



**IT-7993**

**CAPSTONE PROJECT REPORT**

**ID: G01/W01-P4-1**

**Title: Owl Cyber Defense Systems**

**Sponsor: Dr. Ying Xie**

**Project Website: <https://project.ocds.tech/>**

**May 05, 2024**

**Team Members**

Scott Gilstrap (Team Lead/Project Manager)  
Chris Dunbar (Systems Engineer/Webmaster)  
Stephanie Aguirre (Technical Writer/Instructor)  
Ryan LeBlanc (Systems Engineer/AI Developer)  
Justin Place (Research Technologist/Architect)

## Executive Summary

With the ever-maturing sophisticated stature of cybercriminals today, organizations cannot rely on out-of-the-box cybersecurity protections alone. OOB antivirus software and basic firewalls are not enough. With each passing year, cybercriminals are becoming smarter, and continuously evolving. Their tactics are more resilient to conventional cyber defenses. Businesses must address all aspects of cybersecurity to stay well-protected. Owl Cyber Defense Systems is a startup IT cybersecurity company being built from the ground up to meet the evolving cybersecurity defense requirements to protect today's businesses.

This project is based on the requirements of the founder, the project owner/sponsor, for his team to design and develop the company and deliver a presentation utilizing proprietary charts and diagrams where appropriate to convince investors to invest in the IT cybersecurity business model.

Students will be required to exhibit both technical and soft skill components. The student team, made up of five students, will be required to collaborate (physically and/or virtually), communicate efficiently, research thoroughly, and plan accordingly. They will need to define the problem, conduct project management, and engage in technical writing of appropriate documentation; ultimately culminating in a presentation to the instructor (project owner/sponsor) in a format to convince investors to invest in the company. The students will be required to learn and practice new knowledge and skills and the project will have real-world context, requirements, communications, and challenges.

# Table of Contents

- Executive Summary..... 1
- Background..... 3
  - Scope..... 3
  - Business Context and Goals ..... 3
  - Technical Context and Goals..... 3
- Project Outcomes and Achievements ..... 4
  - Overview ..... 4
  - OCDS Business Plan..... 5
  - Company Policies ..... 6
  - OCDS Company Infrastructure ..... 7
  - Project Website..... 8
  - Company Website ..... 13
  - Cyber Awareness Training..... 22
  - IT Security Planning..... 27
  - Proprietary Risk Management Planning ..... 29
  - AI Security Chatbot ..... 31
  - AI-backed Server Hardening Tool ..... 32
  - SIEM Log Analyzer Tool..... 36
- Project Planning and Management Summary..... 38
  - Overview ..... 38
  - Project Process/Milestones ..... 41
  - Workload Summary ..... 43
  - Team Member Roles and Contributions..... 48
- Team Reflection on Project Experience..... 49
  - Project Success Factors ..... 49
  - Team Collaboration and Communication Experiences..... 49
  - Challenges ..... 50
  - Areas to Improve..... 50
- Appendix ..... 50
  - Project Website URL ..... 50
  - OCDS Corporate Website URL ..... 50
  - Project Files ..... 50

References..... 53

## Background

This project was chosen because the team saw a need to provide small businesses with limited budgets a more cost effective and affordable way to increase their cybersecurity posture to help protect their business. In today’s everchanging cybersecurity landscape and increasingly sophisticated cybercriminals the average small business does not have the budget to hire cybersecurity professional firms and do not possess the skills required to organically deploy proper cybersecurity protections for their business. Owl Cyber Defense Systems seeks to fill that need and offer specifically targeted client offerings for the small business to help them protect themselves, their customer data, and their business.

## Scope

The scope of this project is limited to the small business market which is defined by the Small Business Administration (SBA) as an independent business having fewer than 500 employees. [2]

## Business Context and Goals

Research shows 61% of small to medium sized business were the target of a cyberattack in 2023. 87% of SMBs store customer data that could be compromised by an attack. Small Business (less than 500 employees) spend an average of \$3 million USD per cyber incident. [1]

The small businesses simply can’t afford the high-priced protection required in today’s cyber landscape and a cyberattack resulting in a successful breach would put them out of business. These small businesses need a cost effective and affordable solution.

### Strategic Objective/Goal

The single arching strategic goal for this project is to establish Owl Cyber Defense Systems, a small business cybersecurity firm offering to provide small businesses cost effective tools to increase their cybersecurity posture at an affordable rate.

## Technical Context and Goals

With the strategic business goal of establishing Owl Cyber Defense Systems in mind the project has multiple operation objectives/goals which correspond to the project deliverables.

From a technical aspect the **Operational Objectives**, which are the deliverables, are to create/establish the below.

- The OCDS Business Plan – to guide the OCDS business in its journey.
- Company Policies – provide OCDS employees guidance for success.
- Project Website – provide KSU staff and faculty access to project material.

- Company/Corporate Website – provide OCDS customers and potential customers access to OCDS client offerings.
- Cyber Awareness Training – available from the corporate website to help client employees to become more cyber aware.
- IT Security Planning – available via the corporate website to start the process of designing an IT Security Plan for clients.
- Proprietary Risk Management Planning – dovetails into the IT Security planning process to establish proprietary client risk assessments.
- AI Security Chatbot – provide clients with AI generated answers to information security questions in their pursuit to harden their security posture.
- AI-backed Server Hardening Tool – in association with the AI security chatbot provides clients with a means to check and harden their systems to increase their security posture.
- SIEM Log Analyzer Tool – monitor and analyze OCDS client environments to help increase their cyber security posture.

## Project Outcomes and Achievements

Due to the synergy and professionalism of our team and the adherence to the project management SDLC process we successfully completed all Epics and Tasks on time and within budget. Any issue that arose use addressed accordingly and was mitigated in a timely manner before it became an Issue or resulted in required Change Control.

### Overview

With the strategic goal of establishing Owl Cyber Defense Systems in mind the project has multiple operation objectives/goals which correspond to the project deliverables.

OCDS used the **Operational Objectives** to create the below deliverables.

- **OCDS Business Plan** – Scott Gilstrap
  - 25-page detailed plan to include a mission and vision statement.
- **Company Policies** – Stephanie Aguirre
  - 26 sections to be included within the business plan.
- **Project Website** – Chris Dunbar
  - <https://project.ocds.tech/>
- **Company/Corporate Website** – Chris Dunbar
  - <https://www.ocds.tech/>
- **Cyber Awareness Training** - Stephanie Aguirre
  - Three modules to help educate OCDS clients and their employees.
    - Introduction, Safety, and Customizable modules
- **IT Security Planning** – Scott Gilstrap
  - <https://forms.office.com/r/6jnRL8eX8j?origin=lprLink>
  - Guidance: NIST 800-53 and ISO 27001
  - 17 sections, 27 questions, and 10 file upload points for supporting documentation
- **Proprietary Risk Management Planning** – Scott Gilstrap

- Builds off IT Security Plan
- Three Questionnaires
  - Threat analysis resulting in calculated Risk Levels
- **AI Security Chatbot** – Ryan LeBlanc
  - Powered by Nvidia RTX
  - Customized via PyCharm and Visual Studio code
- **AI-backed Server Hardening Tool** – Justin Place
  - VMware Workstation
  - Implemented STIGs (Security Technical Implementation Guides)
  - SCAP Tool (Security Content Automation Protocol)
- **SIEM Log Analyzer Tool** – Chris Dunbar
  - Security Incident and Event Management
  - Security Onion

### OCDS Business Plan

Scott Gilstrap created a 25-page detailed business plan. Sections of the Business Plan include Executive Summary, Company & Business Description, Company Policies, Products & Service Lines, Market Analysis, Marketing Plan, Sales Plan, Legal Structure & Considerations. Appendix structure includes an Organization Chart, Average Buyer Persona, Competitor SWOT Analysis, Startup Cost Analysis, Sales/Revenue Forecasts, Projected Project & Loss Analysis, Initial Funding Requirements, and Client Offering Price Model.

	Business Plan
<b>Business Plan</b>	
<b>Date:</b> March 03, 2024	
<b>Table of Contents</b>	
Business Plan .....	1
Executive Summary.....	2
Company & Business Description .....	4
Company Policies .....	6
Product & Services Line .....	8
Market Analysis .....	9
Marketing Plan.....	11
Sales Plan .....	12
Legal Structure & Considerations .....	15
Financial Considerations .....	16
Appendix .....	20
Owl Cyber Defense Systems Organization Chart.....	20
Average Buyer Persona .....	21
Competitor SWOT Analysis .....	21
Startup Cost Chart.....	22
Sales/Revenue Forecasts.....	22
Projected Project & Loss .....	23
Initial Funding Requirements .....	23
Client Offering Pricing Model.....	24

### Company Policies

Stephanie Aguirre created the OCDS IT and Company Policies. 26 sections of company policies were written and established to guide OCDS employees to success. The policies are incorporated into and an import part of the OCDS Business Plan. The policies are reviewed and updated each quarter. Each employee is required to read agree to each policy each year.

The high-level OCDS Company Polices are:

- Equal Opportunity
- Workplace Health & Safety
- Code of Conduct
- Attendance & Time Off (PTO)
- Ethics Policy
- Substance Abuse
- Compensation & Benefits
- Remote Work

The subsections of the OCDS IT Policies are:

- Usage Guidance
- Network Security
- Resource Allocation
- Legal Compliance
- Risk Mitigation
- Bringing Own Device to Work (BYOD)
- Social Media
- User Accounts and Passwords

- Access Control
- AUP – Acceptable Use Policy
- Backing Up Information
- Purchase and Installation of Software
- Incident Response
- Wireless Use
- Security Awareness and Training
- Data Retention
- E-mail Usage
- Data and Information Security

**Owl Cyber Defense Systems Business Plan**

**Date:** March 03, 2024

**Table of Contents**

Business Plan.....	1
Executive Summary .....	2
Company & Business Description.....	4
Company Policies .....	6
Product & Services Line.....	8
Market Analysis.....	9
Marketing Plan.....	11
Sales Plan.....	12
Legal Structure & Considerations.....	15
Financial Considerations.....	16
Appendix.....	20
Owl Cyber Defense Systems Organization Chart.....	20
Average Buyer Persona .....	21
Competitor SWOT Analysis.....	21
Startup Cost Chart.....	22
Sales/Revenue Forecasts.....	22
Projected Project & Loss.....	23
Initial Funding Requirements.....	23
Client Offering Pricing Model.....	24

**OCDS Company Infrastructure**

The OCDS company infrastructure is a VMware ESXi cluster running in a data center near Atlanta. The websites are hosted on a virtual machine running OpenBSD 7.5 and the native HTTPD web server software and is utilizing *Let's Encrypt* for website security. Both websites have been coded by hand using HTML, CSS, JavaScript and published with Hugo, a static HTML generator application.



The DNS zone file is hosted on dedicated DNS servers running NSD. DNS configurations for both websites, <https://ocds.tech> and <https://project.ocds.tech> are below.

```

$TTL 300      ; Defines the default Time To Live in seconds

@           IN      SOA      ns1.dunbar.net. hostmaster.dunbar.net. (
                    2024020101
                    3600
                    3600
                    604800
                    3600 )

;
; Name Servers authoritative for this domain
;
;               IN NS      ns1.dunbar.net.
;               IN NS      ns2.dunbar.net.
;               IN NS      ns3.dunbar.net.
;
; Mail Servers
;
;               IN MX      10 mail-example.ocds.tech.
;
; Public Addresses
;
;               IN A      38.110.15.77
www          IN A      38.110.15.77
project     IN A      38.110.15.77
;

```

## Project Website

Powered by Hugo and Bootstrap the OCDS project website is hosted on a VMWare ESXi environment and was created and is maintained by Chris Dunbar.

The project website is hosted on a virtual machine running OpenBSD 7.5 and the native HTTPD web server software and is utilizing *Let's Encrypt* for website security. The project website has been coded by hand using HTML, CSS, JavaScript and published with Hugo, a static HTML generator application.

The project website URL is <https://project.ocds.tech>. Sections include:

- Home
  - Project Title, number (G01/W01-P4-1), and description
  - Project Highlights: Project Plan | Business Plan | Department Presentation
- Documentation
  - Business Assets (Business Plan, IT Policies, Cybersecurity Policies, Cyber Awareness Training, Cyber Awareness Training – customer example)
  - Milestones (Milestones 1, 2, and 3)

- Project Assets (Project Proposal, Project Plan, Department Presentation video, Security Chatbot Installer Package, VM files package, Final Project Report)
- Required Links: KSU Website | CCSE Website | CCSE IT Department | Capstone Course | C-Day
- Team: Meet the Team with brief Bios and LinkedIn profile links
- OCDS Website: Link to company/corporate website

The screenshot shows a web browser window with the following elements:

- Browser Tab:** IT 7993 Capstone - Business Assets
- Address Bar:** <https://project.ocds.tech/ocds/assets/>
- Navigation:** Home, Documentation, Required Links, Team, OCDS Website
- Section Header:** Business Assets
- Text:** Business Assets are deliverables created as employees of Owl Cyber Defense Systems. They include documents created for the purpose of developing the business (e.g., the Business Plan), operating the business (e.g., IT and Cybersecurity Policies), as well as content created for potential OCDS customers (e.g., training materials).
- Assets List:**
  - Business Plan:** The Business Plan for Owl Cyber Defense Systems. [Download PDF](#)
  - OCDS IT Policies:** OCDS corporate IT Policies. [Download PDF](#)
  - OCDS Cybersecurity Policies:** OCDS corporate Cybersecurity Policies. [Download PDF](#)
  - OCDS Cybersecurity Training:** OCDS Cybersecurity Training Presentation. [Download PDF](#)
  - OCDS Cybersecurity Training: Customer Example:** OCDS Cybersecurity Training Presentation for Scrappy Tax Service. [Download PPT](#)
- Footer:** Copyright © 2024 IT 7993 Capstone Project ID: G01/W01-P4-01

The screenshot shows a web browser window with the address bar displaying <https://project.ocds.tech/project/milestones/>. The page title is "IT 7993 Capstone - Milestones". The navigation menu includes "Home", "Documentation", "Required Links", "Team", and "OCDS Website".

## Milestones

Project milestones are points within a project's timeline that signify major achievements or important events, working toward the project's overall objectives. This project utilized a hybrid Waterfall and Agile-Scrum project management methodology. The Scrum sprints aligned with the capstone class' required Milestones, which are available for download below.

### Milestone #1

Milestone #1 focused on the initial organization of the project. We divided work amongst the team members to focus on overall project management, development of business documentation, creation of server and website infrastructure, and the initial development of our AI Cybersecurity Chatbot.

[Download PDF](#)

### Milestone #2

Milestone #2 focused on building out the items initiated in the first milestone. The initial business and project websites were put into production, early examples of the AI Chatbot were tested, and our first business documents (e.g. business plan and training materials were completed).

[Download PDF](#)

### Milestone #3

Milestone #3 focused on finalizing many of the outstanding project elements. A new version of the AI Chatbot was in development and undergoing heavy testing. The business and project websites were still undergoing development but more elements were published onto the production server. Additional business offerings were also finalized.

[Download PDF](#)

Copyright © 2024 IT 7993 Capstone Project ID: G01/W01-P4-01

The screenshot shows a web browser window with the URL <https://project.ocds.tech/project/assets/>. The page title is "Project Assets" and it includes a navigation menu with "Home", "Documentation", "Required Links", "Team", and "OCDS Website".

**Project Assets**  
Project Assets are deliverables created for the IT 7993 Capstone project. They include the original Project Proposal, the more detailed Project Plan, and, eventually, the completed Final Project Report.

- Project Proposal**  
The Project Proposal was submitted to the Capstone advisor (i.e., Dr. Xie) for initial approval.  
[Download PDF](#)
- Project Plan**  
The final Project Plan outlines all the components of the Capstone project, and received sign-off from each member of the project team.  
[Download PDF](#)
- Department Presentation**  
Project ID G01/W01-P4-01 Department Presentation recorded April 27, 2024. Available for viewing on YouTube or as direct file download.  
[Watch Video](#) [Download Video](#)
- AI Chatbot Installer**  
Our AI Cybersecurity Chatbot is based on NVIDIA's ChatRTX application. This customized installer will install the application and our training material. Note: this is a large file!  
[Download ZIP](#)
- Virtual Machine Files**  
We created and utilized several VMware virtual machines for building and testing our server hardening tool. The VMs and support files are available in this download. Note: this is a large file!  
[Download ZIP](#)
- Final Project Report**  
The Final Project Report will be available here near the end of spring semester.  
[Download ZIP](#)

Copyright © 2024 IT 7993 Capstone Project ID: G01/W01-P4-01

## Company Website

Powered by Hugo and Bootstrap the OCDS company website is hosted on a VMWare ESXi environment and was created and is maintained by Chris Dunbar.

The company website is hosted on a virtual machine running OpenBSD 7.5 and the native HTTPD web server software and is utilizing *Let's Encrypt* for website security. The project website has been coded by hand using HTML, CSS, JavaScript and published with Hugo, a static HTML generator application.

