Subject: Security Recommendations

Hello Bob,

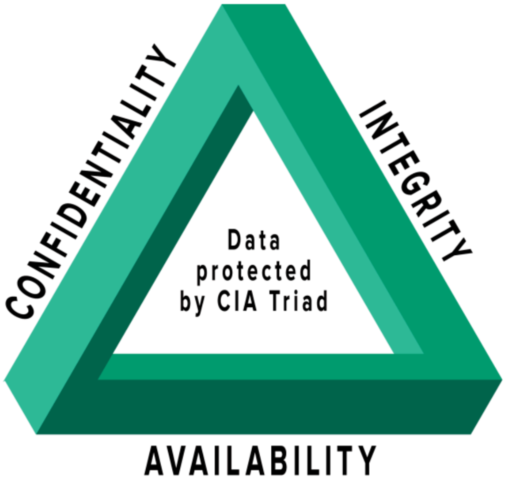
Joe here from the Cyber Security department, and hope you're having a great day so far!

As per your request, I have reviewed security for our company, and I'm confident the following security policy recommendations would improve our security posture.

Please ensure this email has your undivided attention for your review at your earliest convenience. Should take around 15 minutes. Links are embedded for context should you require it, however everything in this email is all you need to know 🙂

Assessing Risk Tolerance:

Cyber Security relies on a key concept called the CIA triad, that assigns security as Confidentiality, Integrity, and Availability. It's one of the core pillars of our decision making when coming up with security policies.



Risk Appetite: Premium House Lights Inc. has a moderate risk appetite, meaning it is willing to accept certain levels of risk to achieve its business goals while prioritizing customer trust and data protection.

Capacity to Absorb Losses: The organization has moderate financial reserves and contingency plans in place, allowing it to absorb moderate financial losses without significant impact on operations. However, a major data breach could severely impact customer trust and business reputation.

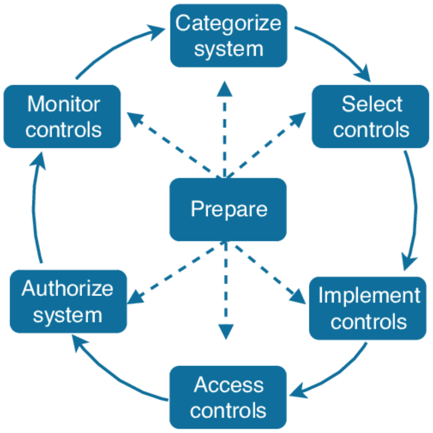
Influence on Security Measures: Given the moderate risk appetite and capacity to absorb losses, the recommended security measures focus on preventing high-probability and high-impact threats, such as data breaches and DDoS attacks, while also ensuring compliance with PCI DSS standards to protect cardholder data and maintain customer trust.

eCommerce businesses must comply with the **PCI Data Security Standard (PCI DSS)**, and given the hybrid nature of an eCommerce business and physical location, we need to examine both aspects independently to determine their Risk, potential threats, and how to best mitigate/recover.

Alongside the CIA Triad, we are using the **NIST Risk Framework (RMF)** to assess and determine the security needs of the company. Loosely speaking, NIST defines **RMF** as a framework that provides a flexible seven-step process that integrates cybersecurity, privacy, standards and guidelines to manage security and privacy risks together. For a full definition, visit the link **seen here**

