BUSINESS PLAN

Owl Cyber Defense Systems

IT7993

IT Capstone Final Project

Dr. Xie

Project Lead: Scott Gilstrap
rgilstra@students.kennesaw.edu

Logo generated with Bing powered by DALL-E3.

Business Plan

Date: March 03, 2024

Table of Contents

Executive Summary

OCDS is a cutting-edge startup cybersecurity firm dedicated to safeguarding businesses and individuals from digital threats at an affordable price point for the small business owner. Our mission is to provide robust, proactive cybersecurity services that empower our clients to thrive in the digital age.

Mission Statement

At Owl Cyber Defense Systems, we create world-class proprietary cyber security solutions for our clients based on direct input and collaboration to provide a competitive edge while maintaining strong, robust cyber protections against today's cyber criminals.

Vision Statement

Our vision is to be the small business go-to for all things cyber security due to our superior, proprietary-based client offerings at the most reasonable, affordable price point.

Core Values:

- **Integrity –** When everything you do is based on integrity you will ensure it is done right and to the best of your ability.
- **Trust** – We will establish Trust within our relationships with our customers. We will always have their best interest in mind as we execute our mission/vision. Every effort will be made to help our clients succeed while protecting their business and infrastructure.
- **Innovation** – We will strive every day to develop new ways to protect our clients and/or improve upon our existing client offerings. It's all about cyber protection at the highest level and lowest cost.

Key Services:

- **Threat Assessment and Mitigation**
  - We conduct comprehensive risk assessments to identify vulnerabilities in our clients' systems.
  - Our team implements customized solutions to mitigate risks, including firewall configuration, intrusion detection, and vulnerability patching.
- **Incident Response and Recovery**
  - In the event of a cyberattack, we respond swiftly to minimize damage.
  - Our experts guide clients through recovery, ensuring business continuity and data integrity.
- **Security Awareness Training**
  - We offer tailored training programs to educate employees on best practices for cybersecurity.
  - Empowering staff to recognize and prevent threats is crucial for overall organizational security.
- **Secure Cloud Solutions**
  - As businesses transition to the cloud, we provide secure migration and ongoing management.

  - Our expertise covers AWS, Azure, and Google Cloud security.

Competitive Edge:

- **Holistic Approach:**
  - We address cybersecurity from multiple angles, considering technology, processes, and human behavior.
  - Our integrated approach ensures comprehensive protection.
- **Certified Experts:**
  - Our team holds industry-leading certifications (CISSP, CEH, etc.).
  - We stay updated on emerging threats and technologies.
- **Client-Centric Focus:**
  - We build strong relationships with clients, understanding their unique needs.
  - Our solutions are tailored to fit each organization's risk profile.

Market Opportunity:

- **Growing Demand**
  - The global cybersecurity market is expanding rapidly due to increased cyber threats.
  - Organizations across sectors seek reliable partners to enhance their security posture.
- **Compliance Requirements**
  - Regulatory frameworks (GDPR, HIPAA, etc.) mandate robust cybersecurity measures.
  - Our services help clients meet compliance standards.

Financial Projections:

- **Projected Revenue**
  - Year 1: $75,000
  - Year 2: $200,000
  - Year 3: $400,000
- **Profit Margin**
  - OCDS will be profitable year three at which point we anticipate a steady profit margin of 20% over the next two years thereafter.

Next Steps:

- **Market Penetration**
  - Expand our client base through targeted marketing and networking.
  - Forge partnerships with other IT service providers.
- **Research and Development**
  - Invest in threat intelligence tools and AI-driven security solutions.
  - Stay ahead of evolving threats.

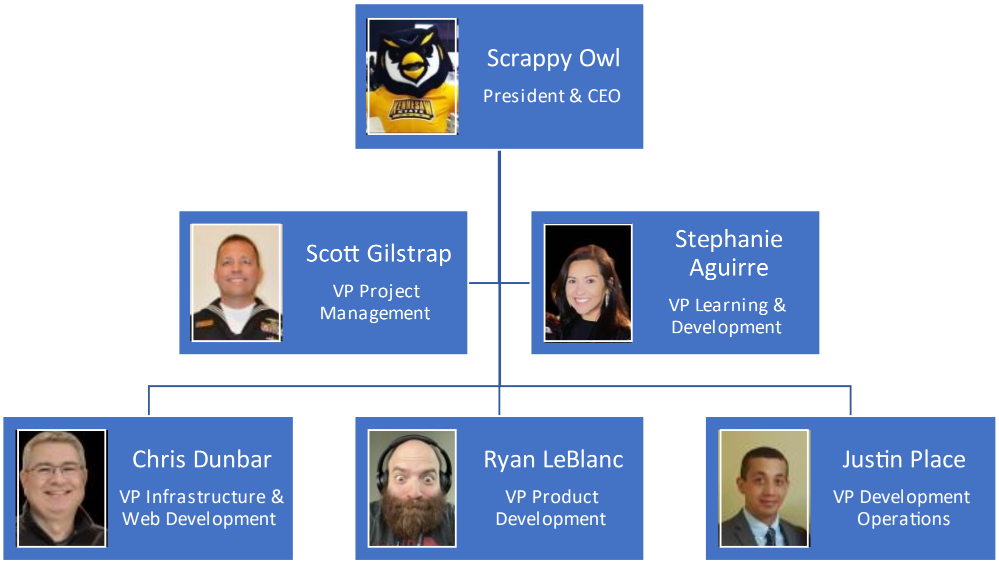
Company & Business Description

Company Purpose

The purpose of the Owl Cyber Defense Systems cybersecurity business is to help small 0businesses safeguard digital assets and protect against cyber threats. OCDS offers a range of services to organizations, including helping clients to create an IT Security and Risk Management Plan. OCDS will also assist organizations with training employees in Cyber Awareness. The flagship client offering is the AI-enable server hardening bot. Another world class client offering is the OCDS SIEM firewall and log analyzer.

All these client offerings are designed to help businesses with Vulnerability Assessments Identifying weaknesses in systems, networks, and applications to prevent potential breaches. Penetration Testing may be recommended to simulate attacks to evaluate security measures and discover vulnerabilities. Threat Intelligence to monitor and analyze cyber threats to proactively defend against them. Incident Response tactics will be recommended to develop strategies to handle security incidents effectively. Security Consulting is an OCDS specialty advising clients on best practices, compliance, and risk management. In essence, OCDS will play a critical role in ensuring client data integrity, privacy, and business continuity in an increasingly interconnected digital landscape.