The OCDS company website URL is <https://ocds.tech>.

Sections include:

- Home
  - Owl Cyber Defense Systems company summary
  - Our Services
    - Cybersecurity Consulting
    - Security Assessments
    - Red Team Services
- About
  - Brief Summary
  - Mission Statement
  - Vision Statement
  - Meet the Leadership Team
- Products
  - Advanced Firewalls
  - AI Security Chatbot
  - SIEMs
- Services
  - Cybersecurity Consulting
  - Red Team Services
  - Security Assessments
- Training
  - Module One – Introduction
  - Module Two – Safety
  - Module three – Customizable (test and activities)

OCDS

https://www.ocds.tech

Home About Products Services Training

# Owl Cyber Defense Systems

OCDS is a cybersecurity startup dedicated to safeguarding businesses and individuals from digital threats at an affordable price. Our mission is to provide robust and proactive cybersecurity services that empower our clients to thrive in the digital age.

## Our Services

### Cybersecurity Consulting

Our expert consultants are available for ad-hoc or project-based engagements. We work closely with our customers to maximize results.

[Learn More](#)

### Security Assessments

Our detailed security assessments will walk you through the cybersecurity process, and help us better understand your current environment and needs.

[Learn More](#)

### Red Team Services

Sometimes the best defense is a good offense. Let our red team experts test your systems to uncover any lurking vulnerabilities.

[Learn More](#)

Copyright © 2024IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01

OCDS - About

https://www.ocds.tech/about/

Home About Products Services Training

# About

*Serving the local community since 2024*

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.


## Leadership Team




**Stephanie Aguirre**  
Vice President, Learning and Development




**Chris Dunbar**  
Vice President, Infrastructure and Web Development



**Scott Gilstrap**  
Vice President, Project Management



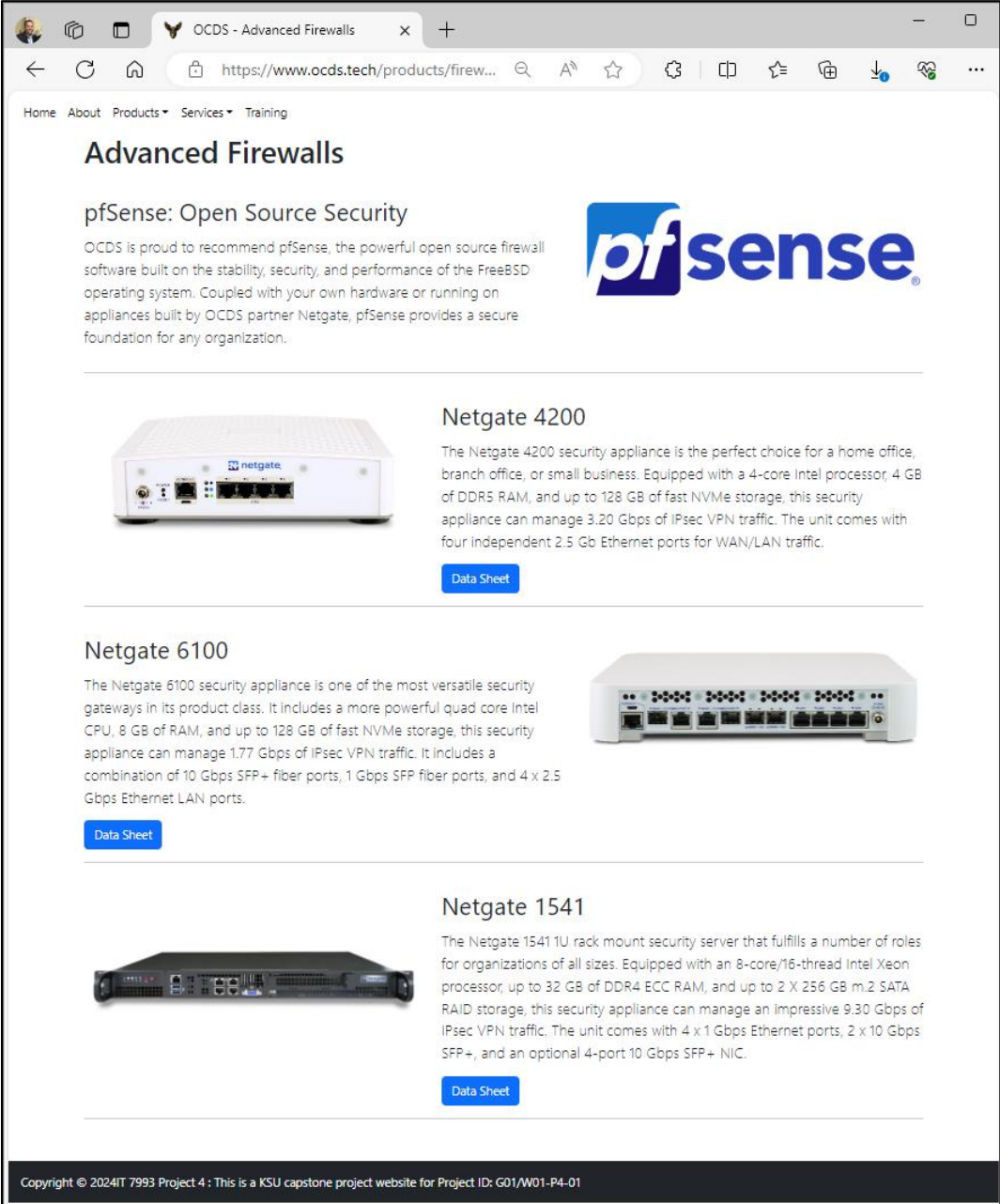
**Ryan LeBlanc**  
Vice President, Product Development



**Justin Place**  
Vice President, Development Operations

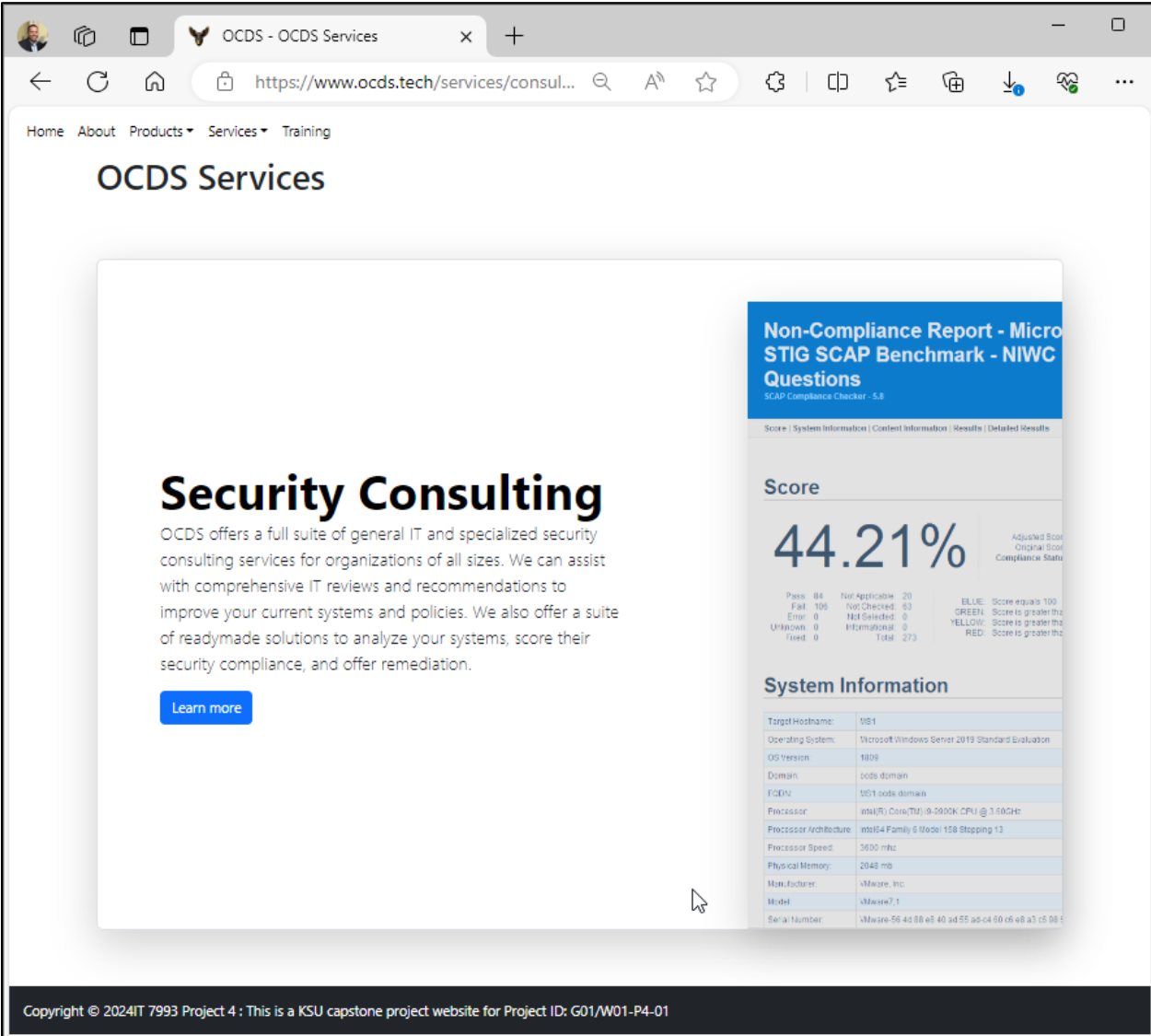
Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01





The screenshot shows a web browser window with the URL <https://www.ocds.tech/products/ai-ch...>. The page title is "AI Chatbot" and the sub-header is "OCDS Cybersecurity Chatbot". The main text describes the chatbot as an AI-powered cybersecurity tool running on NVIDIA's ChatRTX software, capable of answering detailed questions and generating security steps. A "Learn more" button is visible. An inset image shows a chat interface titled "Chat with OCDS" with a question about NIST 800-53 and a detailed answer regarding its publication and use. The footer contains the copyright notice: "Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01".

The screenshot shows a web browser window with the URL <https://www.ocds.tech/products/siems/>. The page title is "SIEMs" and the sub-header is "Security Information and Event Management". The text explains that a SIEM system combines Security Information Management (SIM) and Security Event Management (SEM) to collect and analyze log data from various sources. An inset image shows a SIEM dashboard with charts and a "Group Metrics" section. Below this, the "Security Onion" logo is displayed, followed by text recommending Security Onion Solutions for their open-source SIEM software and hardware appliances. A "Learn more" button is present. The footer contains the copyright notice: "Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01".



The screenshot shows a web browser window with the address bar displaying "https://www.ocds.tech/services/redtea...". The website has a navigation menu with "Home", "About", "Products", "Services", and "Training". The main heading is "OCDS Services". Below this, there is a section for "Red Team" with a blue "Learn more" button. To the right of the text is a vertical image of a woman in a red hoodie. At the bottom of the page, a dark footer contains the text: "Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01".

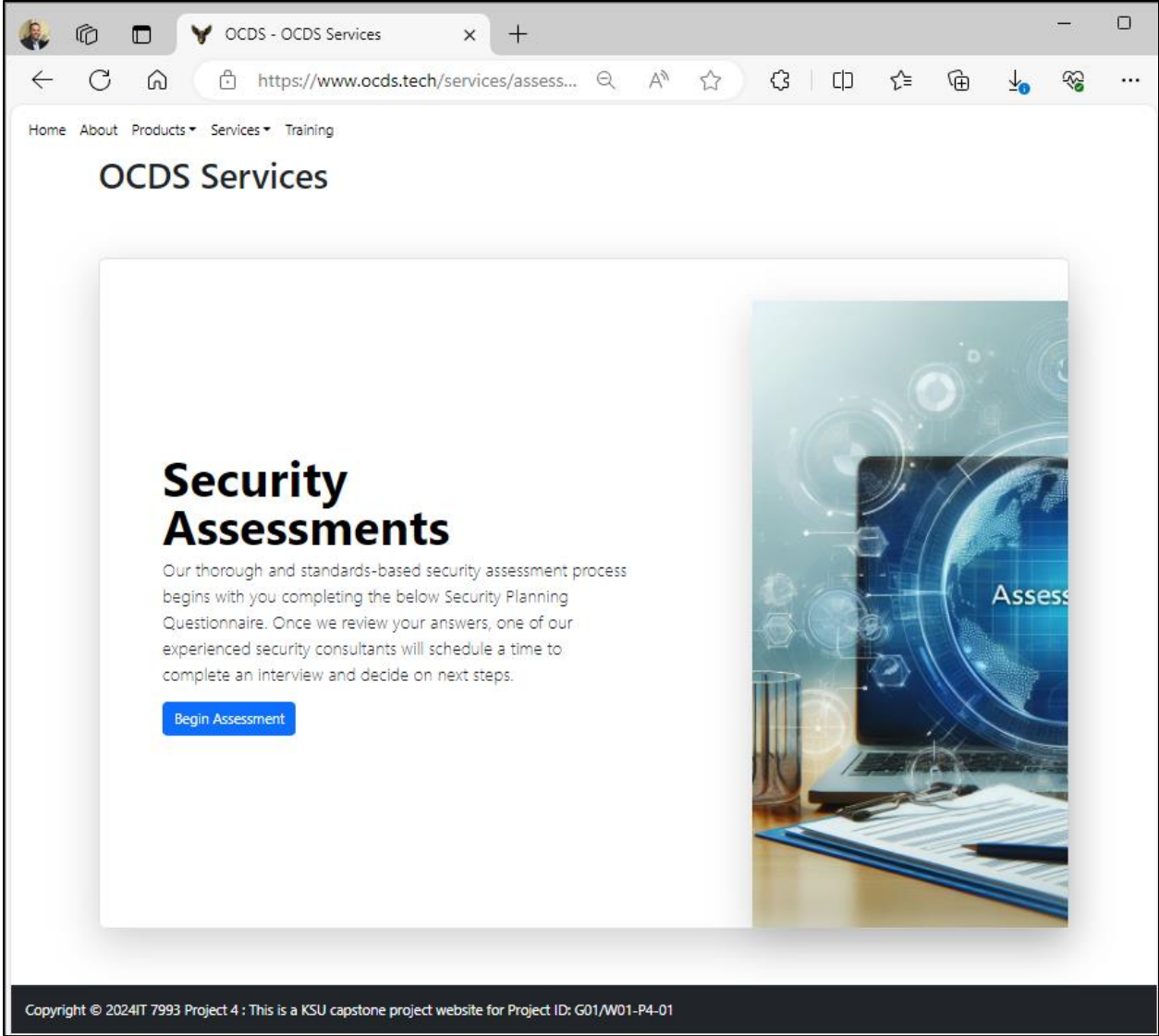
OCDS Services"

## Red Team

OCDS offers comprehensive Red Team services designed to rigorously test and enhance the security resilience of your organization. Our Red Team experts employ a full-spectrum approach to simulate sophisticated cyber-attacks and identify vulnerabilities in your security posture. We can assist with all forms of cybersecurity testing including physical, network, cloud, and applications.

[Learn more](#)

Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01



OCDS - Training


https://www.ocds.tech/training/

Home About Products Services Training

# Training

It is important to have a foundational understanding of cyber intrusion methods and cybersecurity measures. Equipped with this knowledge and understanding, individuals will be able to assist in preventing cyber-attacks and protecting their systems and information. To support the development of this knowledge, OCDS has developed a comprehensive training solution.

The purpose of our training modules is to teach employees/individuals how to protect their organization's assets, data, and technological resources. Employees are the first in line to reduce the likelihood of security incidents and breaches. By doing so, organizations can minimize the risk of incidents and ultimately minimize their financial losses. Cybersecurity and awareness training helps individuals understand the vital role they play in protecting data at work or at home.



OCDS is proud to offer the following training options to support our customers in developing these critical skills:

Module One	Module Two	Module Three
<b>Introduction</b> Module One will introduce the individual to the cyber world with terminology and types of cyber threats.	<b>Safety</b> Module Two will discuss some safety tips to help business and individuals safeguard their network(s) and computers.	<b>Customizable</b> Module Three has tests and activities that are catered to the organization's needs, such as phishing attacks, ransomware attacks, passwords, authentication, etc.
<a href="#">Learn more</a>	<a href="#">Learn more</a>	<a href="#">Learn more</a>

The training is done at the user's own pace. It could take anywhere between 45 minutes to two hours – depending on how quickly the user understands the material. It is recommended for an organization to continue cybersecurity training an awareness at least once a year.

Copyright © 2024 IT 7993 Project 4 : This is a KSU capstone project website for Project ID: G01/W01-P4-01

## Cyber Awareness Training

Stephanie Aguirre researched multiple cybersecurity big business firms and created the OCDS cyber awareness training to include three modules. Stephanie used Microsoft PowerPoint to create slide decks with voice over recordings to walk OCDS clients through their training. Stephanie was assisted by the OCDS Webmaster, Chris Dunbar, using Synthesia to create Carly, an OCDS Training Instructor AI avatar.



