INTERNAL CHANGE REQUEST

Security Operations Center Deployment

Date of Request: January 1st 2025

Change request #:0001

Requested By: SanchezSecOps

Change type: Infrastructure Upgrade

JUSTIFICATION & RATIONALE

Our current network infrastructure relies on ISP-provided consumer devices, which have locked-down admin interfaces, limited security capabilities, and lack the advanced features necessary to ensure our network's confidentiality, availability, and integrity. **Our limited infrastructure inhibits our ability to develop the internal security team's knowledge base and problem-solving skills**. Upgrading to newer, more capable devices will create the opportunity to securely deploy a security operations center. This will overall improve network security, performance, and allow better segmentation and management.

Key reasons for the upgrade include:

- Enhancing **firewall, routing, and access control capabilities** beyond the limitations of ISP-provided hardware.
- Improving **network isolation and segmentation** to prevent security lab activities from interfering with internal network traffic.
- Limited support for advanced **security protocols** and **encryption standards**.
- Improved hardware **reliability**, **performance**, and **control**.
- Establishing a **segmented lab environment** for testing security tools, performing penetration testing, deception engineering, and monitoring network traffic.

Proposed Change

Upgrade the current network infrastructure and allocating lab hardware/software by replacing ISP-provided devices with business-class networking equipment, which includes the following:

- **New Main Router** (e.g., TP-Link Business Router).
- **New Main Switch with VLAN & ACL Support** for better network segmentation.
- **Dedicated Lab hardware** limiting the impact on existing internal systems
- **Network Monitoring & security tools** increasing threat detection capabilities

SCOPE OF CHANGE

Devices Affected:

- ISP-provided router and unmanaged switch
- Wireless network configurations (e.g., SSID & PSKs)
- Internal LAN & WLAN devices

Network Changes:

- **VLAN implementation** to separate cybersecurity lab traffic from other network segments.
- **Advanced firewall rules** to restrict lab traffic and simulate attack/defense scenarios safely.
- **Logging and monitoring setup** for capturing and analyzing network events or security logs.
- **Secure remote access** for off-site lab management via VPN.

RISK ASSESSMENT

RISK	PROBABILITY	IMPACT	MITIGATIONS
Excessive network downtime during transition	MEDIUM	MEDIUM	Schedule downtime before transition. Have rollback plan and procedures on stand-by.
Configuration errors affecting network access	MEDIUM	HIGH	Pre-configure devices before deployment, maintain back-ups
Performance issues due to misconfigured VLANs	LOW	MEDIUM	Test VLANs offline before making physical changed to network
Security lab traffic bleeding into internal network segments	MEDIUM	HIGH	Apply strict Firewall rules, ACLs, and IDS/IPS

IMPLEMENTATION PLAN

PHASE ONE: INFRASTRUCTURE UPGRADE

1. Make appropriate site alterations physically preventing infrastructure improvements/implementation

2. Begin transition after established maintenance window opens and required personnel are on-site

3. Follow network diagrams to create new segments for devices and establish new IP ranges

4. After new main Router/Switch configurations are set replace previous hardware and bring new systems and designated devices back online ensuring network access on all affected devices

PHASE TWO: SECURITY TESTING

1. Implement pre-established ACLs on designated networks
    a. **Example ACL:** `rule 10 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255`
2. Ensure no contact can be established between isolated and internal networks with ping tool
    a. **Example**: **`<root@192.168.4.1>`**`ping 192.168.1.1`
    b. **Expected**: `Packets: Sent= 10, Received= 0, Lost= 10 (100% loss)`
3. Test exploitability of PSKs on segments using older security protocols like WPA2 (Hashcat & Aircrack)
    a. **Attacks Used:** dictionary attack and GPU brute force attack

PHASE THREE: SOC DEPLOYMENT

1. Upgrade newly allocated virtualization servers to 64GB RAM each, totaling 128GB
2. Wipe internal storage devices avoiding supply chain attacks using **DoD 5220.22-M**
3. Remove internal 802.11 devices limiting direct wireless client attacks
4. Create Installation media for type 1 hypervisor
5. Configure server UFEI setting to support hypervisor install
    a. **FAST BOOT**: DISABLE
    b. **SECURE BOOT**: DISABLE
6. Deploy dedicated SOC devices (1xRouter, 1xSwitch, 7xCAT6 patch cables, physical clients)
7. Wiring scheme: Internal Network> SOC Router> SOC Switch> SOC LAN Clients & Servers

PHASE FOUR: END-POINT & SECURITY TOOLS

1. Acquire software tool's documentation for quicker deployment & troubleshooting
2. Create VMs for security and monitoring tools Security Onion, OPNsense, Elastic, etc…
3. Create VMs to deploy desktop environments for SOC personnel use
4. Configure nodes to forward logs to Security Onion SIEM
5. Create VM for honeypots, Create VLAN for honeynet, Write & test ACLs to limit honeynet contact from internal devices

ROLLBACK PLAN

In case Infrastructure upgrades and SOC deployment fail the following rollback plan will be on standby should this transition exceed the established maintenance window.

1. Create Backups (pre-transition)
    a. end-point restoration points
    b. network device configuration files
    c. Firmware version and configuration files
2. During transition keep existing network infrastructure intact
3. If maintenance window closing approaches within two hours while diagnosing complex issues begin rollback plan
4. Allocate secure physical storage space for new network infrastructure
5. Power down all new network devices and ensure they're air-gapped from any network
6. Re-install previous networking equipment and test LAN/WAN access from networked nodes