Team & Organization Structure



Business Goals
Be the first-choice provider for world class proprietary client offerings based directly on customer input and do so at a reasonable price point for the small business owner. Design top notch IT cybersecurity and risk management plans specifically tailor-made for our clients. Deliver specified cyber awareness training for our customers making way for our client to provide a proprietary-based employee training program.

- Establish strong cybersecurity market share in the first 2 years.
- Achieve 20% annual revenue growth.
- Build skilled and motivated team of cybersecurity experts.
- Strengthen our clients' security posture.
- Enable our clients to migrate securely to the cloud.
- Train clients on proper security techniques.
- Collaborate and partner with other cybersecurity firms and technology providers.

Business Strategy
Executing the details laid out in this business plan from sale & marketing strategies to company policies to financial considerations OCDS will invest in quality personnel and provide appropriate means to help them create best in class client offerings to provide cyber protection for our clients.

IT Goals
Aligning with business goals the Information Technology departments will provide OCDS employees with safe, secure, and well preforming technology devices and strive for a solid strategy to improve year over year.

- Purchase developer class laptops for all technology staff and business class laptops for business leaders.
- Implement an advanced proprietary Security Information and Event Management (SIEM) system for each client.
- Create a cloud security policy framework for clients by implementing robust IT Security Plans to monitor cloud workloads for vulnerabilities and increase security posture.
- Develop world-class Cyber Awareness Training programs for clients.
- Identify potential partners and establish communication channels to facilitate integrating threat intelligence feeds and jointly develop solutions for mutual benefit.
- Experiment with emerging technologies (AI, blockchain, etc.).

IT Strategy
The OCDS IT leaders will consistently communicate and collaborate with OCDS business leaders to facilitate alignment. Alliance will be consistent and facilitated by a quarterly sync-up meeting to discuss and re-align goals and strategies. Following the details of this Business Plan, specifically the technology

aspects, the OCDS Technology Department will reinvest in appropriate hardware to focused on the IT goals that are synchronized to help the business meet their goals. Technology personnel will focus on developing products to meet the deliverables to our client offerings to meet the business goals.

Company Policies

Company policies play a crucial role in ensuring the smooth functioning of an organization.

- OCDS will set expectations via written policies detailing what is expected from company employees to including but not limited to performance, values, and behavior. These policies will provide a framework for employees to understand their roles and responsibilities within the organization.
- OCDS will strive to maintain consistency and fairness. OCDS well-defined policies will ensure consistency across the company. When everyone follows the same guidelines, it promotes fairness and prevents favoritism.
- Company policies will serve as a guideline for federal or state regulatory requirements to maintain compliance with laws. They help OCDS stay compliant with labor laws, industry-specific regulations, and legal obligations.
- Legal protection will be afforded as OCDS policies will act as pre-warnings for employees. By outlining the consequences of failing to abide by the rules, OCDS will be protected legally. In case of disputes or claims, these documented policies will be valuable evidence.
- OCDS will promote a positive work environment via well-crafted policies contributing to a safe and enjoyable work environment. OCDS policies will relate to workplace health and safety, employee fraternization, and remote work helping to create a positive atmosphere for everyone.

OCDS Company Policies are as follows:

- **Equal Opportunity Policy**: Ensures fair treatment and prevents discrimination based on protected classes (e.g., race, gender, age, religion) in hiring and employment practices.
- **Workplace Health and Safety**: Addresses safety protocols, emergency procedures, and preventive measures.
- **Employee Code of Conduct**: Sets behavioral standards and expectations.
- **Attendance, Vacation, and Time-Off**: Clarifies leave entitlements and procedures.
- **Ethics Policy**: Guides employees on ethical behavior and integrity.
- **Substance Abuse**: Addresses drug and alcohol use in the workplace.
- **Compensation and Benefits**: Details salary, benefits, and incentives.
- **Remote Work**: Outlines guidelines for working remotely.
- **Access Control**: Only authorized users can have access to the organization’s IT resources, hardware, software, data, and network.

- **Acceptable Use Policy (AUP)**: Set of rules that govern how an OCDS computer network, website, or service may be used. Outlines both permissible and prohibited actions. The OCDS AUP will serve as a roadmap for responsible and secure use of technology resources and maintain order, protecting assets, and fostering a respectful digital environment.
    - **Usage Guidelines**: Define acceptable behavior for users. Specify what actions are allowed and what constitutes misuse. By adhering to these guidelines, users contribute to a positive and secure environment.
    - **Network Security**: To maintain network security these OCDS practices will define and prevent unauthorized access, data breaches, and other security risks. E.g., this policy will prohibit sharing login credentials or attempt systems hacking, etc.
    - **Resource Allocation**: Address resource allocation. Ensure fair usage of network bandwidth, storage, and computing power. Prevent excessive or inappropriate use that could impact overall system performance.
    - **Legal Compliance**: Ensure OCDS compliance with legal requirements. Address copyright infringement, privacy laws, and intellectual property rights. Following this section of the AUPs, OCDS will avoid legal repercussions.
    - **Risk Mitigation**: Mitigate risks associated with misuse. Discourage activities like spreading malware, engaging in cyberbullying, or violating user privacy. These AUP policy section will protect both users and OCDS.
- **Bringing Own Device to Work (BYOD)**: An individual can bring their own device to work, but company software must be installed to protect the organization from malicious software.
- **Social Media**: Under no circumstances should the organization's property (i.e. software, hardware, data) should be on any social media platform. This could lead to legal and cybersecurity risks.
- **User accounts and passwords**: Everyone will have their own account and password(s). If an individual is no longer a part of the organization, then their account will be deleted. Passwords must be updated every ninety (90) days to ensure protection from hackers.
- **Backing Up Information**: Information from devices will be routinely backed up every fifteen (15) days to ensure that information is not lost in case of a cyber-attack. It is also to maintain the integrity of the organization's IT resources.
- **Purchase and Installation of Software**: All hardware and software must be appropriate and provide value for the organization. It must be able to integrate within the other devices of the organization. If an installation or purchase must occur, then it must go through the IT manager for approval. From there, the IT manager will send the approval to the IT team, who will buy it and have it installed from a reliable and authorized vendor.
- **Incident Response**: If you see or receive something out of the ordinary, identify the incident and then report it. The incident will be properly escalated to the appropriate personnel to handle and respond to the incident. Once the incident has been dealt with, then an evaluation of the incident must occur in order to see how well it worked and whether anything else must be done to properly manage the incident.

