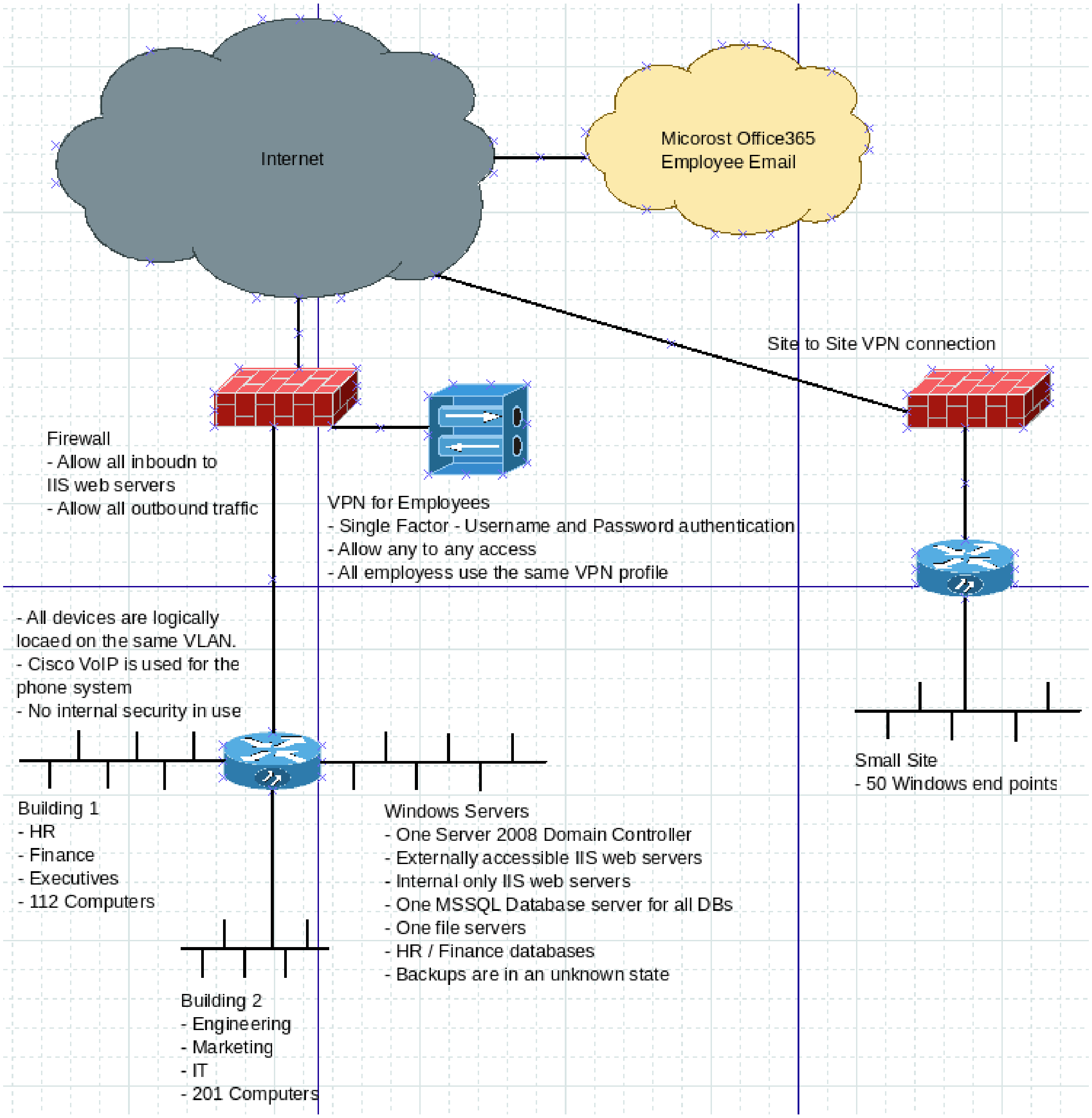
Cybersecurity Maturity Plan

Current Enterprise Network Topology



Firewall
- Allow all inboudn to
IIS web servers
- Allow all outbound traffic

VPN for Employees
- Single Factor - Username and Password authentication
- Allow any to any access
- All employess use the same VPN profile

- All devices are logically locaed on the same VLAN.
- Cisco VoIP is used for the phone system
- No internal security in use

Building 1
- HR
- Finance
- Executives
- 112 Computers

Windows Servers
- One Server 2008 Domain Controller
- Externally accessible IIS web servers
- Internal only IIS web servers
- One MSSQL Database server for all DBs
- One file servers
- HR / Finance databases
- Backups are in an unknown state

Building 2
- Engineering
- Marketing
- IT
- 201 Computers

Small Site
- 50 Windows end points

Current State of Enterprise Security

Endpoint Security:

- Anti-virus is used on all user end points, but there is no state monitoring.
- Users are administrators on all user end points.

