

July 25, 2024

# CyberSense

*Cybersecurity for small businesses*

---

Team Diamond

# TABLE OF CONTENTS

03	Our Team	18-19	Functional Components
04	Our Pitch	20-30	Risks & Mitigation
05-07	The Problem & Process Flow	31	Work Breakdown Structure
08-09	Our Solution & Solution Flow	34	Algorithms
10-12	Our Will Do's & Will Nots	35	Database Schema
13-16	Competition Matrix	36	Real World Product vs Prototype
17	Development Tools	37	Required Libraries, Tools, and Technologies
		38	Conclusion

# TEAM



Emily Seepes



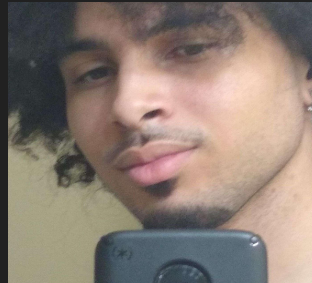
Kyle Hubbs



Christian Parker



Makendra Crosby



Jordan Kane



Michael Porter

# Elevator Pitch

Small businesses face increased threats from cyber attacks, but many lack the resources and expertise to defend themselves effectively.

## **Our Solution?**

An easy to use web application that provides accessible cybersecurity education and real-time threat intelligence tailored for non-technical users. By offering comprehensive, straightforward training modules, curated from sources such as NIST, CISA, and Cybrary, and integrating with external threat intelligence APIs, our platform equips small business owners, IT managers, and employees with the knowledge to strengthen their defensive posture against cyber threats.

# The Societal Problem


Small businesses struggle with cybersecurity due to limited resources and knowledge. They are highly vulnerable to threats like phishing, malware, and ransomware, which can compromise their data and damage relationships with customers, suppliers, and partners. Existing cybersecurity education and threat intelligence platforms are often too complex and expensive, making essential tools and information inaccessible, thus increasing their risk.

# Problem Characteristics & Impact Analysis

## 60%

**Of Small Companies Close  
within 6 Months of Being  
Hacked**

Leading causes of these closures &  
why small businesses should be  
cautious:

- 
- Financial Loss
  - Loss of Trust
  - Reputational Damage

AND your small business is *too broke* to afford help:

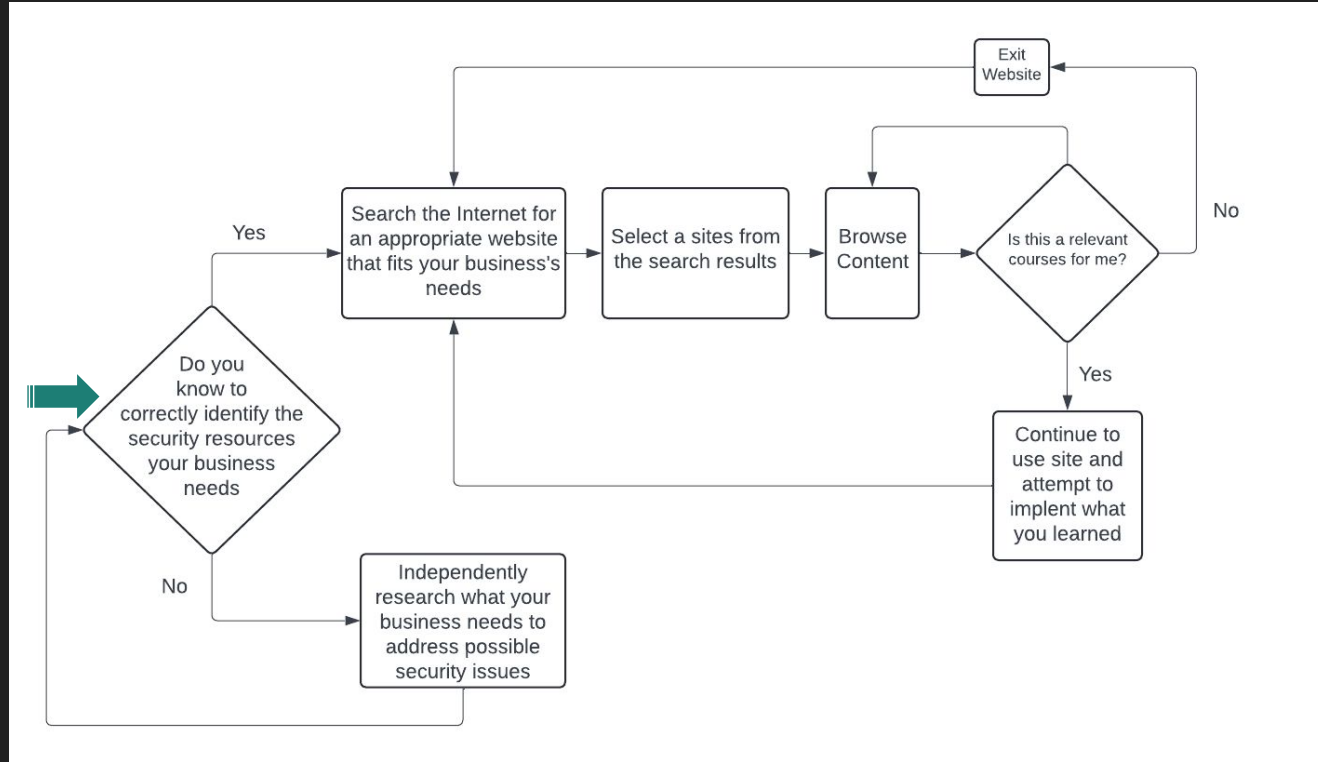
Splunk: Dependent on the volume of data, but anywhere from \$1,800 to \$10,000+ per year