- **Wireless Use**: To maintain regulation of wireless network access to the organization's IT resources. User authentication is required before accessing the organization's wireless networks. The organization monitors all wireless network to ensure reliable access. The organization reserves the right to restrict and/or move any device(s) that have access to the wireless network to prevent infection or any negative impacts to the IT resources.
- **Security Awareness and Training**: Should be administered to all individuals of the organization so they can properly handle tasks without jeopardizing the organization's information and data. Providing proof of completion is required.
- **Data Retention**: All data retrieved from the organization will be stored for three (3) years. After the three (3) years, the data will be completed destroyed and wiped from the organization's backup and storage. All outdated and duplicate data will be removed to keep storage space available. Data includes documents, records, transaction information, contracts, emails or other messaging applications, and customer information.
- **Email Usage**: Personal use of company email is not allowed. This reduces the risk of receiving spam email that could contain phishing or pharming content. Email exchange must be done on-premises or using a virtual machine to access user's desktop. In case of an email security breach, the IT manager and supervisor must be notified. The organization has the right to monitor, read, intercept, store, and disclose emails.
- **Data and Information Security**: The availability, integrity, and confidentiality of the organization's information must be protected from corruption, theft, or unauthorized access.

Product & Services Line

Product Offering(s)

- AI-enabled network and server hardening tool
- Advanced firewall, SIEM, and Log Analyzer

Service Offerings

- Client IT Security Plan proprietary build-out
- Client Risk Management Plan proprietary build-out
- Client Cyber Awareness Training

Pricing Model

OCDS pricing is based on a combination of a **project**-based and a **value**-based pricing model.

Using a project-based pricing strategy OCDS will charge a flat fee per project as opposed to a direct exchange of money for time. Pricing will be estimated based on the value of the project deliverables. For some projects the strategy will consist of flat fee from the estimated time of the project. OCDS uses this strategy as it is good for consultants providing business services.

Using the value-based model OCDS will price product offerings or services based on what the customer is willing to pay. OCDS could charge more for products we will set prices based on customer interest and data to maintain the competitive pricing and establish OCDS as the most affordable option for our clients while maintaining a modest profit margin. The goal is to increase client sentiment and loyalty while prioritizing clients in other areas of the business. This model also works well in any price-sensitive industry such as client-based products and services.

The pricing structure will fluctuate and will be posted and adjusted via the OCDS website.

Market Analysis

Target Market

The OCDS target market is the small business who is most likely a sole proprietary ownership with one to 10 employees. These small businesses may only have one or just a few products. They may be retail small businesses as well. Industries will vary. They may be professional and business service related. These small businesses are the heart of America. At more than 90% of U.S. businesses 33.3 million businesses are small business in the United Sates [1]. These businesses are our target market because they usually can't afford the cyber protections required for robust defense and they are the ones who need it the most because a successful cyber attack against their business will most likely put them out of business. OCDS needs to help protect these businesses.

Reference

Main, K. (2024, January 31). Small business Statistics of 2024. *Forbes Advisor*. https://www.forbes.com/advisor/business/small-business-statistics/#small_business_employment_statistics_section

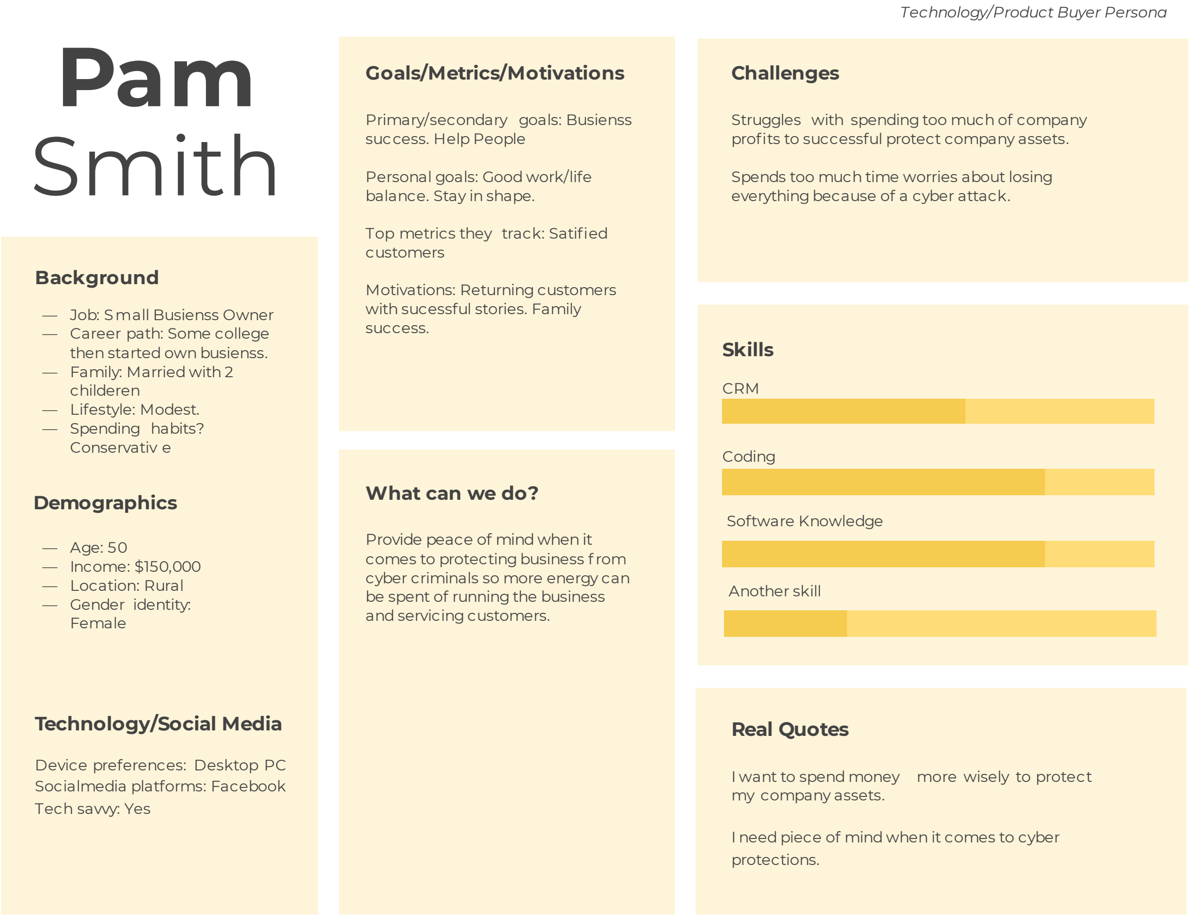
Buyer Personas

Building a buyer persona is essential to understanding the OCDS client. Buyer Personas are fictional, generalized representations of the OCDS ideal customer. They help understand OCDS customers (and prospective customers) better and make it easier for OCDS to tailor content to the specific needs, behaviors, and concerns of different groups.

