KENNESAW STATE UNIVERSITY

https://project.ocds.tech

IT-7993 IT Capstone Project

ID: G01/W01-P4

Title: Owl Cyber Defense Systems

Sponsor: Dr. Ying Xie

April 23, 2024

Team Members: Scott Gilstrap, Stephanie Aguirre, Chris Dunbar, Justin Place, Ryan LeBlanc

KENNESAW STATE
UNIVERSITY

Milestone-3 Presentation

April 23, 2024

Agenda:

Project overall outcome details

- Sprint 3 Milestone Goals and Objectives
- Sprint 3 Milestone Progress Summary
  - One-page Dashboard
  - Overall WBS: Timeline / Gantt Chart
- Sprint 3 Weekly Scrum Updates
- Sprint 3 Epic Task Discussions (all deliverables)
  - Overall WBS: Timeline / Gantt Chart
  - Team member deliverable presentations
  - WBS: Timeline / Gantt Chart for each Epic
  - Discussion with Empirical Evidence & Artifacts
- Time Tracking: Team and individual effort hours via person-hour burn-up pivot tables / charts / graphs associated with Sprint 3
- Review of project performance and takeaways
- Plans & reminders for the rest of the semester
  - C-Day, Department Presentation, Peer Evaluation, & Self-reflection (specific dates/times)

OCDS Team

- Scott Gilstrap
    - Project Manager / Team Leader / Scrum Master
    - OCDS VP of Project Management
- Stephanie Aguirre
    - Project Technical Writer / Instructor
    - OCDS VP of Learning and Development
- Chris Dunbar
    - Project Systems Administrator / Web Master
    - OCDS VP of Infrastructure and Web Development
- Justin Place
    - Project Senior Architect / AI Developer
    - OCDS VP of Development Operations
- Ryan LeBlanc
    - Project Senior Architect / AI Developer
    - OCDS VP of Product Development

Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Sprint 3 Goals & Objectives

Production Deployment & Release

Milestone 3 Goals

Strategic Objective:

Establish the OCDS cybersecurity business providing small businesses cost effective tools to increase their cybersecurity protection posture at an affordable rate

Sprint 3

Mar 26 – Apr 21, 2024

Operational Objectives

- Business Plan fully completed and published
- Company Policies published in Business Plan
- Project Website deployed and released into production with all documentation
- Company Website deployed and released into production
- Cyber Awareness Training Modules deployed and released into production on website
- IT Security Plan deployed and released into production on the website
- Proprietary Risk Assessment deployed and released into production on the website
- AI Security Chatbot deployed and released into production on the website
- Server Hardening Tool deployed and released into production
- SIEM Advanced Firewall and Log Analyzer deployed and released into production

Sprint 3 Milestone/Epic Progress Summary

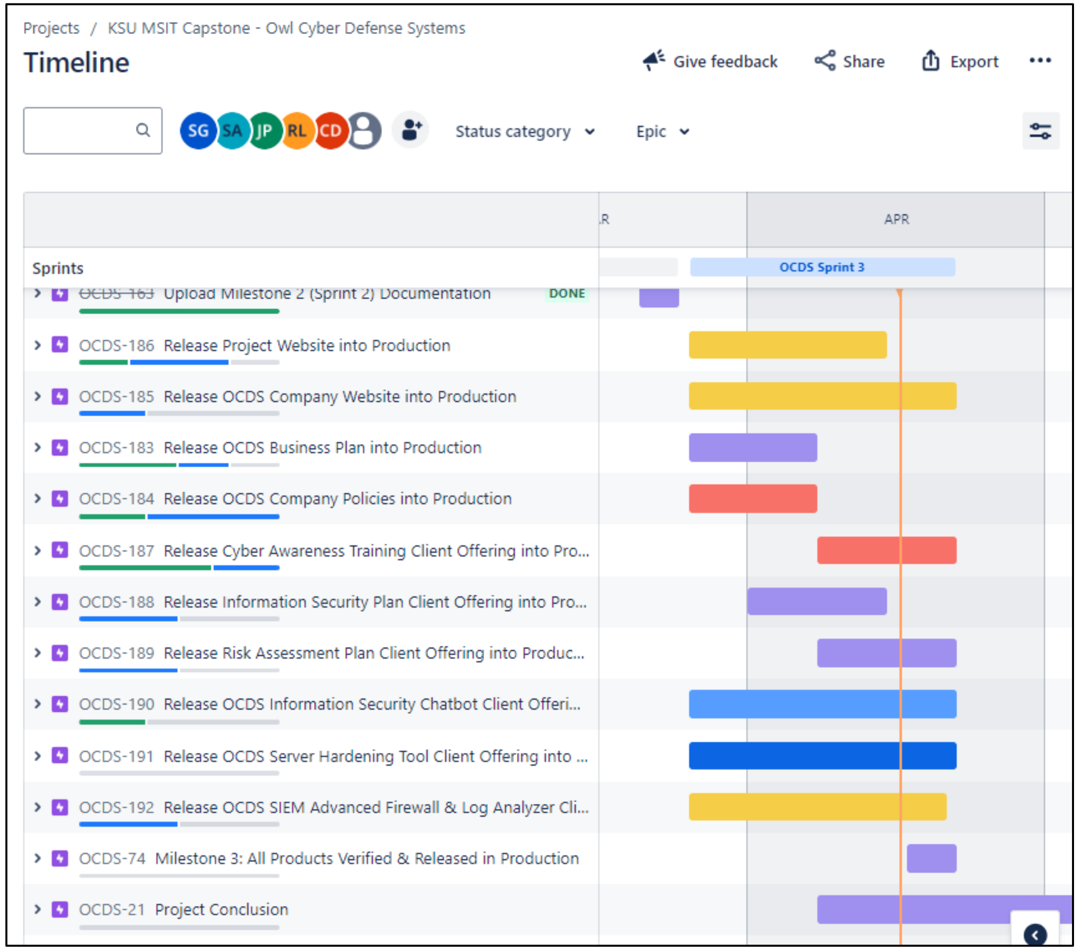
Sprint 1 Milestone Progress One-Slide Dashboard

Epic / Objective	Health	Target Date	Progress	Key Issues & Risks	GTG Action Plan	Leadership Assistance Requested
Release Project Website into Production	B	14-Apr-24	• Successfully completed Project website with documentation. • Project website is self designed/published and self hosted.	NA	NA	NA
Release OCDS Company Website into Production	B	21-Apr-24	• Successfully completed Company website with Products & Services. • Project website is self designed/published and self hosted.	NA	NA	NA
Release OCDS Business Plan into Production	B	14-Apr-24	• Successfully completed Business Plan with all required content. • The Business Plan is published & available via websites.	NA	NA	NA
Release OCDS Company Policies into Production	B	14-Apr-24	• Successfully completed the OCDS Company Policies. • Company Policies are published & available via the Business Plan.	NA	NA	NA
Release Cyber Awareness Training Client Offering into Production	B	14-Apr-24	• Successfully completed Cyber Awareness Training Modules. • All modules are published & available via websites.	NA	NA	NA
Release Information Security Plan Client Offering into Production	B	07-Apr-24	• Successfully completed the IT Security Planning Form Questionnaire. • The IT Security Planning Form Questionnaire is available via website.	NA	NA	NA
Release Risk Assessment Plan Client Offering into Production	B	23-Mar-24	• Successfully Completed the proprietary Risk Assessment Questionnaire and Planning form. (Example: Scrappy Tax Service)	NA	NA	NA
Release OCDS Information Security Chatbot Client Offering into Production	B	18-Mar-24	• The OCDS Security Chatbot was successfully deployed and has learned the appropriate 800-53 security standards.	NA	NA	NA
Release OCDS Server Hardening Tool Client Offering into Production	B	21-Mar-24	• All VM supporting Infrastructure was successfully deployed. • Successful STIG deployment of the OCDS Server Harding Tool.	NA	NA	NA
Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production	B	19-Mar-24	• Successful build out of supporting VM Infrastructure • Successful SIEM tool configuration (Security Onion) & Deployment.	NA	NA	NA

LEGEND B Complete G On Track Y At Risk R Delayed H On-Hold/ Canceled N Not Started

Sprint 3 Milestone Progress Summary

- All Sprint 3 Epics are completed or on target for successful completion by due date.
- All tasks have been completed and/or addressed in a timely manner to be on track.
- Weekly Scrum meetings were conducted, and updates were logged appropriately.
- Project workload has been distributed evenly with each team member contributing appropriately.
- No issues or risks were encountered during Sprint 3
- No change request was required



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Sprints

- ~~OCDS-163~~ Upload Milestone 2 (Sprint 2) Documentation DONE
- OCDS-186 Release Project Website into Production
- OCDS-185 Release OCDS Company Website into Production
- OCDS-183 Release OCDS Business Plan into Production
- OCDS-184 Release OCDS Company Policies into Production
- OCDS-187 Release Cyber Awareness Training Client Offering into Pro...
- OCDS-188 Release Information Security Plan Client Offering into Pro...
- OCDS-189 Release Risk Assessment Plan Client Offering into Produc...
- OCDS-190 Release OCDS Information Security Chatbot Client Offeri...
- OCDS-191 Release OCDS Server Hardening Tool Client Offering into ...
- OCDS-192 Release OCDS SIEM Advanced Firewall & Log Analyzer Cli...
- OCDS-74 Milestone 3: All Products Verified & Released in Production
- OCDS-21 Project Conclusion

Sprint 3 Weekly Scrum Updates

Project – Owl Cyber Defense Systems – Sprint 3

Data as of: 03/30/24

Project Manager	Project Objective	Start Date	End Date
Scott Gilstrap	Design and establish a first-class cybersecurity company offering world-class AI-enable proprietary cyber protections to meet today's robust cybersecurity requirements at a reasonable cost to the client.	01/16/24	05/05/24

Overall	Schedule	Budget	Scope	Resource
🟢	🟢	🟢	🟢	🟢

Key Accomplishments/Activities

- ✓ Review all company policies and prepared them for production release
- ✓ Completed logic in PS to iterate through CSV file and run commands against system
- ✓ Updated .py to fix RTX Chatbot
- ✓ Took all VM snapshots (backup purposes)
- ✓ Setup logic to check registry DWord creation and appropriate entry
- ✓ Completed the IT Security Planning Questionnaire

Next Steps

- ✓ Release company policies into production
- ✓ Review Cyber awareness Training Modules
- ✓ Prepare training modules for production release
- ✓ Finish writing PS script to evaluate and change values against STIG for Windows
- ✓ Continue work on PS script and complete further testing on Windows VM
- ✓ Complete the Proprietary Risk Assessment Questionnaire
- ✓ Reconfigure the VM infrastructure and network cabling for the OCDS SIEM

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/25/24	02/25/24	100%
Development & Testing Complete (Sprint 2)	02/26/24	03/24/24	100%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	25%

ID	Key Risk(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

ID	Key Issue(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

Week-1: 24 – 30 Mar 2024

LEGEND

C	G	A	R	H	N	B
Complete	On Track	At Risk	Delayed	On Hold	Not Started	Cancelled

Project – Owl Cyber Defense Systems – Sprint 3

Data as of: 04/06/24

Project Manager	Project Objective	Start Date	End Date
Scott Gilstrap	Design and establish a first-class cybersecurity company offering world-class AI-enable proprietary cyber protections to meet today's robust cybersecurity requirements at a reasonable cost to the client.	01/16/24	05/05/24

Overall	Schedule	Budget	Scope	Resource
●	●	●	●	●

Key Accomplishments/Activities

- ✓ Conducting troubleshooting of the script handling SCAP scanning/STIGing – determined the multiple registry changes are affecting VM performance
- ✓ Product & Services website configurations
- ✓ Training page website configurations
- ✓ Updated Team photos and BIOs for both websites
- ✓ Added appropriate STIG entries in script
- ✓ Completed section 1 of the Risk Assessment Planning Questionnaire

Next Steps

- ✓ Finish writing PS scripts to evaluate and change values against the STIGs for Windows
- ✓ Website configurations
    - ✓ Product page & child pages
    - ✓ Services page & child pages
    - ✓ Training page and links to modules
    - ✓ Team page content
- ✓ Visit physical data center to resolve network issue for SIEM VM
- ✓ Complete further STIG scripting for STIGing VMs
- ✓ Complete section 2 of Risk Assessment Planning Questionnaire

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/25/24	02/25/24	100%
Development & Testing Complete (Sprint 2)	02/26/24	03/24/24	100%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	50%

ID	Key Risk(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

ID	Key Issue(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

Week-2: 31 Mar – 06 Apr 2024

LEGEND						
C	G	A	R	H	N	B
Complete	On Track	At Risk	Delayed	On Hold	Not Started	Cancelled

Project – Owl Cyber Defense Systems – Sprint 3

Data as of: 04/13/24

Project Manager	Project Objective	Start Date	End Date
Scott Gilstrap	Design and establish a first-class cybersecurity company offering world-class AI-enable proprietary cyber protections to meet today’s robust cybersecurity requirements at a reasonable cost to the client.	01/16/24	05/05/24

Overall	Schedule	Budget	Scope	Resource
●	●	●	●	●

Key Accomplishments/Activities

- ✓ Visited the physical data center – configured correct switch for spanning port (established mirroring)
- ✓ Connected SIEM VM to correctly configured port
- ✓ Identified critical error in SIEM VM
- ✓ Completed minor updates to Company and Project websites
- ✓ Completed section 3 of the Risk Assessment Planning Questionnaire

Next Steps

- ✓ Rebuild SIEM VM (again) to address critical error
- ✓ Complete section 4 of the Risk Assessment Planning Questionnaire
- ✓ Completing an example IT Security Assessment for client Scrappy Tax Service
- ✓ Update OCDS Security Chatbot
- ✓ Finalize all scripts

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/25/24	02/25/24	100%
Development & Testing Complete (Sprint 2)	02/26/24	03/24/24	100%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	75%

ID	Key Risk(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

ID	Key Issue(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

Week 3: 07 – 13 Apr 2024

LEGEND

C	G	A	R	H	N	B
Complete	On Track	At Risk	Delayed	On Hold	Not Started	Cancelled

Project – Owl Cyber Defense Systems – Sprint 3

Data as of: 04/02/24

Project Manager	Project Objective	Start Date	End Date
Scott Gilstrap	Design and establish a first-class cybersecurity company offering world-class AI-enable proprietary cyber protections to meet today's robust cybersecurity requirements at a reasonable cost to the client.	01/16/24	05/05/24

Overall	Schedule	Budget	Scope	Resource
●	●	●	●	●

Key Accomplishments/Activities	Next Steps
✓ Rebuilt SIEM VM to address critical error – issue resolved ✓ Completed section 4 of the Risk Assessment Planning Questionnaire ✓ Created example client reports for IT Security and Risk Assessment Plan ✓ Updated OCDS Security Chat with final datasets ✓ Completed all scripts for STIG and Chatbot learning ✓ Prepare red for Mielstone-3 presentation	✓ Review all deliverables for completion ✓ Meet as a team for final discussions ✓ Complete preparation for milestone-3 presentation ✓ Prepare final presentation ✓ Complete various evaluations and surveys ✓ Sprint 3 retrospective ✓ Identify project accomplishments, challenges, lessons learned, and opportunities for improvement

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/25/24	02/25/24	100%
Development & Testing Complete (Sprint 2)	02/26/24	03/24/24	100%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	95%