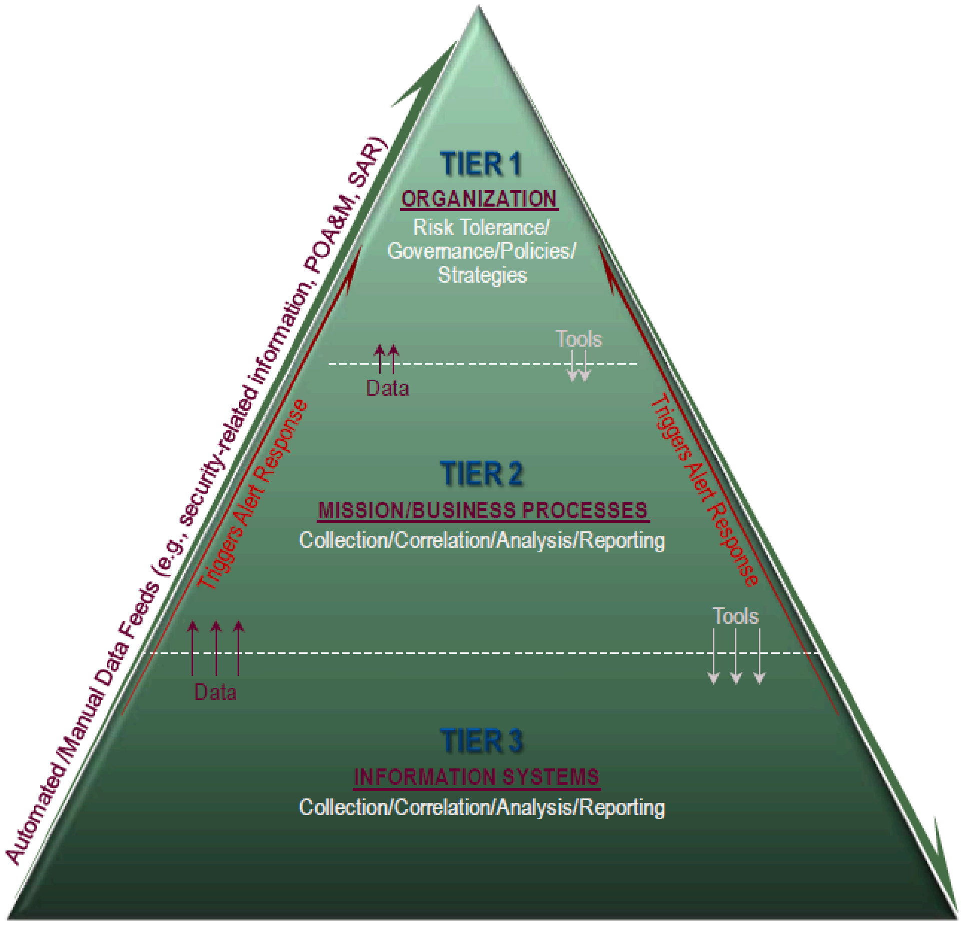
Plus, not only is it free, it's also very comprehensive and widely used across multiple industries, including private, local, and state-level organizations.

Here's an overview of the seven steps involved with the NIST Risk Management Framework:



Alternatively, if the option is within the company's resources, **ISO/IEC 27001** is another framework to consider. While it is a paid framework, it does provide the benefit of a formal certification which can be beneficial for demonstrating compliance and commitment to security best practices.

These policies are also in respect to NISTs framework of information security and **corporate governance**, which aims to amalgamate best security practices with corporate and business strategies and goals:


TIER 1
ORGANIZATION
Risk Tolerance/ Governance/Policies/ Strategies
Data
Tools
TIER 2
MISSION/BUSINESS PROCESSES
Collection/Correlation/Analysis/Reporting
Data
Tools
TIER 3
INFORMATION SYSTEMS
Collection/Correlation/Analysis/Reporting
Automated /Manual Data Feeds (e.g, security-related information, POA&M, SAR)
Triggers Alert Response
Triggers Alert Response

eCommerce Risks:

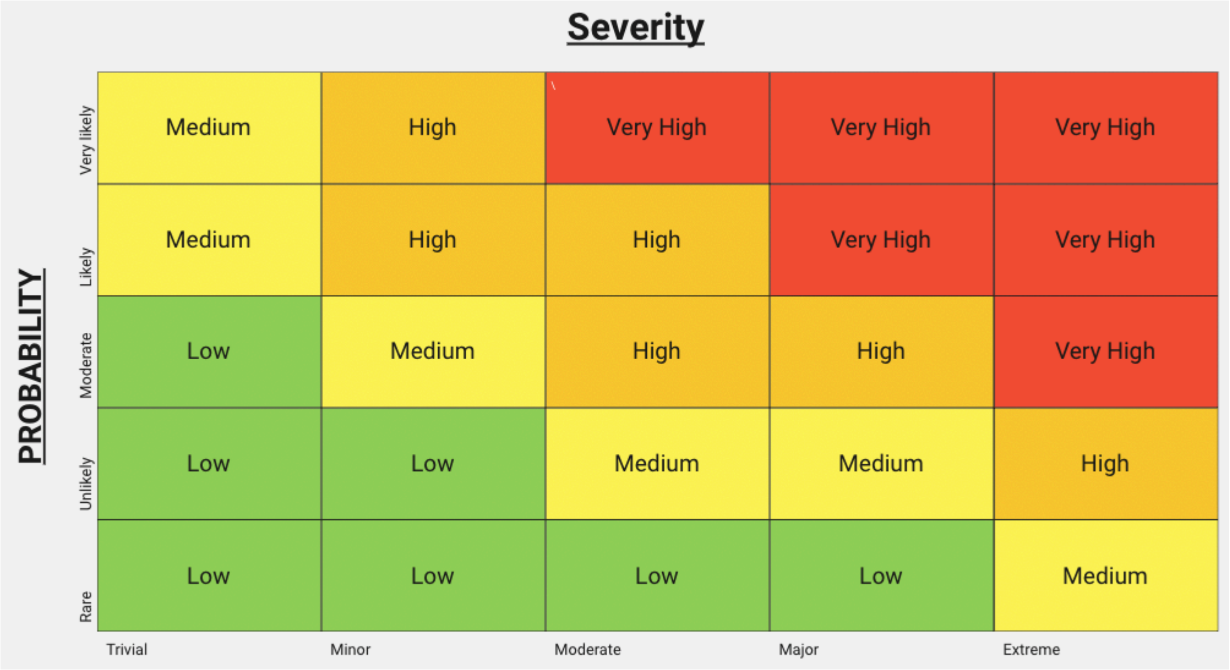
- Data being intercepted during online payments, leading to a leak of sensitive payment data (Man in the Middle Attacks)
- SQL injections into the file server from the website page and contact pages.
- Phishing and spear-phishing campaigns via customer service emails
- Dedicated Denial of Service attacks (DDoS)
- Insider threats (disgruntled workers, accidental leakage of data, etc)
- Internet of Things precautions for specific light bulbs that may get sold, if applicable. Could lead to reputational damage should vulnerabilities get discovered and affect the customers.

Physical Risks

- Authorized personnel losing or stolen keys/access cards to grant unauthorized access into the Store front/store vault/other sensitive data.
- Installation personnel misplacing sensitive devices at a clients house.
- Physical brute-force breach at the store front (breaking the locks, smashed windows, etc)

From this point, we need to assess the Risk Tolerance for each aspect, given that there will always be a limited amount of resources, we do need to accept that some risk could occur: the goal is to limit and mitigate as much as possible to prevent the most likely and most impactful risks from occurring.

In deciding this, we use a Threat Probability and Impact Matrix to score and evaluate the different types of threats that could occur, and have been assessed accordingly. Seen in the tables below:



Severity

PROBABILITY	Trivial	Minor	Moderate	Major	Extreme
Very likely	Medium	High	Very High	Very High	Very High
Likely	Medium	High	High	Very High	Very High
Moderate	Low	Medium	High	High	Very High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Low	Medium

Threat Probability and Impact Table

Risk	Probability	Severity	Impact Assessment	Domain
eCommerce Risks				
Data interception during online payments	Likely	Major	Very High	Confidentiality
SQL injections	Likely	Extreme	Very High	Confidentiality, Integrity
Phishing and spear-phishing campaigns	Very Likely	Major	Very High	Confidentiality
DDoS attacks	Moderate	Extreme	High	Availability
Insider threats	Moderate	Major	High	Confidentiality, Integrity
IoT vulnerabilities	Unlikely	Moderate	Medium	Confidentiality, Integrity, Availability
Physical Risks				
Lost or stolen keys/access cards	Moderate	Major	High	Confidentiality
Misplacing sensitive devices at client sites	Likely	Moderate	Medium	Confidentiality
Physical brute-force breach	Unlikely	Major	Medium	Availability

Key Recommendations:

Based on the criteria of Risk outlined and assessed in the previous section, I'm pleased to present to you these recommendations for security policies, from highest to lowest priority.

Security Policies:

Implementing Encryption between payment providers:

Data interception can occur almost immediately after a service goes online, especially when sensitive payment details are involved. Encryption is therefore used to secure the data between send and receiving points. This would prevent packet sniffers from intercepting and eavesdropping into payment information.