FireEye: Dependent on the number of devices connected to a network (also known as endpoints) and on-site solutions, but can range from \$1,500 to \$30,000+ per year

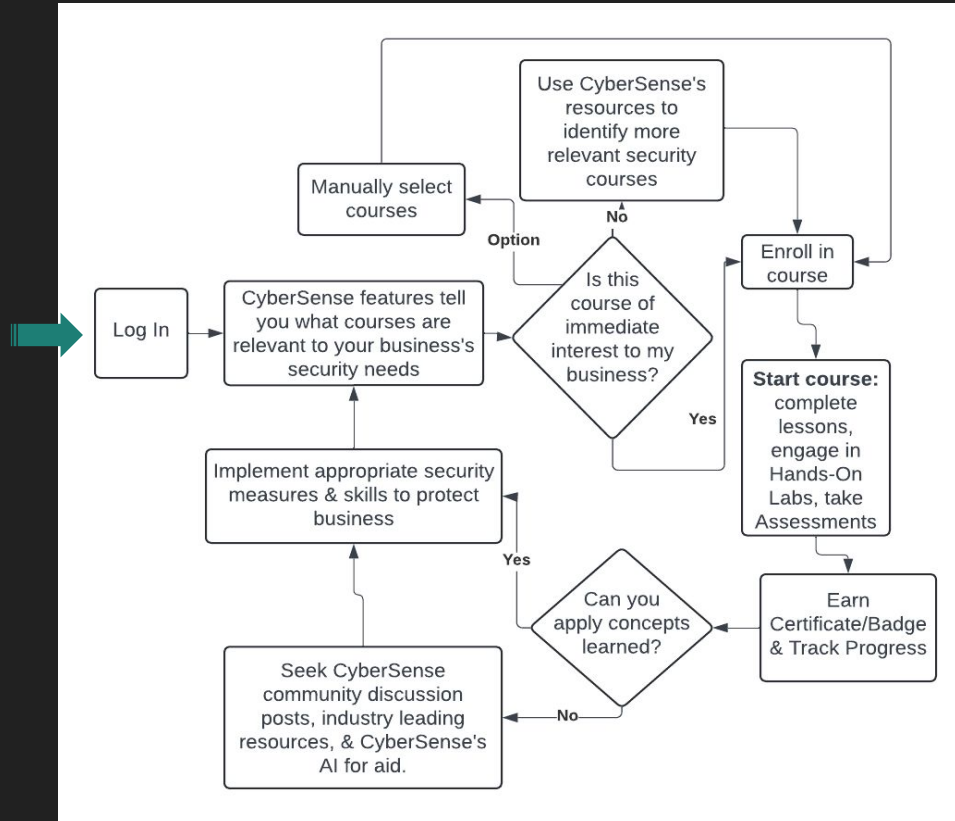
Palo Alto: \$50,000 to \$100,000 per year

Cybersecurity Firms: Dependent on the scope of coverage, but can easily be in the multiple thousands of dollars per month .

# The Societal Problem: Current Process Flow



# Solution: Solution Process Flow





# Solution

CyberSense is a web-based application that offers cyber security education to small businesses. CyberSense allows businesses to educate themselves through readily accessible resources, real-time threat intelligence, and community collaboration tools that enhance cybersecurity awareness.

*Cybersecurity hardening will be “common sense” with CyberSense*

# Features & Functions: What it Will Do

- **CyberSense Dashboard:** A clean and easy-to-navigate dashboard equipped with recent threats, community discussions, user notifications, and educational material.
- **CyberSense Modules:** Modules offering courses and training from the industry's most reputable sources. Material is automatically updated to provide the latest news, guides, and best practices.
- **IoC Reporting:** A form for reporting indications of compromise. Through predefined threat types and additional details of a threat, users are able to simplify the reporting process, clearly define suspected compromise, and have it analyzed and triaged.