ID	Key Risk(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

ID	Key Issue(s)	Description	Mitigation / Action Plan
No Data	None	N/A	N/A

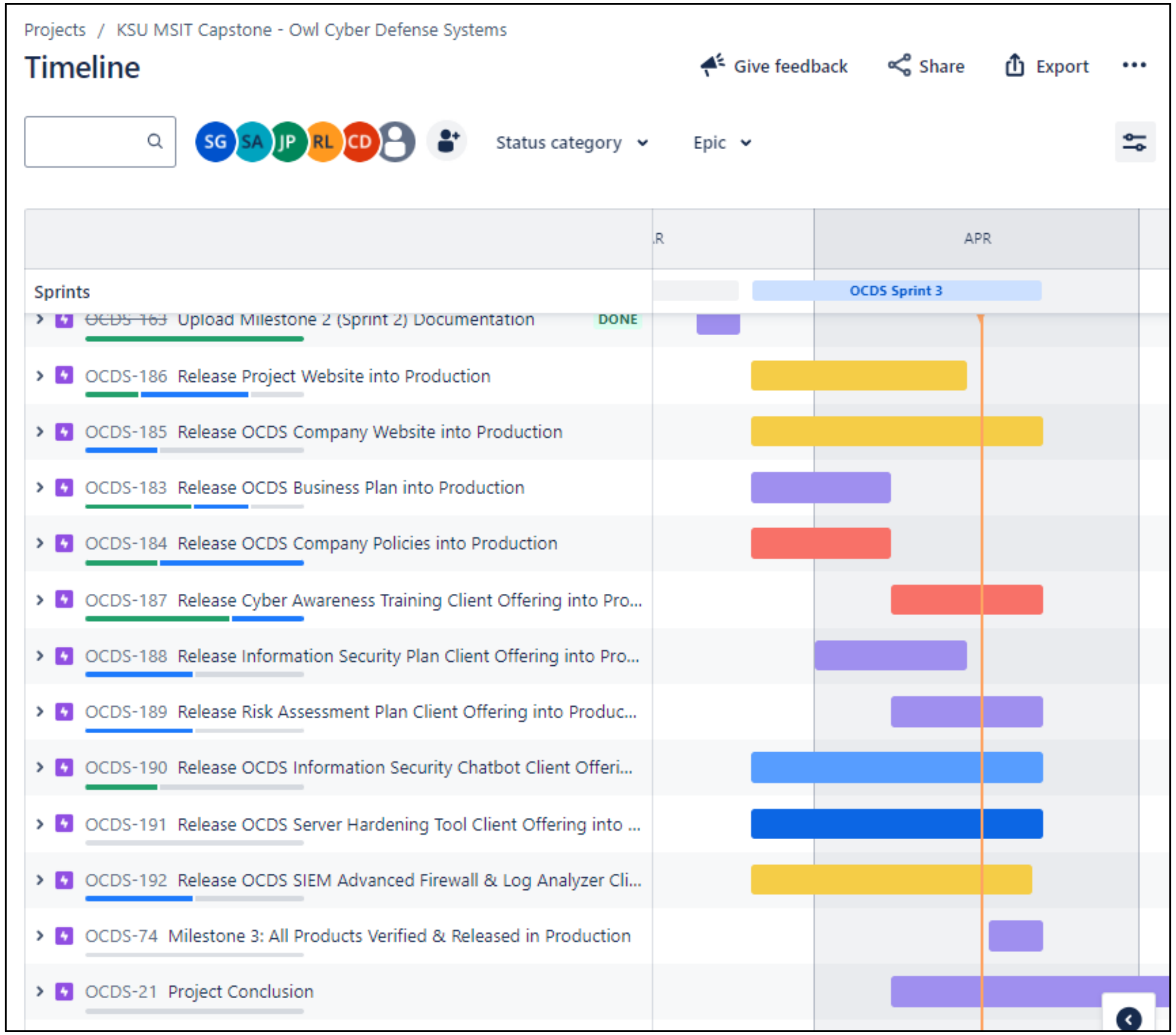
Week 4: 14 – 20 Apr 2024

LEGEND

C	G	A	R	H	N	B
Complete	On Track	At Risk	Delayed	On Hold	Not Started	Cancelled

Sprint 3 Epic & Task Discussions

Overall WBS Epic Timeline for Sprint 3 Milestones



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Sprints

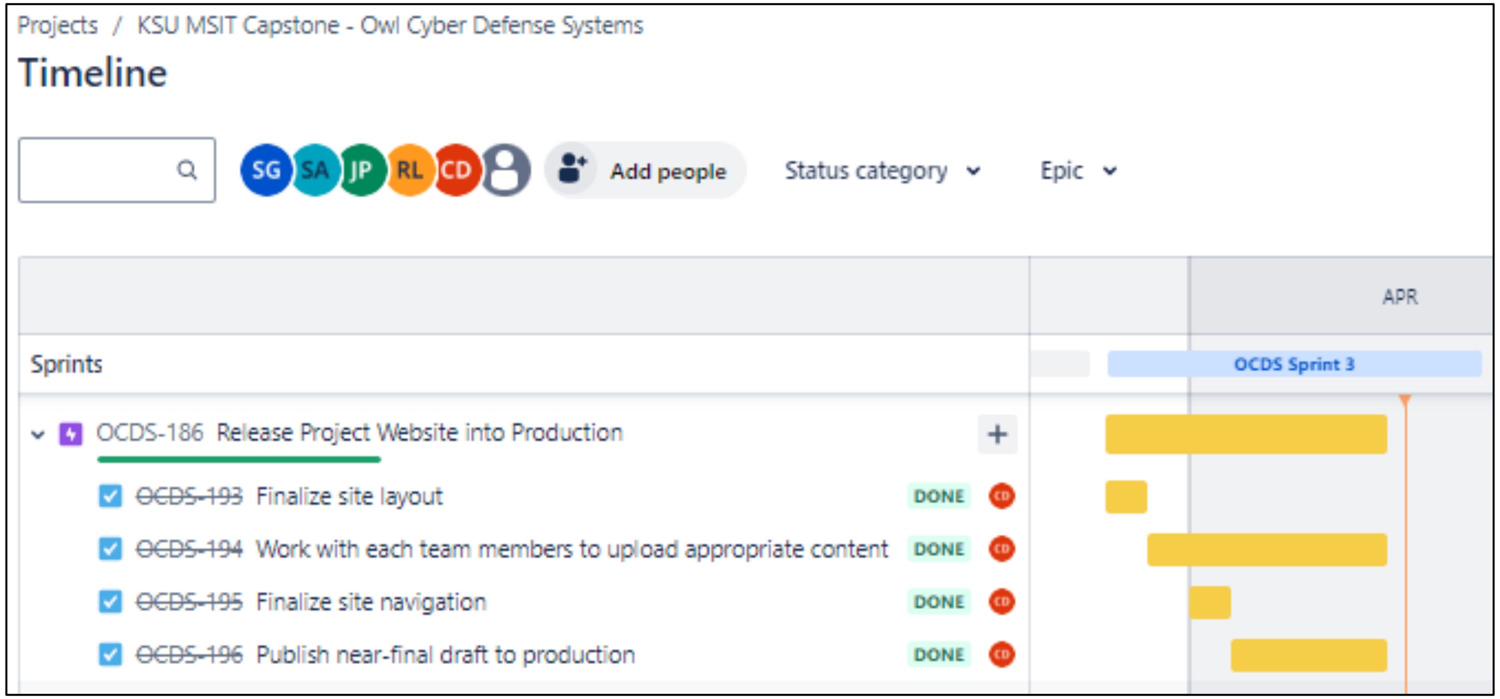
- ~~OCDS-163~~ Upload Milestone 2 (Sprint 2) Documentation DONE
- OCDS-186 Release Project Website into Production
- OCDS-185 Release OCDS Company Website into Production
- OCDS-183 Release OCDS Business Plan into Production
- OCDS-184 Release OCDS Company Policies into Production
- OCDS-187 Release Cyber Awareness Training Client Offering into Pro...
- OCDS-188 Release Information Security Plan Client Offering into Pro...
- OCDS-189 Release Risk Assessment Plan Client Offering into Produc...
- OCDS-190 Release OCDS Information Security Chatbot Client Offeri...
- OCDS-191 Release OCDS Server Hardening Tool Client Offering into ...
- OCDS-192 Release OCDS SIEM Advanced Firewall & Log Analyzer Cli...
- OCDS-74 Milestone 3: All Products Verified & Released in Production
- OCDS-21 Project Conclusion

Sprint 3 Milestones have been completed or are on target to be completed by due date

Epic: Release Project Website into Production

Chris Dunbar

Release Project Website into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

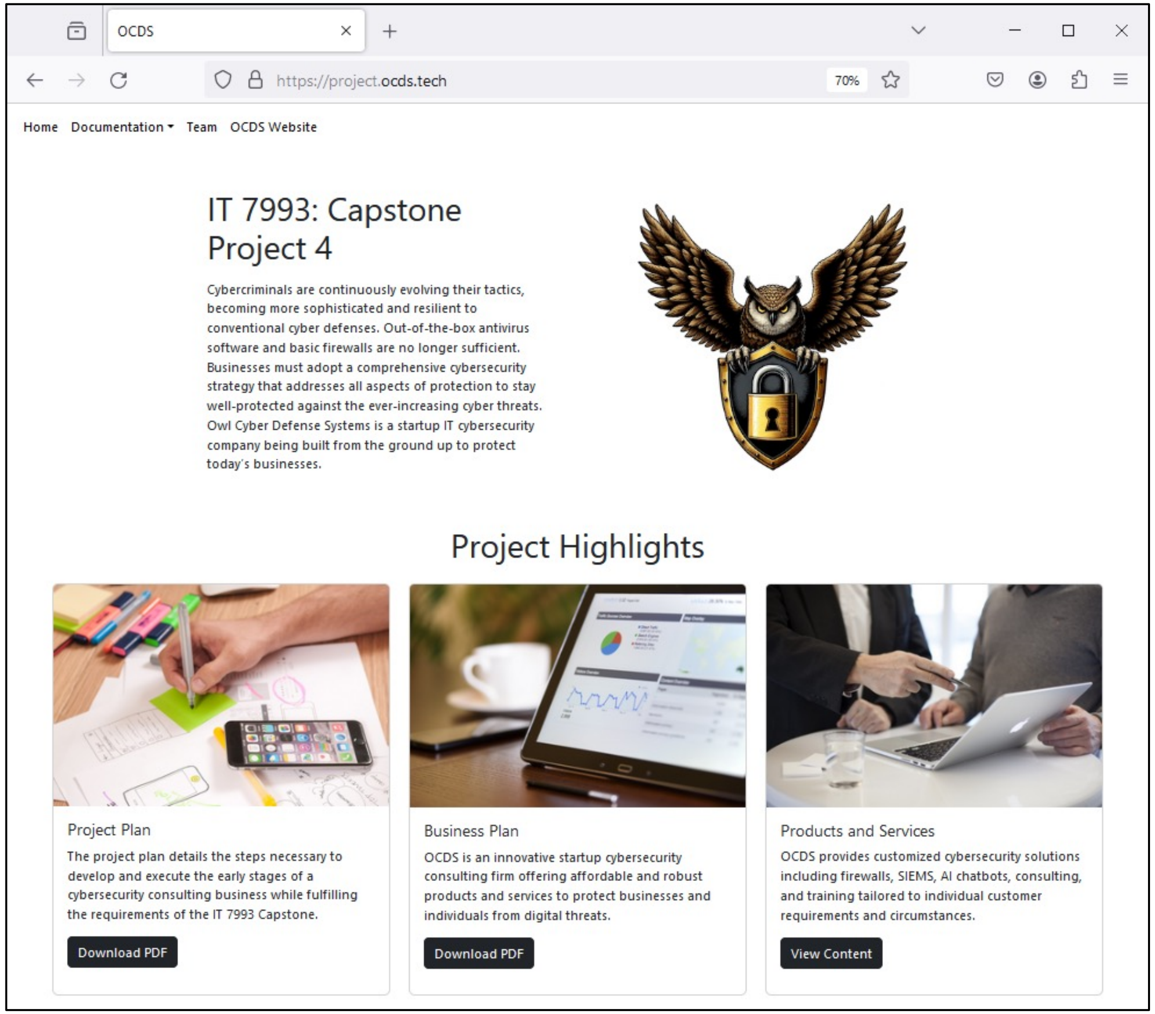
OCDS-186 Release Project Website into Production

☑	~~OCDS-193~~ Finalize site layout	DONE	CD
☑	~~OCDS-194~~ Work with each team members to upload appropriate content	DONE	CD
☑	~~OCDS-195~~ Finalize site navigation	DONE	CD
☑	~~OCDS-196~~ Publish near-final draft to production	DONE	CD

Complete/On Track

Release Project Website into Production

- Project website URL: https://project.ocds.tech/
- Hugo & Bootstrap
- **Home**
  - Project Plan Download
  - Business Plan Download
  - Products & Services
- **Documentation**
  - Business Assets
  - Milestones
  - Project Assets
- **Team** – Headshots with Bios
- Link to OCDS Company website



IT 7993: Capstone Project 4

Cybercriminals are continuously evolving their tactics, becoming more sophisticated and resilient to conventional cyber defenses. Out-of-the-box antivirus software and basic firewalls are no longer sufficient. Businesses must adopt a comprehensive cybersecurity strategy that addresses all aspects of protection to stay well-protected against the ever-increasing cyber threats. Owl Cyber Defense Systems is a startup IT cybersecurity company being built from the ground up to protect today's businesses.

Project Highlights

Project Plan

The project plan details the steps necessary to develop and execute the early stages of a cybersecurity consulting business while fulfilling the requirements of the IT 7993 Capstone.

Download PDF

Business Plan

OCDS is an innovative startup cybersecurity consulting firm offering affordable and robust products and services to protect businesses and individuals from digital threats.

Download PDF

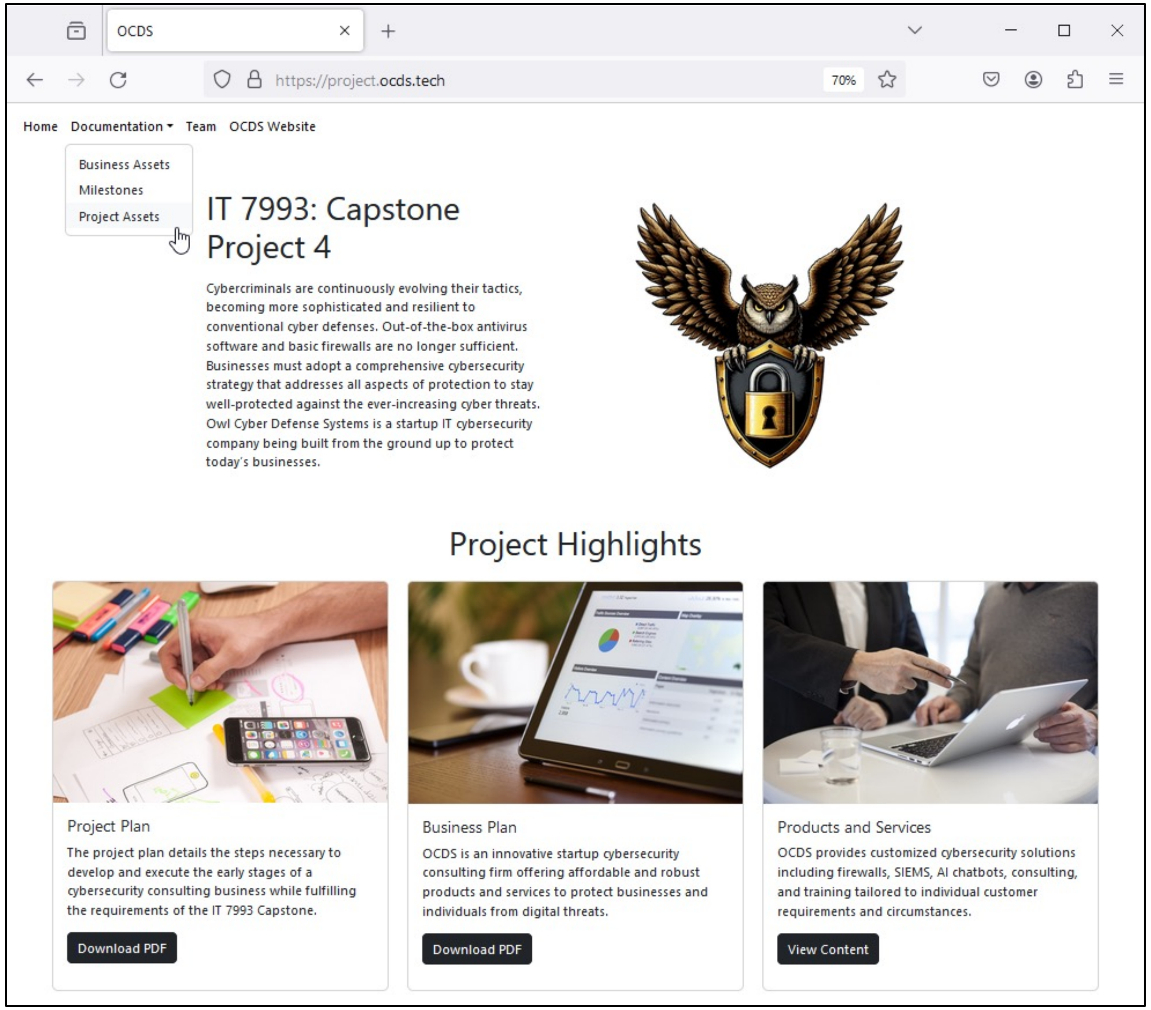
Products and Services

OCDS provides customized cybersecurity solutions including firewalls, SIEMS, AI chatbots, consulting, and training tailored to individual customer requirements and circumstances.

View Content

Owner: Chris Dunbar

Release Project Website into Production



IT 7993: Capstone Project 4

Cybercriminals are continuously evolving their tactics, becoming more sophisticated and resilient to conventional cyber defenses. Out-of-the-box antivirus software and basic firewalls are no longer sufficient. Businesses must adopt a comprehensive cybersecurity strategy that addresses all aspects of protection to stay well-protected against the ever-increasing cyber threats. Owl Cyber Defense Systems is a startup IT cybersecurity company being built from the ground up to protect today's businesses.

Project Highlights

Project Plan

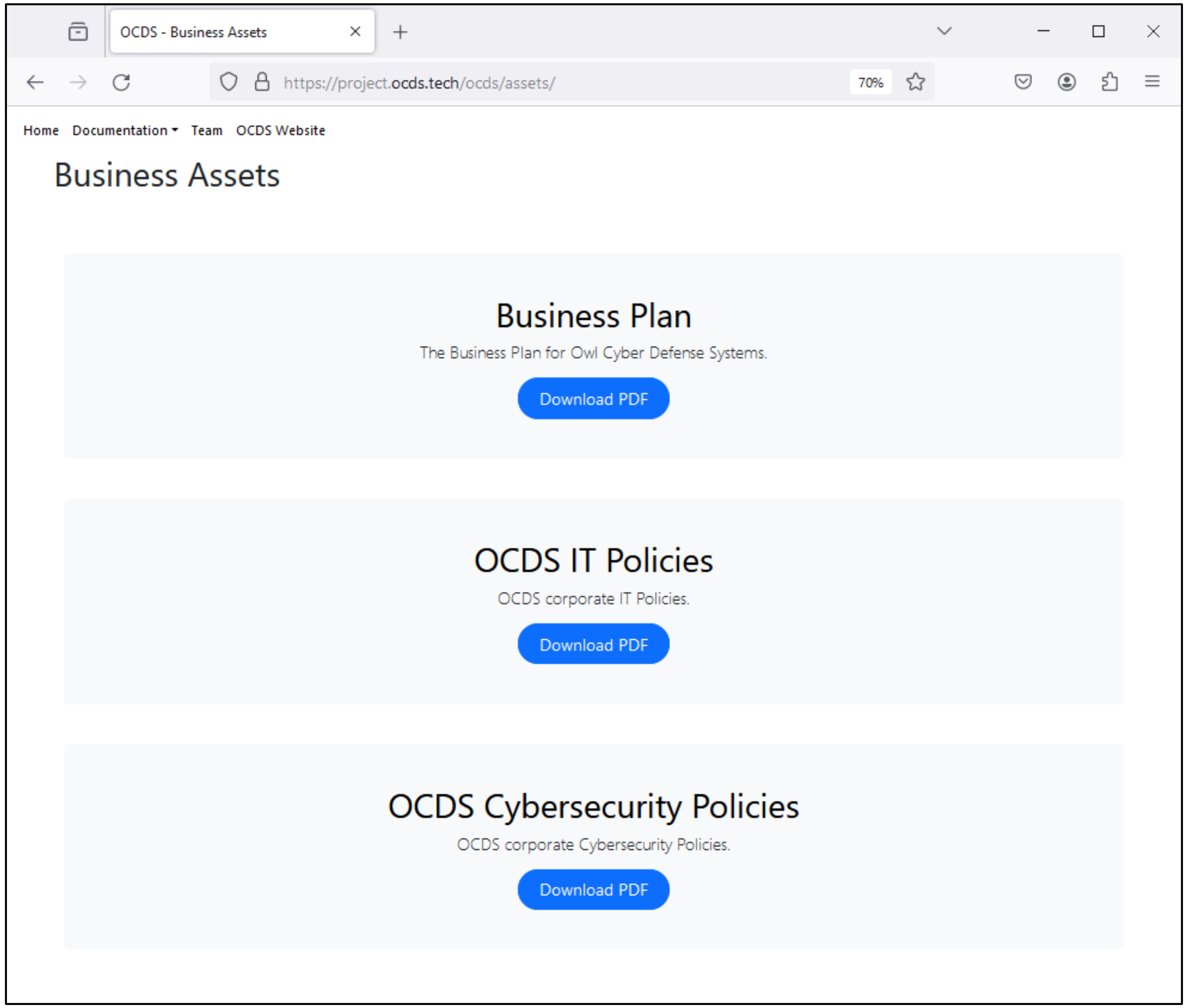
The project plan details the steps necessary to develop and execute the early stages of a cybersecurity consulting business while fulfilling the requirements of the IT 7993 Capstone.