### **Module One**

The first module is an introduction to cybersecurity and includes terminology and describes the different types and threats/attacks.

### **Module Two**

The second module is about cybersecurity safety and cyber attack prevention.

### **Module Three**

The third module is customizable and proprietary to each client and includes specific tests and activities particular to the client business and their environment.

Scrappy Tax Service  
**Cybersecurity  
Training**



▸ **Welcome to Cybersecurity training!**

- Cyber security is defending computers, servers, electronic devices, data, and networks from malicious attacks.
- Cyber attacks happen daily and the attacks are always evolving
- With the growing cyber attacks, there is an increase to cybersecurity
- We developed this training guide to help individuals, like yourself, better understand the risks of the cyberworld





## TRAINING PROGRAM MODULE 1

- The first module will introduce you to the cyber world with terminology and types of cyber threats



## Types of Cyber Threats

- Cybercrime – an individual or group that target a system for financial gain or to cause disturbance
- Cyber attack – this often includes a political motive
- Cyberterrorism – attacks systems to cause panic and fear




## TRAINING MODULE 2

- This second module will discuss some safety tips to help business and individuals safeguard their network(s) and computers



### How to protect your systems and electronic devices?



-  End-user protection- an individual (the user) could accidentally upload malware to a desktop or mobile device, and it could spread to the network.
-  Security protocols must be in place
-  Cyber security training programs help professionals identify new threats and ways to combat them. Employees need to be educated and up to date on how to protect their devices and network.
-  Our training program offers safety tips and tests to help business and individuals guard themselves against cyber threats and attacks

## CYBER SAFETY TIPS



Updating software and operating system is crucial. The user will benefit from the latest security patches. If the user does not update their software or operating system, then they are exposed to the cybercriminals.



Using strong passwords – using a series of numbers, letters (capital and lowercase), and symbols will make up a great password. Making sure that passwords are not easily guessable. Using hashed passwords are recommended. Aside from using strong passwords, it is also recommended to change passwords every 90 days.




Do not open email attachments from an unknown sender. If the user is unsure of whether it is a phishing or malicious email, then it is important to report it to their IT department. Opening an attachment from an unknown sender is how the malware is spread.

## Training Module 3

- The third module will consist of a mini exam that will test what the individual has learned throughout the program and activities to continue the learning






## PHISHING TEST #2

**2. A company vendor sends you a text message asking you to renew password by clicking the link in the text and it will redirect you to their website to change it. You should:**

- A. Reply to the text and confirm whether you really need to change your password
- B. Call the vendor using a phone number that you know is correct for them and asking them to confirm the request
- C. Click the link and if it takes you to the vendor's website, then you know it's not a scam

## Other resources recommended:

- Cybersecurity Trivia – spin the wheel!  
<https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html?category=smartphone>
- Counter Intelligence Trivia – spin the wheel!  
<https://securityawareness.usalearning.gov/cdse/multimedia/games/citrivia/index.html>
- Cyber security Jeopardy -  
<https://securityawareness.usalearning.gov/cdse/multimedia/games/con-jep-gameone/story.html>
- Hidden Objects Security Game -  
<https://securityawareness.usalearning.gov/cdse/multimedia/games/hiddenobject/story.html>

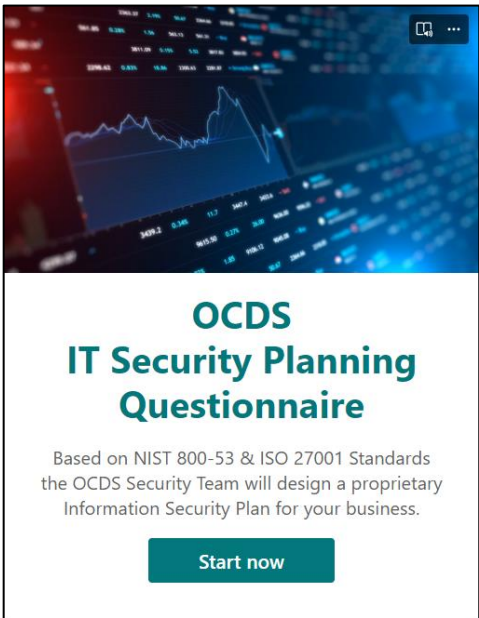


### IT Security Planning

Using the NIST 800-53 Standards for Security and Privacy Controls as well as the ISO 27001 Standards for Information Security Management Systems (ISMS) Scott Gilstrap designed and created a detailed IT Security Planning Questionnaire.

This initial client security planning questionnaire consists of 17 sections and is made up of 27 questions. There are 10 file upload points for client supporting documentation.

<https://forms.office.com/r/6jnRL8eX8j?origin=lpLink>



The IT Security planning section of the OCDS security assessment is the asset identification stage.

Client will complete the IT Security Planning Questionnaire. The client will receive notification of completion. OCDS security professional will receive notification of completion. Using the detailed asset identifications OCDS creates a proprietary Risk Assessment Questionnaire for client to complete.

11. Describe the specifics of your company's server environment. How many web servers? How many application servers? How many database servers? How many other servers (be specific)? How does your company maintain security updates for these servers? Provide documentation and diagrams if you have them. \*

Server Hardware Inventory

Enter your answer

12. Describe the specifics of your company's storage infrastructure. What does your company use for network storage devices? Be specific. Describe the storage configuration. How does your company maintain security updates for these storage devices? Provide documentation and diagrams if you have them. \*

Storage Hardware Inventory

Enter your answer

13. Describe the specifics of your company's desktop environment. Does your company utilize designated IDEs

\* Required

Data Landscape & Inventory

16. Describe the type of data your company is storing. What kind of data? Do you have a data classification program in place? If so, please describe and provide documentation.

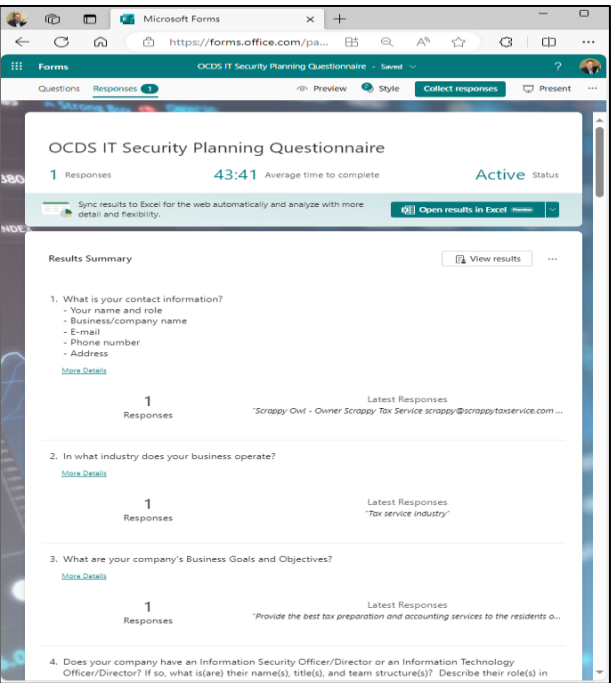
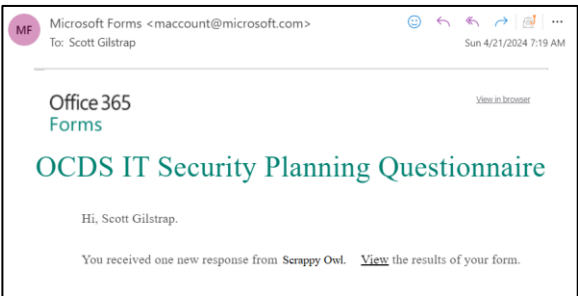
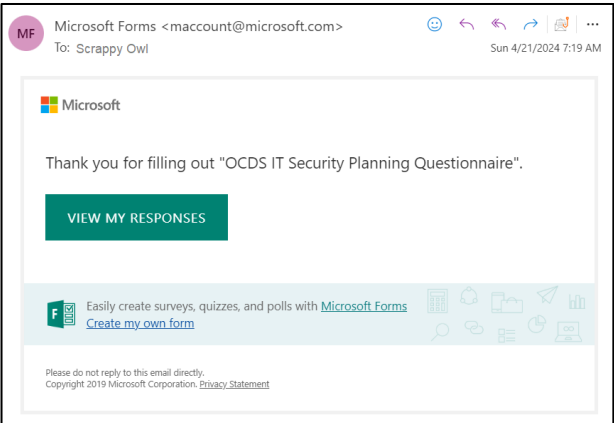
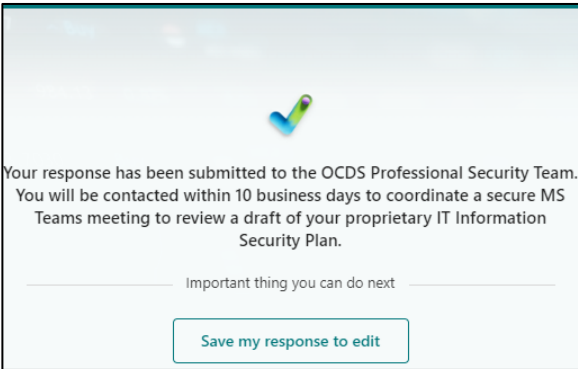
Describe your company's data workflow of customer or proprietary data. Where/how does your company store data at rest? Storage devices? Databases? Etc.? Where is each data type stored? How is data protected in transit? Does your company currently have any encryption in place? Describe how you are protecting the Confidentiality, Integrity, and Availability of your data. Provide documentation and diagrams if you have them. \*

Data Type, Classification & Protection

Enter your answer

Back Next

Page 9 of 17



### Proprietary Risk Management Planning

Still adhering to the NIST 800-53 Standards for Security and Privacy Controls as well as the ISO 27001 Standards for Information Security Management Systems (ISMS) Scott Gilstrap designed and created the client Risk Management Planning Questionnaire.

The Risk Management Planning pulls from the asset identification conducted via the IT Security Planning and performs a detailed Impact Analysis to include Threat Impact and Threat Likelihood Assessments.

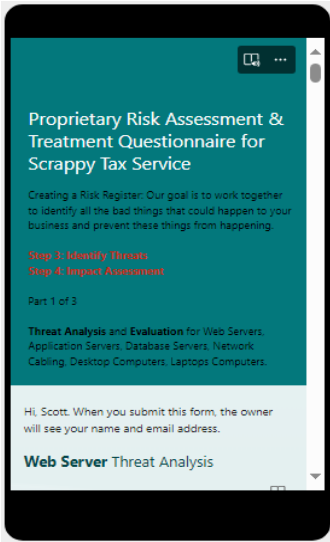
This assessment is completed via three steps.

- Step 1 of 3: <https://forms.office.com/r/eaZpRaMDH9?origin=lpLink>
- Step 2 of 3: <https://forms.office.com/r/UQdQsCCSgz?origin=lpLink>
- Step 3 of 3: <https://forms.office.com/r/bj2kaz9nkS?origin=lpLink>

Based on the results from Threat Analysis OCDS calculates Risk Levels for each threat. The client accepts Risks that are of an appropriate level. OCDS identifies treatment options for the Risks that are not acceptable using appropriate security controls to mitigate each risk to an acceptable level. The client accepts treatment options, and the **Risk Treatment Plan** is created.

OCDS generates two reports:

1. Risk Assessment and Treatment
2. Statement of acceptance of residual risks



**Proprietary Risk Assessment & Treatment Questionnaire for Scrapy Tax Service**

Creating a Risk Register. Our goal is to work together to identify all the bad things that could happen to your business and prevent these things from happening.

**Step 3: Identify Threats**  
**Step 4: Impact Assessment**

Part 1 of 3

**Threat Analysis and Evaluation for Web Servers, Application Servers, Database Servers, Network Cabling, Desktop Computers, Laptops Computers.**

Hi, Scott. When you submit this form, the owner will see your name and email address.

**Web Server Threat Analysis**

**Step 3: Identify Threats**

**Step 4: Impact Assessment**

To effectively manage threats, your organization will need to adopt a risk-based approach, prioritize resources, and stay informed about emerging risks. Cybersecurity is an ongoing process, and proactive measures are essential to protect your valuable assets.

For Step 3 identify any threats or negative happenings that could exploit the vulnerabilities in your assets. Answer only the ones you think apply. Leave the others blank.

Step 4 is the Evaluation Stage. You are conducting a threat analysis and impact assessment of a possible exploitation.

Thinking about the vulnerabilities you selected in Step 2 select the **Impact** (severity of consequence if compromised) for each Risk/Threat as well as the **Likelihood** of its occurrence against your assets.

**Impact Assessment Guide:**

- If the consequences of compromising the Confidentiality, Integrity and/or Availability of the information related to the asset are very "big" select a higher number.
- If the consequences are negligible select a lower number.
- Select an appropriate middle-ground number for any level of consequence in between.
- If it does not apply to your assets leave it blank.

**Likelihood Assessment Guide:**

- If you are certain this will happen within the next couple of years select a higher number.
- If you think this will almost never happen select a lower number.
- Select an appropriate middle-ground number for any level of likelihood in between.
- If it does not apply to your assets leave it blank.

1. **Web Servers** [ScrapyWebSrvr1 | ScrapyWebSrvr2 | ScrapyWebSrvr3]

**Threat Impact:**

Physical theft, vandalism, or sabotage: Theft of physical assets (e.g., laptops, servers) can lead to data breaches.

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

Low Impact High Impact

2. **Web Servers** [ScrapyWebSrvr1 | ScrapyWebSrvr2 | ScrapyWebSrvr3]

**Threat Likelihood:**

Physical theft, vandalism, or sabotage: Theft of physical assets (e.g., laptops, servers) can lead to data breaches.

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

Low Likelihood High Likelihood

3. **Web Servers** [ScrapyWebSrvr1 | ScrapyWebSrvr2 | ScrapyWebSrvr3]

**Threat Impact:**

Denial-of-Service (DoS) Attacks: Overwhelming a system or network to disrupt services.

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

Low Impact High Impact

4. **Web Servers** [ScrapyWebSrvr1 | ScrapyWebSrvr2 | ScrapyWebSrvr3]

**Threat Likelihood:**

Denial-of-Service (DoS) Attacks: Overwhelming a system or network to disrupt services.

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

Low Likelihood High Likelihood

5. **Web Servers** [ScrapyWebSrvr1 | ScrapyWebSrvr2 | ScrapyWebSrvr3]

**Threat Impact:**

Interruption of power supply from public network

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

Low Impact High Impact

## AI Security Chatbot

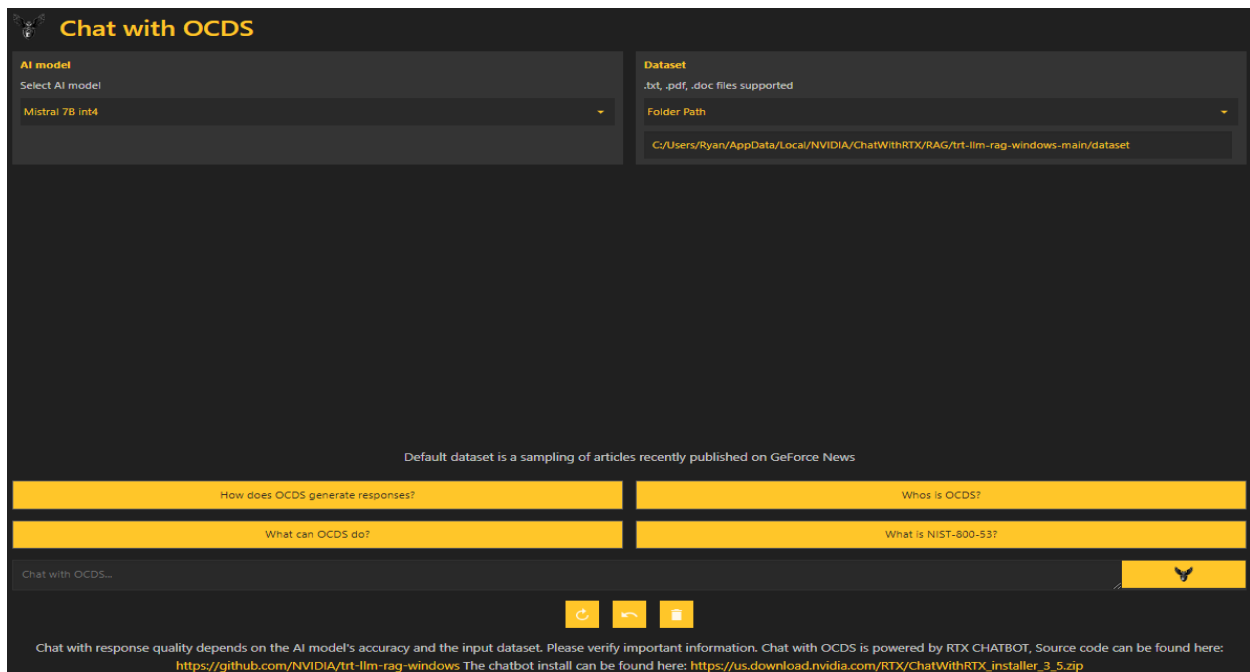
Ryan LeBlanc created the OCDS AI Security Chatbot. Powered by Nvidia RTX Ryan used NIST 800-53 information security controls and standards to populate datasets to teach the OCDS Chatbot. He used PyCharm and Visual Studio Code scripting to modify RTX Chatbot source code.