## Features & Functions: What it Will Do - cont.

- **CyberSense Real Time Response (RTR):** RTR displays recent threat reports and categorizes them through existing external threat intelligence APIs. This makes it easier for users to be on the lookout for such threats.
- **Community Boards:** Allows users to share experiences, discuss threats, and collaborate on cybersecurity best practices.
- **AI Q&A:** Python-based AI Q&A solution is equipped to understand user queries, search existing databases and the internet, and provide up-to-date and accurate answers, as well as relevant internal and external resources.

# Features & Functions: What it Will Not Do

- **Complex User Interface:** Should not overwhelm small business owners who may not have extensive technical knowledge.
- **Lack of Customization:** Should not provide a “one size fits all” solution but rather a customized or tailored solution according to the needs of the small business.
- **Redundant Features:** Should not have overlapping functions that perform the same thing or have unnecessary tools that add little value and are rarely used.
- **Extensive Training Programs:** Should not include in-depth training programs. Basic training and resources will still be available, but extensive training programs can be resource-intensive and may not be feasible for small businesses to fully utilize.
- **Replace Other Business Functions/Operations:** Should not replace IT departments, other key functions, or cybersecurity personnel.

# Competition Matrix: Existing Solutions

## Direct Competitors:

- Cybrary
- Infosec Institute
- Cybersecurity Consulting Firms
- FireEye

## Indirect Competitors:

- VirusTotal
- AlienVault OTX (Open Threat Exchange)
- NIST Cybersecurity Framework
- SANS Institute

# Competition Matrix: Existing Features & Functionality

- **Certification Preparation:** Provides resources and training materials to prepare users for industry-standard cybersecurity certifications.
- **Customizable Content:** Enables organizations to customize training content to align with their specific policies and requirements.
- **Feedback/Discussion Forums:** Includes feedback mechanisms and discussion forums where users can provide input, ask questions, and engage with peers and experts.
- **Gamification & Performance Tracking:** Utilizes gamified elements to enhance user engagement and motivation while also tracking user progress and provide detailed reports.
- **Resource Library:** Maintains a comprehensive library of cybersecurity resources, including articles, e-books, and research papers.

# Competition Matrix: Limitations of Existing Solutions

- **Compliance Challenges:** Existing solutions may struggle to meet regulatory compliance requirements, lacking tailored support for small business needs.
- **Financial Impediment:** Many options on the market carry a substantial price, rendering them unattainable for small businesses operating on restricted budgets.
- **Inadequate Support:** Limited customer support could impede users from resolving issues or obtaining assistance as required.
- **Ineffective Instruction:** Several platforms may provide training materials that are too technical or advanced for users with limited cybersecurity knowledge, leading to ineffective training outcomes.
- **Limited Scalability:** Competitors can face limited scalability issues as small businesses grow and their cybersecurity needs evolve over time.

# Competition Matrix: How do we compare?

Feature/Functionality	CyberSense	Cybrary	Virus Total	AlienVault OTX	Traditional Cybersecurity Consulting	FireEye
Accessible educational modules	✓	✓				
Real-time threat intelligence	✓ (via APIs)		✓	✓	✓	✓
Community collaboration tools	✓	✓				
User-friendly dashboard	✓					✓
AI-powered Q&A for cybersecurity queries	✓					
Simplified threat reporting forms	✓				✓	
Cost-effective for small businesses	✓	✓				
Scalability	✓				✓	✓