Network Security:

- No SIEM or central log collection.
- Internet filtering is not currently implemented.
- Only standard stateful ACL and NAT overload functionality is in use on the pfSense firewalls.
- No active vulnerability management.

Access Control:

- All employees are granted VPN access by default.
- Users have never had to change their passwords. Some user accounts are over 10 years old.
- Helpdesk and pc support have domain admin privileges.
- Vendors and other 3rd parties have access, including remote access, into the internal networks.

Legacy System:

- There is a legacy web application that forces the use of an unsupported Linux OS and, therefore, a non-patchable server.

The following includes the recommended changes needed for the enterprise’s network from highest priority to lowest priority changes:

1. Implement Security Onion.
2. Change VPN policy and add multi-factor authentication (MFA).
3. Remove administrator rights on all user, Helpdesk, and pc support endpoints.
4. Update password policy.
5. Implement vulnerability management.
6. Adjust Vendor and 3rd party access to the network.
7. Implement state monitoring to monitor Anti-Virus (AV) software.
8. Upgrade pfSense firewalls.
9. Implement Virtual local area networks (VLANs), network segmentation, and Demilitarized Zone (DMZ).
10. Enable Internet filtering.
11. Isolate legacy web application and plan data migration to new platform.
12. Implement new security policies.
13. Hire a penetration tester.

Proposed Physical Setup and Network Design

The network will be segmented into multiple VLANs to isolate different parts of the infrastructure. This segmentation reduces the attack surface and limits lateral movement within the network in case of a compromise.

VLAN 1: Management/Administrator

- Isolate management and administrator traffic from regular user traffic.
- This traffic includes accessing servers, firewalls, routers, switches, and Security Onion.
- SSH traffic for device configuration and monitoring.

VLAN 2: VoIP VLAN

- Isolate VoIP traffic from other network traffic.
- Enhances call quality by reducing latency and jitter.
- Secures voice data.

VLAN 3: User VLAN

- All users excluding management and administrators.
- Standard user traffic including email, web browsing, and accessing internal applications.

VLAN 4: Wireless VLAN

- Separate wireless traffic from wired traffic to improve management and security.
- Includes devices like smartphones, laptops, and tablets.

VLAN 5: Vendor/Third-Party VLAN:

- Isolate and monitor traffic from vendors that require remote or on-site access.

VLAN 6: Guest VLAN

- For guests visiting on-site.

The following servers will be segmented into VLANs to enhance security:

VLAN 7: Domain Controller Server

- Manages authentication and access control for the entire network.

VLAN 8: Internal IIS Web Servers

- Hosts internal web applications.

VLAN 9: MSSQL Database Server

- Hosts all enterprise databases.
- Includes HR/Finance databases.

VLAN 10: File Server

- Provides centralized file storage and sharing.

VLAN 11: Network Access Control Server

- Manage and monitor all NAC operations including:
    - Communication between network devices.
    - Authentication of endpoint devices.

VLAN 12: External IIS Web Servers

- Hosts external web applications.

VLAN 13: Legacy Web Application

- Non-patchable server that forces the use of an unsupported Linux OS.

Demilitarized Zone (DMZ):

- A dedicated DMZ will be implemented between the main site router and the internet to provide an additional layer of security.
- VLAN 12 (external IIS web servers) and 13 (legacy web application server) will be placed inside the DMZ to isolate public-facing servers from the internal network.
- An additional firewall will be placed between the DMZ and the internet to filter inbound and outbound traffic, ensuring only necessary connections are allowed to the IIS web servers.
- This design ensures that if an attacker compromises a public-facing server, they will be contained within the DMZ and unable to access internal network resources.

Proposed Hardware

SecurityOnion Nodes:

- **Primary Node:** Handles data processing, log ingestion, and serves as the central management interface.
- **Sensor Nodes:** Placed across network segments to monitor traffic, capture packets, and generate alerts, with data forwarded to the primary node for centralized analysis.

Network Tap:

- Passively monitors network traffic for the sensor nodes without disrupting the flow of data.

Firewall Hardware:

- Capable of deep packet inspection, intrusion detection, VPN, and traffic filtering, with multiple interfaces to support VLAN segmentation.

Additional Networking Hardware:

- **Core Switches:** Layer 3 switches with Quality of Service (QoS) and VLAN support to enable network segmentation and manage traffic efficiently.

Data Retention Storage:

- Network-attached storage (NAS) to store logs and backup data, with adequate storage for the organization's data retention policies.

Note: Exact hardware specifications, including CPU, RAM, and storage requirements, should be customized based on a detailed analysis of the organization’s traffic volume, log retention needs, and processing requirements.