The OCDS Chatbot utilizes the NIST standards to answer client security questions providing security advice based. This enables our clients to ask IT security questions and receive the appropriate answer to properly secure their environment. The clients can use the OCDS chatbot to determine steps to take to harden their systems when utilizing the AI backed server hardening tool created by Justin Place.

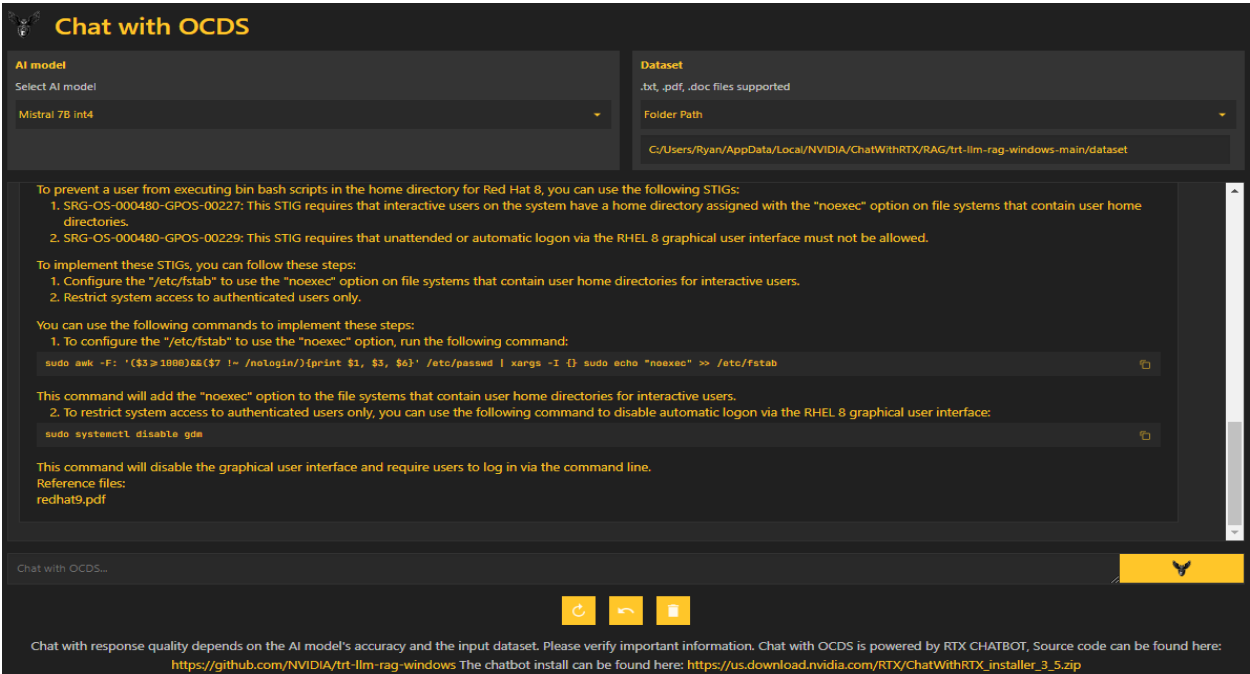
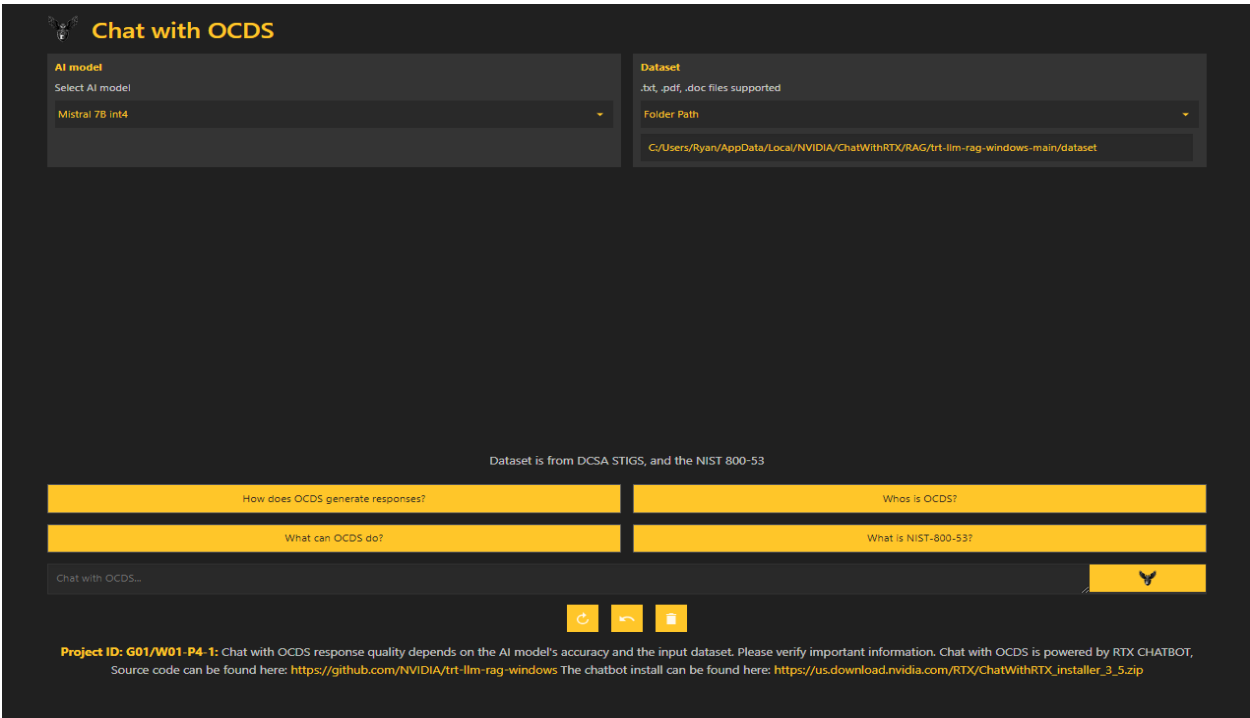
The AI model deployed is the Mistral 7B int4. There are several built in example questions to help guide clients in the use of the OCDS AI Security Chatbot.

The OCDS Security Chatbot dataset is based on DCSA STIGs, OCDS business files, NIST 800-53 version 5 (NIST.SP.800-53r5.pdf), support file input for dataset is .TXT, .PDF, and .DOC/.DOCX. The dataset is local to where RTX is installed.

One of the useful benefits of the OCDS Security Chatbot is the guidance provided in assistance for hardening operating systems like Windows 10, Server 2022, Server 2019, Server 2016, Ubuntu 2004, REDHAT 8, and REDHAT 9.







### AI-backed Server Hardening Tool

In direct association with the OCDS AI Security Chatbot, Justin Placed designed and built an entire virtual infrastructure to support the OCDS Client Server Hardening Tool.

Just utilized VMWare Workstation Pro 16 to build a virtual infrastructure hosting multiple VMs, Domain Controller (DC1), a Windows 10 client machine (Win10Client), and Ubuntu client machines (UC1), and a management server (MS1).

Justin used PowerShell for system administration he entered different PSSessions to provide connection to Windows machines remotely. SSH was used in PowerShell to connect to Ubuntu systems.

The SCAP tool (Security Content Automation Protocol) was used to execute pre-STIG scans to establish a baseline and determine required security changes.

Specific STIGs (Security Technical Implementation Guide) are applied to obtain required hardening results. Then using the AI Security Chatbot clients can ask the appropriate questions based on the SCAP results to further harden their environments.

Post-STIG scans are performed to obtain the client security score to determine if further hardening is required.

The screenshot displays the SCAP Compliance Checker 5.8 application window. The interface is divided into several sections:

- Scan Configuration (Left Panel):**
  - 1. Choose a scan type: **UNIX SSH and Windows WMI Remote Scan**
  - 2. Select remote Windows Hosts:
    - Select method of determining hosts: **Host File**
    - Create or Select a Windows host file: **C:\Program Files\SCAP Compliance**
    - Windows Hosts: **3**
  - 3. Select remote UNIX Hosts and Credentials:
    - UNIX Hosts: **1 of 2 Enabled**
  - 4. Select Content:
    - SCAP: **3 of 40 Enabled**
  - 5. Start Scan: **Start Scan**
- Content (Main Table):**

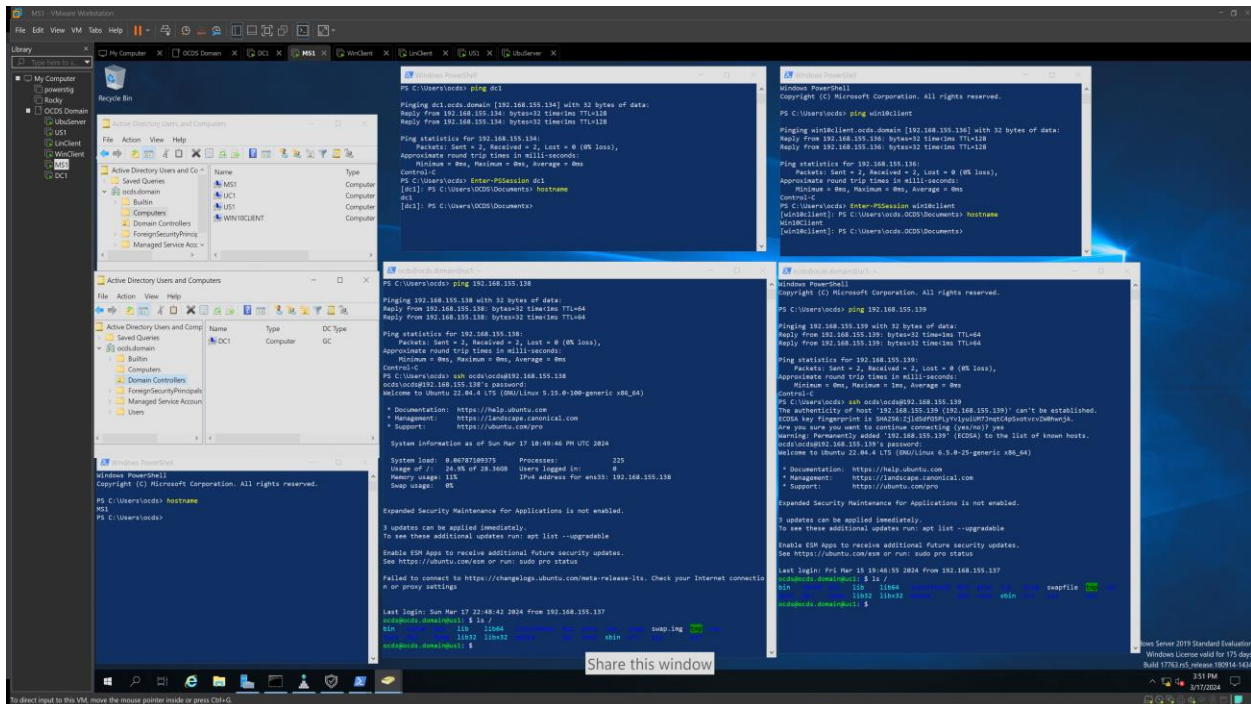
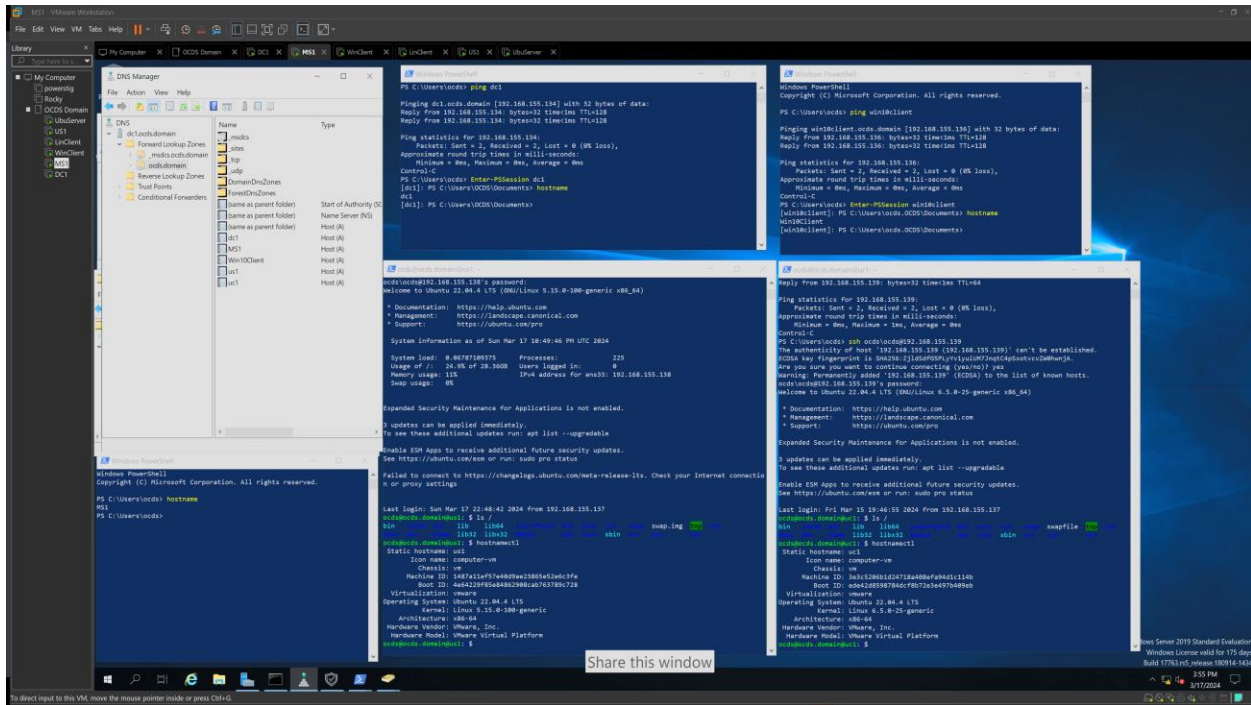
Stream	Version	Publisher	SCAP	Manual Question
<input type="checkbox"/> Linux				
<input type="checkbox"/> CAN_Ubuntu_19-04_STIG	2.9.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Canonical_Ubuntu_16-04_LTS	2.3.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> Canonical_Ubuntu_20-04_LTS_STIG	1.7.4	DISA+NIWC	1.2	yes
<input checked="" type="checkbox"/> Canonical_Ubuntu_22-04_LTS_STIG	001.009	DISA	1.2	no
<input type="checkbox"/> MOZ_Firefox_Linux	6.3.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> Oracle_Linux_7_STIG	2.12.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Oracle_Linux_8_STIG	1.6.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> RHEL_6_STIG	2.2.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> RHEL_7_STIG	3.12.5	DISA+NIWC	1.3	yes
<input type="checkbox"/> RHEL_8_STIG	1.10.5	DISA+NIWC	1.3	yes
<input type="checkbox"/> SLES_12_STIG	2.10.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> SLES_15_STIG	1.4.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> MacOS				
<input type="checkbox"/> macOS_11_0	6.1		1.3	no
<input type="checkbox"/> macOS_12_0	3.1		1.3	no
<input type="checkbox"/> macOS_13_0	1.1		1.3	no
<input type="checkbox"/> Solaris				
<input type="checkbox"/> Solaris_10_SPARC_STIG	2.4.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> Solaris_10_x86_STIG	2.4.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> Solaris_11_SPARC_STIG	2.4.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Solaris_11_x86_STIG	2.4.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> Windows				
<input type="checkbox"/> Adobe_Acrobat_Reader_DC_Continuous_Track_STIG	2.2.3	DISA+NIWC	1.3	yes
<input type="checkbox"/> Google_Chrome_Current_Windows	2.8.3	DISA+NIWC	1.2	yes
<input type="checkbox"/> IE_11_STIG	2.5.4	DISA+NIWC	1.2	yes
<input type="checkbox"/> MS_16.0_Scanner_STIG	2.6.5	NIWC	1.3	yes
- Log (Bottom Panel):**