Business Plan

OCDS is an innovative startup cybersecurity consulting firm offering affordable and robust products and services to protect businesses and individuals from digital threats.

Products and Services

OCDS provides customized cybersecurity solutions including firewalls, SIEMS, AI chatbots, consulting, and training tailored to individual customer requirements and circumstances.



Business Assets

Business Plan

The Business Plan for Owl Cyber Defense Systems.

OCDS IT Policies

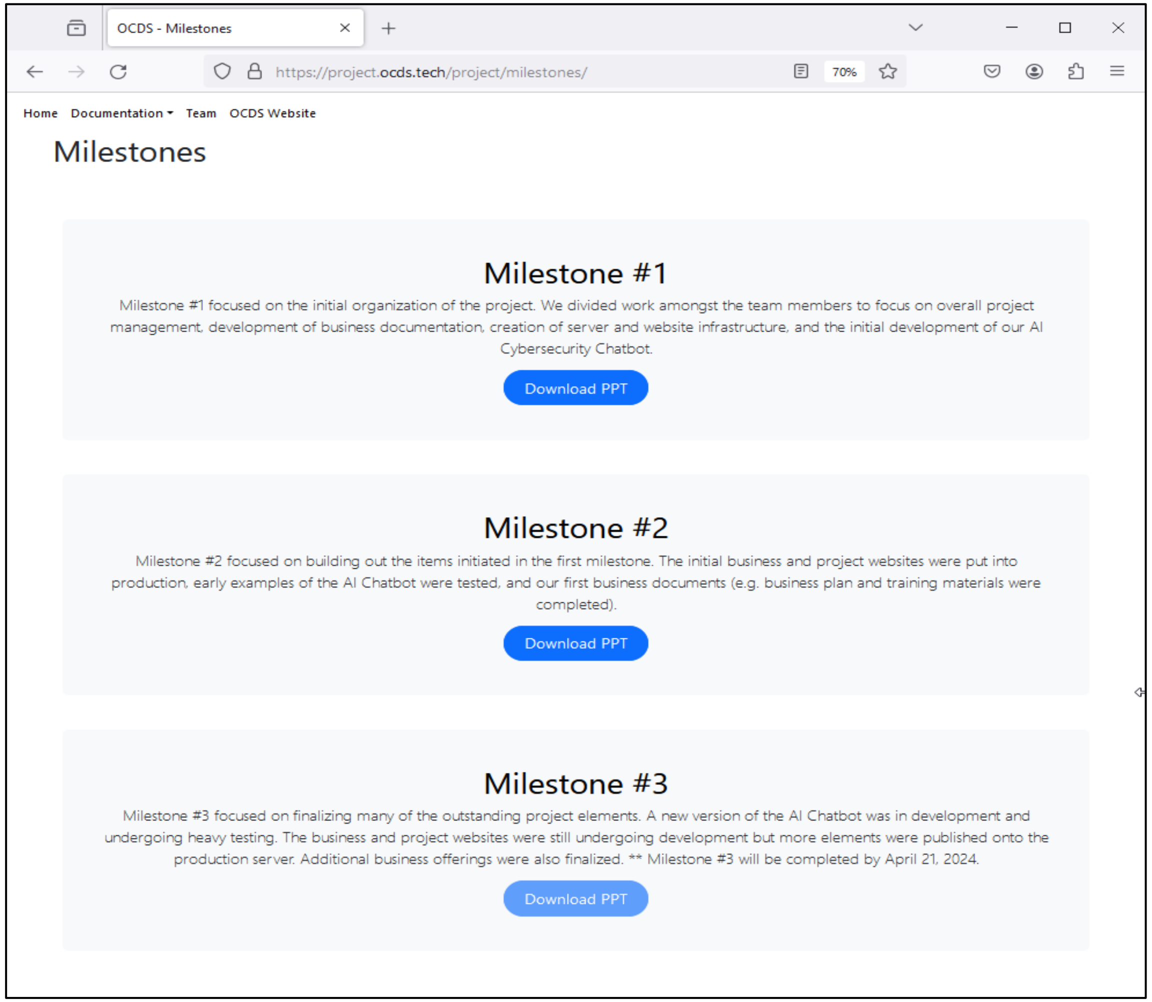
OCDS corporate IT Policies.

OCDS Cybersecurity Policies

OCDS corporate Cybersecurity Policies.

Owner: Chris Dunbar

Release Project Website into Production



Milestones

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 PPT

Milestone #2

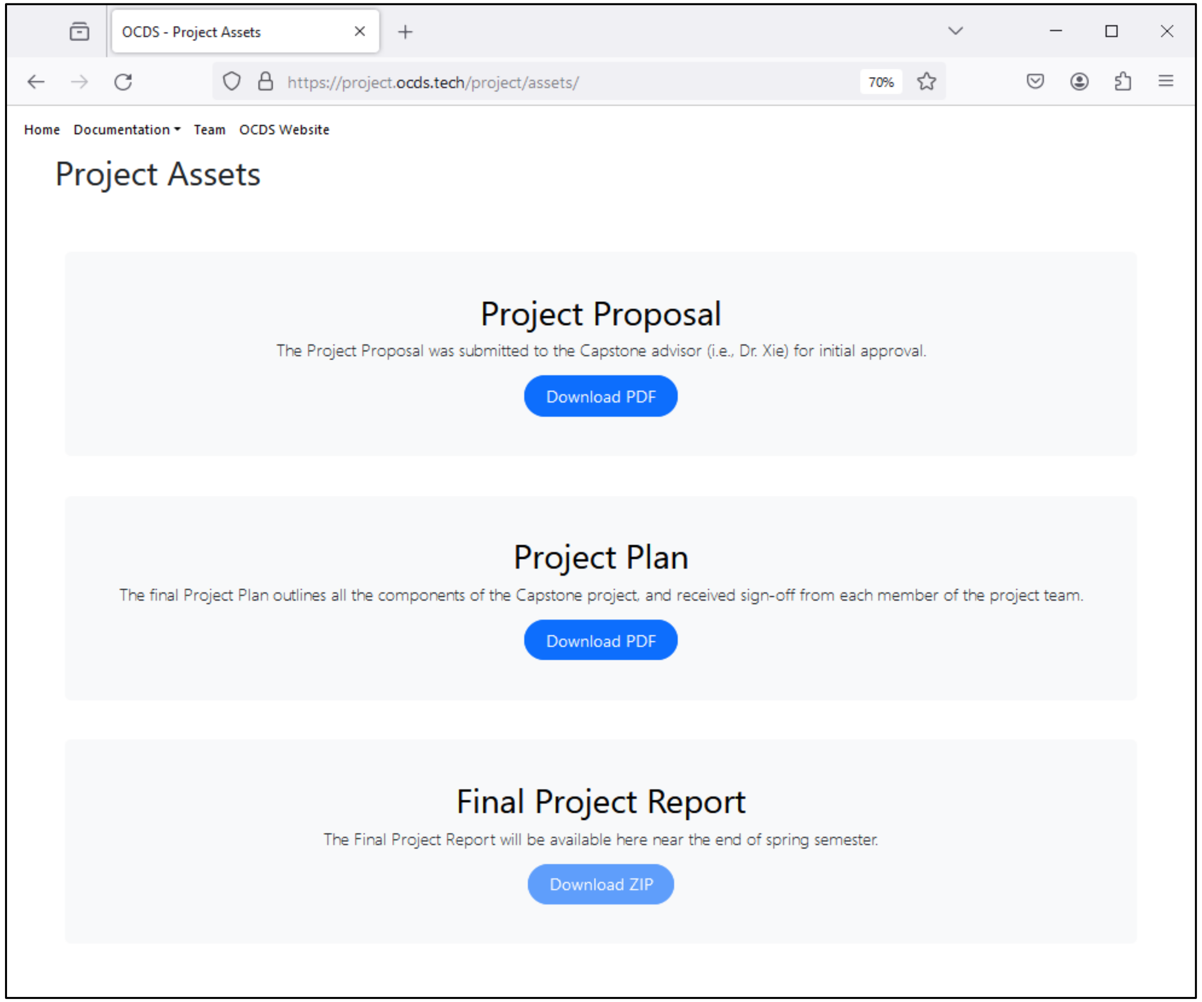
Milestone #2 focused on building out the items initiated in the first milestone. The initial business and project websites were put into production, early examples of the AI Chatbot were tested, and our first business documents (e.g. business plan and training materials were completed).

Download PPT

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. ** Milestone #3 will be completed by April 21, 2024.

Download PPT



Project Assets

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

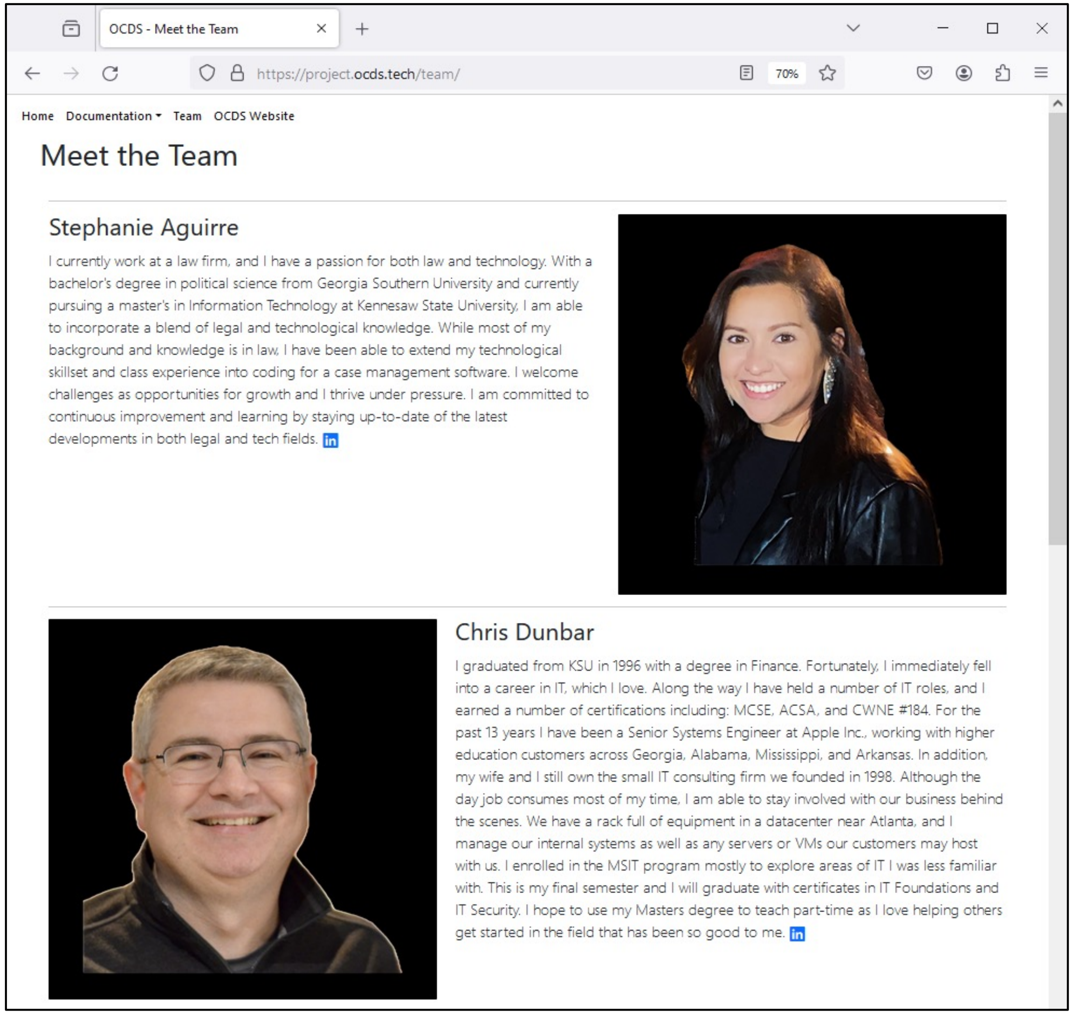
Final Project Report

The Final Project Report will be available here near the end of spring semester.

Download ZIP

Owner: Chris Dunbar

Release Project Website into Production



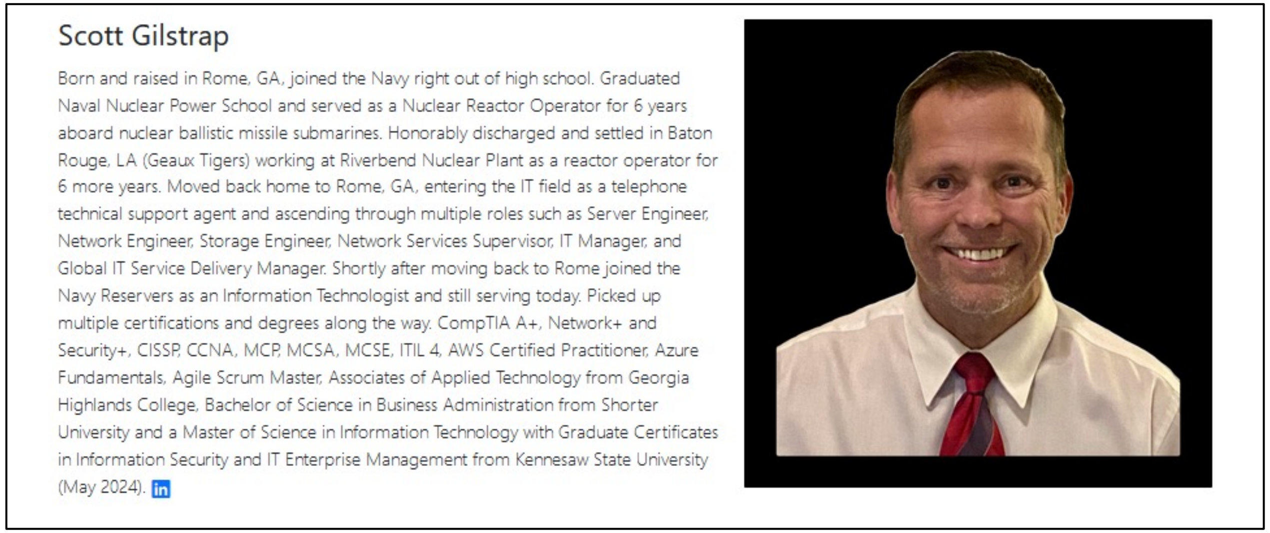
Meet the Team

Stephanie Aguirre

I currently work at a law firm, and I have a passion for both law and technology. With a bachelor's degree in political science from Georgia Southern University and currently pursuing a master's in Information Technology at Kennesaw State University, I am able to incorporate a blend of legal and technological knowledge. While most of my background and knowledge is in law, I have been able to extend my technological skillset and class experience into coding for a case management software. I welcome challenges as opportunities for growth and I thrive under pressure. I am committed to continuous improvement and learning by staying up-to-date of the latest developments in both legal and tech fields.

Chris Dunbar

I graduated from KSU in 1996 with a degree in Finance. Fortunately, I immediately fell into a career in IT, which I love. Along the way I have held a number of IT roles, and I earned a number of certifications including: MCSE, ACSA, and CWNE #184. For the past 13 years I have been a Senior Systems Engineer at Apple Inc., working with higher education customers across Georgia, Alabama, Mississippi, and Arkansas. In addition, my wife and I still own the small IT consulting firm we founded in 1998. Although the day job consumes most of my time, I am able to stay involved with our business behind the scenes. We have a rack full of equipment in a datacenter near Atlanta, and I manage our internal systems as well as any servers or VMs our customers may host with us. I enrolled in the MSIT program mostly to explore areas of IT I was less familiar with. This is my final semester and I will graduate with certificates in IT Foundations and IT Security. I hope to use my Masters degree to teach part-time as I love helping others get started in the field that has been so good to me.

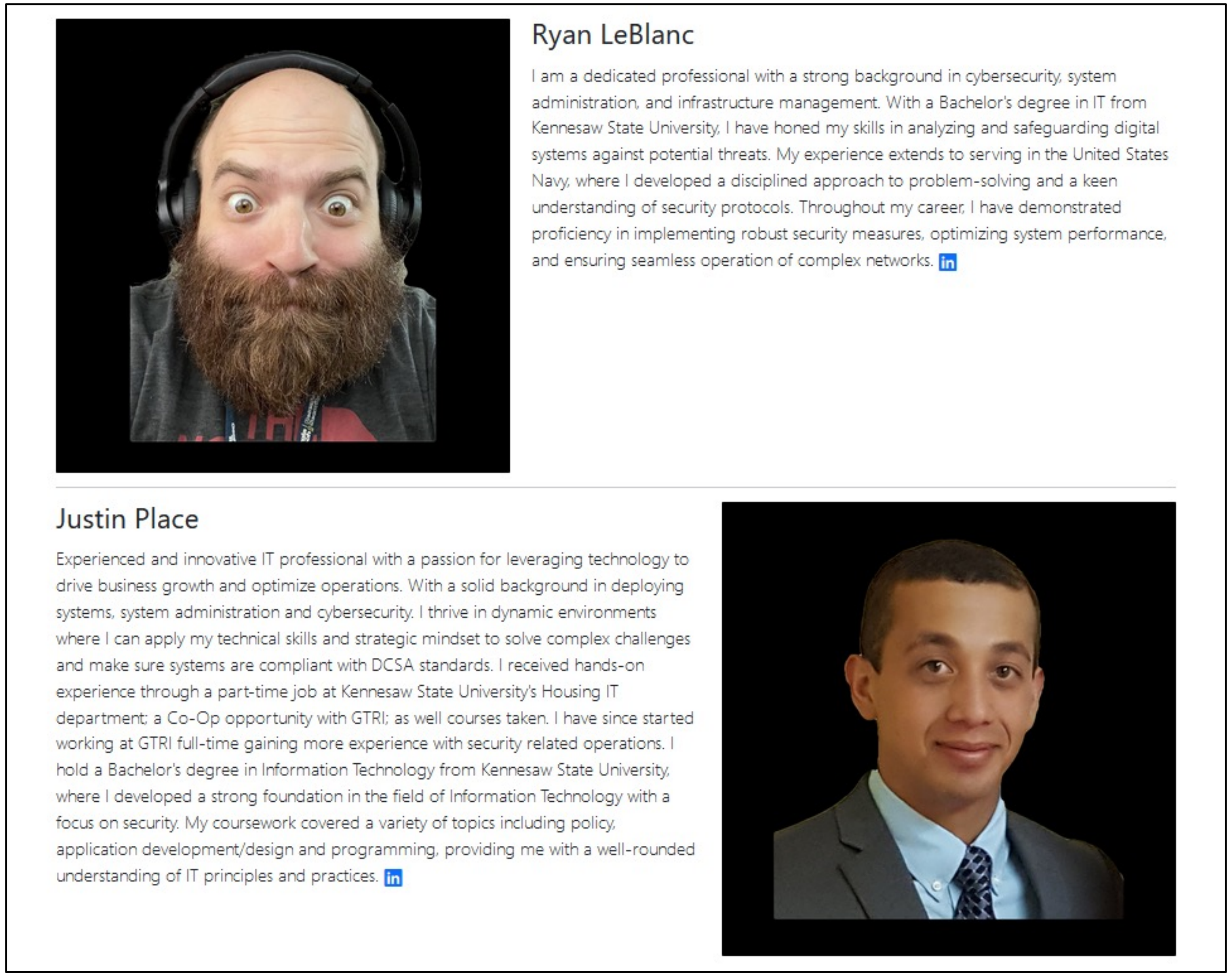


Scott Gilstrap

Born and raised in Rome, GA, joined the Navy right out of high school. Graduated Naval Nuclear Power School and served as a Nuclear Reactor Operator for 6 years aboard nuclear ballistic missile submarines. Honorably discharged and settled in Baton Rouge, LA (Geaux Tigers) working at Riverbend Nuclear Plant as a reactor operator for 6 more years. Moved back home to Rome, GA, entering the IT field as a telephone technical support agent and ascending through multiple roles such as Server Engineer, Network Engineer, Storage Engineer, Network Services Supervisor, IT Manager, and Global IT Service Delivery Manager. Shortly after moving back to Rome joined the Navy Reservers as an Information Technologist and still serving today. Picked up multiple certifications and degrees along the way. CompTIA A+, Network+ and Security+, CISSP, CCNA, MCP, MCSA, MCSE, ITIL 4, AWS Certified Practitioner, Azure Fundamentals, Agile Scrum Master, Associates of Applied Technology from Georgia Highlands College, Bachelor of Science in Business Administration from Shorter University and a Master of Science in Information Technology with Graduate Certificates in Information Security and IT Enterprise Management from Kennesaw State University (May 2024).