# Development Tools

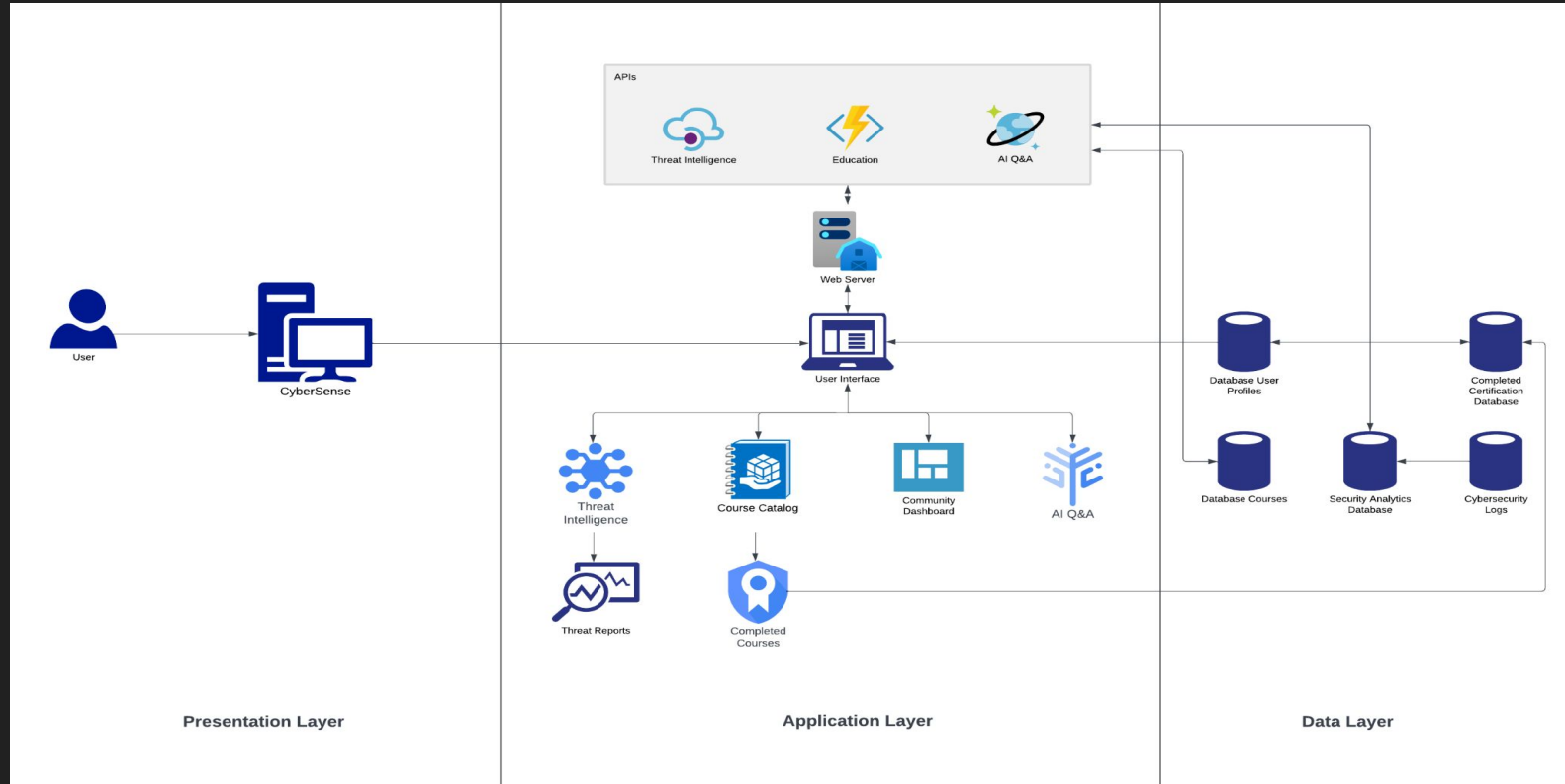
- Integrated Development Environment (IDE): VSCode
- Version Control: Git, GitHub
- Continuous Integration (CI): Github Actions & Workflows
- Continuous Deployment (CD): Github Actions & Workflows

- Backend Language: Python
- Frontend Language: HTML, CSS, JavaScript, React.js
- Testing Frameworks: PyTest, unittest
- Documentation Tool: pydoc

# Major Functional Components:

- Operating System: Linux
- Web Server: Django
- Database: PostgreSQL
- Server Side Language: Python

# Major Functional Components: Diagram



# Risks and Mitigation Disclaimer

CyberSense is a ***tool*** intended to aid in a business's efforts to decrease the likelihood of cybersecurity risks. CyberSense is ***not a security service***, but an educational tool catered to your business's security needs.

## Risks Include:

- Customer & End User
  - What Can Happen to the Customer & End User
  - End User & Customer Behavior
- Technical
- Security
- Legal

*All risks and mitigation plans are generalized and not specific to only those who use CyberSense.*

# Risks: Customer & End User

## What Can Happen to the Customer & End User

- **Fraudulent Activities:** Malicious actors may target the application to deceive, manipulate, or exploit systems, processes, or data for personal gain or to cause harm. (Likelihood: 4 / Severity: 5)
- **Privacy Violations:** Personal and business data collected by the application could be exposed to unauthorized access or breaches. (Likelihood: 4 / Severity: 5)

## End User & Customer Behavior

- **User Errors:** Users may make mistakes while interacting with the web application due to lack of knowledge, misunderstanding of features, and etc. (Likelihood: 5 / Severity: 4)
- **Lack of User Engagement:** Users may not find the application engaging or useful, resulting in limited usage. (Likelihood: 4 / Severity: 3)
- **Insufficient Cyber Knowledge:** Users with limited cybersecurity knowledge may misinterpret information or fail to implement security measures properly. (Likelihood: 5 / Severity: 3)
- **Over-reliance on the Application:** Businesses may rely solely on the application for their cybersecurity needs, neglecting other important features. (Likelihood: 5 / Severity: 3)

