DEVICE NAME | IP ADDRESS | NOTES |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

* **Verification Steps:**
  + Conducted connectivity tests using ssh [IP Placeholder].
  + Analyzed routing configurations with netstat -rn or ip route. ( add images here)

#### **Private Subnet: [Subnet 2 Range Placeholder]**

* Dedicated to internal servers and critical systems that require restricted access for security purposes.
* **Devices Identified:**

| DEVICE NAME | IP ADDRESS | NOTES |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* **Jump Point/ Access ip address:**Access to this subnet is controlled and not exposed to external networks.
* **Verification Steps:**
  + Used nmap -Pn [Target Network] to identify accessible services within the subnet. (add images here)

#### **DMZ Subnet: [Subnet 3 Range Placeholder]**

* Provides an isolated area to host semi-public services
* **Devices Identified:**

| DEVICE NAME | IP ADDRESS | NOTES |
| --- | --- | --- |
|  |  |  |
|  |  |  |

* **Jump point:**These systems are accessed from
* **Verification Steps:**
  1. **Internal Isolation Testing:** We tested connectivity to private/internal subnets using:  
     ping [Private Subnet IP] or traceroute [Private Subnet IP].
  2. **Routing Validation:** netstat -rn or ip route ( add images here)

Observed Misconfigurations

1. **Public-Facing IPs:**
   * We identified **public-facing IPs** with open ports (e.g., HTTP, HTTPS, SSH) requiring hardening.
   * **Verification:**
   * We used nmap -p [Port Range] [IP Address] to scan for open ports.
   * We used netstat -tuln to list open ports on local machines.
2. **Unusual or Misconfigured Devices:**
   * We observed routing issues that may require resolution.
   * **Command Used:** netstat -rn or ip route to analyze and update configurations

Network Diagram

Our team prepared a visual representation of public and private subnets, devices, and jump points.