Owner: Chris Dunbar

Release Project Website into Production



Ryan LeBlanc

I am a dedicated professional with a strong background in cybersecurity, system administration, and infrastructure management. With a Bachelor's degree in IT from Kennesaw State University, I have honed my skills in analyzing and safeguarding digital systems against potential threats. My experience extends to serving in the United States Navy, where I developed a disciplined approach to problem-solving and a keen understanding of security protocols. Throughout my career, I have demonstrated proficiency in implementing robust security measures, optimizing system performance, and ensuring seamless operation of complex networks.

Justin Place

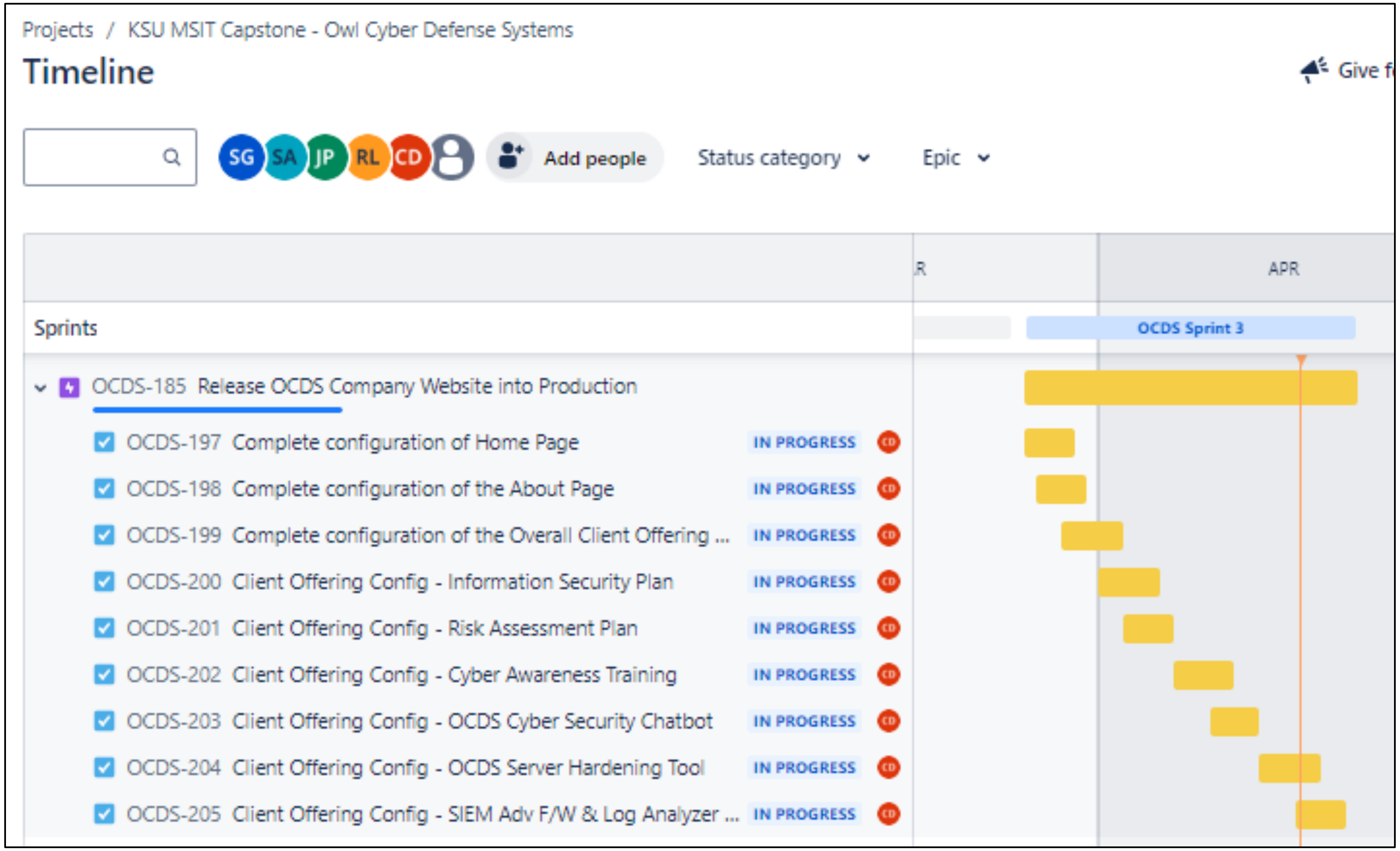
Experienced and innovative IT professional with a passion for leveraging technology to drive business growth and optimize operations. With a solid background in deploying systems, system administration and cybersecurity. I thrive in dynamic environments where I can apply my technical skills and strategic mindset to solve complex challenges and make sure systems are compliant with DCSA standards. I received hands-on experience through a part-time job at Kennesaw State University's Housing IT department; a Co-Op opportunity with GTRI; as well courses taken. I have since started working at GTRI full-time gaining more experience with security related operations. I hold a Bachelor's degree in Information Technology from Kennesaw State University, where I developed a strong foundation in the field of Information Technology with a focus on security. My coursework covered a variety of topics including policy, application development/design and programming, providing me with a well-rounded understanding of IT principles and practices.

Owner: Chris Dunbar

Epic: Release OCDS Company Website into Production

Chris Dunbar

Release OCDS Company Website into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

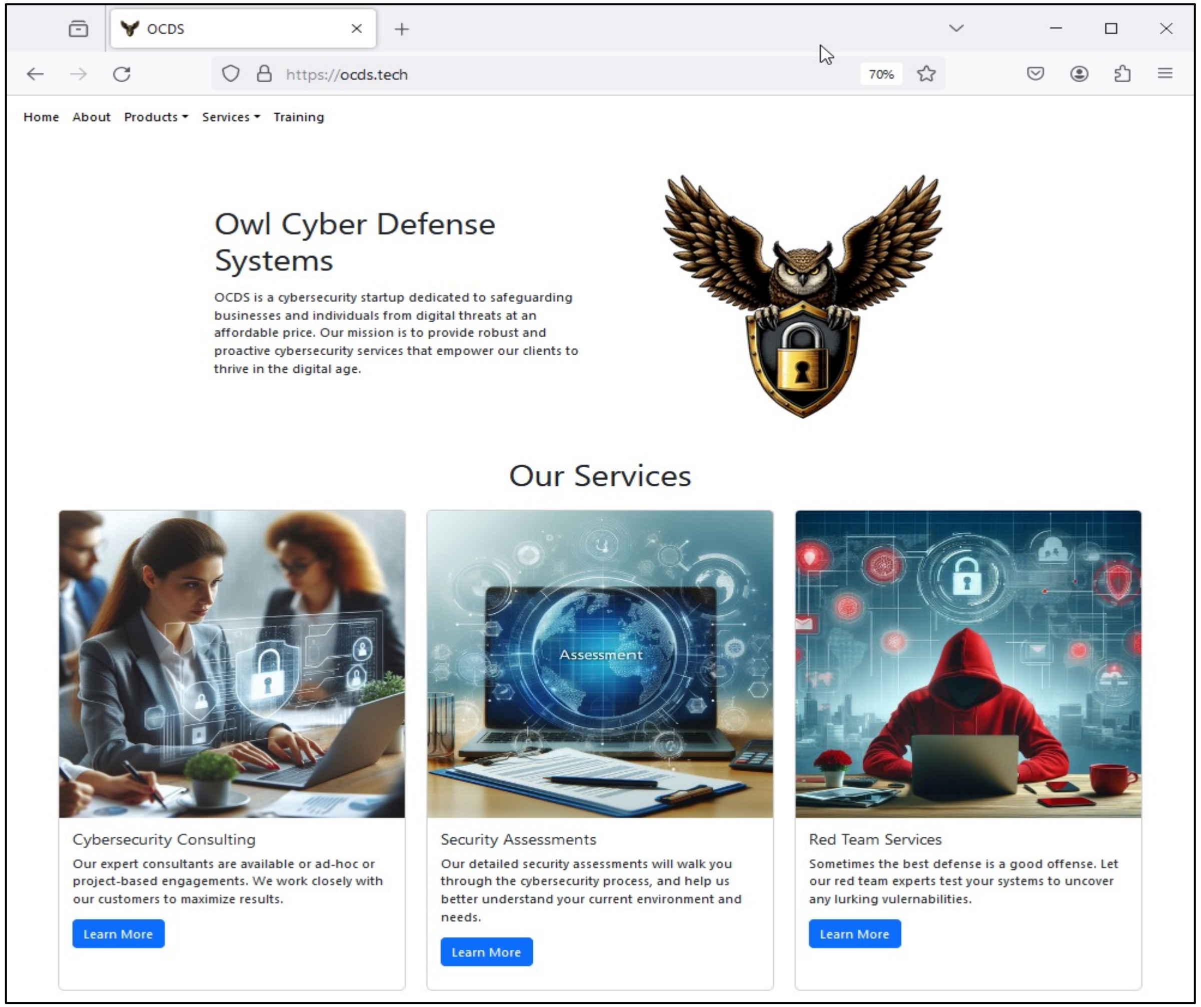
OCDS-185 Release OCDS Company Website into Production

☑ OCDS-197	Complete configuration of Home Page	IN PROGRESS
☑ OCDS-198	Complete configuration of the About Page	IN PROGRESS
☑ OCDS-199	Complete configuration of the Overall Client Offering ...	IN PROGRESS
☑ OCDS-200	Client Offering Config - Information Security Plan	IN PROGRESS
☑ OCDS-201	Client Offering Config - Risk Assessment Plan	IN PROGRESS
☑ OCDS-202	Client Offering Config - Cyber Awareness Training	IN PROGRESS
☑ OCDS-203	Client Offering Config - OCDS Cyber Security Chatbot	IN PROGRESS
☑ OCDS-204	Client Offering Config - OCDS Server Hardening Tool	IN PROGRESS
☑ OCDS-205	Client Offering Config - SIEM Adv F/W & Log Analyzer ...	IN PROGRESS

Complete/On Track

Release OCDS Company Website into Production

- Company website URL: https://ocds.tech/
- Hugo & Bootstrap
- **Home**
  - Cybersecurity Consulting
  - Security Assessments
  - Red Team Services
- **About**
  - Mission & Vision Statements
  - Leadership Team
- **Products** – Firewalls, AI Chatbot, SIEMs
- **Services** – Cybersecurity Consulting, Red Team, Security Assessments
- **Training** – 3 modules



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 or ad-hoc or project-based engagements. We work closely with our customers to maximize results.

Security Assessments

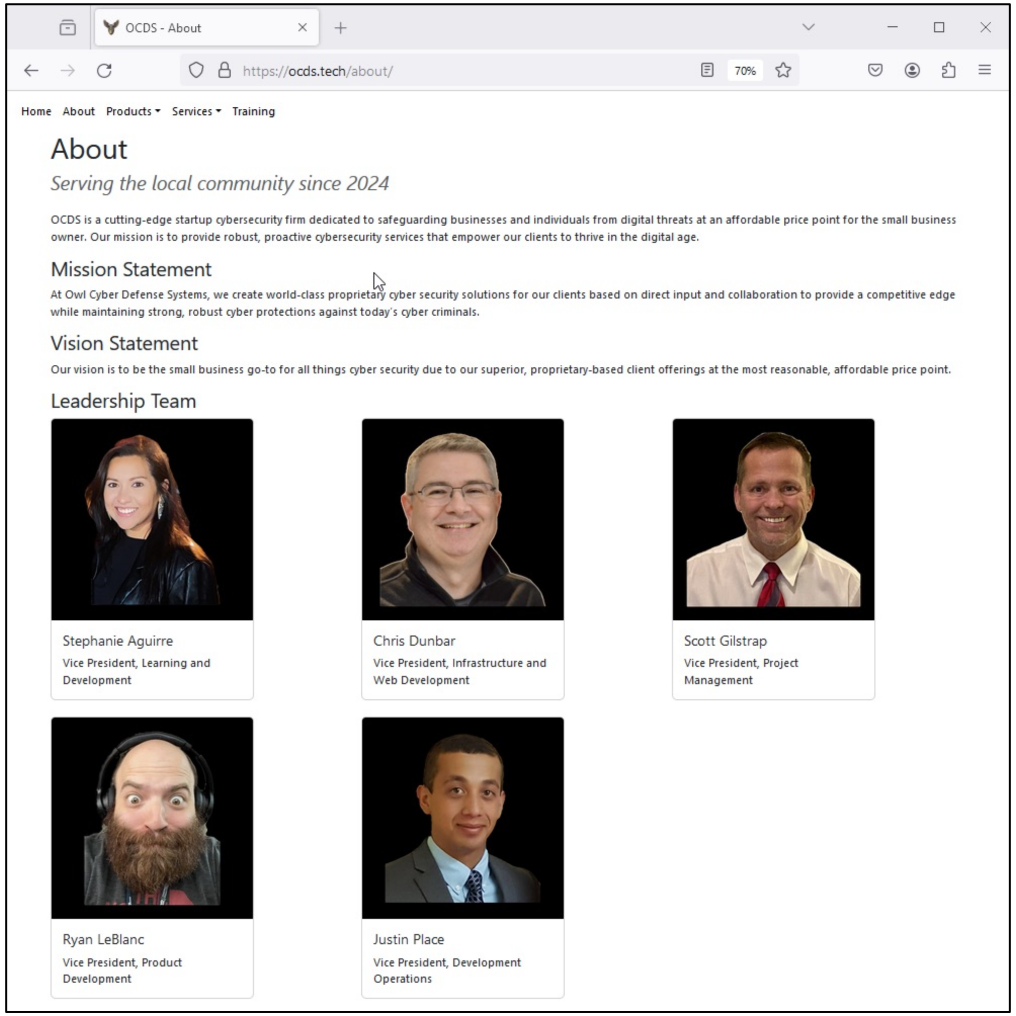
Our detailed security assessments will walk you through the cybersecurity process, and help us better understand your current environment and needs.

Red Team Services

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

Owner: Chris Dunbar

Release OCDS Company Website into Production



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

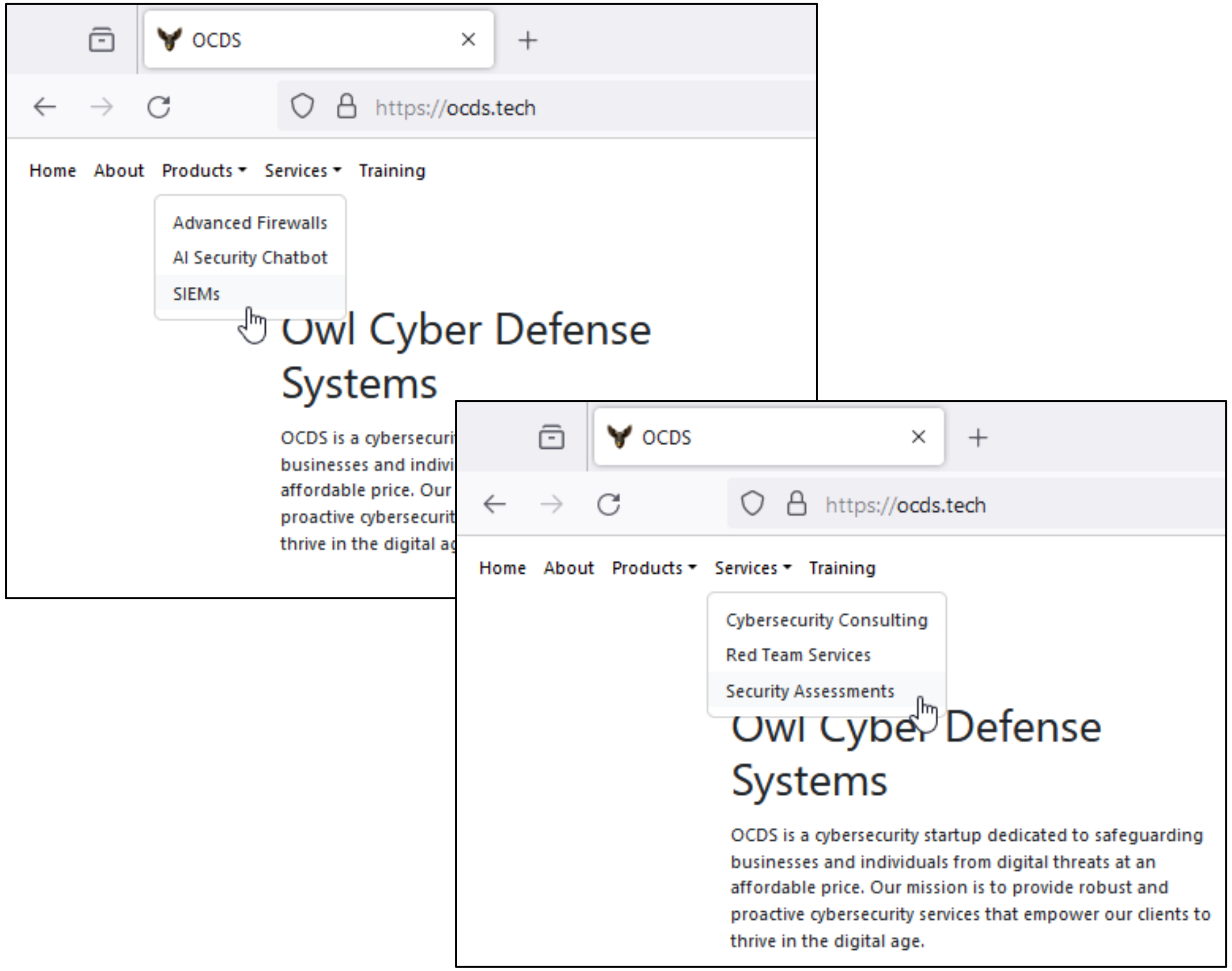
Stephanie Aguirre
Vice President, Learning and Development