# Risks: Customer & End User (Mitigation)

## What Can Happen to the Customer & End User

- **Fraudulent Activities:** Provide training and suitable security measures that will recognize unusual activities through activity logs, as well as clear instructions on how to report suspicious activity. (Likelihood: 2 / Severity: 3)
- **Privacy Violations:** Ensure compliance with data protection regulations and implement access controls. (Likelihood: 2 / Severity: 4)

## End User & Customer Behavior

- **User Errors:** Incorporate playbooks and a chain of command in order to prevent human error due to lack of knowledge. (Likelihood: 2 / Severity: 2)
- **Lack of User Engagement:** Incorporate interactive and practical learning modules, and gather user feedback to continuously improve content. (Likelihood: 1 / Severity: 1)
- **Insufficient Cyber Knowledge:** Provide clear, concise, and step-by-step instructions as well as offer additional support through forums. (Likelihood: 1 / Severity: 2)
- **Over-reliance on the Application:** Emphasize the importance of having a thorough security strategy covering all aspects beyond just focusing on the application. (Likelihood: 1 / Severity: 2)

*\*\*To be completed bi-annually or annually\*\**

# Risks: Technical

- **Compatibility Issues:** New updates or integrations may not be compatible with existing systems, causing malfunctions or performance degradation. (Likelihood: 4 / Severity: 4)
- **Data Loss:** Technical malfunctions such as hard drive failures, software bugs, or accidental deletions can result in the loss of critical data. (Likelihood: 4 / Severity: 5)
- **Insufficient Backup:** Lack of reliable backup systems can make recovery difficult or impossible in the event of data loss or corruption. (Likelihood: 4 / Severity: 5)
- **Network Vulnerabilities:** Insecure network configurations can be exploited by attackers to gain unauthorized access to systems. (Likelihood: 3 / Severity: 5)
- **System Failures:** Can disrupt business operations and lead to data loss or downtime. (Likelihood: 5 / Severity: 5)
- **Loss of Support:** Expiring licenses, warranties, and technical support periods lead systems to being vulnerable when a business does not have a dedicated IT team. (Likelihood: 3 / Severity: 3)

# Risks: Technical (Mitigation)

- **Compatibility Issues:** Keep systems and applications up to date to stable builds to ensure compatibility. (Likelihood: 2 / Severity: 4)
- **Data Loss:** Implement a robust data backup plan in place in order to be able to recover loss data at multiple intervals (on-site and off-site). (Likelihood: 2 / Severity: 4)
- **Insufficient Backup:** Utilize multiple backup tools and strategies to prevent downtime and loss of potential future backups. (Likelihood: 2 / Severity: 4)
- **Network Vulnerabilities:** Physical and logical firewalls as well as a properly setup network prevent unwarranted network issues. Frequent patching and vulnerability mitigation work best alongside end user training. (Likelihood: 1 / Severity: 4)
- **System Failures:** Have scheduled backups and imaging in place with a long term system refresh schedule to keep hardware within their supported lifecycle. (Likelihood: 2 / Severity: 4)
- **Loss of Support:** Renewing licenses and the acquisition of new hardware will keep all systems in compliance and under support of the system manufacturer. (Likelihood: 1 / Severity: 4)



# Risks: Security

- **Data Breaches:** Unauthorized access to sensitive information can lead to financial loss, legal penalties, and reputational damage. (Likelihood: 5 / Severity: 4)
- **Denial of Service (DoS) Attacks:** These attacks can cripple business operations by overwhelming systems, making services unavailable to legitimate users. (Likelihood: 5 / Severity: 4)
- **Insider Threats:** Employees or contractors with malicious intent or who inadvertently compromise security can cause significant damage. (Likelihood: 2 / Severity: 5)
- **Malware Attacks:** Infections by malware such as viruses, ransomware, and spyware can disrupt operations and compromise data integrity. (Likelihood: 4 / Severity: 5)
- **Phishing Scams:** Employees may be tricked into revealing confidential information, leading to unauthorized access and potential data theft. (Likelihood: 5 / Severity: 5)

# Risks: Security (Mitigation)

- **Data Breaches:** (Likelihood: 1 / Severity: 4)
  - **Encryption** - Encrypt sensitive data both at rest and in transit.
  - **Access Controls** - Implement access controls to ensure only authorized personnel have access to sensitive data.
  - **Patch Management** - Ensure all systems and applications are regularly updated and patched against known vulnerabilities.
- **Denial of Service (DoS) Attacks:** (Likelihood: 2 / Severity: 4)
  - **DNS hardening** - Protect DNS Infrastructure with Domain Name System Security Extensions (DNSSEC) and use a reliable DNS provider.
  - **IDS (Intrusion Detection Systems)** - Deploy IDS to monitor and analyze network traffic.
  - **Firewalls** - Use firewalls to filter out malicious traffic and block unauthorized access.