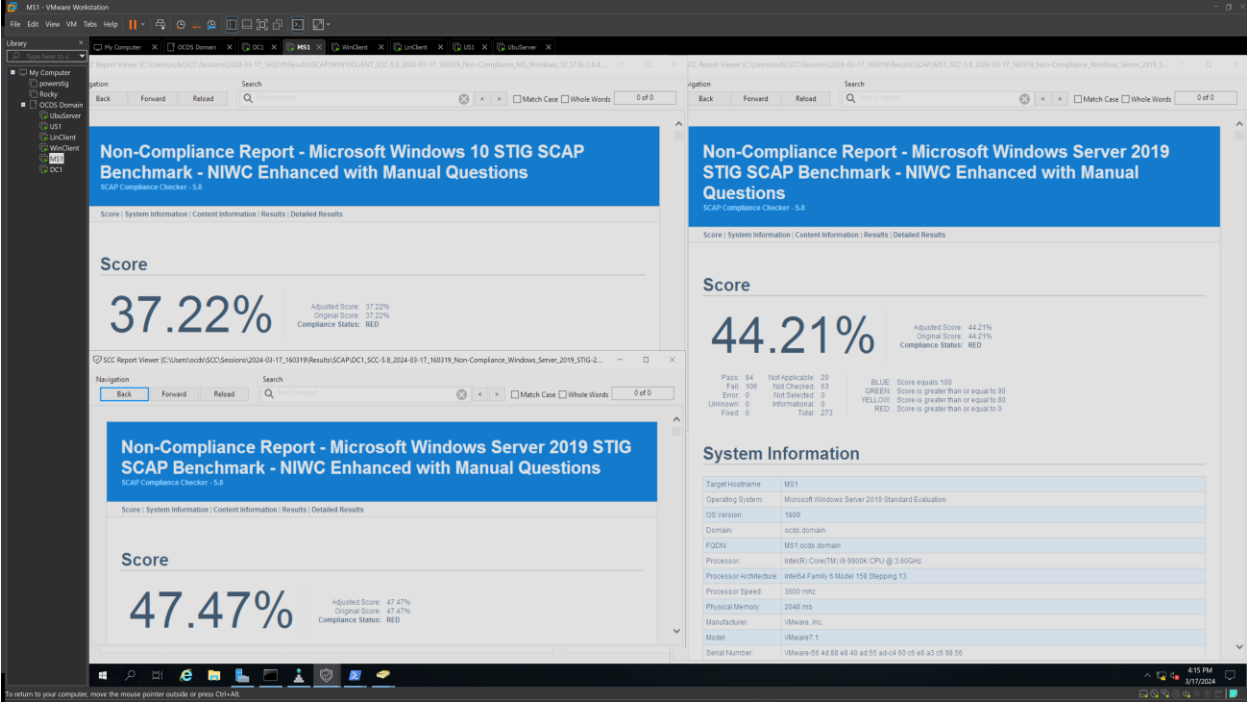
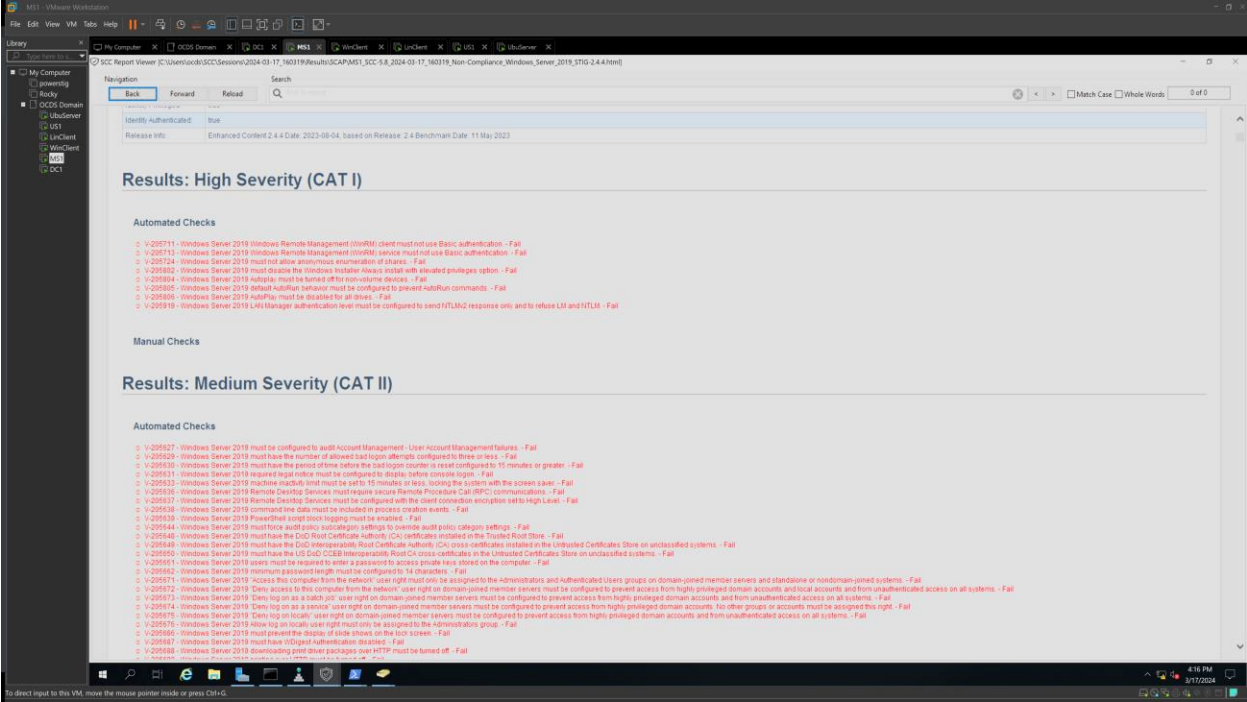
```

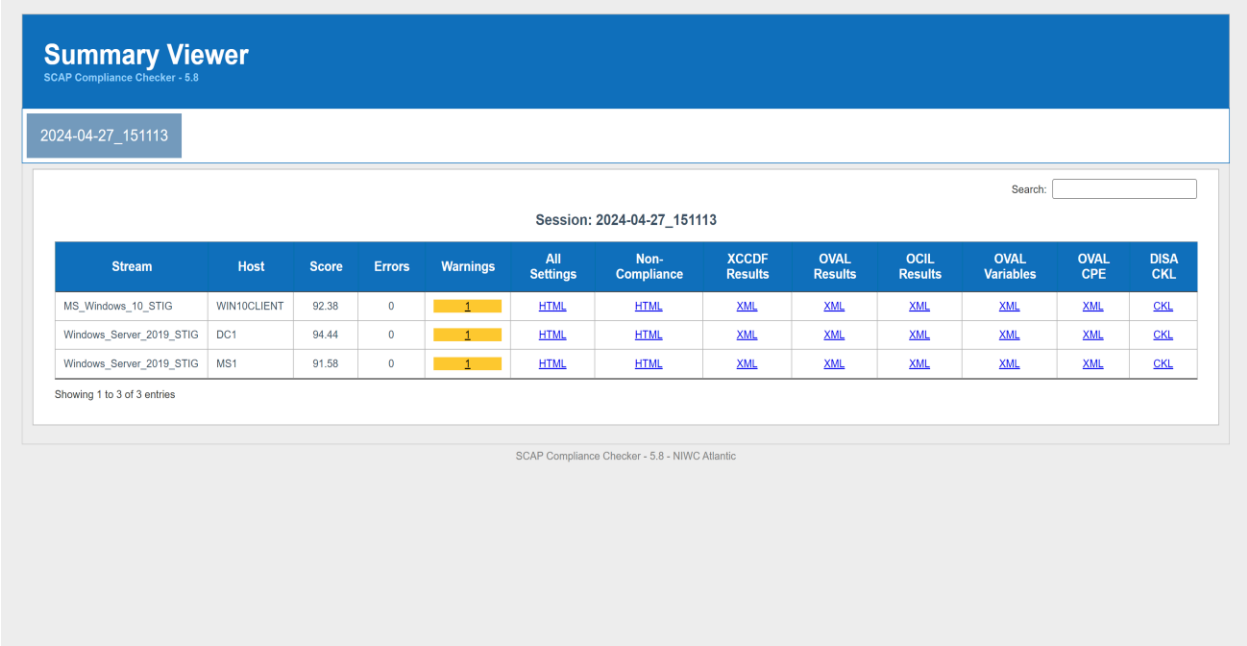
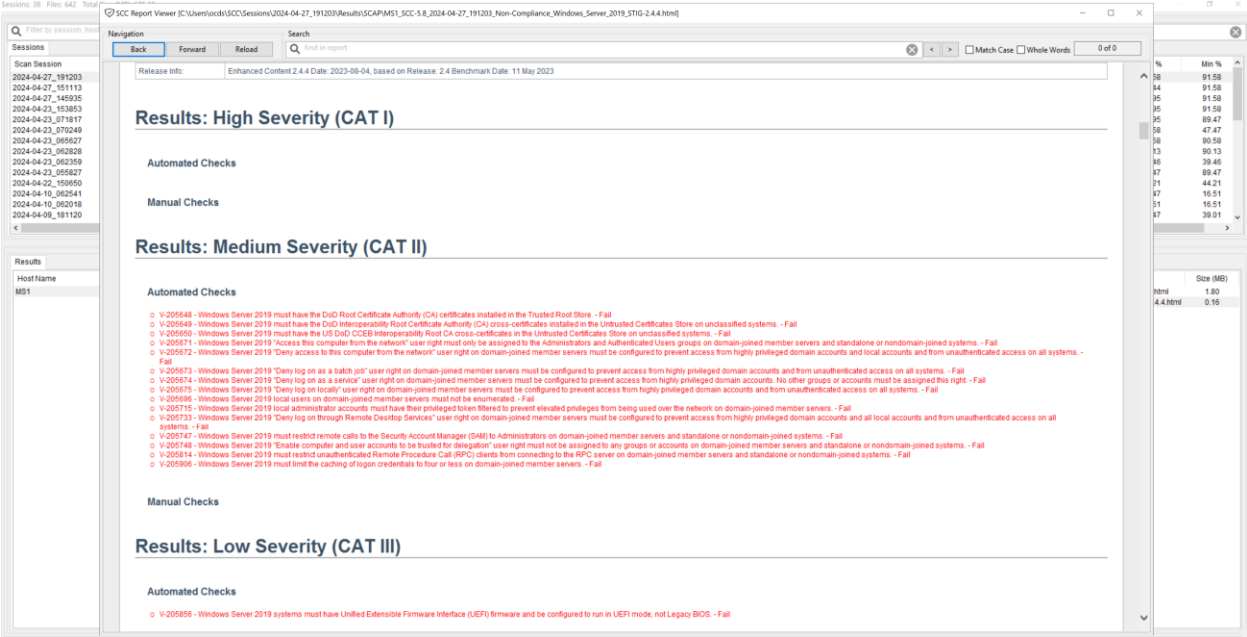
17:54:50: Checking 41 SCAP 1.2 content streams from: C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\SCAP12_Content\
17:54:51: Checking 0 OVAL content files from C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\OVAL_Content\
17:54:51: Checking 0 OCIL content files from C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\OCIL_Content\
17:54:51: Content verification complete.
17:55:01: Starting installation of C:\Users\jccds\Desktop\U_CAN_Ubuntu_22-04_LTS_V1R9_STIG_SCAP_1-2_Benchmark (1)\U_CAN_Ubuntu_22-04_LTS_V1R9_STIG_SCAP_1-2_Benchmark.xml
17:55:01: Validating U_CAN_Ubuntu_22-04_LTS_V1R9_STIG_SCAP_1-2_Benchmark.xml...
17:55:01: XML schema validation successful for U_CAN_Ubuntu_22-04_LTS_V1R9_STIG_SCAP_1-2_Benchmark.xml
17:55:01: Successfully installed: Canonical_Ubuntu_22-04_LTS_STIG

17:55:03: Checking for new/modified content, please wait...
17:55:03: Checking 0 SCAP 1.0/1.1 content streams from: C:\Program Files\SCAP Compliance Checker 5.8\Resources\Content\SCAP_Content\

```







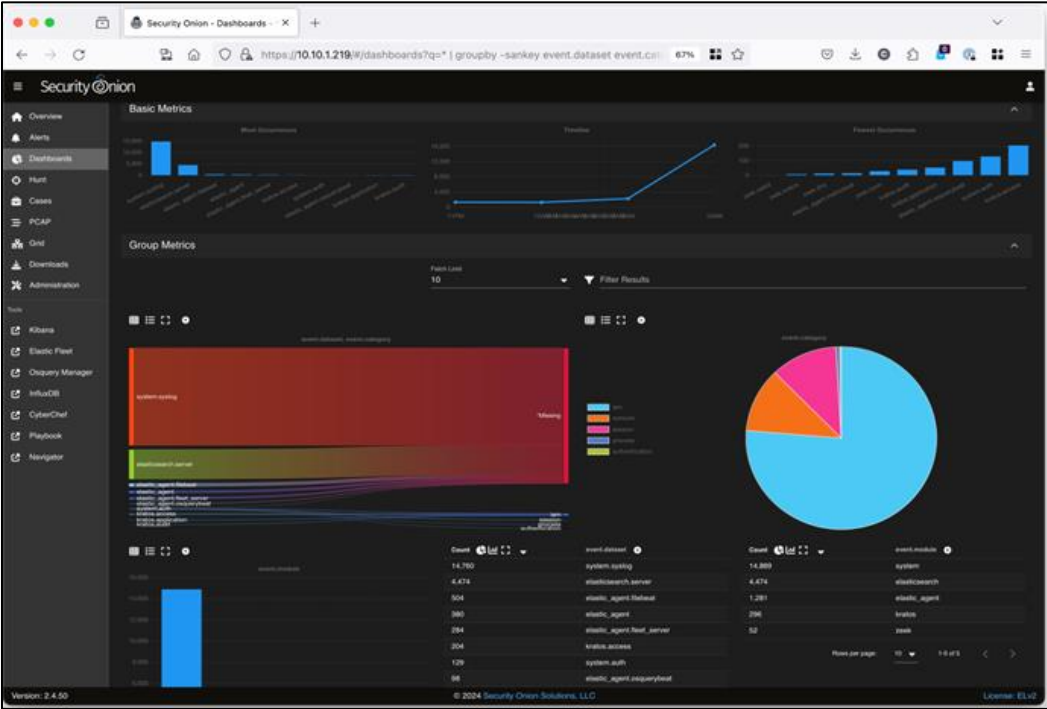
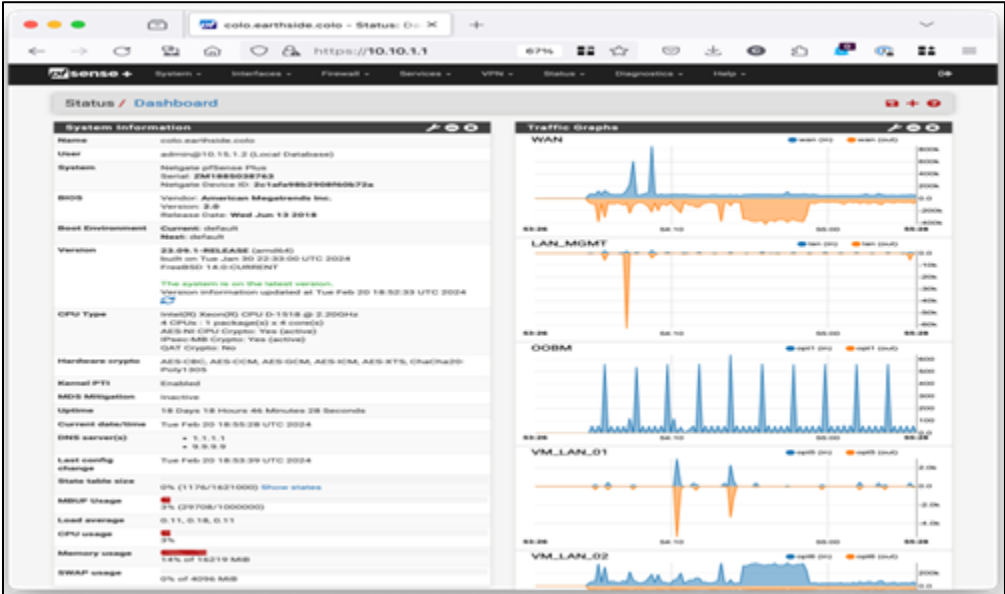
### SIEM Log Analyzer Tool

Chris Dunbar configured the OCDS SIEM (Security Incident and Event Management) Log Analyzer Tool. The OCDS SIM of choice is the Security Onion.

Chris utilized the VMware infrastructure running on VMware ESXi to configure a Security Onion VM and open source SEIM network & security monitoring tool for the OCDS SIEM client offering. He had to

configure a SPAN port in the data center. As mentioned, this is self-hosted on VMWare ESXi virtual infrastructure.

The OCDS SIEM Tool assists clients to continuously monitor/management their network and increase their cybersecurity protection posture.



## Project Planning and Management Summary

Project planning and project management play a key role in the success of a project. Planning for and adhering to good, sound project management practices is essential.

### Overview

OCDS used Jira Project Management to plan, schedule, track, and complete our project. All our team members were assigned a Jira user login/account. We were able to use all needed features included in the free version as our Agile team was made up of five members which is less than the required 10 or less users to use the free version. As Jira is a 100% SaaS product all team members were able to access the Project online at any time and collaborate in a real-world and in real-time scenario.