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

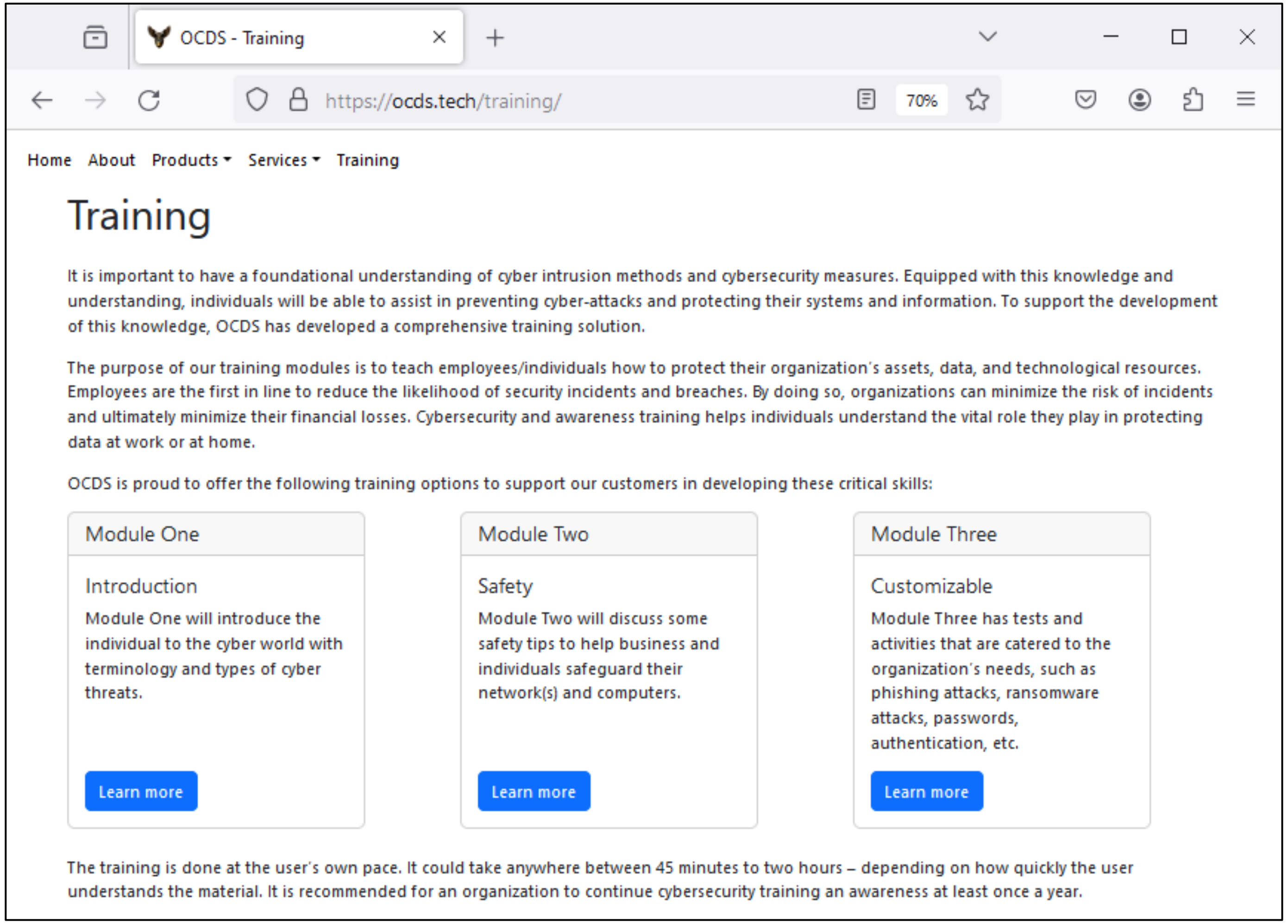


Owl Cyber Defense Systems

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.

Owner: Chris Dunbar

Release OCDS Company Website into Production



OCDS - Training
https://ocds.tech/training/
70%
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

Introduction

Module One will introduce the individual to the cyber world with terminology and types of cyber threats.

Learn more

Module Two

Safety

Module Two will discuss some safety tips to help business and individuals safeguard their network(s) and computers.

Learn more

Module Three

Customizable

Module Three has tests and activities that are catered to the organization's needs, such as phishing attacks, ransomware attacks, passwords, authentication, etc.

Learn more

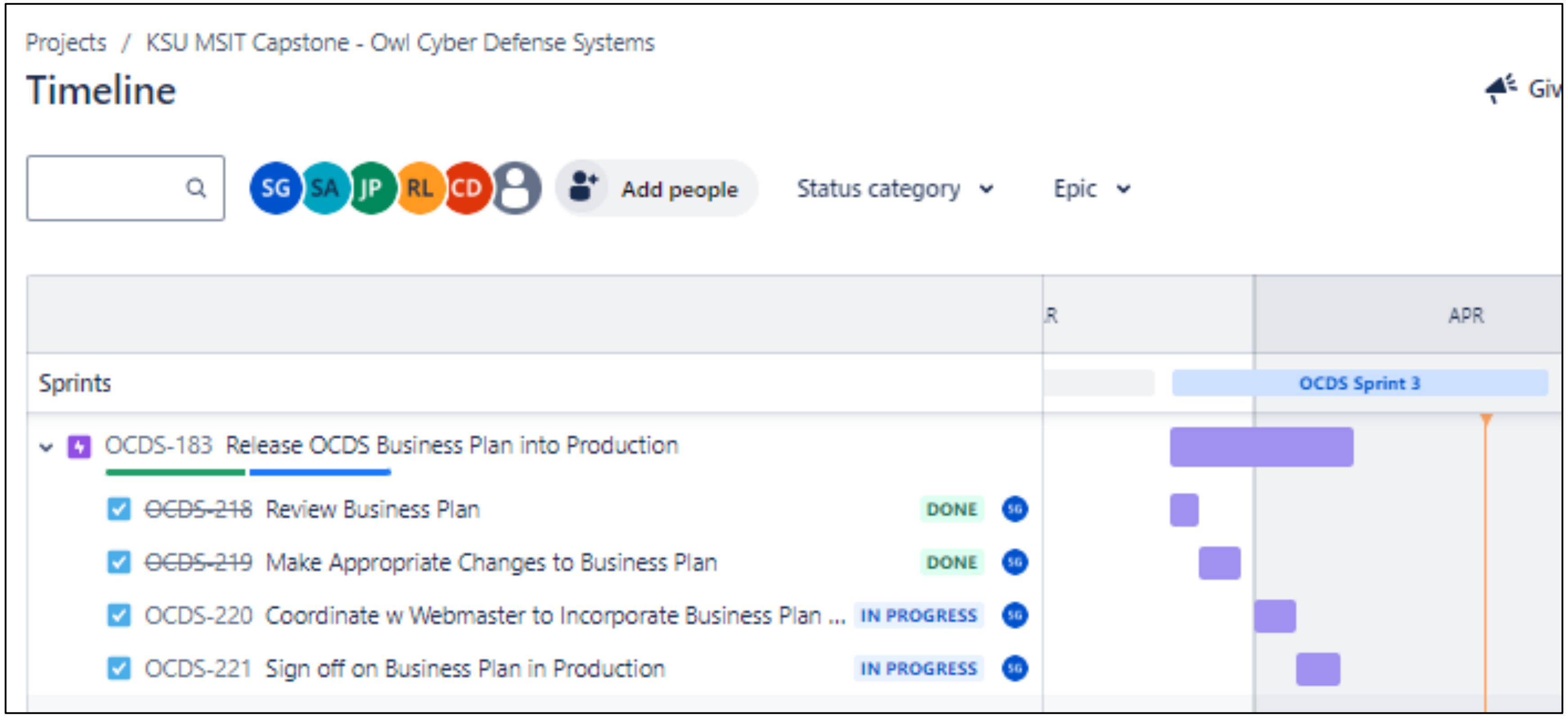
The training is done at the user's own pace. It could take anywhere between 45 minutes to two hours – depending on how quickly the user understands the material. It is recommended for an organization to continue cybersecurity training an awareness at least once a year.

Owner: Chris Dunbar

Epic: Release OCDS Business Plan into Production

Scott Gilstrap

Release OCDS Business Plan into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

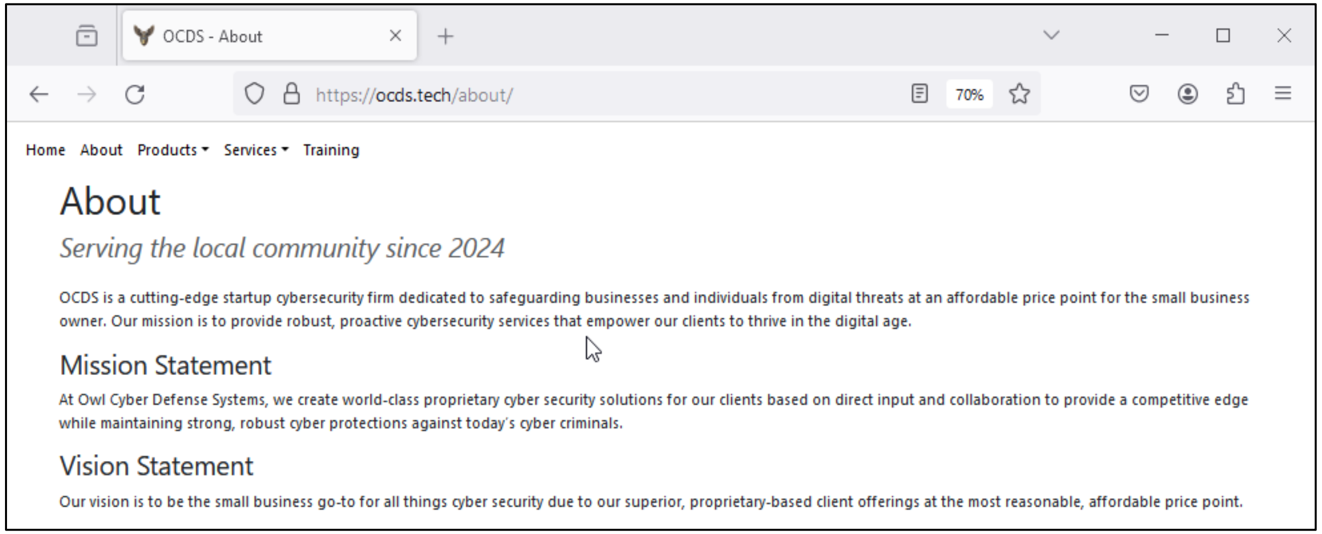
OCDS-183 Release OCDS Business Plan into Production

- ☑ ~~OCDS-218~~ Review Business Plan DONE SG
- ☑ ~~OCDS-219~~ Make Appropriate Changes to Business Plan DONE SG
- ☑ OCDS-220 Coordinate w Webmaster to Incorporate Business Plan ... IN PROGRESS SG
- ☑ OCDS-221 Sign off on Business Plan in Production IN PROGRESS SG

Complete/On Track

Release OCDS Business Plan into Production

- Verified Business Plan is complete (24-page document)
- Worked with Webmaster for the Business Plan to be accessible from the **Project** Website
- Worked with Webmaster to ensure the **Mission** Statement and **Vision** Statement from the Business Plan are displayed on the **Company** Website



About

Serving the local community since 2024

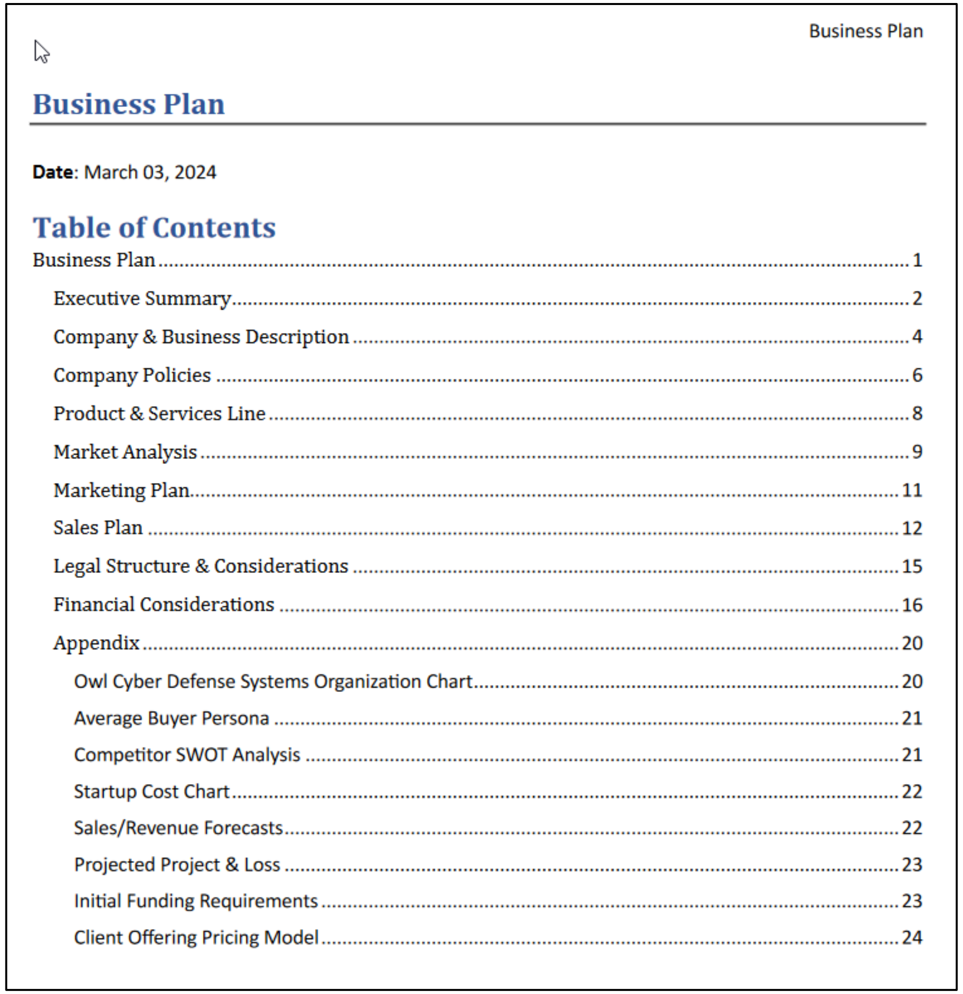
OCDS is a cutting-edge startup cybersecurity firm dedicated to safeguarding businesses and individuals from digital threats at an affordable price point for the small business owner. Our mission is to provide robust, proactive cybersecurity services that empower our clients to thrive in the digital age.

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.