Since the topology suggests the payments are being processed in house, to remain **PCI DSS compliant**, their quick reference guide suggests the following to share with the development team:

"The PCI Data Security Standard PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

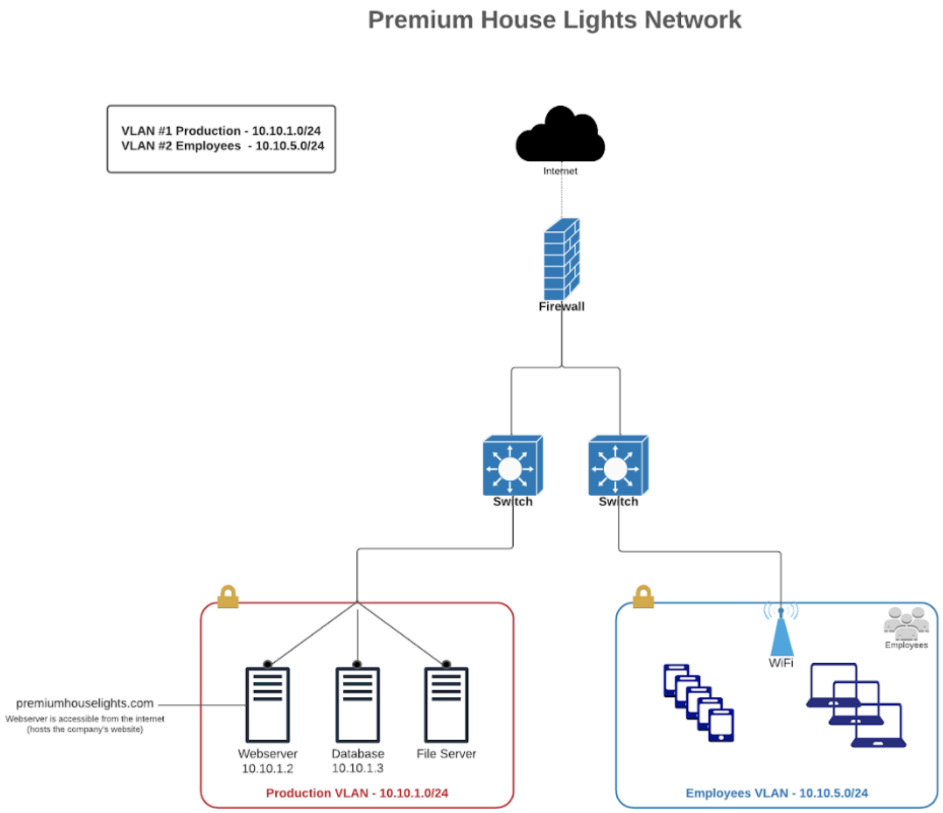
12. Maintain a policy that addresses information security for all personnel"

Alternatively, You could use a third-party payment provider that can set up your business to process payments, as they are widely used by eCommerce and Brick and Mortar stores alike, such as: **Stripe Payments** or **Square Payments**

Note*: Introducing any third-party services into any system introduces its own security risks. While they (Stripe and Square) are widely used, analyzing those risks specifically with third party payment providers is outside the scope of this assessment.*