# Risks: Security (Mitigation) - continued

- **Insider Threats:** (Likelihood: 1 / Severity: 5)
  - Background checks - Thorough background checks during the hiring process to identify potential threats.
  - Monitoring and Auditing - Monitoring and auditing of user activities to detect any unusual or unauthorized behavior.
  - Least Privilege Access Controls - Ensure employees have only the permissions necessary to perform their job functions.
- **Malware Attacks:** (Likelihood: 2 / Severity: 5)
  - Antivirus/Antimalware software - Install and regularly update antivirus/antimalware software on all systems.
  - Email filtering - Use email filtering software to block malicious attachments and links.
  - Software updates - Keep all software and operating systems updated with the latest security patches.
- **Phishing Scams:** (Likelihood: 2 / Severity: 5)
  - Awareness Training - Educate employees on recognizing and reporting phishing attempts.
  - Multi Factor Authentication (MFA) - Use MFA to add an additional layer of security for accessing systems and sensitive data

# Risks: Legal

- **Compliance Audits:** Regular audits require for compliance which can be resource-intensive and costly.  
(Likelihood: 4 / Severity: 4)
- **Contractual Violations:** Breach of contractual obligations related to data security can lead to lawsuits and financial penalties. (Likelihood: 2 / Severity: 5)
- **Intellectual Property Infringement:** Legal disputes arising from the theft or unauthorized use of intellectual property.  
(Likelihood: 1 / Severity: 4)
- **Licensing Issues:** Mismanagement of software licenses can lead to legal penalties and additional costs.  
(Likelihood: 3 / Severity: 5)
- **Non-Compliance:** Failure to adhere to industry regulations and legal standard can result in fines and legal action.  
(Likelihood: 1 / Severity: 4)

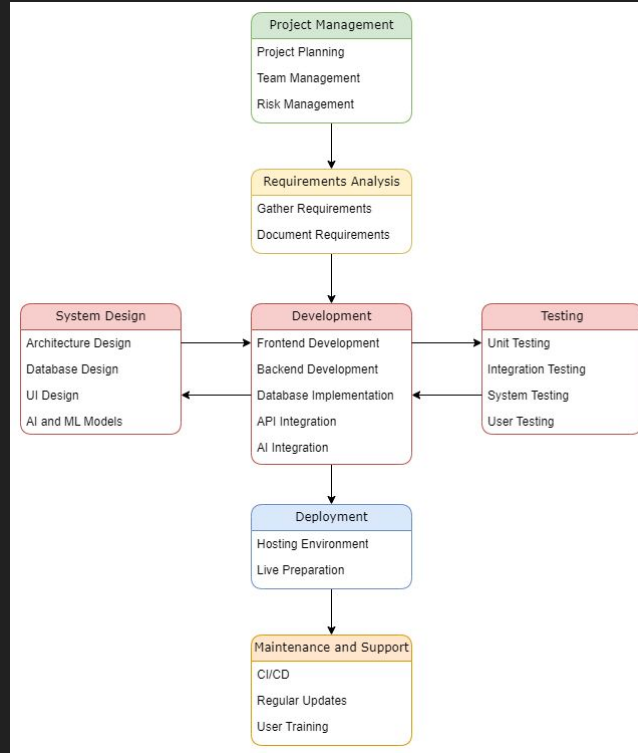
# Risks: Legal (Mitigation)

- **Compliance Audits:** (Likelihood: 2 / Severity: 4)
  - Conduct regular audits - Conduct regular audits to ensure the organization adheres to all relevant legal and regulatory standards. This practice helps identify compliance gaps in advance.
  - Use Third-Party auditors - Third-party auditors provide an unbiased view since they are separate from the organization. Record the findings - Make records of the results gathered from the audits.
- **Contractual Violations:** (Likelihood: 2 / Severity: 4)
  - Use contract management software - Allows the user to keep track of legal terms and conditions.
  - Train employees - Training employees on contract terms will inevitably reduce the number of contract violations.

# Risks: Legal (Mitigation) - continued

- **Intellectual Property Infringement:** (Likelihood: 2 / Severity: 4)
  - Monitor Intellectual Property - Keep a close eye out for illegal use of intellectual property to mitigate infringement.
  - Take Legal Action - Take action against the illegal use of intellectual property.
- **Licensing Issues:** (Likelihood: 2 / Severity: 4)
  - Perform compliance checks - Check if the licensing agreements are compliant with the law.
  - Track usage - Perform usage tracking by using software to mitigate the risk of licensing issues.
- **Non-Compliance:** (Likelihood: 1 / Severity: 4)
  - Monitor Intellectual Property - Monitor for use that does not adhere to industry regulations and legal standards.