Business Plan

Business Plan

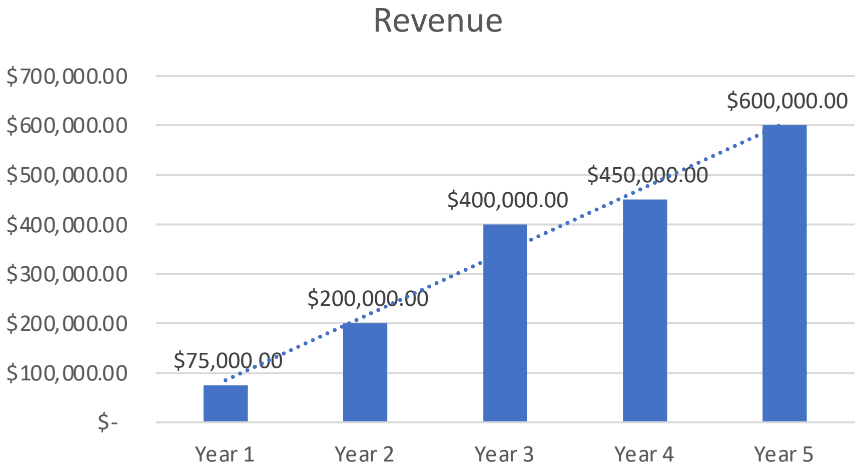
Date: March 03, 2024

Table of Contents

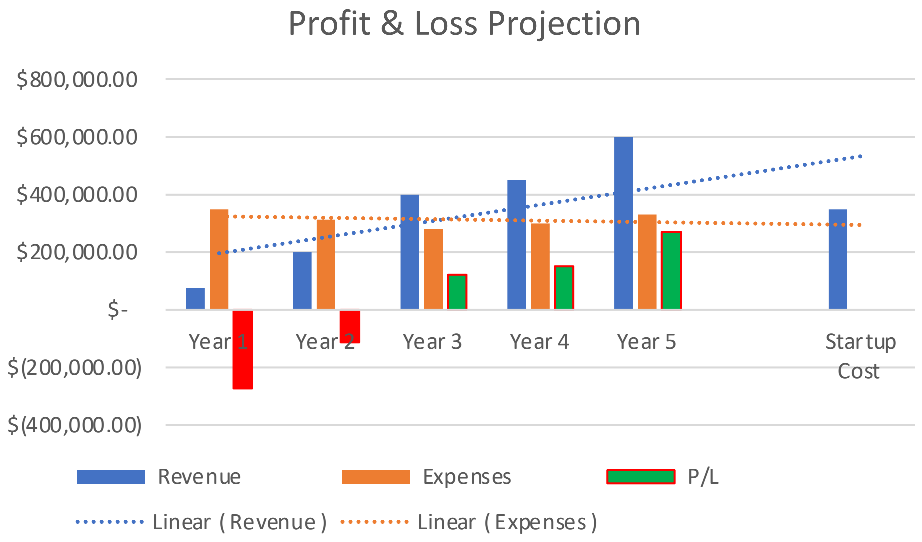
Owner: Scott Gilstrap

Release OCDS Business Plan into Production

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



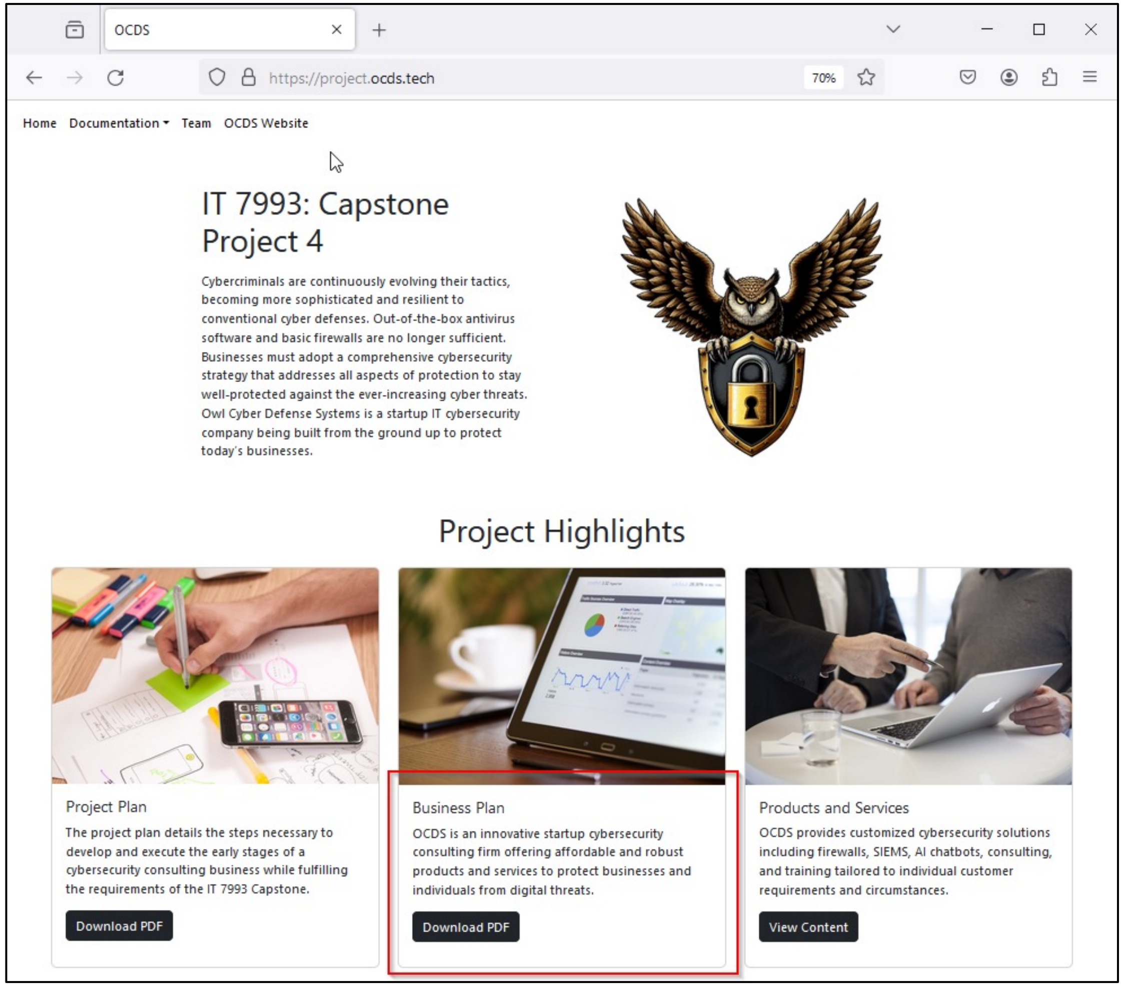
Year	Revenue	Expenses	P/L
Year 1	$ 75,000.00	$ 348,250.00	$(273,250.00)
Year 2	$ 200,000.00	$ 313,425.00	$(113,425.00)
Year 3	$ 400,000.00	$ 278,600.00	$ 121,400.00
Year 4	$ 450,000.00	$ 300,000.00	$ 150,000.00
Year 5	$ 600,000.00	$ 330,000.00	$ 270,000.00
Startup Costs	$ 348,250.00		



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

Owner: Scott Gilstrap

Release OCDS Business Plan into Production



IT 7993: Capstone Project 4

Cybercriminals are continuously evolving their tactics, becoming more sophisticated and resilient to conventional cyber defenses. Out-of-the-box antivirus software and basic firewalls are no longer sufficient. Businesses must adopt a comprehensive cybersecurity strategy that addresses all aspects of protection to stay well-protected against the ever-increasing cyber threats. Owl Cyber Defense Systems is a startup IT cybersecurity company being built from the ground up to protect today's businesses.

Project Highlights

Project Plan

The project plan details the steps necessary to develop and execute the early stages of a cybersecurity consulting business while fulfilling the requirements of the IT 7993 Capstone.

Download PDF

Business Plan

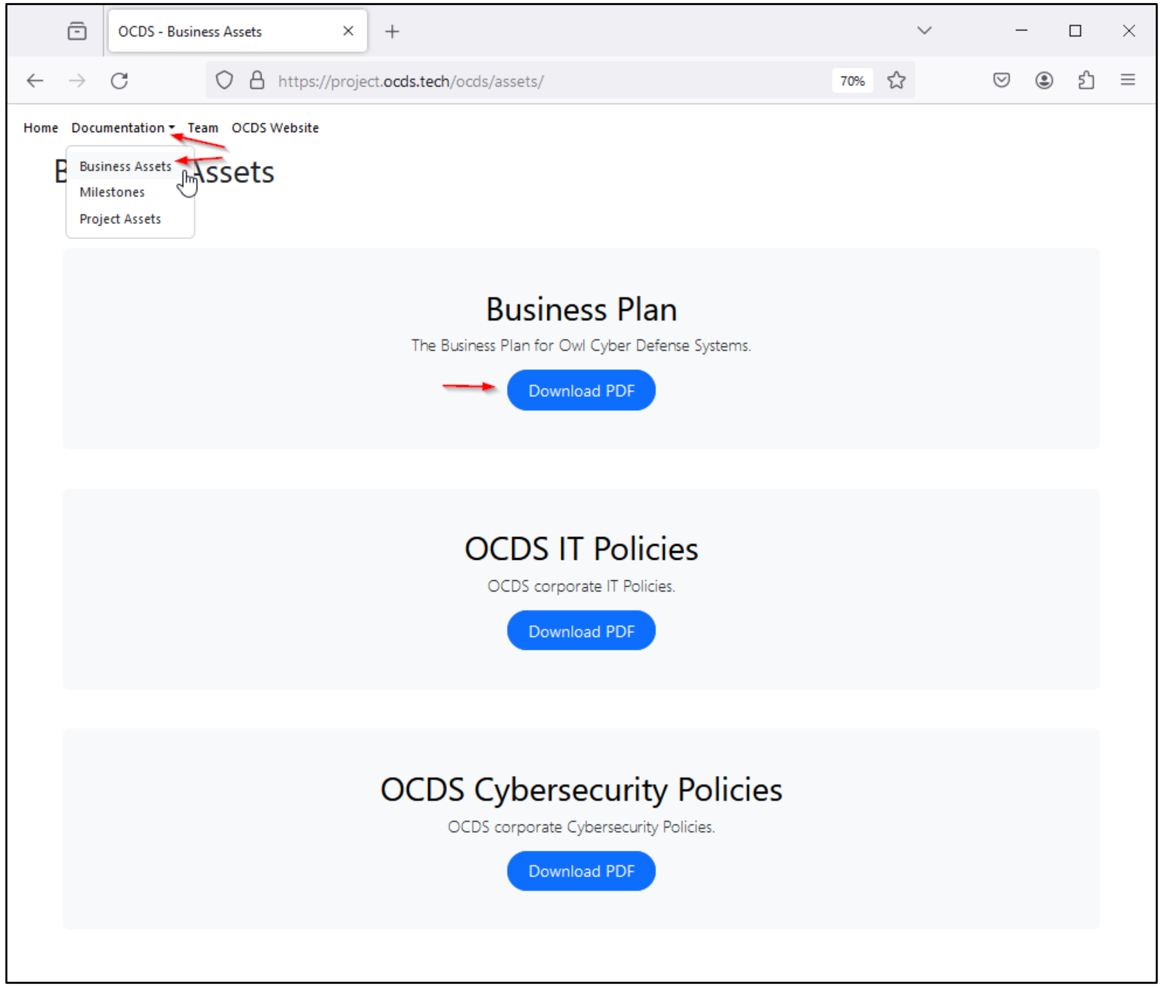
OCDS is an innovative startup cybersecurity consulting firm offering affordable and robust products and services to protect businesses and individuals from digital threats.

Download PDF

Products and Services

OCDS provides customized cybersecurity solutions including firewalls, SIEMS, AI chatbots, consulting, and training tailored to individual customer requirements and circumstances.

View Content



Business Assets

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.

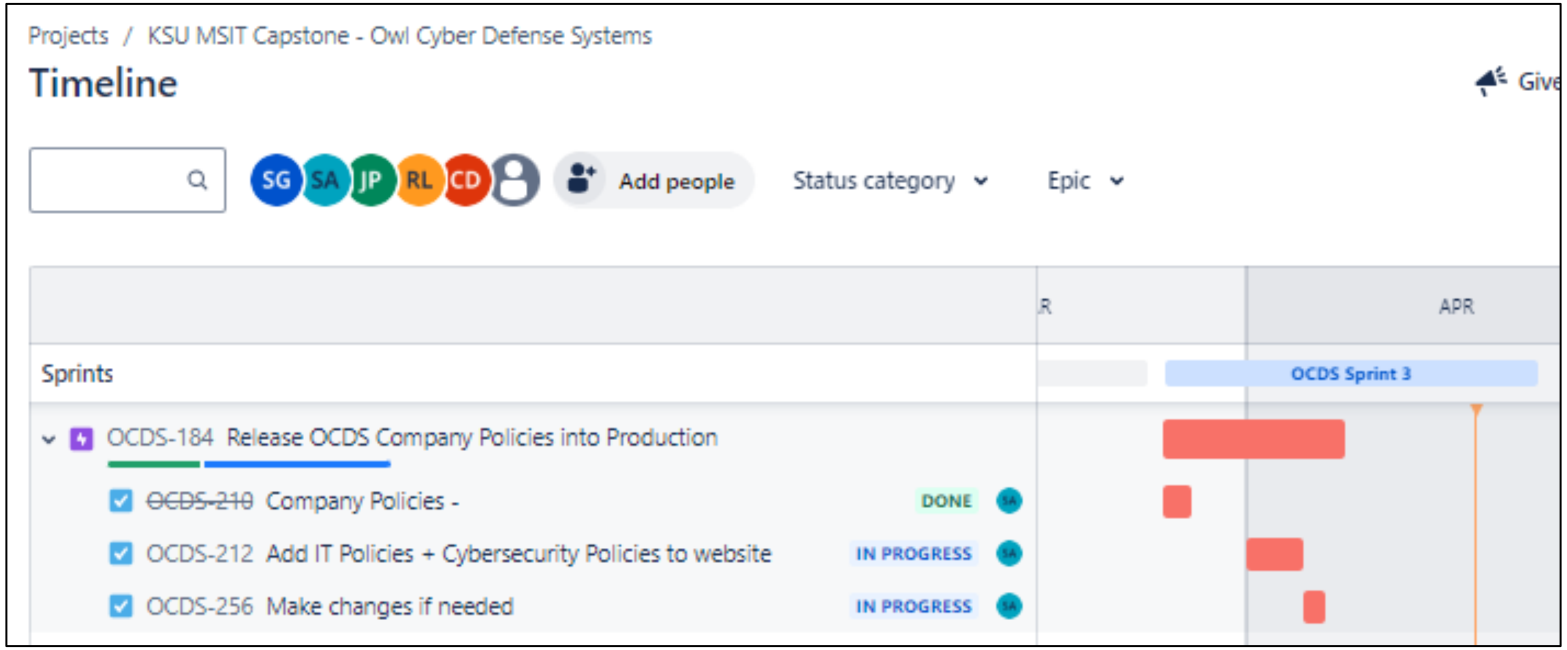
Download PDF

Owner: Scott Gilstrap

Epic: Release OCDS Company Policies into Production

Stephanie Aguirre

Release OCDS Company Policies into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

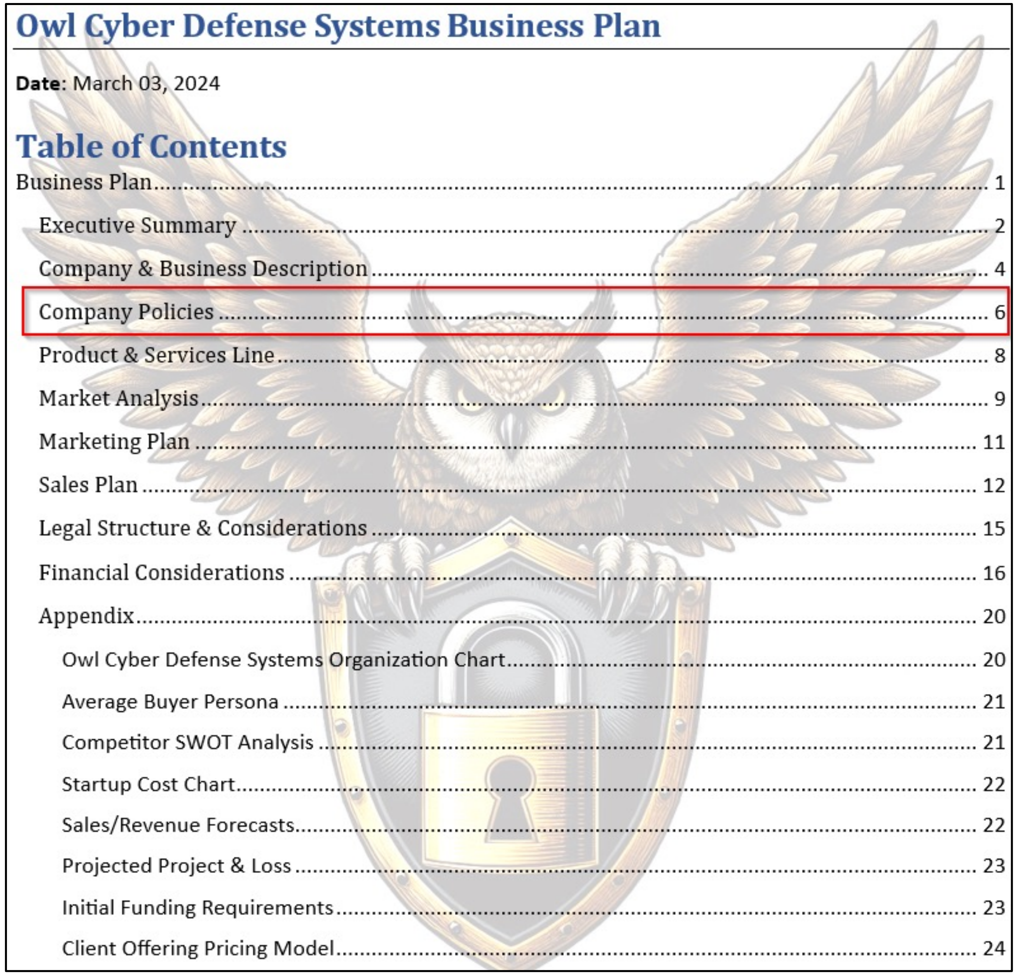
OCDS-184 Release OCDS Company Policies into Production

- ☑ ~~OCDS-210~~ Company Policies - DONE
- ☑ OCDS-212 Add IT Policies + Cybersecurity Policies to website IN PROGRESS
- ☑ OCDS-256 Make changes if needed IN PROGRESS

Complete

Release OCDS Company Policies into Production

- Company policies have been reviewed and successfully completed
- Polices are part of the Business Plan and accessible on the Websites
    - Equal Opportunity
    - Workplace Health & Safety
    - Code of Conduct
    - Attendance & Time Off (PTO)
    - Ethics Policy
    - Substance Abuse
    - Compensation & Benefits
    - Remote Work
    - Access Control
    - AUP – Acceptable Use Policy
- Updated by OCDS each quarter
- Each employee required to read and agree to each year

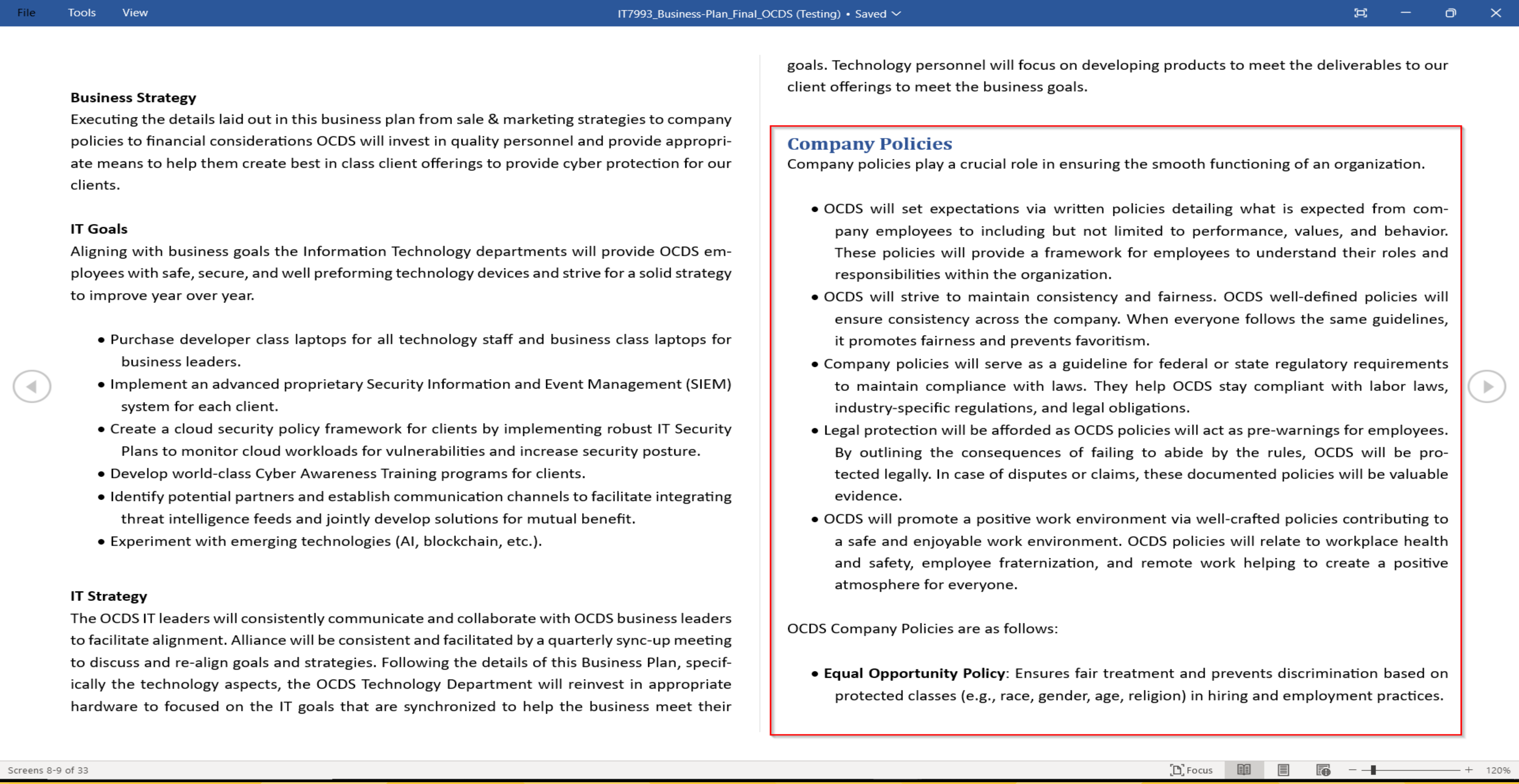


Owl Cyber Defense Systems Business Plan

Date: March 03, 2024

Table of Contents

Owner: Stephanie Aguirre



Business Strategy

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

IT Goals

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

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

IT Strategy

The OCDS IT leaders will consistently communicate and collaborate with OCDS business leaders to facilitate alignment. Alliance will be consistent and facilitated by a quarterly sync-up meeting to discuss and re-align goals and strategies. Following the details of this Business Plan, specifically the technology aspects, the OCDS Technology Department will reinvest in appropriate hardware to focused on the IT goals that are synchronized to help the business meet their goals. Technology personnel will focus on developing products to meet the deliverables to our client offerings to meet the business goals.