### Scheduling

The Project Manager scheduled multiple Epics within each Sprint to accomplish the tasks designed to meet the goals and objectives. Each Epic and Task has a Start and End date which coincides with its placement within the graphical Timeline view which is the Gantt chart. Each Epic and Task also has a Time Tracking section where the reporter of the Epic or Task, usually the Project Manager, can record an initial estimate of the time needed to complete the task. The assignee team member can use the same Time Tracking section to record their work on the Task through the project to completion as well as indicate the status of the task. The Timeline view (Gantt Chart view) will assist the Project Manager in scheduling the Epics and Tasks within the Project to schedule each Task accordingly and establish any required dependencies.

### Task Distribution

Each Epic and Task has an assignee. The Project Manager was able to establish the Epics and Tasks in an appropriate flow using the Timeline/Gantt view. With the Epics and Task aligned the Project Manager was able to distribute the Tasks according to the appropriate Assignee which support the proper distribution of work. Jira support color coding the Epics and Tasks. We chose to color code each Epic and Task according to the Assignee which made for ease of Epic and Task assignee identification.

### Progress Monitoring

Each Assignee logged the hours worked on each Task and marked the appropriate Task Status (Backlog, In Progress, and Done) as work progressed on the Task. This enabled the Project Manager to track and monitor the progress of each Task and the overall Project. As each task moved from Backlog to In Progress to Done Jira provides a Dashboard view to display the project in Board view. Tasks can be dragged from one bucket to another via the Board view if so desired.

### Project Management Practices

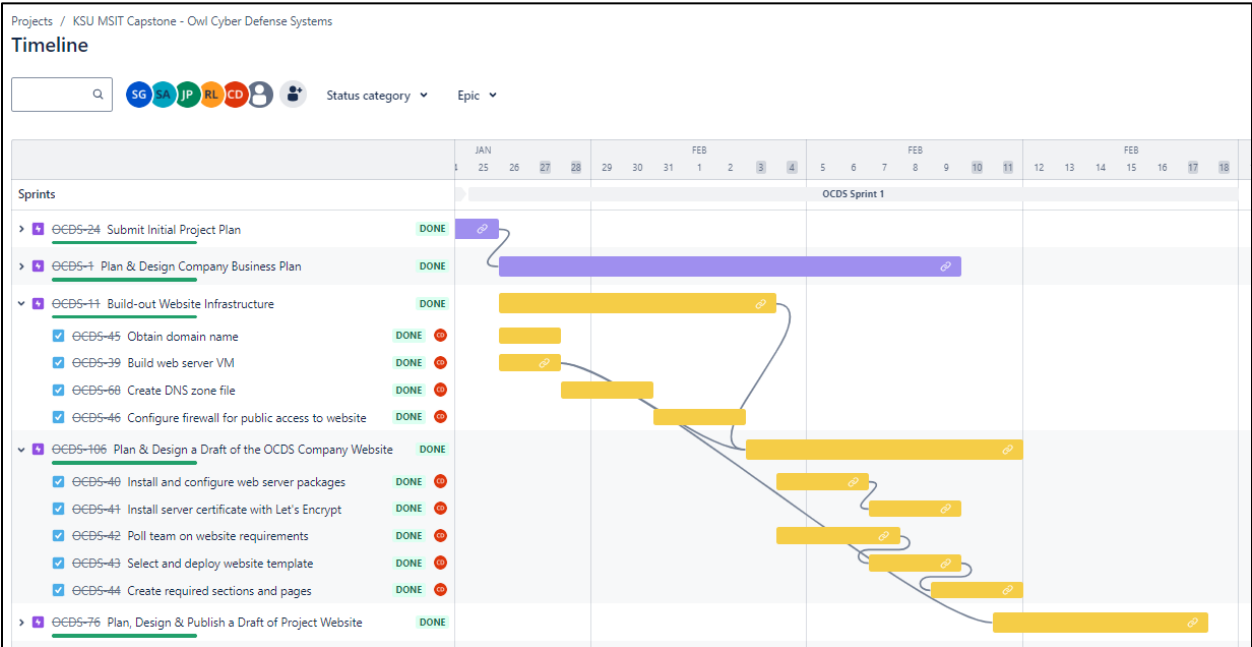
We followed project management best practices by getting together as early as we could to assemble a qualified team and we established the appropriate Project Scope. In early planning meetings as well as carrying out through the lifecycle of the project we planned and managed our resources accordingly. Led by the Project Manager we tracked and reported our progress as we worked on and completed each task along the way. We skillfully set clear objectives and milestones to be cornerstones of the project. We met regularly and communicated often (sometimes every day) through the entire life of the project. If a risk arose, we took action to manage it quickly and adjust where needed.

Adhering to SDLC (Software Development Life Cycle) best practices we devised a combination of the traditional Waterfall model and the Agile Scrum methodology. Our project consisted of four sprints with the first sprint being Sprint 0 where we proposed the project idea to obtain acceptance from our sponsor. The project work took place in three sprints. Each sprint coincided with the timeline established for due dates for each Milestone culminated in a completed project with appropriate deliverables.

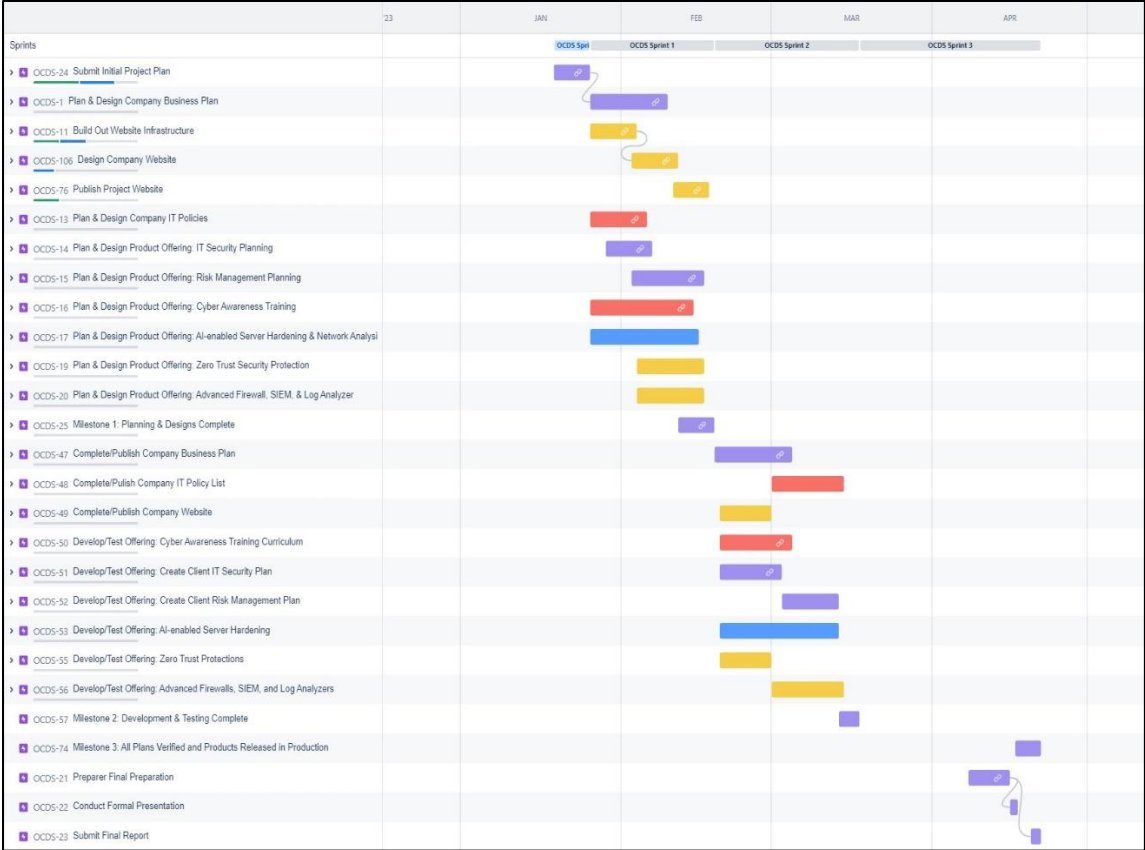
The screenshot shows a Jira issue titled "Build-out Website Infrastructure" with a status of "Done". The issue is assigned to Chris Dunbar and reported by Scott Gilstrap. It includes a list of child issues, all of which are marked as "DONE":

- GCDS-45 Obtain domain name
- GCDS-39 Build web server VM
- GCDS-68 Create DNS zone file
- GCDS-46 Configure firewall for public access to ...

There is also one linked issue: GCDS-196 Plan & Design a Draft of the O... (DONE). The activity section shows a comment from Scott Gilstrap (SG) with a "Pro tip: press M to comment" note.







Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

### OCDS Sprint 3

Complete Milestone 3. Department Presentation. Final Project report. All OCDS client offerings in production.

SEARCH [ ] | SG CD SA RL JP | Epic ▾

BACKLOG

TO DO 8

- Create Products catalog on website  
05 MAR | OCDS-182 | 5h | CD
- Troubleshooting virtual infrastructure  
RELEASE OCDS SERVER HARDENING TOO...  
06 APR | OCDS-241 | 3h | JP
- troubleshoot script bsod windows 10  
RELEASE OCDS SERVER HARDENING TOO...  
20 APR | OCDS-245 | 3h | JP
- Preparer Final Presentation  
PROJECT CONCLUSION | 21 APR | OCDS-254 | 1d 2h | SG
- Upload Milestone-3 Documents  
PROJECT CONCLUSION | 21 APR | OCDS-250 | 15m | SG

IN PROGRESS 19

- Complete configuration of Home Page  
RELEASE OCDS COMPANY WEBSITE INTO...  
29 MAR | OCDS-197 | 3h | CD
- Complete configuration of the About Page  
RELEASE OCDS COMPANY WEBSITE INTO...  
30 MAR | OCDS-198 | 3h | CD
- Complete configuration of the Overall Client Offering Catalogue Page  
RELEASE OCDS COMPANY WEBSITE INTO...  
02 APR | OCDS-199 | 3h | CD
- Client Offering Config - Information Security Plan  
RELEASE OCDS COMPANY WEBSITE INTO...  
05 APR | OCDS-200 | 3h | CD

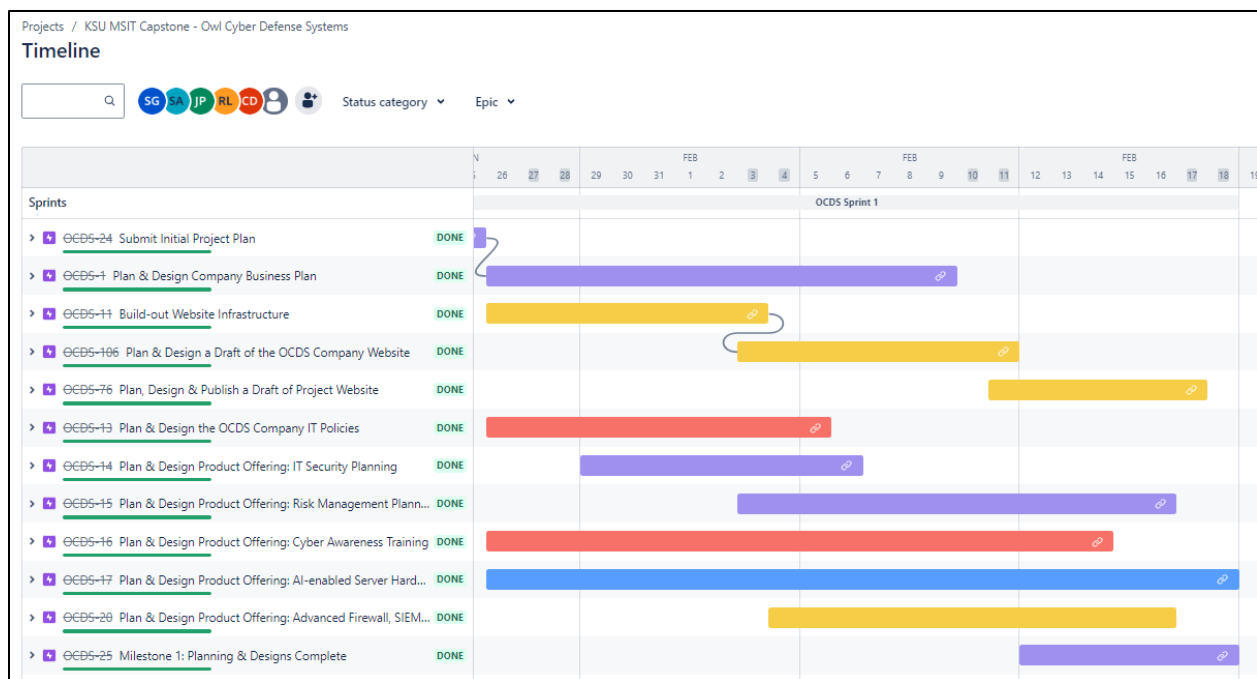
DONE 26 ✓

- Finalize site layout  
RELEASE PROJECT WEBSITE INTO PRODU...  
28 MAR | @EBS-493 | 3h | CD
- Work with each team members to upload appropriate content  
RELEASE PROJECT WEBSITE INTO PRODU...  
14 APR | @EBS-494 | 3h | CD
- Finalize site navigation  
RELEASE PROJECT WEBSITE INTO PRODU...  
03 APR | @EBS-495 | 3h | CD
- Publish near-final draft to production  
RELEASE PROJECT WEBSITE INTO PRODU...  
14 APR | @EBS-496 | 3h | CD
- Company Policies -  
RELEASE OCDS COMPANY POLICIES INTO...  
27 MAR

## Project Process/Milestones

The project progress was tracked via stages/milestones. Using the Agile Scrum methodology, we established Sprints in sync with the four-week timeline and due dates of each Milestone. Each Sprint was loaded with appropriate Epics to accomplish in support of each objective/goal along the way. We worked in an iterative fashion to produce working models of our Epic during each Sprint. Using the traditional SDLC Waterfall concept we worked to Plan & Design our deliverables in Sprint 1. In Sprint 2 we flowed into the next stage of Developing and Testing our deliverables. The work in Sprint 3 consisting of the Go Live stage where we rolled our deliverables into our production environment.

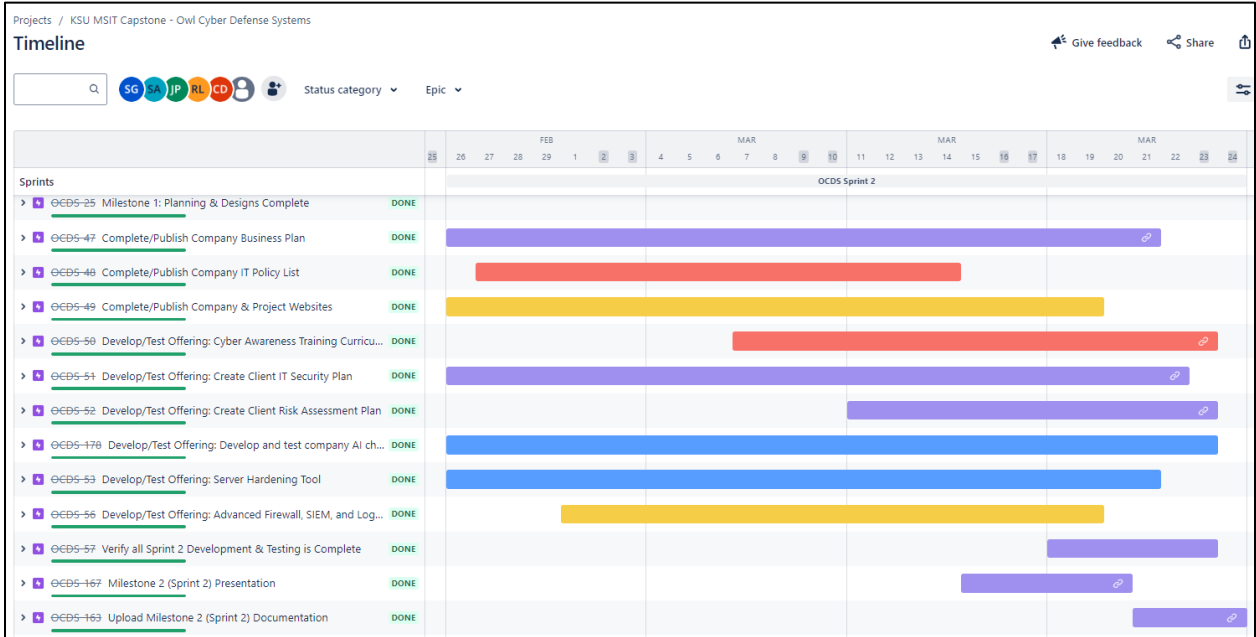
**In Sprint 1, Jan 25 to Feb 18, 2024, we planned and designed each deliverable culminating in the presentation of Milestone 1 to our Sponsor on Wed Feb 21, 2024.**