Proposed Software/Policies

SecurityOnion:

- **Purpose:** Enhance visibility across the enterprise network, enabling proactive detection of threats and reducing response times. Centralized monitoring through SecurityOnion allows for efficient log aggregation, real-time intrusion detection, and comprehensive analysis of network traffic using tools like Zeek and Suricata.
- **Deployment Architecture**: One primary node and multiple sensor nodes.
  - The primary node will handle data processing, log ingestion, and provide the central management interface. It will be responsible for collecting and correlating logs from all sensor nodes.
  - The sensor nodes will be strategically placed across different network segments to monitor traffic, capture packets, and generate alerts. Each sensor node will forward its data to the primary node for centralized analysis.
- **Log Management**: Kibana, Elasticsearch, and Logstash for centralized log aggregation and analysis.
- **Intrusion detection and prevention systems:** Zeek and Suricata to provide real-time traffic analysis and threat detection.
- **Incident Response:** Playbook for response automation and The Hive for case management.
- **Automated Threat Intelligence:** Integrate with threat intelligence feeds to identify and respond to emerging threats.
  - This helps with log enrichment by additional context to raw log data to make it more useful for analysis.

Network Security:

- **Cisco Identity Services Engine (ISE):** Deploy network access control (NAC) software to enforce role-based access control (RBAC).
  - Ensure only authorized devices can connect to specific networks within the enterprise.
- **Nord VPN:** Upgraded VPN solution that supports multi-factor authentication (MFA).
  - Switch from single factor authentication to multi-factor authentication.
  - Remove shared VPN profiles and implement unique VPN profiles for each user.
  - Remove any to any access and implement RBAC policies.
- **pfSense XG-1541:** Next-generation firewall appliance that provides advanced security features.
  - Enable web filtering to monitor web activity and prevent users from accessing malicious and inappropriate content.
  - Limit inbound traffic to the IIS web servers.
  - Limit and monitor outbound traffic to prevent unauthorized data exfiltration.
  - Enable IDS/IPS to enhance network security.
- **Cloudflare Web Application Firewall (WAF):** Cloud-based WAF solution deployed in front of web servers.
  - Monitor and filter HTTP/HTTPS traffic and protect against web application attacks.

Identity and Access Management:

- **Multi-factor Authentication (MFA):** Implemented for VPN access for all employees.
  - Employees will enter a username and password followed by confirming a token sent to their smartphones.
- **Password Policy:** All employees will be required to change their password immediately and adhere to the new password policy.
  - Frequency of password change: Every 90 days
  - Character length: 12
  - Must include at least one uppercase letter
  - Must include at least one lowercase letter
  - Must include at least one numerical character.
  - Must include at least one special character.
- **CyberArk Software:** Add privileged access management (PAM) software to monitor access to privileged accounts and reduce the risk of unauthorized access.
- **Revoke Admin Rights:** Remove administrator privileges on all user endpoints, including Helpdesk and PC support staff, to reduce security risks, excluding the system administrator.

Endpoint Security:

- **Norton Antivirus:** Integrated with SecurityOnion and equipped with endpoint detection and response (EDR) capabilities.
  - Implement state monitoring through a centralized management console to continuously monitor the antivirus software across all endpoints and servers. This ensures that the antivirus is always active, up-to-date, and functioning correctly.
  - Used on all endpoints and servers.

Vulnerability Management:

- **OpenVAS:** Implement a vulnerability scanning solution with OpenVAS to regularly scan the network for vulnerabilities.
- **SolarWinds Patch Manager:** Patch management software to automatically update all endpoints and servers and avoid lapses of unpatched systems causing vulnerabilities.
- Hire a penetration tester to periodically test the network for vulnerabilities.
- **Legacy Web Application Strategy:**
  - The legacy web application will be isolated in a dedicated VLAN with strict access controls.
  - A plan will also be developed to migrate the data from the legacy web application to a newer, more secure platform. This will eventually phase out the unsupported Linux OS and non-patchable server.

Data Protection:

- **Forcepoint Data Loss Prevention (DLP):** DLP solution to prevent data from being lost, leaked, or accessed by unauthorized users.
- **Acronis Backup:** Data backup solution.
  - Create a hot, warm, or cold site for disaster recovery.
  - Implement automated backups stored both on-site and off-site.
  - Encrypt all backup data.
  - Daily incremental backups with weekly full backups.
  - Regular testing of backed up data.

Security Awareness Training:

- Introduce mandatory, ongoing security awareness training for all employees to enhance the overall security posture on the enterprise.
- Training will take place quarterly covering topics such as recognizing phishing attempts, proper password management, data handling, and new emerging threats.