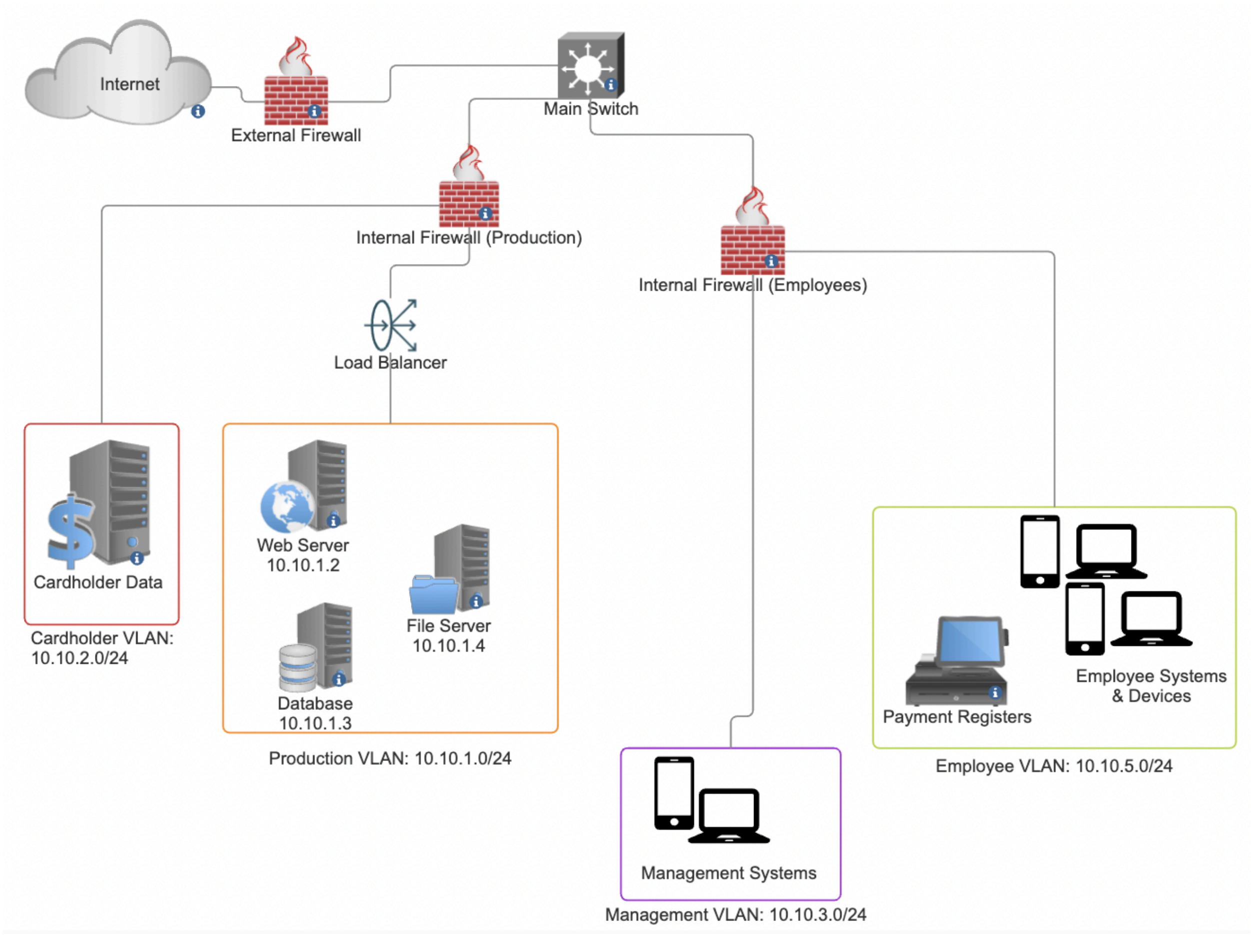
Establishing Role-Based Access Control (RBAC):
There are few types of access control we can implement, however given the structure of your business **Role-Based Access Control** is our recommendation. From StrongDM.com: *"RBAC is a security approach that authorizes and restricts system access to users based on their role(s) within an organization."* - This ensures that only dedicated employees have specific access privileges to sensitive data and systems. This minimizes the risk of unauthorized access and data breaches.

Improve Network Segmentation:
The networks are currently quite centralized between the production and employee teams outlined in the original topology diagram we received:


Premium House Lights Network
VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
Internet
Firewall
Switch
Switch
premiumhouselights.com
Webserver is accessible from the internet
(hosts the company's website)
Webserver
10.10.1.2
Database
10.10.1.3
File Server
Production VLAN - 10.10.1.0/24
WiFi
Employees
Employees VLAN - 10.10.5.0/24

Segmenting the network provides security professionals with more precise control for investigating and troubleshooting network issues in the event that a threat actor does manage to infiltrate the system. This modular approach facilitates containment and malware eradication, and prevents attacks by limiting lateral movement across our networks.

Below is a recommendation for an updated network topology and VLAN configuration:



This topology ensures that data can move between the internet and our internal systems, while also remaining PCI DSS compliant with the Cardholder Data being secure in its own VLAN. We manage access to it with proper firewall configurations.

Next, will be the outline of the VLANs, which are contained network segments.

List of VLANs and their function:

VLAN Name	Subnet	Purpose	Device
Cardholder Data	10.10.2.0/24	To securely store, process, and transmit cardholder data, a requirement for PCI DSS	Cardholder Server
Production	10.10.1.0/24	To host production environment, including web server, database, and file server	Web Server (10.10.1.2)
			Database Server (10.10.1.3)
			File Server (10.10.1.4)
Management	10.10.3.0/24	For Management and administrator access.	Management Systems
Employee	10.10.5.0/24	For employee devices, systems, payment registers, and reserved for future expansion	Employee Systems
			Payment Registers

Monitoring & Detection:
As online traffic grows, our security also needs to scale up to meet the demand. Since it is impractical to manually review thousands of requests, Cyber Security professionals use something called a **Security Information and Event Management System (SIEM)** for analyzing logs, detecting Indicators of Compromise (IoCs), and conducting incident response should they occur. These central logs are essential and must be contained for cyber security professionals to effectively investigate any breaches and monitor network traffic.