We asked questions such as What is their profession? What does a typical day in their life look like? Where do they go for information? How do they prefer to obtain goods and services? What is important to them when choosing a vendor? What do they value most? What are their goals?

Well-built personas allow OCDS to personalize and target marketing for different segments of our audience. OCDS can segment buyer persona and tailor advertisement messaging according to what we know about those different personas. Buyer personas will allow OCDS to produce highly targeted content that leads to a higher influx of new and repeat customers who are pre-qualified by data.

One such Persona is Pam Smith…



Technology/Product Buyer Persona

Pam
Smith

Background

- Job: Small Busienss Owner
- Career path: Some college then started own busienss.
- Family: Married with 2 childeren
- Lifestyle: Modest.
- Spending habits? Conservative

Demographics

- Age: 50
- Income: $150,000
- Location: Rural
- Gender identity: Female

Technology/Social Media

Device preferences: Desktop PC
Socialmedia platforms: Facebook
Tech savvy: Yes

Goals/Metrics/Motivations

Primary/secondary goals: Busienss success. Help People

Personal goals: Good work/life balance. Stay in shape.

Top metrics they track: Satified customers

Motivations: Returning customers with sucessful stories. Family success.

What can we do?

Provide peace of mind when it comes to protecting business from cyber criminals so more energy can be spent of running the business and servicing customers.

Challenges

Struggles with spending too much of company profits to successful protect company assets.

Spends too much time worries about losing everything because of a cyber attack.

Skills

Real Quotes

I want to spend money more wisely to protect my company assets.

I need piece of mind when it comes to cyber protections.

Location Analysis

OCDS location will be 100% online as our research indicates a brick-and-mortar office is not required. The cost of a physical location will be a savings and will be put back into the business as capital.

We are located at https://ocds.tech.

Competitor Analysis

OCDS conducted a SWOT analysis to explain the state of competition in the Cybersecurity industry. The results are recorded here in this competitor analysis section.

To summarize the top competitor details are below:

- **Comparative Strength** – *OCDS assets that this competitor does not have?*
- **Comparative Weakness –** *What areas or attributes do competitors outperform OCDS?*

- **Counterpoints –** *If a comparative weakness is mentioned in sales negotiations, which counterpoints can be used to address those OCDS weaknesses?*

Competitor Name	Comparative Strength(s)	Comparative Weakness(es)	Counterpoint(s)
BigBox Information Security	BigBox InfoSec will have walk by clients, but OCDS has have better knowledge of clients	BigBox will have more capitol because they are a bigger company	OCDS is a smaller company and will be able to reactive quicker
Cyber Protection Online (CPO)	CPO has a larger budget, but OCDS has a more streamlined approach to spending to better target expenditures	CPO has been in business for longer and has more experience in the industry	OCDS has a niche approach for data collection and service delivery
ACME Cyber	ACME has a wider variety of products but, OCDS has more client detailed proprieties in each client offering	ACME has a larger research & development department supporting robust programming	OCDS has expert developers supporting a proprietary AI product

Marketing Plan

Positioning Strategy

Potential buyers will be interested in ODDS products for two primary reasons, best price point in the specific market and the proprietary sense of the client offerings? OCDS will address each buyer persona’s biggest challenges and goals which primarily deal with cyber protection at an affordable rate. OCDS website will be positioned to directly speak to the clients via a form-based questionnaire resulting in proprietary products geared specifically for the particular needs of the client’s business.

Acquisition Channels

The main customer acquisition channels will be traffic driven to the website via search engine marketing and event marketing at seminars and conferences. OCDS will launch a blog help drive acquisitions as well. In year one the focus will be on web advertisements and conference/trade show circuits. OCDS will also implement a word-of-mouth referral acquisition discount.

Tools and Technology

OCDS will partner with HubSpot to take advantage of free marketing, sales, and customer service software (CRM) which will eventually grow into a paid service when we grow to that point. HubSpot offers a marketing automation software which will assist OCDS with market appropriately and turn marketing opportunities into sales and eventually revenue.

Sales Plan

Sales Methodology

OCDS understands a strategic sales approach is required to be successful. OCDS will deploy multiple different and effective strategies to attract, engage, and convert potential leads.

- **Targeted Content Marketing**:
  - Create blog posts, whitepapers, and case studies that address common cybersecurity challenges. Offer valuable insights and practical solutions.
  - Optimize your content for relevant keywords to improve search engine visibility.
- **Social Media Engagement**:
  - Regularly share cybersecurity tips, industry news, and success stories on platforms like LinkedIn, Twitter, and Facebook.
  - Engage with your audience by responding to comments and messages promptly.
- **Webinars and Virtual Events**:
  - Host webinars on topics like threat intelligence, data privacy, or secure remote work.
  - Collaborate with industry experts and thought leaders to attract a wider audience.
- **Email Campaigns**:
  - Segment your email list based on interests and behavior.
  - Send targeted emails with educational content, product updates, and special offers.
- **Search Engine Optimization (SEO)**:
  - Optimize your website for relevant keywords related to cybersecurity services.
  - Focus on local SEO if you serve specific regions.
- **Paid Advertising**:
  - Run Google Ads campaigns targeting high-intent keywords.
  - Use LinkedIn ads to reach IT professionals in medium to large businesses.
- **Landing Pages and Lead Magnets**:
  - Create optimized landing pages for specific services or solutions.
  - Offer lead magnets (e.g., e-books, checklists) in exchange for contact information.
- **Networking and Partnerships**:
  - Attend industry conferences, trade shows, and networking events.
  - Collaborate with complementary businesses (e.g., IT service providers, software vendors).
- **Client Testimonials and Case Studies**:
  - Showcase successful projects and client testimonials on your website.
  - Highlight real-world examples of how your solutions have improved security.
- **Remarketing**:
  - Use remarketing ads to target users who have visited your website but haven’t converted.
  - Remind them of your services and encourage them to take action.
- **Consistent Follow-Up**:
  - Nurture leads through personalized follow-up emails and phone calls.
  - Provide additional resources and address any concerns they may have.