Company Policies

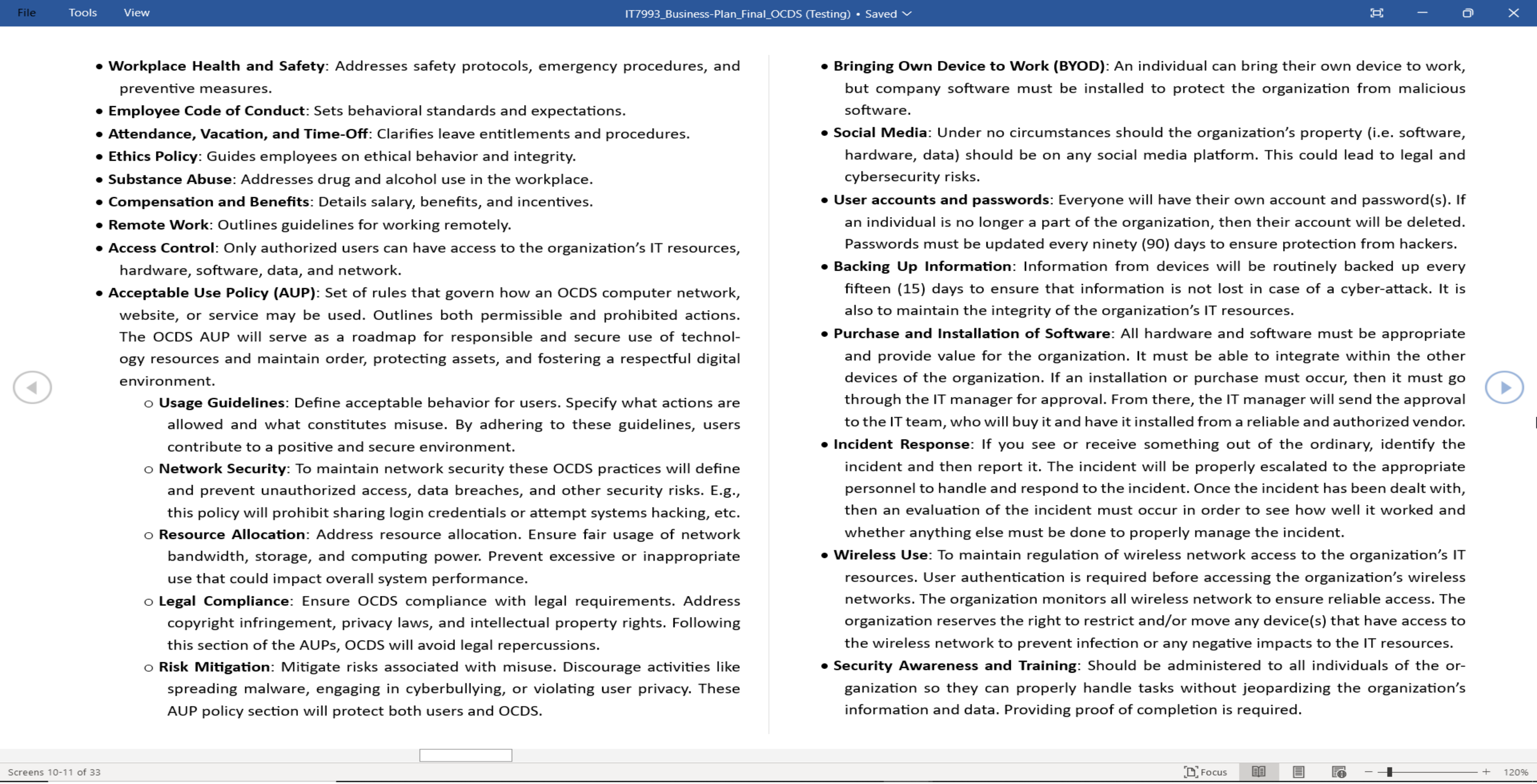
Company policies play a crucial role in ensuring the smooth functioning of an organization.

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

OCDS Company Policies are as follows:

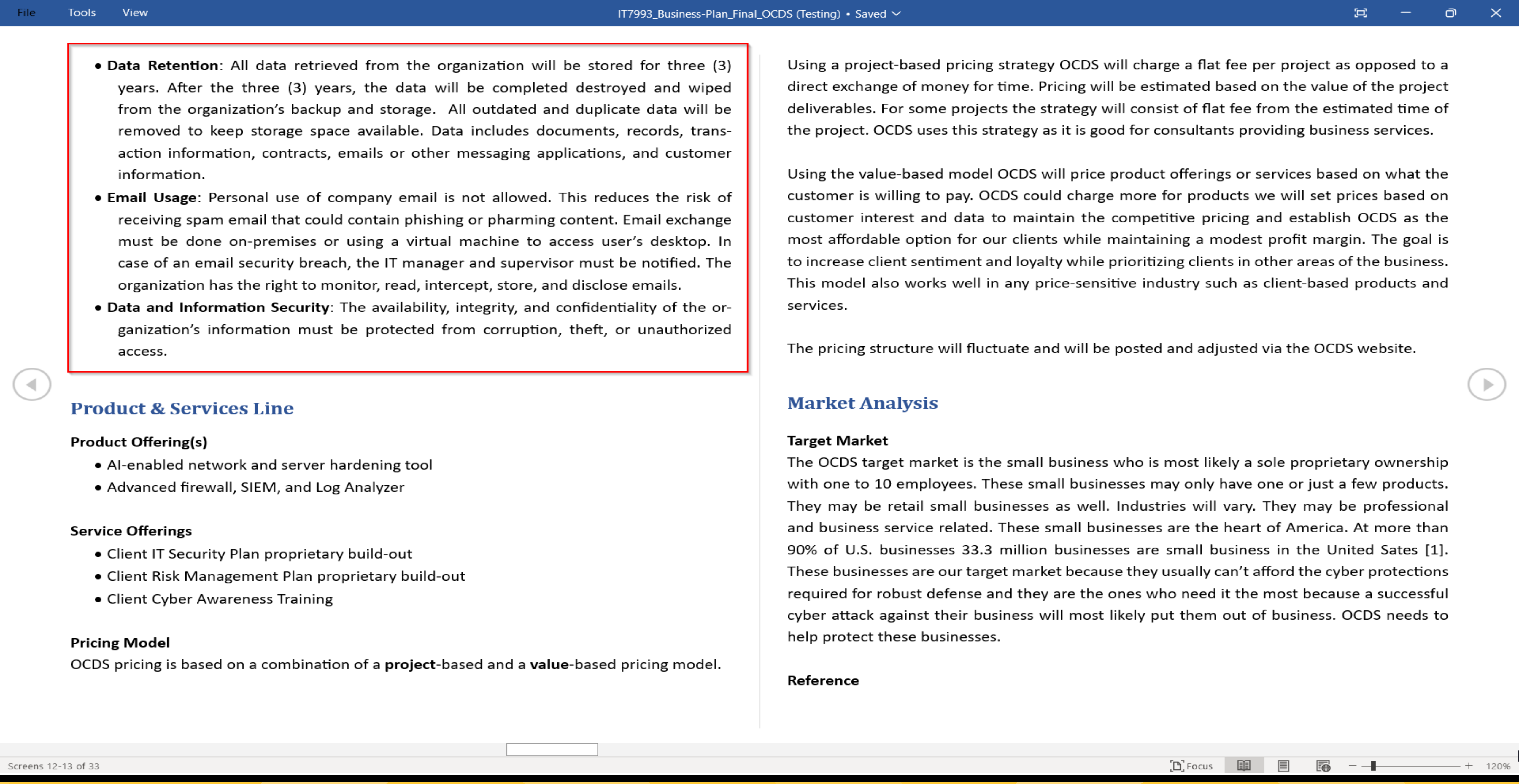
- **Equal Opportunity Policy**: Ensures fair treatment and prevents discrimination based on protected classes (e.g., race, gender, age, religion) in hiring and employment practices.

Owner: Stephanie Aguirre



- **Workplace Health and Safety**: Addresses safety protocols, emergency procedures, and preventive measures.
- **Employee Code of Conduct**: Sets behavioral standards and expectations.
- **Attendance, Vacation, and Time-Off**: Clarifies leave entitlements and procedures.
- **Ethics Policy**: Guides employees on ethical behavior and integrity.
- **Substance Abuse**: Addresses drug and alcohol use in the workplace.
- **Compensation and Benefits**: Details salary, benefits, and incentives.
- **Remote Work**: Outlines guidelines for working remotely.
- **Access Control**: Only authorized users can have access to the organization's IT resources, hardware, software, data, and network.
- **Acceptable Use Policy (AUP)**: Set of rules that govern how an OCDS computer network, website, or service may be used. Outlines both permissible and prohibited actions. The OCDS AUP will serve as a roadmap for responsible and secure use of technology resources and maintain order, protecting assets, and fostering a respectful digital environment.
  - **Usage Guidelines**: Define acceptable behavior for users. Specify what actions are allowed and what constitutes misuse. By adhering to these guidelines, users contribute to a positive and secure environment.
  - **Network Security**: To maintain network security these OCDS practices will define and prevent unauthorized access, data breaches, and other security risks. E.g., this policy will prohibit sharing login credentials or attempt systems hacking, etc.
  - **Resource Allocation**: Address resource allocation. Ensure fair usage of network bandwidth, storage, and computing power. Prevent excessive or inappropriate use that could impact overall system performance.
  - **Legal Compliance**: Ensure OCDS compliance with legal requirements. Address copyright infringement, privacy laws, and intellectual property rights. Following this section of the AUPs, OCDS will avoid legal repercussions.
  - **Risk Mitigation**: Mitigate risks associated with misuse. Discourage activities like spreading malware, engaging in cyberbullying, or violating user privacy. These AUP policy section will protect both users and OCDS.
- **Bringing Own Device to Work (BYOD)**: An individual can bring their own device to work, but company software must be installed to protect the organization from malicious software.
- **Social Media**: Under no circumstances should the organization's property (i.e. software, hardware, data) should be on any social media platform. This could lead to legal and cybersecurity risks.
- **User accounts and passwords**: Everyone will have their own account and password(s). If an individual is no longer a part of the organization, then their account will be deleted. Passwords must be updated every ninety (90) days to ensure protection from hackers.
- **Backing Up Information**: Information from devices will be routinely backed up every fifteen (15) days to ensure that information is not lost in case of a cyber-attack. It is also to maintain the integrity of the organization's IT resources.
- **Purchase and Installation of Software**: All hardware and software must be appropriate and provide value for the organization. It must be able to integrate within the other devices of the organization. If an installation or purchase must occur, then it must go through the IT manager for approval. From there, the IT manager will send the approval to the IT team, who will buy it and have it installed from a reliable and authorized vendor.
- **Incident Response**: If you see or receive something out of the ordinary, identify the incident and then report it. The incident will be properly escalated to the appropriate personnel to handle and respond to the incident. Once the incident has been dealt with, then an evaluation of the incident must occur in order to see how well it worked and whether anything else must be done to properly manage the incident.
- **Wireless Use**: To maintain regulation of wireless network access to the organization's IT resources. User authentication is required before accessing the organization's wireless networks. The organization monitors all wireless network to ensure reliable access. The organization reserves the right to restrict and/or move any device(s) that have access to the wireless network to prevent infection or any negative impacts to the IT resources.
- **Security Awareness and Training**: Should be administered to all individuals of the organization so they can properly handle tasks without jeopardizing the organization's information and data. Providing proof of completion is required.

Owner: Stephanie Aguirre



- **Data Retention**: All data retrieved from the organization will be stored for three (3) years. After the three (3) years, the data will be completed destroyed and wiped from the organization's backup and storage. All outdated and duplicate data will be removed to keep storage space available. Data includes documents, records, transaction information, contracts, emails or other messaging applications, and customer information.
- **Email Usage**: Personal use of company email is not allowed. This reduces the risk of receiving spam email that could contain phishing or pharming content. Email exchange must be done on-premises or using a virtual machine to access user's desktop. In case of an email security breach, the IT manager and supervisor must be notified. The organization has the right to monitor, read, intercept, store, and disclose emails.
- **Data and Information Security**: The availability, integrity, and confidentiality of the organization's information must be protected from corruption, theft, or unauthorized access.

Product & Services Line

Product Offering(s)

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

Service Offerings

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

Pricing Model

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

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

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

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

Market Analysis

Target Market

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

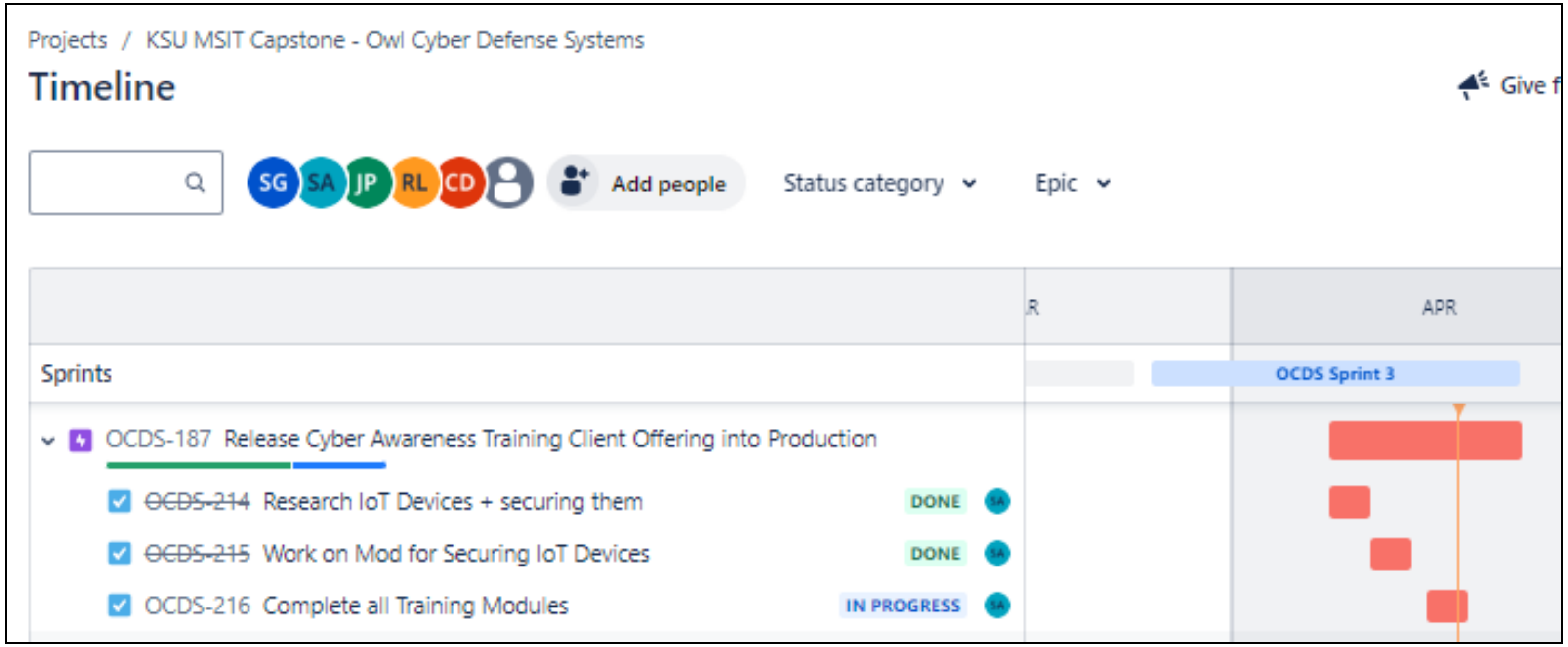
Reference

Owner: Stephanie Aguirre

Epic: Release Cyber Awareness Training Client Offering into Production

Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Sprints

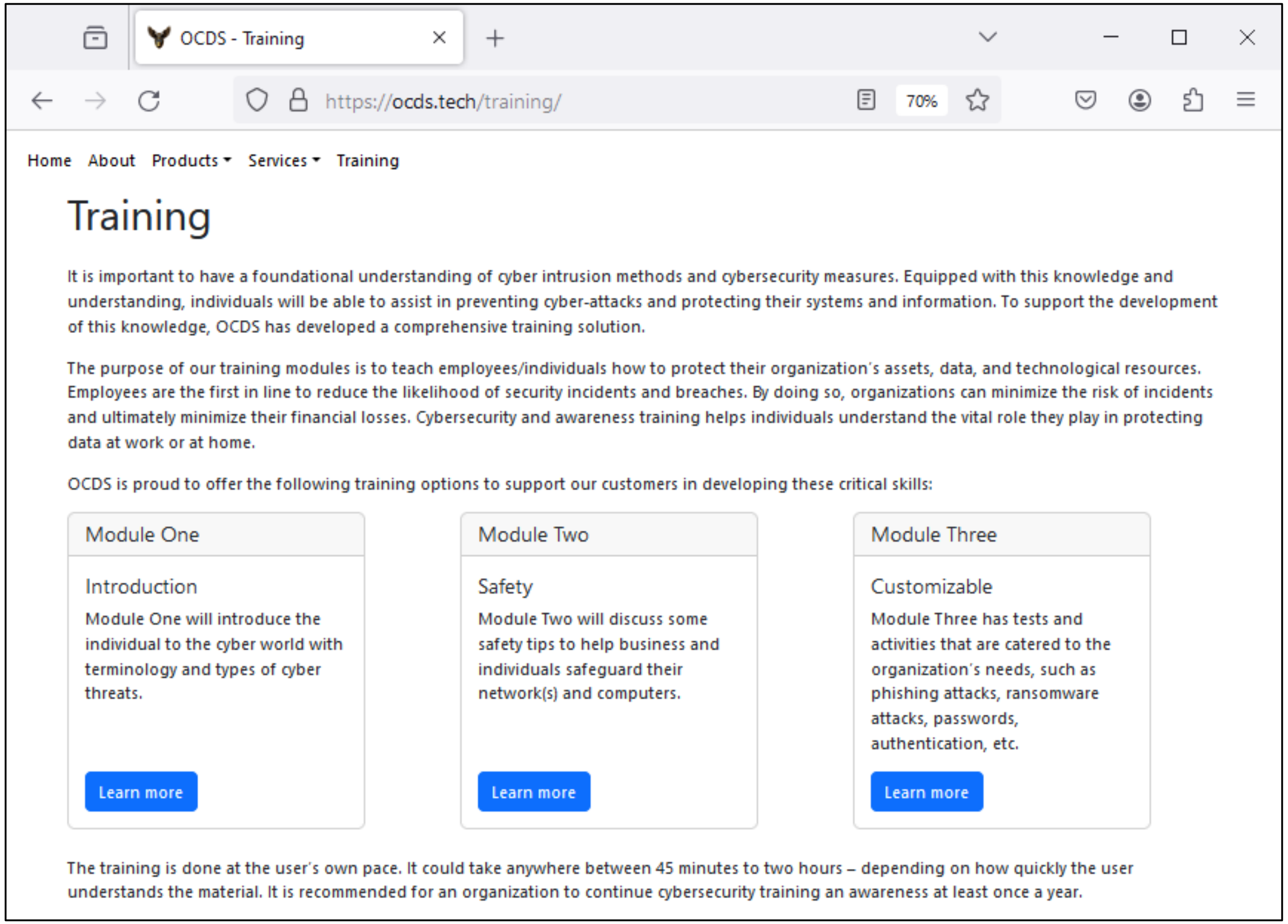
OCDS-187 Release Cyber Awareness Training Client Offering into Production

