# GC-84 OWL CYBER DEFENSE SYSTEMS [OCDS]

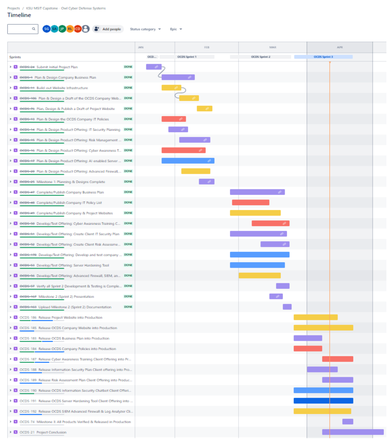
## Introduction

Half of all cyber breaches impact small businesses (SMBs) with less than 1,000 employees. 61% of SMBs were the target of a cyberattack in 2023. Most SMBs do not have an adequate cybersecurity posture due to insufficient education and funding. As cybercriminals increasingly target smaller companies, it's crucial SMBs take proactive measures to protect sensitive data and systems. This project addresses this need by chronicling the startup and tool development of a cybersecurity firm offering affordable security assessments, employee cyber awareness training, an AI-enabled hardening tool in association with an OCDS AI chatbot, as well as deployment of a SIEM tool for firewall and log analysis assisting small businesses with protecting their assets at an affordable cost.

## Objectives

- **Strategic Goal:** Establish the OCDS cybersecurity business providing SMBs cost effective tools to increase their cybersecurity protection posture

- **Operational Goals:** Build Project & Company Websites, Business Plan, and Client Offerings: **1)** IT Security Planning & Risk Assessment, **2)** Cyber Awareness Training, **3)** AI-enabled Server Hardening Tool, **4)** AI Security Chatbot, & **5)** SIEM tool



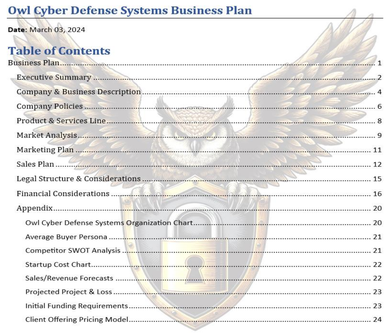

- Sprint 1 – Plan & Design
- Sprint 2 – Development & Testing
- Sprint 3 – Production Deployment

## Tools, Technology & Methods

- **Jira Project Management:** Over the life of the project *Jira* tracked & charted Epics, Milestones, Tasks, Timelines, and Person-hour contributions.
- **Scrum Framework:** Applied hybrid development lifecycle approach utilizing Waterfall Model & Agile Scrum Framework to chronicle project via 3 Sprints.
- **Security Assessments:** Created proprietary IT Security Planning & Risk Assessment questionnaires & collected responses using Microsoft Forms.
- **VMWare ESXi:** Created OCDS company server infrastructure. VMs (virtual machines) for web hosting with a backup & recovery program for resiliency.
- **Hugo Site Generator:** Used Hugo and Bootstrap in conjunction with hand-coded HTML and CSS for company and project websites. Utilized SSH and SFTP for web server management.
- **PyCharm / VS Code / RTX:** Modified RTX chatbot source code to execute AI server hardening advise utilizing NIST 800-53 standards.
- **VMWare Workstation:** Created a virtualization infrastructure as the client environment utilizing multiple VMs providing various servers and operating systems for hardening examples.
- **DISA SCAP v5.8:** Scanned client VM's to produce STIG scores/reports.
- **STIG Viewer:** Used with the SCAP scanning tool to track system vulnerabilities by creating checklists & importing scanner generated data.
- **PowerShell & SSH:** Used to remotely connect and manage remote systems from the management server.

## Deliverables

Detailed **Business Plan** to include Company Mission, Vision, Goals, Policies, Products/Services, Market Analysis, Sales Plan, & Financial Considerations.

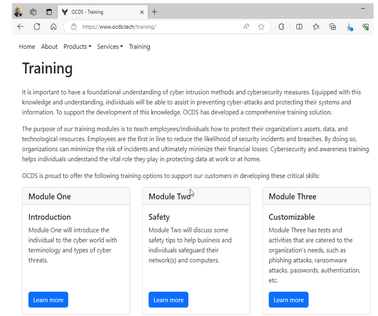


Owl Cyber Defense Systems Business Plan

**Date:** March 03, 2024

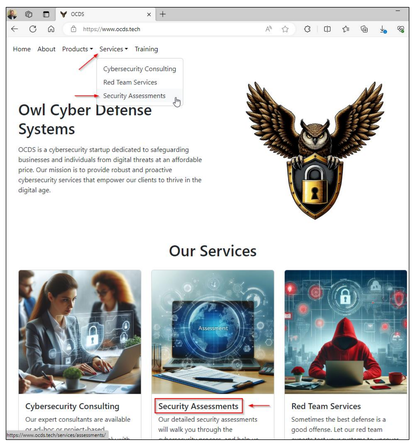
Table of Contents



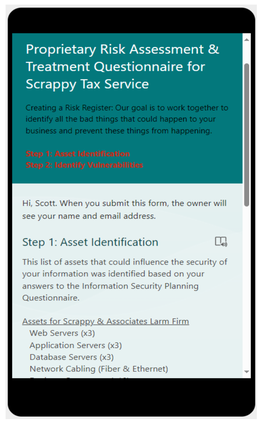



Employees of small businesses experience **350%** more social engineering attacks than those at larger enterprises. Therefore, we designed multiple **Cyber Awareness Training Modules** for our SMB client learning and development intended to increase employee awareness therefore, increasing companies' security posture.