OCDS lead generation will be an ongoing process. OCDS will continuously analyze efforts, adapt to industry changes, and refine strategies to stay ahead in the cybersecurity market.

Sales Organization Structure

OCDS will deploy a converged senior leadership for Sales and Marketing to be led by an Executive Vice President of Sales & Marketing. This EVP leader will develop high level strategy and ensure the cohesive approach of both Sales and Marketing to develop appropriate plans for current positioning and future development. The EVP of Sales & Marketing will have separate VPs reporting under them, a VP of Sales and a VP of Marketing. Each of these VP roles will be charged with designing goals to meet the strategies of the EVP and will lead the specific development of each tower. Each VP will have Directors to run the day to day and execute the strategies by meeting the goals needed to drive sales and marketing respectively.

Sales Channels

OCDS will deliver sales via multiple effective sales channels.

- **E-commerce (Online Store/Website)**: https://ocds.tech
  - **Best for**: Companies selling digital security solutions or software.
  - **Description**: Set up an e-commerce website where customers can purchase your cybersecurity products online. Highlight features, benefits, and use cases to attract potential buyers.
- **B2B Sales and Partnerships**:
  - **Best for**: Selling to other businesses or organizations.
  - **Description**: Establish partnerships with IT service providers, managed security service providers (MSSPs), or system integrators. Collaborate with them to offer your products as part of their cybersecurity solutions.
- **Industry-Specific Trade Shows and Other Events and Conferences**:
  - **Best for**: Networking and showcasing your products.
  - **Description**: Attend cybersecurity conferences, trade shows, and industry events. These platforms allow you to connect with potential clients, demonstrate your products, and build relationships.
- **Direct Sales and Consultative Selling**:
  - **Best for**: High-touch sales with personalized advice.
  - **Description**: Engage in consultative selling by understanding your client's specific security needs. Provide tailored solutions and demonstrate how your products address their unique challenges.
- **Marketplaces and Aggregators**:
  - **Best for**: Expanding your reach.
  - **Description**: List your products on cybersecurity marketplaces or platforms where buyers can discover and compare different solutions. Examples include Capterra, G2 Crowd, and Spiceworks.
- **Content Marketing and Thought Leadership**:
  - **Best for**: Building trust and authority.
  - **Description**: Create valuable content such as blog posts, whitepapers, and webinars. Position yourself as an industry expert and educate potential buyers about cybersecurity trends and best practices.

- **Referral Programs and Affiliates**:
    - **Best for**: Leveraging existing networks.
    - **Description**: Encourage satisfied customers, partners, or affiliates to refer your products. Offer incentives for successful referrals.

OCDS will execute this **multichannel approach** mix of sales channels to maximize reach and impact on the OCDS target audience, product complexity, and business goals.

Tools and Technology

The right tools and strategies will help OCDS reach prospects. OCDS will utilize multiple different tools and technologies.

- **To understand prospects' needs**:
    - We will assume prospects do not have a working knowledge of OCDS product. We will tailor our sales pitch to address their specific needs and educate them about the importance of cybersecurity.
- **Avoid Fear Tactics**:
    - While it's essential to convey the danger of cyberattacks, leading with horror stories may not always be effective. Instead, we will focus on the benefits of our products, such as compliance with regulations, threat preparedness, and customer confidence.
- **Ask the Right Questions**:
    - During the sales qualifying process, we will ask questions to assess our prospect's understanding of cybersecurity. We want to understand their pain points, concerns, and existing security measures.
- **Industry-Specific Requirements**:
    - We will strive to understand all varying cybersecurity needs. We will tailor our approach based on our prospects' specific requirements. For example, healthcare, finance, and government sectors will have distinct compliance standards and we will know these standards.
- **Leverage AI SaaS Sales Tips**:
    - When selling OCDS AI cybersecurity software, we will consider SaaS (Software as a Service) sales strategies. We will highlight scalability, ease of deployment, and cost-effectiveness. We will emphasize how our SaaS solution can adapt to their evolving security needs.
- **Stay Informed**:
    - We will continuously educate employees on the latest tactics and technologies in cybersecurity sales. The field evolves rapidly, so staying informed is crucial for success.
- **Use Industry-Recognized Tools**:
    - OCDS will use specialized tools designed for cybersecurity sales.
    - **CRM (Customer Relationship Management)**:
        - We will use HubSpot CRM software to manage leads, track interactions, and nurture relationships with prospects.
    - **Sales Enablement Platforms**:
        - These platforms provide content, training, and tools to empower your sales team. They help streamline processes and improve efficiency.
    - **Marketing Automation Tools**:

        - Automate marketing campaigns, lead scoring, and nurturing. Personalize communication based on prospect behavior.
    - **Lead Generation Tools**:
        - Identify potential customers through lead databases, social media, and website analytics.
    - **Sales Intelligence Tools**:
        - Gather insights about prospects, their company, and industry trends.
    - **Communication Tools**:
        - Use email, video conferencing, and chat tools to engage with prospects.
    - **Proposal and Contract Management Tools**:
        - Streamline the proposal creation process and manage contracts efficiently.

Building trust and understanding potential clints' unique needs are key to successful sales. The process will involve adaptation along the way as we adapt our approach based on the context and continuous defining of strategies.

Legal Structure & Considerations

Legal Structure

Corporation

- Taxation (C-Corp): Tax return must be filed with Form 1120. The C-Corporation is subject to corporate income tax on profits. Shareholders will have to pay personal income tax on the profits made by the corporation.
- Liability: Corporation is immortal, meaning that it does not terminate or dissolve upon a shareholder's death. Shareholders cannot lose more money greater than the amount they have invested in the corporation. Personal checking accounts should not be used for business purposes and the name of the corporation should always be used when interacting with customers.
- Formation: Board of directors will make the decisions of the corporation. Shareholders or investors could be involved in the decision making, but it prolongs it.

Legal Considerations

- Compliance with Data Protection Laws:
    - The handling of all personal data (of employees, customers, and suppliers) will comply with data protection requirements. OCDS will adhere to all applicable regional regulations as deemed required by quarterly audits.
    - OCDS will ensure proper data handling, consent mechanisms, and privacy policy adherence.
- Intellectual Property (IP) Protection:
    - Intellectual property will be protected, including patents, trademarks, and copyrights.
    - Proprietary software, algorithms, and cybersecurity methodologies will be safeguarded.