Security Information and Event Management Systems (SIEM) overview:

The following SIEMs are Open-Source, and therefore no costs to running the software. While open-source tools are cost-effective and flexible, they might require more maintenance and monitoring. According to **Comparitech.com** some commonly used ones are:

- **AlienVault**: This is one of the oldest SIEM systems around but it is very well supported by AT&T, so it is still being improved on solid, reliable code that has been extensively tested in the field. Runs as a virtual appliance.

- **ELK Stack**: A free suite of data collection, sorting, and visualization tools that let you create your own SIEM threat detection rules. Available for Windows, Linux, and macOS.
- **OSSEC**: This tool has good threat detection routines but weak log management functions so splice it with ELK Stack for the best of breed. Agents available for Windows, Linux, macOS, and Unix but the server only runs on Linux or Unix.
- **Wazuh**: A fork of OSSEC that has better logfile management services than the original and relies on ELK. Runs on Linux.
- **MozDef:** A basic SIEM for small businesses that integrates ELK Stack. Run it on Docker or CentOS Linux.
- **SIEMonster:** A competent SIEM for small businesses with a paid version for larger organizations. Runs on Docker, Linux, and macOS, or as a virtual appliance.

For commercial Solutions, they do offer a lot more robust features with a ton of features already built in, plus they're typically an all-in-one solution so there are less parts overall that could interfere with a system. Commercial options like **Splunk**, **DataDog**, and others offer greater reliability and professional support. For pricing details, please reach out to any vendors that interest you directly, as it is outside the scope of this email.

Open-Source vs. Commercial:

Ultimately, the choice to go with open-source or commercial solutions comes down to how much maintenance & potential risk, compared to resources available to maintain security systems. Open-source is generally more cost-effective and flexible but may require more initial setup and maintenance throughout its use. While commercial solutions are significantly more expensive, they offer robust features, professional support, and continuous updates throughout its lifespan.

Personal SIEM Recommendation:

ELK Stack (**ElasticSearch**, **LogStash**, **Kibana**) plus **Wazuh**. This way we get fantastic synergy between central logging, detection and event management. While there is quite a bit of setup necessary, since it is widely used it enhances onboarding efficiency and offers a lot of flexibility as the business's security needs evolve, and this saves resources meaning you can reinvest what the company would allocate towards other business goals.

Intrusion Detection Systems (IDS) Overview:

Intrusion Detection Systems (IDS) significantly help our teams monitor network traffic for suspicious activities and take appropriate action when required. Here are some recommended IDS solutions:

Open-Source Solutions:

- **Snort**: One of the most widely used open-source network intrusion detection systems. It performs real-time traffic analysis and packet logging.
- **Suricata**: An open-source network IDS, intrusion prevention system (IPS), and network security monitoring engine. Known for its high performance and advanced multithreading capabilities.
- **Zeek (formerly Bro)**: An open-source network monitoring framework. It focuses on network traffic analysis and is highly extensible.

Commercial IDS Solutions:

- **Cisco Secure IPS**: Offers comprehensive threat protection and visibility into network traffic. Integrates well with Cisco's security ecosystem.
- **Palo Alto Networks Next-Generation Firewall (NGFW)**: While primarily a firewall, it includes robust IDS/IPS capabilities, offering deep packet inspection and advanced threat prevention.
- **McAfee Network Security Platform (NSP)**: Provides advanced threat detection and intrusion prevention with high performance and integration capabilities.

Recommendation:

We use **Snort**. Snort gives us a lot of tooling, while the same traits do apply when using any open-source, it will nicely adapt to our existing ELK Stack + Wazuh tooling.

Implementing an IDS will enhance our ability to detect and prevent malicious activities, improve network visibility, and strengthen our security posture.

Vulnerability Management:

Lastly, we should implement the following practices regularly so we can proactively manage vulnerabilities and maintain an effective overall security posture:

- Conduct regular vulnerability assessments and penetration tests to identify security gaps.
- Ensure timely patching of software and systems to protect against known vulnerabilities.
- Provide ongoing security training and awareness programs to employees to help them recognize and respond to threats.
- Develop and maintain an incident response plan to quickly address and mitigate the impact of security incidents.

Phew! You made it! I know that was a lot of information to review, however it is quite comprehensive and aligns with our business strategies. If you do require further details or clarification on any of the topics, please let us know!

Cheers,
Joseph D.

Cyber Security Specialist
Premium House Lights Inc.