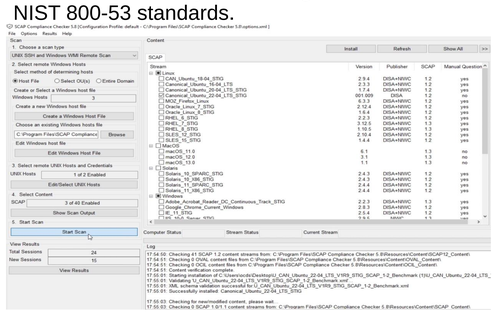
**Security Assessments:** The IT Security Planning Questionnaire collects client feedback. OCDS creates a client **IT Security Plan**. With a completed IT Security Plan, a proprietary **Risk Assessment & Treatment Plan** is created.



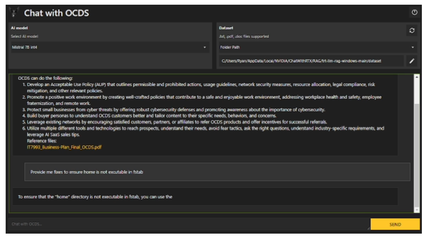





**AI-enabled security hardening tool trained with** NIST 800-53 standards.



**OCDS Security Chatbot** powered by RTX & trained with NIST 800-53 security standards.

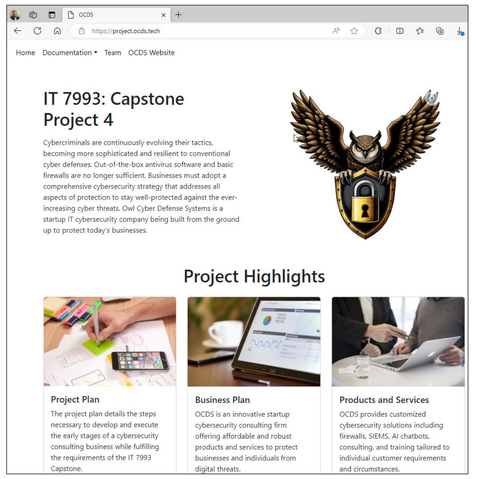



**SIEM Tool** to monitor/protect client network security.


Using Hugo & Bootstrap the project Webmaster created project & company websites.

Project Website: https://project.ocds.tech/

Company Website: https://www.ocds.tech/




## Contact Information


**Scott Gilstrap**: rgilstra@students.kennesaw.edu | https://www.linkedin.com/in/randolph-scott-gilstrap-00144b21/
- Team Lead | Project Manager | Scrum Master

**Stephanie Acquire**: saguirr5@students.kennesaw.edu | https://www.linkedin.com/in/stephanie-a-b7336b262/
- Lead Instructor | Technical Writer

**Chris Dunbar:** cdunbar@students.kennesaw.edu | https://www.linkedin.com/in/chdunbar/
- Senior Systems Engineer | Webmaster

**Ryan LeBlanc**: rleblanc@students.kennesaw.edu | https://www.linkedin.com/in/ryan-leblanc1/
- Information Systems Engineer | AI Developer

**Justin Place**: jplace2@students.kennesaw.edu | https://www.linkedin.com/in/j-98b303142/
- Research Technologist | Infrastructure Architect

**Dr. Jing Xie**: yxie2@kennesaw.edu | https://www.linkedin.com/in/ying-xie-96231367/
- IT Capstone Professor | Mentor | Project Advisor


## References


Home. (n.d.). Scrum.org. https://www.scrum.org/

Agile Alliance. (2024, April 12). What is Agile? | Agile 101 | Agile Alliance. Agile Alliance |. https://www.agilealliance.org/agile101/

Clayton, J. (2024, March 5). Chat with RTX now free to download. NVIDIA Blog. https://blogs.nvidia.com/blog/chat-with-rtx-available-now/

Microsoft Windows 10 security technical implementation guide. STIG Viewer | Unified Compliance Framework®. (n.d.). https://stigviewer.com/stig/microsoft_windows_10/2023-09-29/

Hogan, B. P. (2020). Build websites with Hugo fast web development with Markdown. The Pragmatic Bookshelf.

Hugo. (n.d.). The World's Fastest Framework for Building Websites. Retrieved April 11, 2024, from https://gohugo.io/

Otto, M., & Thornton, J. (n.d.). Bootstrap. Bootstrap. Retrieved April 11, 2024, from https://getbootstrap.com/

Force, J. T. (2020). Security and privacy controls for information systems and organizations. https://doi.org/10.6028/nist.sp.800-53r5

National Institute of Standards and Technology. (2018). Framework for improving Critical Infrastructure Cybersecurity. In NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments. In NIST Special Publication 800-30 (p. 95 pages). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001


KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING


**Authors: Scott Gilstrap, Stephanie Aguirre, Chris Dunbar, Ryan LeBlanc, Justin Place**
**Advisor: Dr. Ying Xie**