- Contracts and Agreements:
  - All contracts with clients, vendors, and partners will be clear and comprehensive.
  - OCDS will specify terms related to services, liability, confidentiality, and data protection.
- Liability and Insurance:
  - Professional liability insurance to cover potential claims arising from cybersecurity services will be always in place.
  - Legal representation will ensure understand of liability for any breach or security incidents related to OCDS.
- Cybersecurity Regulations and Standards:
  - OCDS will conduct quarterly audits to stay informed about industry-specific regulations and standards such as NIST, ISO 27001, PCI DSS.
  - Security controls and practices aligned with these standards will be implemented.
- Incident Response and Reporting:
  - OCDS will develop and test incident response plans to handle security breaches.
  - Understanding legal requirements for reporting data breaches to authorities and affected parties is mandatory.
- Employee Training and Compliance:
  - In accordance with OCDS standards all employees will be trained on legal and ethical aspects of cybersecurity.
  - Compliance with internal policies and external regulations is required.

Financial Considerations

Startup Costs

The first year of OCDS will not be profitable as there will be multiple aspects of startup costs coupled with limited revenue. The plan will be to initialize with substantial capital to navigate the first few years until revenue catches up. Startup costs consist of the below.

- **Professional Certifications for Specific Employees**:
  - $15,000
  - Before starting OCDS specific employees will need to obtain the relevant certifications to build credibility. Some popular cybersecurity certifications include:
    1. **Certified Ethical Hacker (CEH)**: Focuses on identifying security weaknesses.
    2. **GIAC Security Essentials (GSEC)**: Validates information security knowledge.
    3. **Certified Information Systems Security Professional (CISSP)**: Demonstrates expertise in designing and maintaining cybersecurity programs.
    4. **Certified Cloud Security Professional (CCSP)**: Indicates skills in securing cloud data and infrastructure.
- **Employee Education and Training**:
  - $25,000
  - While individual employee bachelor’s degree and master’s graduate degrees in information technology or computer science is beneficial, real-world experience matters

more. OCDS will invest in attending workshops, online courses, and hands-on training to enhance employee skills.

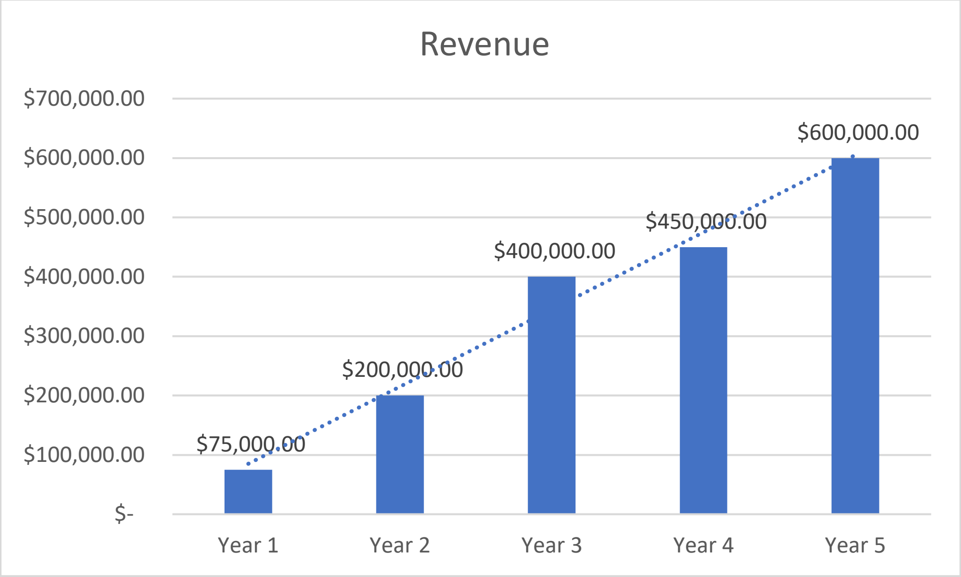
- **Technology and Equipment**:
  - $20,000
  - Invest in high-end computer systems, software licenses, and cybersecurity tools.
  - Costs may include firewalls, intrusion detection systems, antivirus software, and encryption tools.
  - This aspect of costs will be SaaS-related.
- **Business Structure and Legal Fees**:
  - $1500
  - OCDS will establish a C-corporation.
  - Registering the business, obtain necessary licenses, and consult with legal professionals.
- **Office Space and Utilities**:
  - $10,000
  - A physical office will not be required (rent, utilities, and furnishings).
  - Employee work from home expenses will be incurred.
- **Marketing and Branding**:
  - $25,000
  - Developing a professional website is crucial, as well as creating a logo, and investing in initial marketing materials.
  - Digital marketing, social media, and networking events.
- **Insurance**:
  - $1750
  - Cyber liability insurance is crucial. It covers data breaches, cyberattacks, and related legal expenses.
- **Personnel Costs**:
  - $250,000
  - Employees insurance, salaries, benefits, and training.
- **Miscellaneous Expenses**:
  - $10,000
  - These may include travel costs (for client meetings), accounting fees, and other incidentals.
- **Total Startup Costs**:

Expense	Cost
Certifications	15,000
Education and Training	25,000
Technology and Equipment	10,000
Business Structure/Legal Fees	1,500
Office Space and Utilities	10,000
Marketing and Branding	25,000
Insurance	1,750
Personnel Costs	250,000
Miscellaneous Expenses	10,000
Total	**$348,250**

Successful continuous planning and financial management for readjustments will be conducted to maintain success in research, sales, marketing, and revenue to culminate in a successful business.

Sales Forecasts

Sales is forecasted to start slow but build quickly as marketing begins to penetrate the cybersecurity marketplace and sales begins to take hold and increase year over year.