### Sprint 1 Epics / Objectives: Jan 25 - Feb 18, 2024

- Plan & Design Company Business Plan: Jan 26 - Feb 9
- Buildout Website Infrastructure: Jan 26 - Feb 3
- Plan & Design a Draft of the OCDS Company Website: Feb 3 - 11
- Plan & Design the OCDS Company IT Policies: Jan 26 - Feb 5
- Plan & Design Product Offering - IT Security Planning: Jan 29 - Feb 6
- Plan & Design Product Offering - Risk Management Planning: Feb 3 - 16
- Plan & Design Product Offering - Cyber Awareness Training: Jan 26 - Feb 14
- Plan & Design Product Offering - AI-enabled Server Hardening Tool: Jan 26 - Feb 18
- Plan & Design Product Offering - Advance Firewall SIEM Tool: Feb 4 - 16

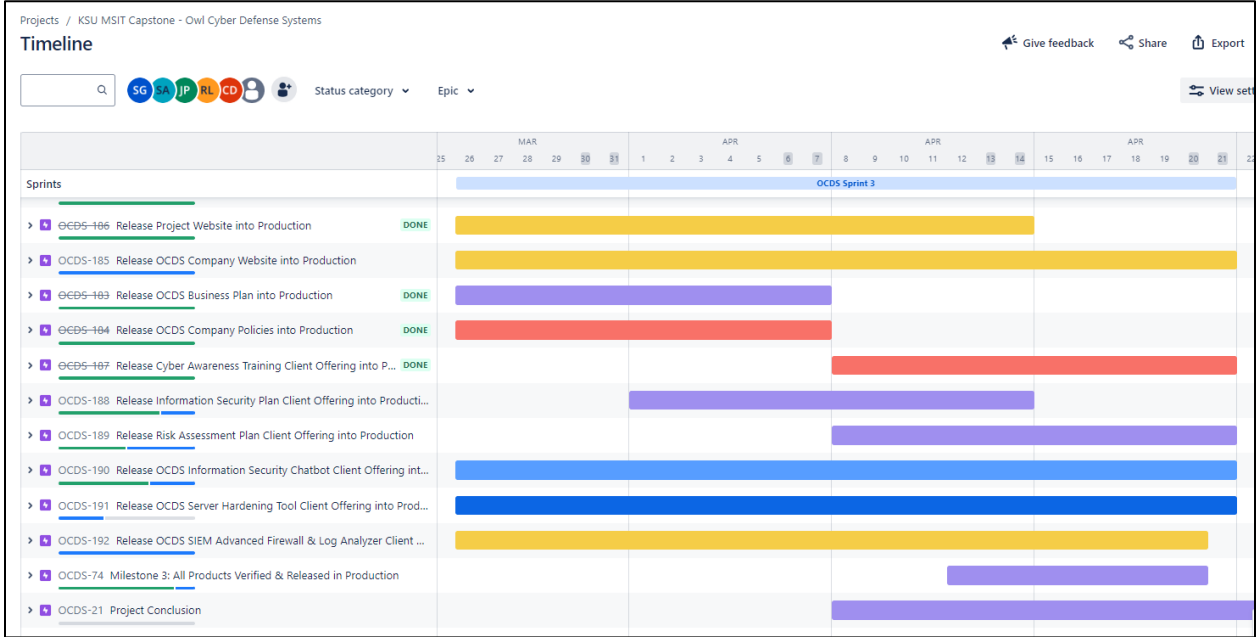
In Sprint 2, Feb 26 to Mar 24, 2024, we developed and tested each deliverable culminating in the presentation of Milestone 2 to our Sponsor on Wed Mar 20, 2024.



**Sprint 2 Epics / Objectives: Feb 26 - Mar 24, 2024**

- Complete/Publish the OCDS Company Business Plan: Feb 26 - Mar 21
- Complete/Publish OCDS Company IT Policies: Feb 27 - Mar 14
- Complete/Publish Company and Project Websites: Feb 26 - Mar 19
- Develop & Test Product Offering - Cyber Awareness Training: Mar 7 - 23
- Develop & Test Product Offering - IT Security Planning: Feb 26 - Mar 22
- Develop & Test Product Offering - Risk Management Planning: Mar 11 - 23
- Develop & Test Product Offering – OCDS AI Security Chatbot: Feb 26 - Mar 23
- Develop & Test Product Offering - AI-enabled Server Hardening Tool: Feb 26 - Mar 21
- Develop & Test Product Offering - Advance Firewall SIEM Tool: Mar 1 – 19

In Sprint 3, Mar 26 to Apr 21, 2024, we went through a Go Live scenario where we moved each of our deliverables into production culminating in the presentation of Milestone 3 to our Sponsor on Tue Apr 23, 2024.



**Sprint 3 Epics / Objectives: Mar 26 - Apr 21, 2024**

- Release Project Website into Production: Mar 26 - Apr 14
- Release Company Website into Production: Mar 26 - Apr 21
- Release the OCDS Company Business Plan: Mar 26 - Apr 7
- Release OCDS Company IT Policies: Mar 26 - Apr 7
- Release Product Offering - Cyber Awareness Training: Apr 8 - 21
- Release Product Offering - IT Security Planning: Apr 1 - 14
- Release Product Offering - Risk Management Planning: Apr 8 - 21
- Release Product Offering - OCDS AI Security Chatbot: Mar 26 - Apr 21
- Release Product Offering - AI-enabled Server Hardening Tool: Mar 26 - Apr 21
- Release Product Offering - Advance Firewall SIEM Tool: Mar 26 - Apr 20

**Workload Summary**

Jira Project Management was a great tool for tracking person-hour totals and sub-totals along each project phase/milestone. Each project deliverable is recorded as an Epic within each Sprint. Each Epic has multiple tasks to complete to complete the Epic. Jira Epics and Tasks provide a mechanism to track the work performed by the assignee. This workload is trackable via an automated person-hour tracking tool in Jira. The data is exportable to Excel. Excel was used to created Pivot tables to record tracking of person-hour workload and ensure equal distribution across the life cycle of the project.

The Jira Timeline view was used to track and record the Tasks for each Epic and provide person-hour tracking with ease along with the Status of each Task.

In the event the automated Jira Person-hour tracking chart showed a team member having to spend too much time along the way in a Sprint the Project Manager can adjust that workload by adjusting the task assigned with the Sprint.

**Person-hours (Jira)**  
Project: KSU MSIT Capstone - Owl Cyber Defense Systems  
Sorted by: Sprint ascending, then Created descending  
1-130 of 130 as at: 28/Jan/24 7:59 PM

T	Sprint	Summary	Assignee	Status	Due	Original estimate	Time Spent
<input checked="" type="checkbox"/>	OCDS Sprint 0	Geneerate Team Logo	Chris Dunbar	DONE	23/Jan/24	2 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 0	Upload Project Plan Document	Scott Gilstrap	TO DO	25/Jan/24	15 minutes	
<input checked="" type="checkbox"/>	OCDS Sprint 0	Get Plan Document Approved by Project Sponsor	Scott Gilstrap	TO DO	23/Jan/24	1 hour	30 minutes
<input checked="" type="checkbox"/>	OCDS Sprint 0	Get Plan Document Approved by Team Members	Scott Gilstrap	DONE	23/Jan/24	30 minutes	1 hour, 30 minutes
<input checked="" type="checkbox"/>	OCDS Sprint 0	Create Plan Document	Scott Gilstrap	DONE	23/Jan/24	3 hours	5 hours
<input checked="" type="checkbox"/>	OCDS Sprint 0	Create Dependencies	Scott Gilstrap	IN PROGRESS	24/Jan/24	1 hour	4 hours
<input checked="" type="checkbox"/>	OCDS Sprint 0	Create Tasks	Scott Gilstrap	IN PROGRESS	24/Jan/24	5 hours	4 hours
<input checked="" type="checkbox"/>	OCDS Sprint 0	Create Epics	Scott Gilstrap	IN PROGRESS	23/Jan/24	3 hours	6 hours
<input checked="" type="checkbox"/>	OCDS Sprint 0	Interview team members	Scott Gilstrap	DONE	22/Jan/24	30 minutes	1 hour, 30 minutes
<input checked="" type="checkbox"/>	OCDS Sprint 1	Verify Infrastructure Build Out	Chris Dunbar	TO DO	13/Feb/24	30 minutes	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Plan/Design AI Training	Unassigned	TO DO	15/Feb/24	5 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Plan/Design Dataset Configuration	Unassigned	TO DO	10/Feb/24	5 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research NIST 800-53 Family Standards	Unassigned	TO DO	02/Feb/24	4 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Design OCDS IT Risk Mgmt Product Offering	Scott Gilstrap	TO DO	15/Feb/24	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Conduct OCDS Planning Based on Reseach	Scott Gilstrap	TO DO	10/Feb/24	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research IT Risk Management Planning	Scott Gilstrap	TO DO	07/Feb/24	5 hours	

**Sprint 1 (Milestone 1) Time Tracking**

Person-hours Edited Save Details ★ 📄 📄 🔗 Share 📄 Export

KSU MSIT Capstone - Owl Cyb... Type: All Status: All Assignee: All + More Contains text Search Switch to JQL

Sprint: OCDS Sprint 1

1-50 of 54

T	Sprint	Summary	Assignee	Status	Due	Original estimate	Time Spent	Updated
<input checked="" type="checkbox"/>	OCDS Sprint 1	Obtain domain name	Chris Dunbar	DONE	27/Jan/24	1 hour	1 hour	28/Jan/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Build web server VM	Chris Dunbar	DONE	27/Jan/24	3 hours	3 hours	05/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Company Mission & Vision	Scott Gilstrap	DONE	27/Jan/24	1 hour	2 hours	08/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Plan/Design Layout on Website	Chris Dunbar	TO DO	29/Jan/24	3 hours	1 hour, 30 minutes	13/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research/Create list of IT Policies	Stephanie Aguirre	DONE	29/Jan/24	5 hours	3 hours, 9 minutes	29/Jan/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Business Strategy	Scott Gilstrap	DONE	29/Jan/24	1 hour	1 hour	08/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Plan/Design Webpage	Chris Dunbar	TO DO	30/Jan/24	3 hours	1 hour, 30 minutes	13/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Create DNS zone file	Chris Dunbar	DONE	30/Jan/24	2 hours	1 hour	05/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	IT Strategy	Scott Gilstrap	DONE	31/Jan/24	1 hour	1 hour, 30 minutes	08/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research IT Security Plan Methodologies	Scott Gilstrap	DONE	01/Feb/24	3 hours	3 hours	19/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research/Create Cybersecurity Policies	Stephanie Aguirre	DONE	01/Feb/24	5 hours	3 hours	31/Jan/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Create employee education related to cybersecurity (i.e. cybersecurity resources)	Stephanie Aguirre	DONE	02/Feb/24	5 hours	3 hours, 25 minutes	06/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Create legal structure for business	Stephanie Aguirre	DONE	02/Feb/24	2 hours	2 hours, 30 minutes	13/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Configure firewall for public access to website	Chris Dunbar	DONE	02/Feb/24	45 minutes	15 minutes	05/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Designate List of Appropriate IT Policies	Stephanie Aguirre	DONE	02/Feb/24	2 hours	1 hour, 31 minutes	29/Jan/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Business Goals	Scott Gilstrap	DONE	02/Feb/24	1 hour	1 hour, 30 minutes	08/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	Research AI Toolset	Justin Place	IN PROGRESS	03/Feb/24	7 hours	7 hours, 2 minutes	12/Feb/24
<input checked="" type="checkbox"/>	OCDS Sprint 1	IT SP Planning Based on Research	Scott Gilstrap	DONE	03/Feb/24	2 hours	2 hours	19/Feb/24

Sprint OCDS Sprint 1

Week of (Multiple Items)

Sum of Time Spent Calc Column Labels

Row Labels	Chris Dunbar	Justin Place	Ryan LeBlanc	Scott Gilstrap	Stephanie Aguirre	Grand Total
Build web server VM	3.0					3.0
Build-out Website Infrastructure	5.0					5.0
Business Goals				1.5		1.5
Business Strategy				1.0		1.0
Company Mission & Vision				2.0		2.0
Complete Design of Cybersecurity Awareness Training					3.0	3.0
Complete Development of Curriculum					3.0	3.0
Complete IT Policy List					3.6	3.6
Complete Milestone 1 Report Documentation				5.0		5.0
Conduct OCDS Planning Based on Reseach				2.5		2.5
Configure firewall for public access to website	0.3					0.3
Create DNS zone file	1.0					1.0
Verify Initial Policy List is Complete					2.0	2.0
Verify Planning & Design of all Client Offerings are Complete				1.0		1.0
Implement AI Toolset		5.0				5.0
Plan & Design Dataset Accuracy Improvement			4.0			4.0
Implement Dataset Accuracy Improvement		5.0				5.0
Implement AI Training			8.0			8.0
Publish site contents/folders	3.0					3.0
Publish draft site/go live	3.6					3.6
<b>Grand Total</b>	<b>41.1</b>	<b>40.7</b>	<b>41.4</b>	<b>41.5</b>	<b>41.0</b>	<b>205.7</b>

**Sprint 2 (Milestone 2) Time Tracking**

Person-hours Edited Save Details

KSU MSIT Capstone - Owl Cyb... Type: All Status: All Assignee: All + More Contains text Search Switch to JQL

Sprint: OCDS Sprint 2

1-50 of 64

Sprint	Summary	Assignee	Status	Due	Original estimate	Time Spent	Updated
OCDS Sprint 2	Upload all documentation to D2L	Scott Gilstrap	IN PROGRESS	24/Mar/24	1 hour		24/Mar/24
OCDS Sprint 2	Verify all documentation for upload	Scott Gilstrap	DONE	23/Mar/24	3 hours	2 hours	24/Mar/24
OCDS Sprint 2	Test Client Risk Mngmnt Form Process	Scott Gilstrap	DONE	23/Mar/24	2 hours	2 hours	24/Mar/24
OCDS Sprint 2	Test Each Training Module	Stephanie Aguirre	DONE	23/Mar/24	5 hours	5 hours	24/Mar/24
OCDS Sprint 2	Implement Ubuntu dataset	Ryan LeBlanc	DONE	22/Mar/24	2 hours	2 hours	24/Mar/24
OCDS Sprint 2	Test IT Security Plan Form Process	Scott Gilstrap	DONE	22/Mar/24	3 hours	3 hours	24/Mar/24
OCDS Sprint 2	Coordinate with Chris to incorporate form on website	Scott Gilstrap	DONE	21/Mar/24	3 hours	3 hours	24/Mar/24
OCDS Sprint 2	Coordinate w Chris to incorporate form on website	Scott Gilstrap	DONE	21/Mar/24	5 hours	5 hours	24/Mar/24
OCDS Sprint 2	implement RHEL8 dataset	Ryan LeBlanc	DONE	21/Mar/24	5 hours	2 hours	24/Mar/24
OCDS Sprint 2	Make Milestone 2 Presentation to Sponsor/instructor	Scott Gilstrap	DONE	20/Mar/24	1 hour	1 hour	24/Mar/24
OCDS Sprint 2	Create Training Content Based on Curriculum	Stephanie Aguirre	DONE	20/Mar/24	1 day, 7 hours	2 hours, 35 minutes	13/Mar/24
OCDS Sprint 2	Implement Server 2019 dataset	Ryan LeBlanc	DONE	20/Mar/24	5 hours	2 hours	24/Mar/24
OCDS Sprint 2	Prepare all documentation for Milestone 2 Presentation	Scott Gilstrap	DONE	19/Mar/24	3 hours	3 hours	24/Mar/24
OCDS Sprint 2	Create Milestone 2 PPT Presentation	Scott Gilstrap	DONE	19/Mar/24	5 hours	5 hours	24/Mar/24
OCDS Sprint 2	Confirm SEIM operation and collect initial data	Chris Dunbar	DONE	19/Mar/24	5 hours	5 hours	24/Mar/24
OCDS Sprint 2	Publish/Upload Company Business Plan	Scott Gilstrap	DONE	19/Mar/24	15 minutes	15 minutes	24/Mar/24
OCDS Sprint 2	Create VMs to demo system hardening	Justin Place	DONE	18/Mar/24	5 hours	4 hours, 30 minutes	19/Mar/24
OCDS Sprint 2	Begin updating placeholder text with real content	Chris Dunbar	DONE	18/Mar/24	5 hours		17/Mar/24
OCDS Sprint 2	Coordinate w Chris to incorporate links on website	Stephanie Aguirre	DONE	18/Mar/24	5 hours	5 hours	24/Mar/24

Sprint	OCDS Sprint 2					
Week of	(All)					
Sum of Time Spent Calc	Column Labels					
Row Labels	Chris Dunbar Justin Place Ryan LeBlanc Scott Gilstrap Stephanie Aguirre Grand Total					
Begin updating placeholder text with real content	2.2					2.2
Complete Business Goals				2.5		2.5
Complete Business Model				3.5		3.5
Complete Business Strategy				2.5		2.5
Complete Company Mission Statement				2.0		2.0
Complete Company Vision Statement				2.5		2.5
Complete Development of Curriculum					3.0	3.0
Complete IT Goals				2.0		2.0
Complete IT Policy List					3.0	3.0
Complete IT Strategy				2.0		2.0
Complete Product Offering Catalogue				2.0		2.0
Test hardening content tool		3.3				3.3
Test IT Security Plan Form Process				1.1		1.1
Upload all documentation to D2L				0.0		0.0
Verify all documentation for upload				1.3		1.3
Write Bash script to check against Linux STIGs				5.0		5.0
Write PowerShell script to scan windows systems against STIG & show results				2.0		2.0
Write script for hardening content tool		4.4				4.4
<b>Grand Total</b>	<b>30.8</b>	<b>23.8</b>	<b>20.0</b>	<b>51.5</b>	<b>25.0</b>	<b>151.0</b>

**Sprint 3 (Milestone 3) Time Tracking**

Person-hours Filter details Apps Share Export issues LIST VIEW DETAIL VIEW ID ...