# Work Breakdown Structure - Diagram



# Work Breakdown Structure - 1/2

- Project Management
  - Project Planning
    - Develop project timeline
    - Allocate resources
  - Team Management
    - Assign roles and responsibilities
    - Conduct team meetings
  - Risk Management
    - Identify potential risks
    - Develop mitigation strategies
- Requirements Analysis
  - Gather Requirements
    - Conduct end user and stakeholder interviews
    - Analyze current needs
  - Document Requirements
    - Create requirements specification document
- System Design
  - Architecture Design
    - Define system architecture
  - Database Design
    - Design database schema
  - UI Design
    - Create wireframes and mockups
    - Design dashboard
  - AI and ML Models
    - Select appropriate algorithms
    - Design model architecture



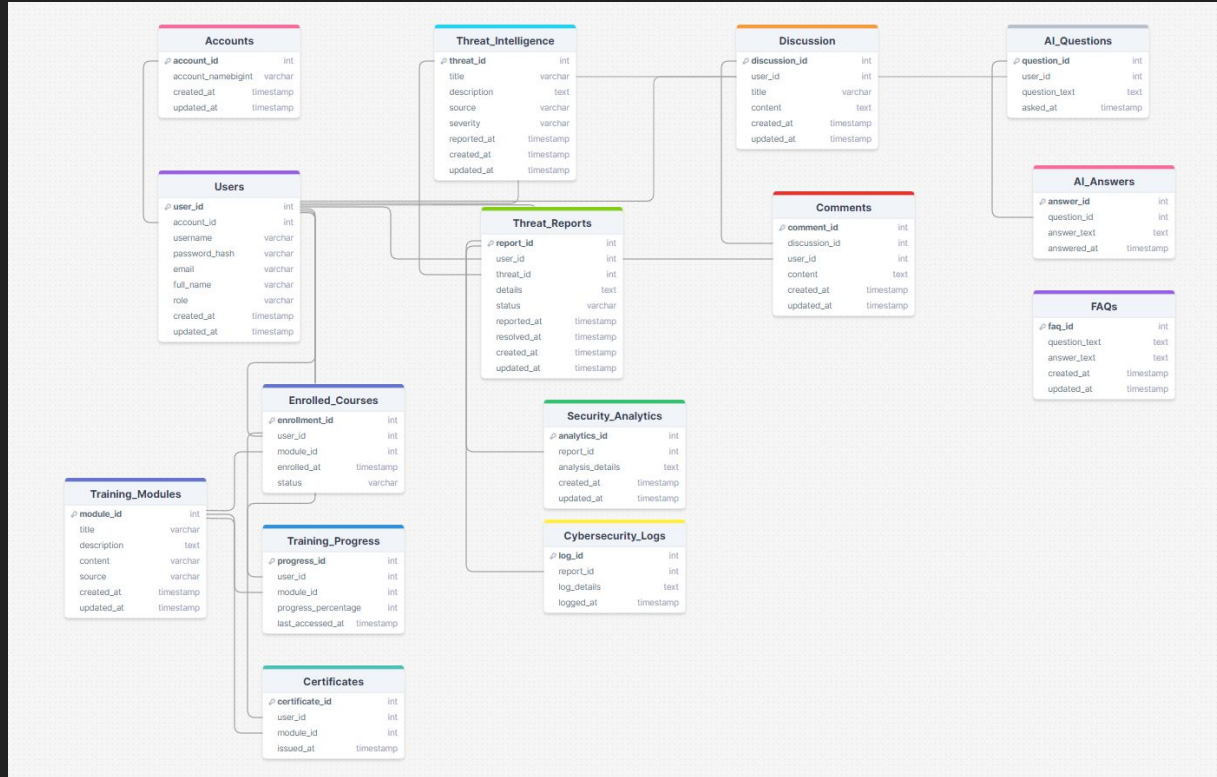
# Work Breakdown Structure - 2/2

- Development
  - Frontend Development
    - Implement UI using HTML, CSS, JS, React.js
    - Develop interactive dashboard
  - Backend Development
    - Set up server environment
    - Implement backend using Python and Django
  - Database Implementation
    - Create database instances
    - Integrate database with backend
  - API Integration
    - Integrate VirusTotal API
    - Integrate AlienVault OTX API
  - AI Integration
    - Implement AI Q&A system using NLTK, spaCy, TensorFlow
    - Train and test models
- Testing
  - Unit Testing
    - Test individual components
    - Validate functionality
  - Integration Testing
    - Test integrated components
    - Ensure system interoperability
  - System Testing
    - Conduct end-to-end testing
    - Validate overall system performance
  - User Acceptance Testing (UAT)
    - Conduct testing with end users
    - Gather user feedback
    - Implement necessary changes

# Algorithms

- Data Scraping
  - Real-Time Threat Intelligence data
- Data Analysis
  - Completed Course Analysis
  - Recommend Course Analysis
- Anomaly Detection
  - Site Security Monitoring
- Machine Learning/Natural Language Processing
  - AI Q&A