Break-Even Analysis

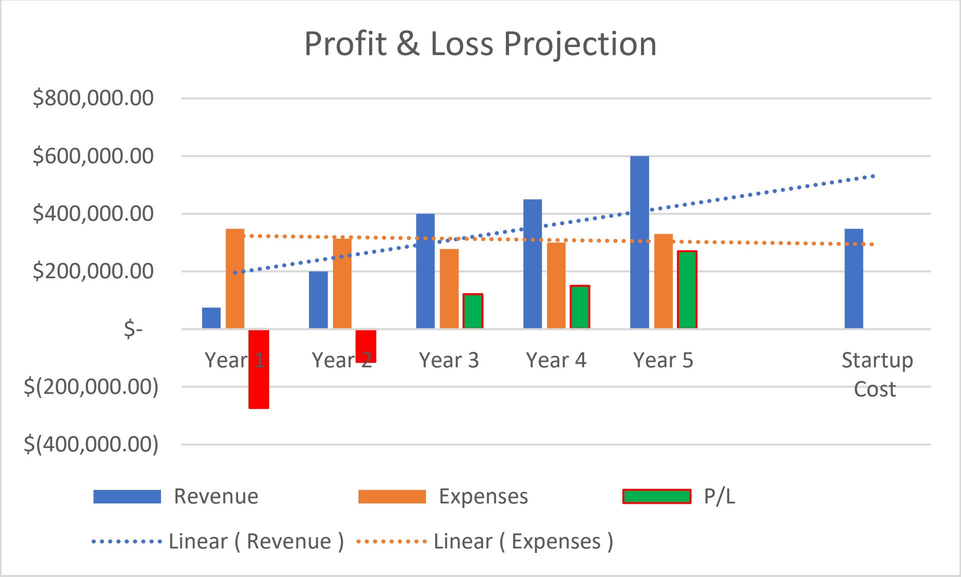
Based on the above sales projection and a varying percentage of the start up cost for yearly expense, the OCDS breakeven analysis puts OCDS breaking even somewhere around the mid-way point of year 3. Year 3 will be the first profitable year for OCDS.

Projected P&L

As with the break-even analysis, the projected profit and loss analysis is based on the above sales projections coupled with a detailed analysis on expenditures year over year. Using the initial startup cost analysis year 2 and 3 are projected at a percentage decrease while year 3 and 4 will see an increase in expenses.

Year	Revenue	Expenses	P/L
Year 1	$ 75,000.00	$ 348,250.00	$(273,250.00)
Year 2	$ 200,000.00	$ 313,425.00	$(113,425.00)
Year 3	$ 400,000.00	$ 278,600.00	**$ 121,400.00**
Year 4	$ 450,000.00	$ 300,000.00	$ 150,000.00
Year 5	$ 600,000.00	$ 330,000.00	$ 270,000.00

Startup Costs	$ 348,250.00



Funding Requirements

Initial Funding will be investment capital based on a 3-year requirement.

Year	Costs/Expenses
Year 1 (Startup)	348,250
Year 2	313,425
Year 3	278,600
Total Initial Investment	$ 940, 275

As an indication of dedication and belief in the business some of initial investments in the business will come from equal amounts of individual employee capital investments covering a portion of the required startup costs. This investment will be repaid of appropriate percentage ownership and awarded via stakeholder payouts when applicable.

Employee	Investment
Scott Gilstrap	50,000
Stephanie Aguirre	50,000
Chris Dunbar	50,000
Ryan LaBlanc	50,000
Justin Place	50,000
Total	**$250,000**

The remaining initial investment will be funding through a small business loan with the Small Business Association based on Scott's veteran status.

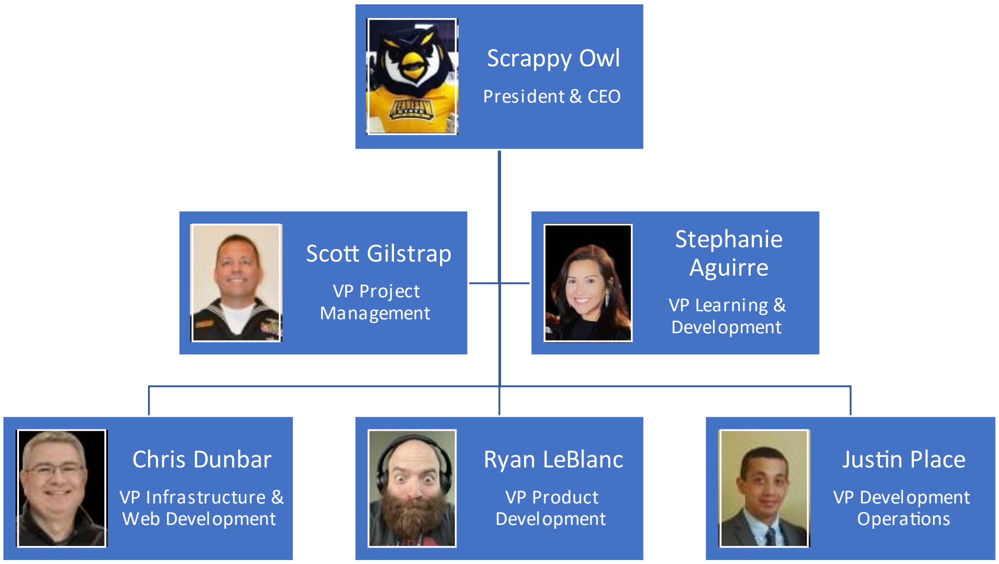
Year	Capital Investment
Employee Investments	250,000
SBA Veteran Loan	690,275
Total Initial Investment	$ 940, 275

Client Offering Pricing Model

OCDS Client Offering	Retail Cost
Proprietary IT Security Plan	$699.99
Proprietary Risk Management & Assessment Plan	$499.99
AI-enabled Security Chatbot Tool	$1499.99
SIEM Tool	$999.99
Cyber Awareness Training	$399.99 per course

Appendix

Owl Cyber Defense Systems Organization Chart



Average Buyer Persona

Technology/Product Buyer Persona

Pam Smith

Background

- Job: Small Busienss Owner
- Career path: Some college then started own busienss.
- Family: Married with 2 childeren
- Lifestyle: Modest.
- Spending habits? Conservativ e

Demographics

- Age: 50
- Income: $150,000
- Location: Rural
- Gender identity: Female

Technology/Social Media

Device preferences: Desktop PC
Socialmedia platforms: Facebook
Tech savvy: Yes

Goals/Metrics/Motivations

Primary/secondary goals: Busienss success. Help People

Personal goals: Good work/life balance. Stay in shape.

Top metrics they track: Satified customers

Motivations: Returning customers with sucessful stories. Family success.

What can we do?

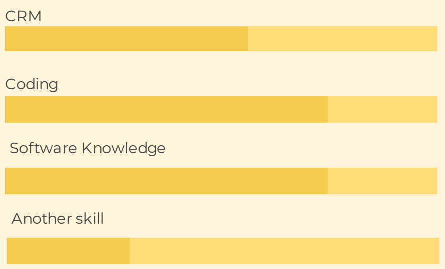
Provide peace of mind when it comes to protecting business from cyber criminals so more energy can be spent of running the business and servicing customers.

