Proof of Concept

Demonstration of a typical network environment, malware included.

Introduction of a Firewall, SIEM, Greenbone, etc. included within the Bronze Tier.

**How much of an impact could we make on an average small pharmacy?**

Tiers for Pricing : Bronze, Silver, Gold.

**Possible software :**

Security Onion

Greenbone

Sophos Firewall

Bitwarden Password Management

Ticketing System | osTicket?

$36,000 Billed Annually

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\* Responsibilities \*

Cade

* SIEM (Security Onion)
* osTicket

Jubilee

* Documentation & Compliance
* Bitwarden Password Management

Michael

* vCenter Infrastructure
* Sophos Firewall
* Penetration Testing

Research Enterprise-Grade equipment

(Fortinet, Palo, Cisco)

Host Environment in vCenter to access it from WebUI, Running on Room 115 Server.

—---------------------------------------------------------------------------------------------------------------------------

**ONBOARDING PROCESS**

Audit Windows Active Directory Environment to find exploits that they might be vulnerable to.

Document Operations of the Audit

Audit Environment performing 1:1 Commands/Exploits from initial Audit.

Compare grades from both evaluations to gauge differences in performance and security.

—---------------------------------------------------------------------------------------------------------------------------

**ONGOING MANAGEMENT**

After the Initial Onboarding, clients will return to their operations as normal.

We will do our part in monitoring from our Remote Access Operations Center

In the case that there is any suspicious activities in your Environment, Our SIEM (Security Information Event Management) Platform will pick up on it, Alert us and you through Email and System Notifications.

In the case of any further maintenance we will remain on call

Monday - Friday

8AM - 5PM

Contact Us @Services@easysec.com

—---------------------------------------------------------------------------------------------------------------------------

**ENVIRONMENT HARDENING**

**Environment hardening includes**

Deployment of Network Security Appliances :

Security Onion SIEM

Sophos Firewall / IPS

Hardening of the Domain Through :

GPO

Password Policies / Management

Security Groups

Elimination of Default and Administrator Users

Training of Staff in matters such as :

Phishing

Social Engineering

—--------------------------------------------------------------------------------------------------------------------------