# Database Schema



# Real World Product vs Prototype

Feature	Real World Product (RWP)	Prototype
User Authentication	OAuth 2.0, JWT, multi-factor authentication	Basic login/logout, simple user roles
Dashboard	Fully functional, interactive dashboard with analytics	Basic UI with limited data display
Educational Modules	Dynamic content, full integration with Cybrary, NIST, CISA, and SANS APIs	Static content, basic integration with Cybrary
Threat Intelligence Integration	Real-time threat intelligence from VirusTotal, AlienVault OTX	Display sample threat reports
Community Discussion Board	Advanced features like tagging, search, and moderation	Basic posting and commenting
Threat Reporting Forms	Interactive forms with dropdowns, checkboxes, and automated data processing	Basic forms with manual data entry
AI Q&A System	Advanced AI with spaCy, TensorFlow for comprehensive Q&A, context-aware recommendations	Basic NLP for simple queries using NLTK
Frontend Development	Advanced UI/UX with React.js, responsive design	Basic HTML, CSS, JavaScript implementation
Backend Development	Robust backend with Django, scalable infrastructure	Simple server setup with Python (Flask)
Database Implementation	Optimized schema, advanced querying, and indexing	Basic schema with MongoDB or PostgreSQL
Testing	Comprehensive testing including unit, integration, system, and UAT	Unit tests for individual components
Deployment	Full deployment on AWS with CI/CD pipelines	Local or basic cloud deployment
User Training and Documentation	Comprehensive training materials, tutorials, and user manuals	Basic user guides
Monitoring and Logging	Advanced monitoring and logging using tools like ELK stack	Basic error logging
Security Features	Comprehensive security protocols including encryption, secure data storage, regular security audits	Basic security measures
Regular Updates	Automated updates, continuous improvement based on feedback	Manual updates
Maintenance and Support	Structured support system with SLAs, regular maintenance schedules	Ad-hoc support

# Required Libraries, Tools, & Technologies:

- **Libraries:** TensorFlow, spaCy, Natural Language Toolkit (NLTK), Cybrary
- **Languages:** Python
- **Frameworks:** Django
- **Other:** PostgreSQL

# Conclusion

- Small businesses are at a greater risk of going under after a cybersecurity attack.
  - 60% of businesses close 6 months after cybersecurity attack.
- Current solutions are not cost effective for small businesses.
  - Solutions can cost more than a small business can afford.
- There is a need for small businesses to practice cybersecurity hardening.
  - Non-technical employees and owners need to understand cybersecurity and ways to mitigate risks associated with cyber attacks.

*CyberSense is common sense.*

# References

- Cybersecurity and Infrastructure Security Agency (CISA). *CISA Cyber Essentials*. 2020,  
<https://www.cisa.gov/cyber-essentials> Accessed 11 June 2024
- Manning, Aimee “Splunk Pricing: How Much Does It Cost?”, *Vertice* 26 February, 2024  
<https://www.vertice.one/inside-saas/splunk-pricing> Accessed 2 July 2024
- National Cyber Security Alliance. “60 Percent of Small Companies Close Within 6 Months of Being Hacked.”  
*Stay Safe Online*, 2020, <https://staysafeonline.org> Accessed 11 June 2024
- National Institute of Standards and Technology (NIST). *Cybersecurity Framework*. 2020,  
<https://www.nist.gov/cyberframework> Accessed 11 June 2024

# References, the awaited sequel

- Palo Alto Networks Pricing guide for 2024 & Insights. *Vendr*  
<https://www.vendr.com/buyer-guides/palo-alto-networks> Accessed 2 July 2024.
- Robb, Drew “FireEye Endpoint Features & Pricing” *eSecurity Planet*,  
<https://www.esecurityplanet.com/products/fireeye-endpoint/> Accessed 2 July 2024
- SysAdmin, Audit, Network, and Security (SANS) Institute. *SANS Cybersecurity Resources*. 2020,  
<https://www.sans.org> Accessed 11 June 2024
- Verizon. *2020 Data Breach Investigations Report*. 2020, <https://www.verizon.com/business/resources/reports/dbir/>  
Accessed 11 June 2024



# Appendix

# Work Breakdown Structure - 3/3

- Deployment
  - Setup Hosting Environment
    - Configure AWS environment
    - Deploy application to AWS
  - Live Preparation
    - Conduct final system checks
    - Prepare deployment checklist
- Maintenance and Support
  - Post-Deployment Support
    - Monitor system performance
    - Address any post-deployment issues
  - Regular Updates
    - Schedule periodic updates
    - Implement new features and improvements
  - User Training and Documentation
    - Provide user training sessions
    - Create and maintain user manuals

# Developmental Tools

- **Version Control:** Git, GitHub
- **IDE:** PyCharm, VS Code
- **Testing Frameworks:** unittest, pytest