Challenges

Struggles with spending too much of company profits to successful protect company assets.

Spends too much time worries about losing everything because of a cyber attack.

Skills



Real Quotes

I want to spend money more wisely to protect my company assets.

I need piece of mind when it comes to cyber protections.

Competitor SWOT Analysis

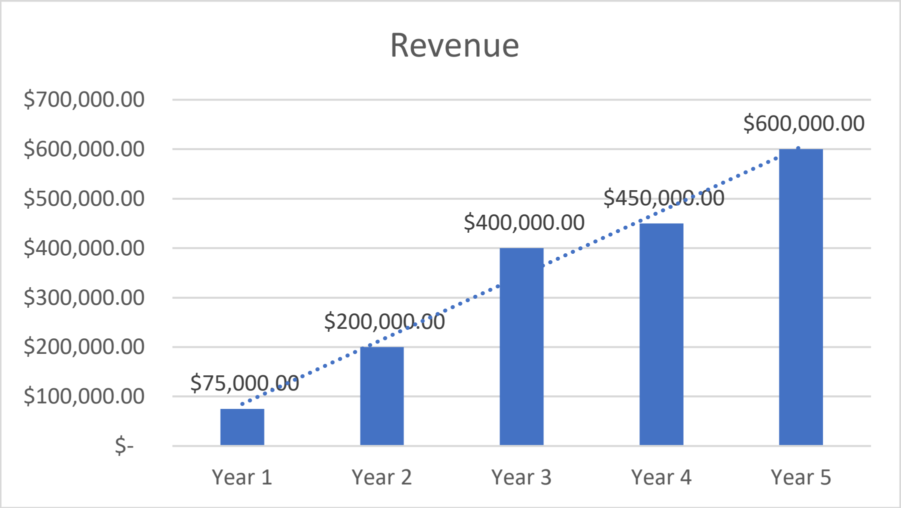
Competitor Name	Comparative Strength(s)	Comparative Weakness(es)	Counterpoint(s)
BigBox Information Security	BigBox InfoSec will have walk by clients, but OCDS has have better knowledge of clients	BigBox will have more capitol because they are a bigger company	OCDS is a smaller company and will be able to reactive quicker
Cyber Protection Online (CPO)	CPO has a larger budget, but OCDS has a more streamlined approach to	CPO has been in business for longer and has more experience in	OCDS has a niche approach for data collection and service

	spending to better target expenditures	the industry	delivery
ACME Cyber	ACME has a wider variety of products but, OCDS has more client detailed proprieties in each client offering	ACME has a larger research & development department supporting robust programming	OCDS has expert developers supporting a proprietary AI product

Startup Cost Chart

Expense	**Cost**
Certifications	15,000
Education and Training	25,000
Technology and Equipment	10,000
Business Structure/Legal Fees	1,500
Office Space and Utilities	10,000
Marketing and Branding	25,000
Insurance	1,750
Personnel Costs	250,000
Miscellaneous Expenses	10,000
Total	**$348,250**

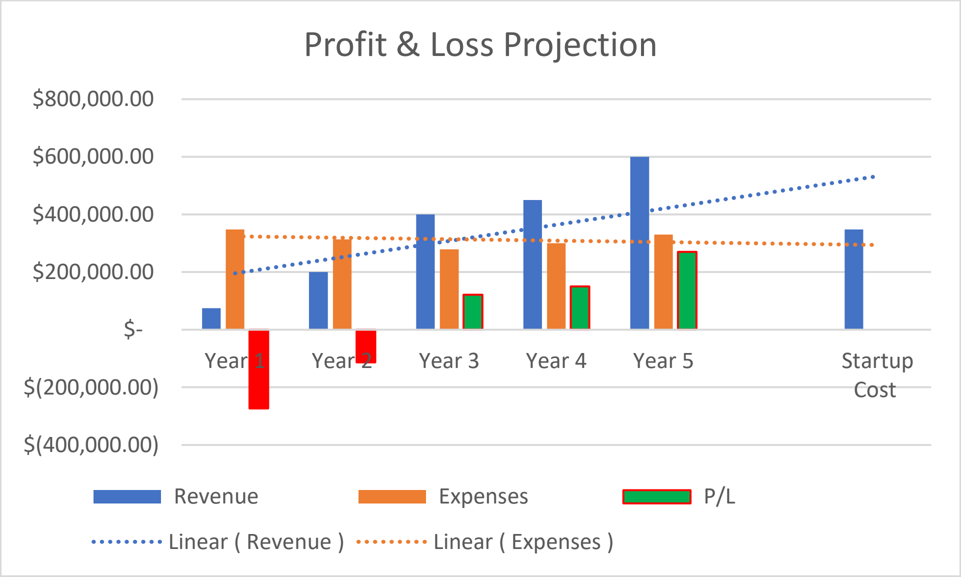
Sales/Revenue Forecasts



Projected Project & Loss

Year	Revenue	Expenses	P/L
Year 1	$ 75,000.00	$ 348,250.00	$(273,250.00)
Year 2	$ 200,000.00	$ 313,425.00	$(113,425.00)
Year 3	$ 400,000.00	$ 278,600.00	**$ 121,400.00**
Year 4	$ 450,000.00	$ 300,000.00	$ 150,000.00
Year 5	$ 600,000.00	$ 330,000.00	$ 270,000.00

Startup Costs	$ 348,250.00



Initial Funding Requirements

Year	Costs/Expenses
Year 1 (Startup)	348,250
Year 2	313,425
Year 3	278,600
Total Initial Investment	$ 940, 275

Employee	Investment
Scott Gilstrap	50,000
Stephanie Aguirre	50,000

Chris Dunbar	50,000
Ryan LaBlanc	50,000
Justin Place	50,000
Total	**$250,000**

Year	Capital Investment
Employee Investments	250,000
SBA Veteran Loan	690,275
Total Initial Investment	$ 940, 275

Client Offering Pricing Model

OCDS Client Offering	Retail Cost
Proprietary IT Security Plan	$699.99
Proprietary Risk Management & Assessment Plan	$499.99
AI-enabled Security Chatbot Tool	$1499.99
SIEM Tool	$999.99
Cyber Awareness Training	$399.99 per course