Search issues  Project: KSU MSIT Capstone - Owl Cyber D... Type Status Assignee Sprint: OCDS Sprint 3 More + Go back to filter Save filter BASIC JQL

Type	Sprint	Summary	Assignee	Status	Due date	Original estimate	Time
<input checked="" type="checkbox"/>	OCDS Sprint 3	Create Products catalog on website	CD Chris Dunbar	TO DO	Mar 05, 2024	5 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Review Business Plan	SG Scott Gilstrap	DONE	Mar 27, 2024	3 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Company Policies -	SA Stephanie Aguirre	DONE	Mar 27, 2024	5 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Patch chatbot.	RL Ryan LeBlanc	DONE	Mar 28, 2024	3 hours	1 hour
<input checked="" type="checkbox"/>	OCDS Sprint 3	Finalize site layout	CD Chris Dunbar	DONE	Mar 28, 2024	3 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Complete configuration of Home Page	CD Chris Dunbar	IN PROGRESS	Mar 29, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Take VM Snapshots	JP Justin Place	DONE	Mar 30, 2024	3 hours	15 minutes
<input checked="" type="checkbox"/>	OCDS Sprint 3	Make Appropriate Changes to Business Plan	SG Scott Gilstrap	DONE	Mar 30, 2024	3 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Advanced Firewall	CD Chris Dunbar	IN PROGRESS	Mar 30, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Complete configuration of the About Page	CD Chris Dunbar	IN PROGRESS	Mar 30, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Complete configuration of the Overall Client Offering Catalogue Page	CD Chris Dunbar	IN PROGRESS	Apr 02, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Coordinate w Webmaster to Incorporate Business Plan on Websites	SG Scott Gilstrap	IN PROGRESS	Apr 03, 2024	3 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Finalize site navigation	CD Chris Dunbar	DONE	Apr 03, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Verify InfoSec Questionnaire to be based on ISO 27001 and NIST Standards.	SG Scott Gilstrap	DONE	Apr 04, 2024	3 hours	5 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Add IT Policies + Cybersecurity Policies to website	SA Stephanie Aguirre	IN PROGRESS	Apr 04, 2024	5 hours	3 hours, 38 mi
<input checked="" type="checkbox"/>	OCDS Sprint 3	Client Offering Config - Information Security Plan	CD Chris Dunbar	IN PROGRESS	Apr 05, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Troubleshooting virtual infrastructure	JP Justin Place	TO DO	Apr 06, 2024	3 hours	
<input checked="" type="checkbox"/>	OCDS Sprint 3	Complete InfoSec Questionnaire	SG Scott Gilstrap	DONE	Apr 06, 2024	3 hours	2 hours
<input checked="" type="checkbox"/>	OCDS Sprint 3	Sign off on Business Plan in Production	SG Scott Gilstrap	IN PROGRESS	Apr 06, 2024	3 hours	1 hour
<input checked="" type="checkbox"/>	OCDS Sprint 3	SIEM	CD Chris Dunbar	IN PROGRESS	Apr 06, 2024	3 hours	

Sprint	OCDS Sprint 3					
Issue Type	Task					
Week of	(All)					
Updated	(All)					
<b>Sum of Time Spent Calc</b>						
Tasks	TeamMember					
	Chris Dunbar Justin Place Ryan LeBlanc Scott Gilstrap Stephanie Aguirre Grand Total					
Create Products catalog on website	0.0					0.0
Review Business Plan				2.0		2.0
Company Policies -					2.0	2.0
Patch chatbot.			1.0			1.0
Finalize site layout	2.0					2.0
Complete configuration of Home Page	0.0					0.0
Take VM Snapshots		0.3				0.3
Make Appropriate Changes to Business Plan				2.0		2.0
Advanced Firewall	0.0					0.0
Complete configuration of the About Page	0.0					0.0
Complete configuration of the Overall Client Offering Catalogue Page	1.0					1.0
<hr/>						
Client Offering Config - SIEM Adv F/W & Log Analyzer Tool	3.0					3.0
Preparer Final Presentation				0.0		0.0
Upload Milestone-3 Documents				0.0		0.0
Department Presentation				0.0		0.0
Deliver Project Deliverable Pkg to Owner				0.0		0.0
Final Project Report				0.0		0.0
<b>Grand Total</b>	<b>22.8</b>	<b>6.3</b>	<b>9.3</b>	<b>36.0</b>	<b>17.0</b>	<b>91.3</b>



## Team Member Roles and Contributions

### Scott Gilstrap

Real world: Global IT Service Delivery Manager at Wolters Kluwer, [Randolph Scott Gilstrap | LinkedIn](#)

Project: Project Manager | Team Lead | Scrum Master

In addition to designing and managing the Project Plan within Jira and performing as Project Manager/Scrum Master Scott planned, designed, developed, tested, and released the following deliverables into production.

- Detailed Business Plan
- IT Security Planning Questionnaire mechanism
- Proprietary client Risk Management program

### Stephanie Aguirre

Real world: Case Manager at Roden Law, [Stephanie Aguirre | LinkedIn](#)

Project: Technical Writer and Lead Instructor

Working an average of 27.9 hours per sprint Stephanie successfully managed all her assigned tasks within Jira, and she planned, designed, developed, tested, and released the following deliverables into production.

- OCDS Legal considerations and formation
- Company IT Policies for incorporation into the Business Plan
- Cyber Awareness Training to include all shared and client proprietary modules

### Chris Dunbar

Real world: Senior Systems Engineer at Apple, Inc., [Chris Dunbar | LinkedIn](#)

Project: Systems Administrator and Webmaster

Working an average of 31.6 hours per sprint Chris successfully managed all his assigned tasks within Jira, and he planned, designed, developed, tested, and released the following deliverables into production.

- Project website
- Company/corporate website
- Security Incident and Event Management (SIEM) Advanced Log Analyzer Tool

### Ryan LeBlanc

Real world: Information Systems Engineer at Georgia Tech Research Institute, [Ryan LeBlanc | LinkedIn](#)

Project: Senior Architect and AI Developer

Working an average of 23.6 hours per sprint Ryan successfully managed all his assigned tasks within Jira, and he planned, designed, developed, tested, and released the following deliverables into production.

- AI related research and alignment

- AI Information Security Chatbot client offering
- Direct collaboration with Justin engaging with the Server Hardening client offering

### **Justin Place**

Real world: Research Technologist at Georgia Tech Research Institute, [Justin Place | LinkedIn](#)

Project: Senior Infrastructure Architect & Administrator

Working an average of 23.6 hours per sprint Justin successfully managed all his assigned tasks within Jira, and he planned, designed, developed, tested, and released the following deliverables into production.

- Built out virtual infrastructure to support server hardening client offering
- AI-backed Server Hardening client offering
- Direct collaboration with Ryan engaging with the AI client offering

## **Team Reflection on Project Experience**

The synergy and collaboration of this team was on full display throughout the entire project. From team formation, conception of the project idea, and throughout the entire project lifecycle including carrying out tasks and collaborative milestone presentations culminating in a successful project completion and several opportunities for exposure. The obvious enthusiasm demonstrated by each team member along with the above-mentioned collective interactions directly contributed to the outstanding communication throughout the project which in large part is the reason for our project success.

### **Project Success Factors**

Our team was very productive and had excellent planning, leadership, group dynamics, communication, and skill sets. Every team member was devoted to producing outstanding results, and we all put our best efforts into the tasks that we were given. Weekly Scrum calls and daily Team Chat communication made sure that we were always aware of each other's plans and objectives. Efficient planning aided in time management and goal clarification for the project. Strong leadership furnished guidance and inspiration, while transparent and clear communication promoted problem-solving and seamless project progression. Having a team of knowledgeable, driven individuals with a range of specialties, improved task execution even more. Overall, the coordination and cooperation of our team was essential to the success of our project.

### **Team Collaboration and Communication Experiences**

The cooperation of our team was excellent! It was demonstrated by frequent check-ins, weekly goals and accomplishment reports, and mutual assistance as required. Everyone collaborated well in order to develop a workable and effective plan. Project tracking was made easier by using Microsoft Teams for general communication, file tracking, weekly scrum sessions, and task reporting. By using milestones, a JIRA process facilitated the tracking of individual progress. The team persevered in their efforts despite

obstacles including integrating Linux computers and improving AI training models. Project communication was improved by standardizing on Teams despite its limitations. The well-attended weekly meetings were essential for discussing future projects and ideas as well as for keeping everyone on schedule. Assigning responsibilities to team members promoted focused ownership and guaranteed excellent results.

## Challenges

Given our full-time job schedules and obligations to our families, time management presented an enormous challenge for our team. We occasionally fell behind schedule, but we managed to overcome these obstacles thanks to excellent communication. We were upfront with the team about any delays, and they were willing to adjust or help in catching up. The chatbot's development was initially hindered by a lack of experience with Python and machine learning. But after thorough research, we were able to overcome this challenge by using an open-source program. To improve our webpages even more, we really wished we had more time to explore Hugo's sophisticated features. We had big aspirations for our AI products, but we also had a fallback strategy, which made it easy for us to switch to ChatRTX and get great results.

## Areas to Improve

The team determined that time management needed to be improved the most. Even though we were mostly on schedule, there were some minor issues that needed more time to make up. It would have also been beneficial to have more broad knowledge of computer programming and a better understanding of the JIRA process tracking, since it was thought to be essential to the accomplishment of the project. Improvements were also indicated for more accurate datasets for AI models and a better comprehension of AI dataset optimization. Furthermore, a more remarkable training approach utilizing AI avatars and improving project demos would have resulted from learning about Synthesia sooner.

## Appendix

Project Website URL

<https://project.ocds.tech/>

OCDS Corporate Website URL

<https://www.ocds.tech/>

## Project Files

This package of files includes all relevant work associated with the project goals and deliverables.

## **Project Proposal**

[https://project.ocds.tech/pdf/IT7993-Capstone\\_P4\\_Project-Proposal\\_OCDS.pdf](https://project.ocds.tech/pdf/IT7993-Capstone_P4_Project-Proposal_OCDS.pdf)

- The Project Proposal is a one-page document used to submit our entrepreneurship project idea to our Sponsor for review and approval
- This document contains a project Description to include Business Requirements and Functional Requirements

## **Project Plan**

[https://project.ocds.tech/pdf/IT7993\\_Project-Plan\\_OCDS\\_vJan28.pdf](https://project.ocds.tech/pdf/IT7993_Project-Plan_OCDS_vJan28.pdf)

- The Project Plan is the official project document to get official approval
- The document lays out the Overview of the project, introducing the Project Team, Project URL, what the final Deliverables will be, Milestones, Communication Plan, Scheduling, Task Tracking plan, and a spot for approval signatures.

## **Business Plan**

[https://project.ocds.tech/pdf/IT7993\\_Business-Plan\\_Final\\_OCDS.pdf](https://project.ocds.tech/pdf/IT7993_Business-Plan_Final_OCDS.pdf)

- This is the OCDS Business Plan project deliverable
- It outlines the goals for Owl Cyber Defense Systems and the strategies to achieve those goals
- It also includes mission and vision statements to drive the company to success
- Market and Sales analysis to include a P&L statement

## **OCDS Company IT Policies**

[https://project.ocds.tech/pdf/OCDS\\_IT\\_Policies.pdf](https://project.ocds.tech/pdf/OCDS_IT_Policies.pdf)

- These company IT policies are another project deliverable
- As part of the Business Plan these policies help to shape the culture of the OCDS business
- They help to ensure compliance where applicable
- Assist with internal risk management
- Employee engagement and satisfaction
- There's also an aspect of legal protections

## **OCDS Cybersecurity Policies**

[https://project.ocds.tech/pdf/OCDS\\_Cybersecurity\\_Policies.pdf](https://project.ocds.tech/pdf/OCDS_Cybersecurity_Policies.pdf)

- Part of the policies deliverable the OCDS company cybersecurity policies will help to protect OCDS sensitive information/data
- Help OCDS meet compliance and legal requirements
- Protect brand reputation as well as prevent financial loss
- Enhance overall security position and secure critical infrastructure

## **OCDS Cyber Awareness Training**

[https://project.ocds.tech/pdf/OCDS\\_Cybersecurity\\_Training.pdf](https://project.ocds.tech/pdf/OCDS_Cybersecurity_Training.pdf)

- As one of the primary operational objectives and final deliverables the cyber awareness training is intended to help OCDS clients to increase their overall security posture by training their employees to be more cyber aware
- OCDS provides clients with three training modules
  - Intro/terminology
  - Safety/types of cyber attacks
  - Customized proprietary tests and activities

### **OCDS Cybersecurity Training: Customer Example**

[https://project.ocds.tech/ppt/CyberSecurity\\_Training\\_for\\_Scrappy-Tax-Service.pptx](https://project.ocds.tech/ppt/CyberSecurity_Training_for_Scrappy-Tax-Service.pptx)

- This is an example of a completed training program for Scrappy Tax Service

### **Milestone 1 Presentation**

[https://project.ocds.tech/pdf/IT7993\\_Milestone1\\_OCDS.pdf](https://project.ocds.tech/pdf/IT7993_Milestone1_OCDS.pdf)

- PowerPoint presentation for Sprint 1
- Presented to project sponsor on Wednesday Feb 21, 2024

### **Milestone 2 Presentation**

[https://project.ocds.tech/pdf/IT7993\\_Milestone2\\_OCDS.pdf](https://project.ocds.tech/pdf/IT7993_Milestone2_OCDS.pdf)

- PowerPoint presentation for Sprint 2
- Presented to project sponsor on Wednesday Mar 20, 2024

### **Milestone 3 Presentation**

[https://project.ocds.tech/pdf/IT7993\\_Milestone3\\_OCDS.pdf](https://project.ocds.tech/pdf/IT7993_Milestone3_OCDS.pdf)

- PowerPoint presentation for Sprint 3
- Presented to project sponsor on Tuesday Apr 23, 2024

### **Department Presentation**

Watch Video: <https://youtu.be/4PCfTgl0rvw>

Download Video: [https://project.ocds.tech/video/OCDS\\_DepartmentPresentation.mp4](https://project.ocds.tech/video/OCDS_DepartmentPresentation.mp4)

- Department presentation recorded Saturday Apr 27 and delivered via D2L Sunday Apr 28, 2024

### **AI Chatbot Installer**

[https://project.ocds.tech/archives/ChatWithOCDS\\_installer\\_3\\_5.zip](https://project.ocds.tech/archives/ChatWithOCDS_installer_3_5.zip)

- OCDS flagship product the AI Chatbot is a primary operational objective and deliverable
- The AI Security OCDS Chatbot is powered by RTX Nvidia and was customized by Ryan via scripts using PyCharm and Visual Studio
- The AI Security OCDS Chatbot is used in conjunction with the OCDS Server Hardening Tool to increase the cyber security posture of OCDS clients

### Virtual Machine Files

[https://project.ocds.tech/archives/OCDS\\_VMs\\_Files.zip](https://project.ocds.tech/archives/OCDS_VMs_Files.zip)

- As part of another project deliverable this virtual infrastructure supports the environment required to support the OCDS AI-backed server hardening tool
- This environment also supports running the SCAP tool (Security Compliance Automation Protocol) which, in conjunction with the AI Security Chatbot, helps increase the clients security posture

### Final Project Report

[https://project.ocds.tech/archives/IT7993\\_Final-Report-G01-W01-P4-1.zip](https://project.ocds.tech/archives/IT7993_Final-Report-G01-W01-P4-1.zip)

- This file is this report which describes, in the detail, the entire Owl Cyber Defense Systems project

## References

1. *123 SMB Cybersecurity Statistics*. (2023, November 7). Packetlabs. <https://www.packetlabs.net/posts/123-smb-cybersecurity-statistics/#:~:text=The%20Top%20SMB%20Cybersecurity%20Statistics%20of%202023%20%28So,could%20be%20compromised%20by%20an%20attack%20More%20items>
2. Daugherty, G. (2024, March 29). *What is a small business? Definition, characteristics, and challenges*. Investopedia. <https://www.investopedia.com/small-business-8611031>