- ☑ ~~OCDS-214~~ Research IoT Devices + securing them DONE SA
- ☑ ~~OCDS-215~~ Work on Mod for Securing IoT Devices DONE SA
- ☑ OCDS-216 Complete all Training Modules IN PROGRESS SA

On Track – no risks

Release Cyber Awareness Training Client Offering into Production

- Employees of small businesses experience 350% more social engineering attacks than those at larger enterprises.
- OCDS offers three training modules
  1) **Module 1**: Introduction – terminology and types of threats
  2) **Module 2**: Safety and cyber attack prevention.
  3) **Module 3**: Customized per client with activities and tests.
- Proprietary Cyber Awareness Training prepare specifically for Scrappy Tax Service
  - [CyberSecurity_Training_for_Scrappy-Tax-Service.pptx (sharepoint.com)]



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

Introduction

Module One will introduce the individual to the cyber world with terminology and types of cyber threats.

Learn more

Module Two

Safety

Module Two will discuss some safety tips to help business and individuals safeguard their network(s) and computers.

Learn more

Module Three

Customizable

Module Three has tests and activities that are catered to the organization's needs, such as phishing attacks, ransomware attacks, passwords, authentication, etc.

Learn more

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.

Owner: Stephanie Aguirre

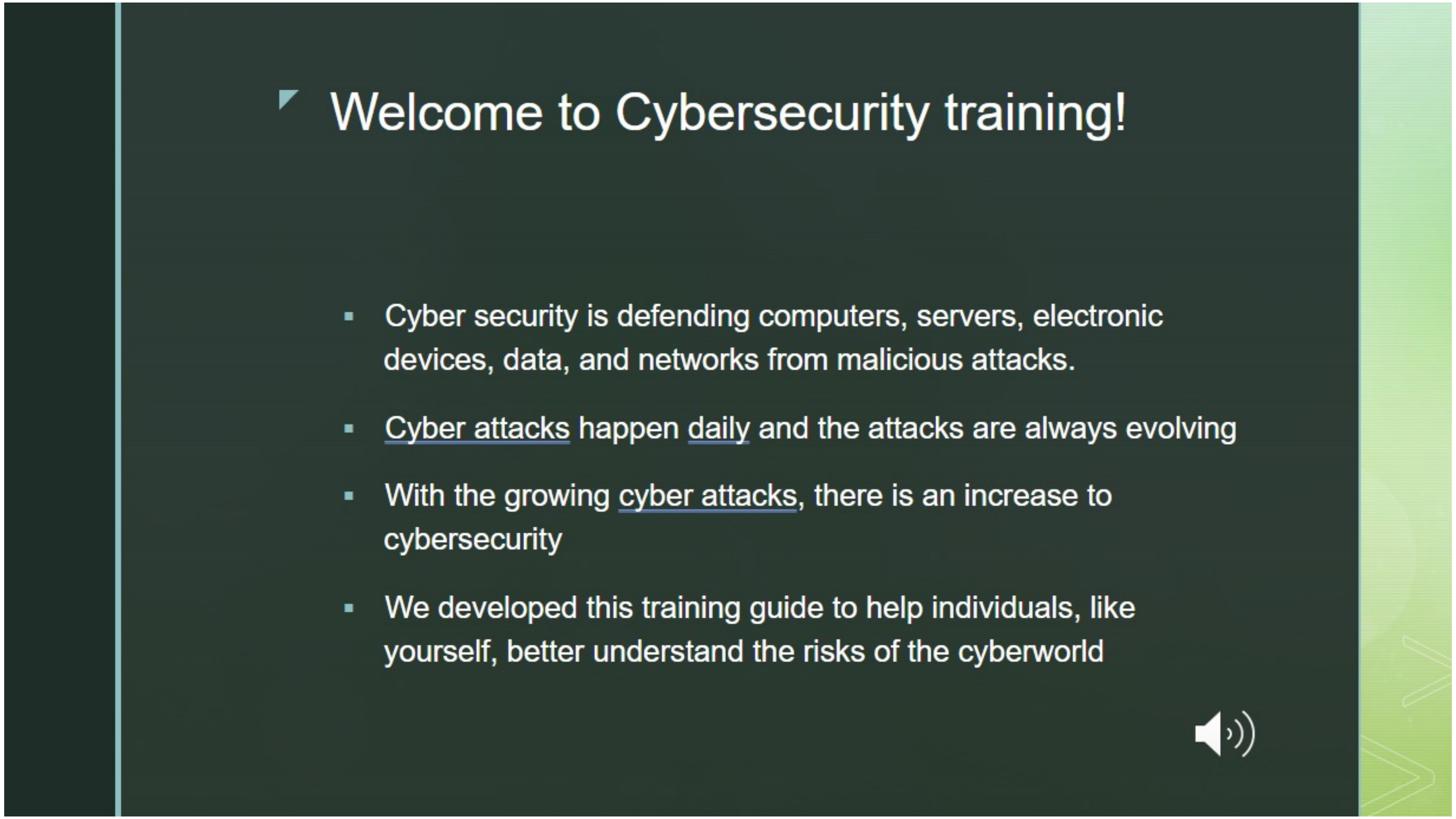
Release Cyber Awareness Training Client Offering into Production

Scrappy Tax Service

Cybersecurity Training

Owner: Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production

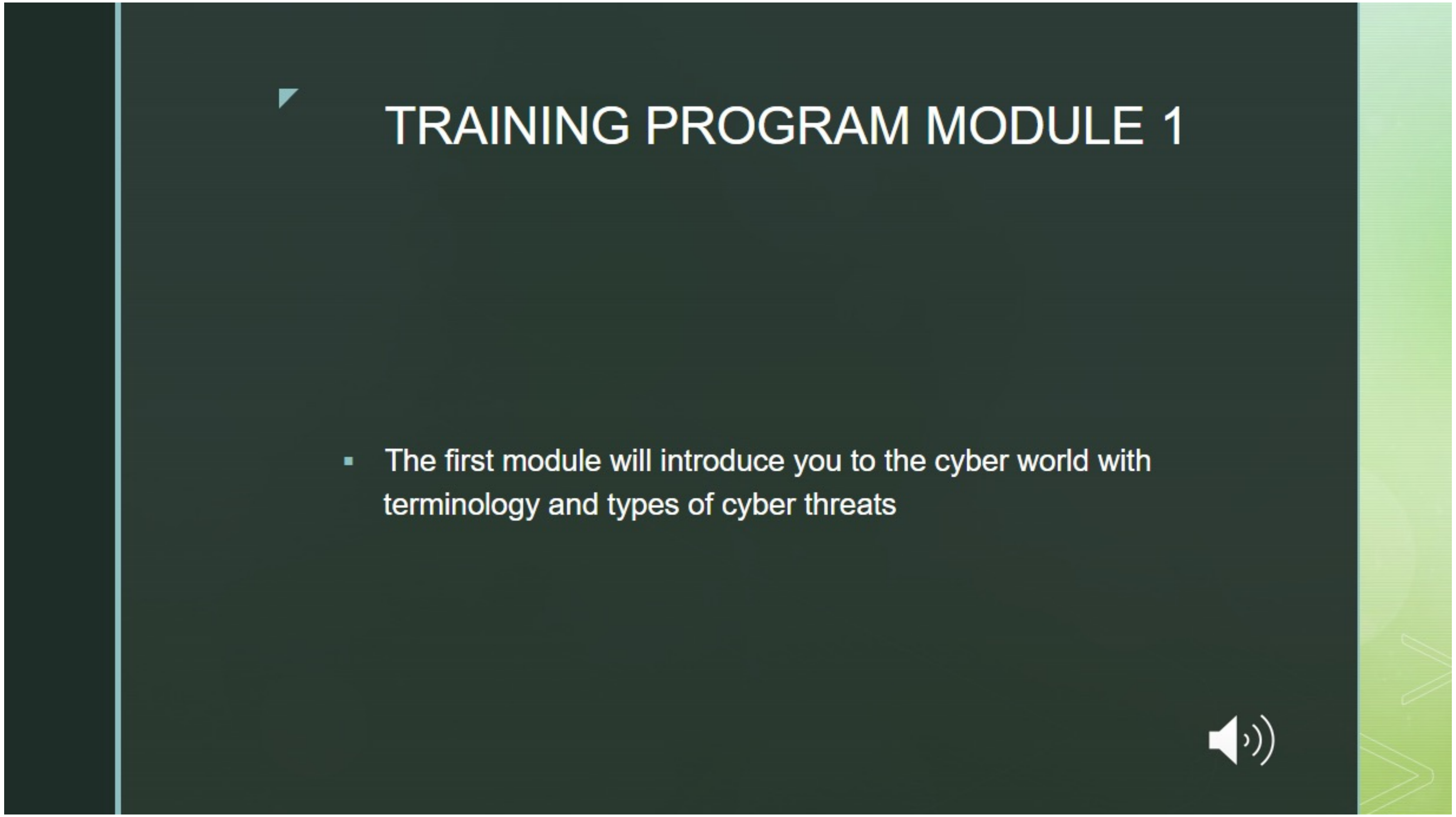


Welcome to Cybersecurity training!

- 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

Owner: Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production

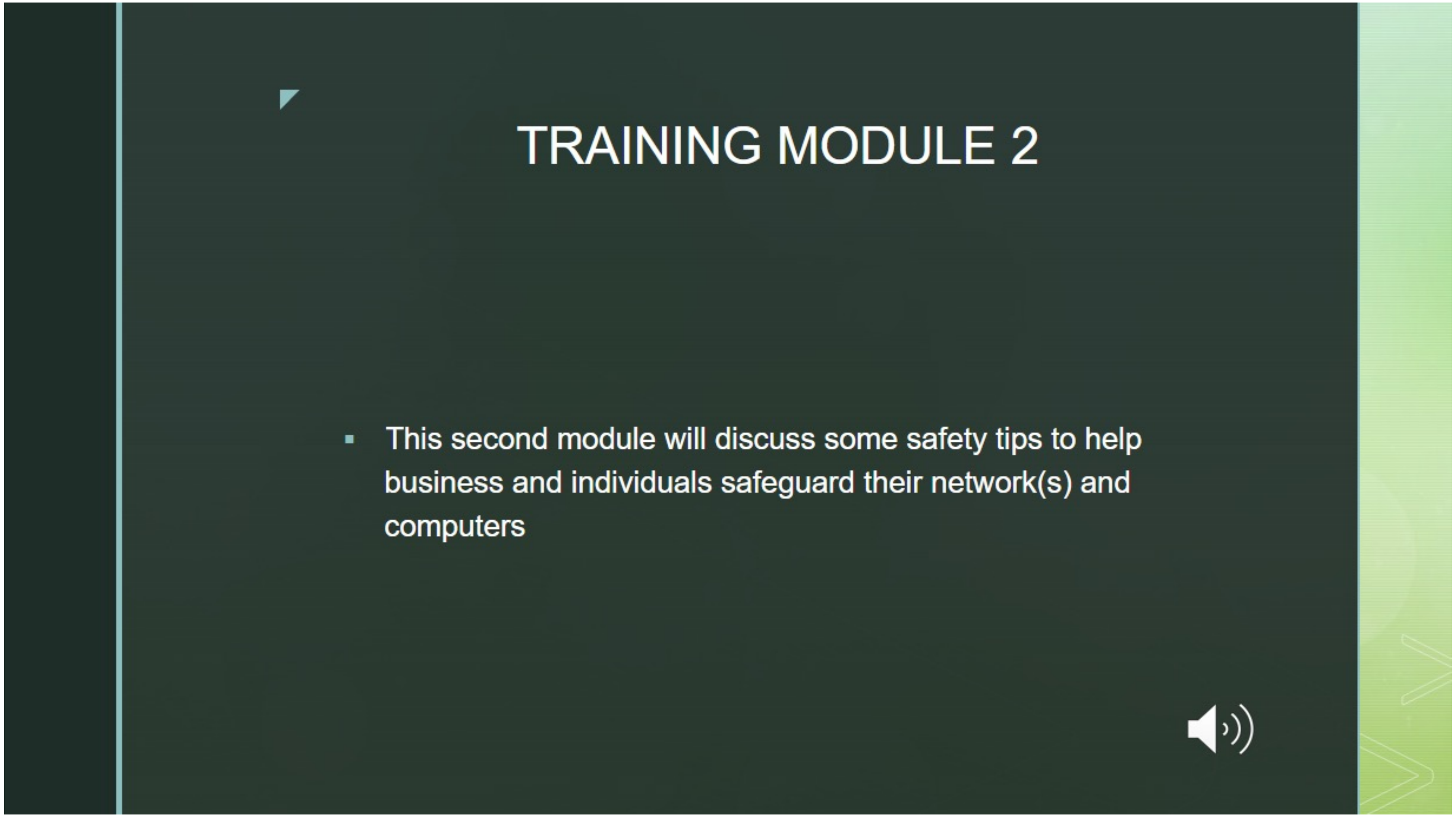


TRAINING PROGRAM MODULE 1

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

Owner: Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production

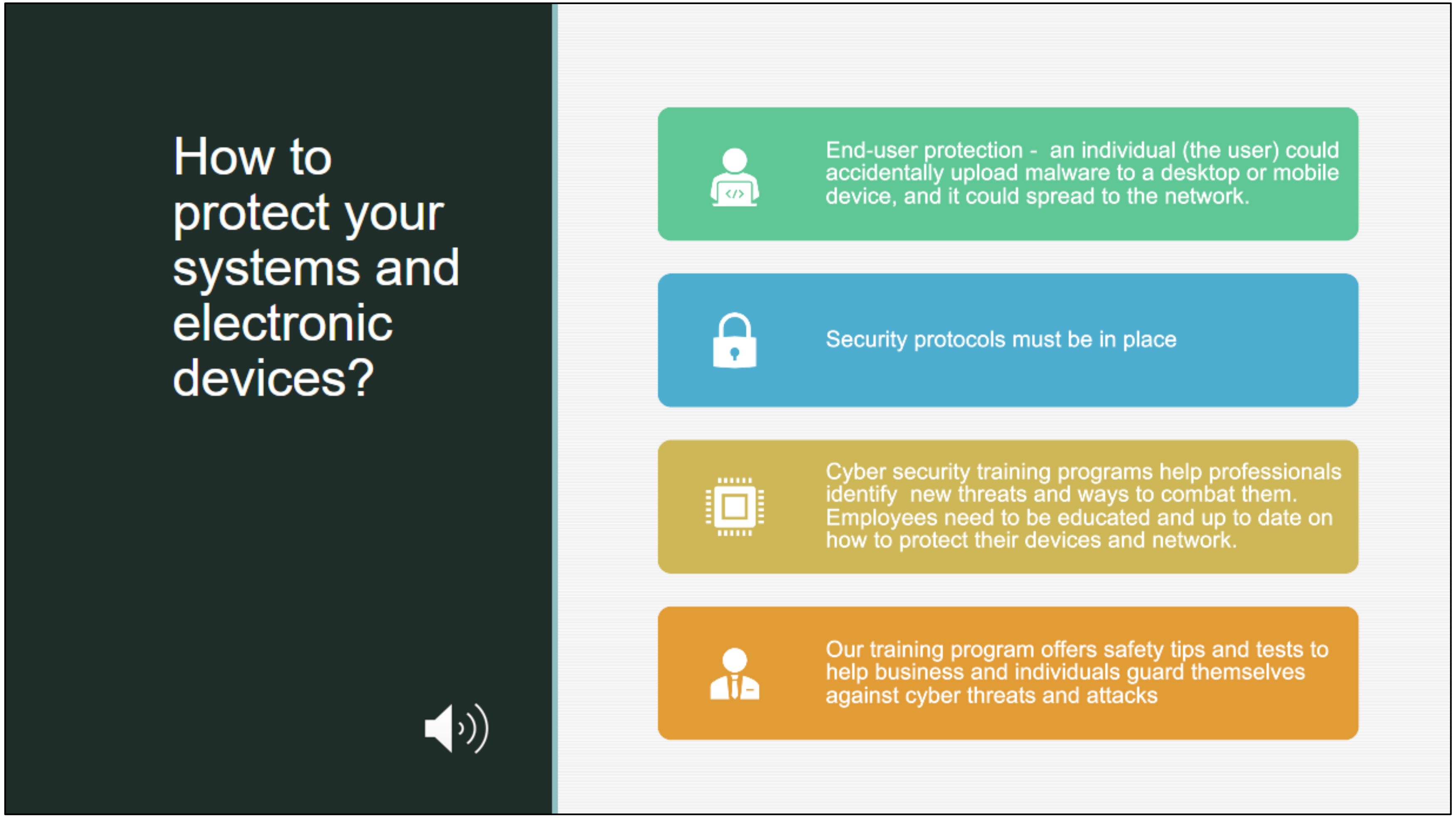


TRAINING MODULE 2

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

Owner: Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production



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.

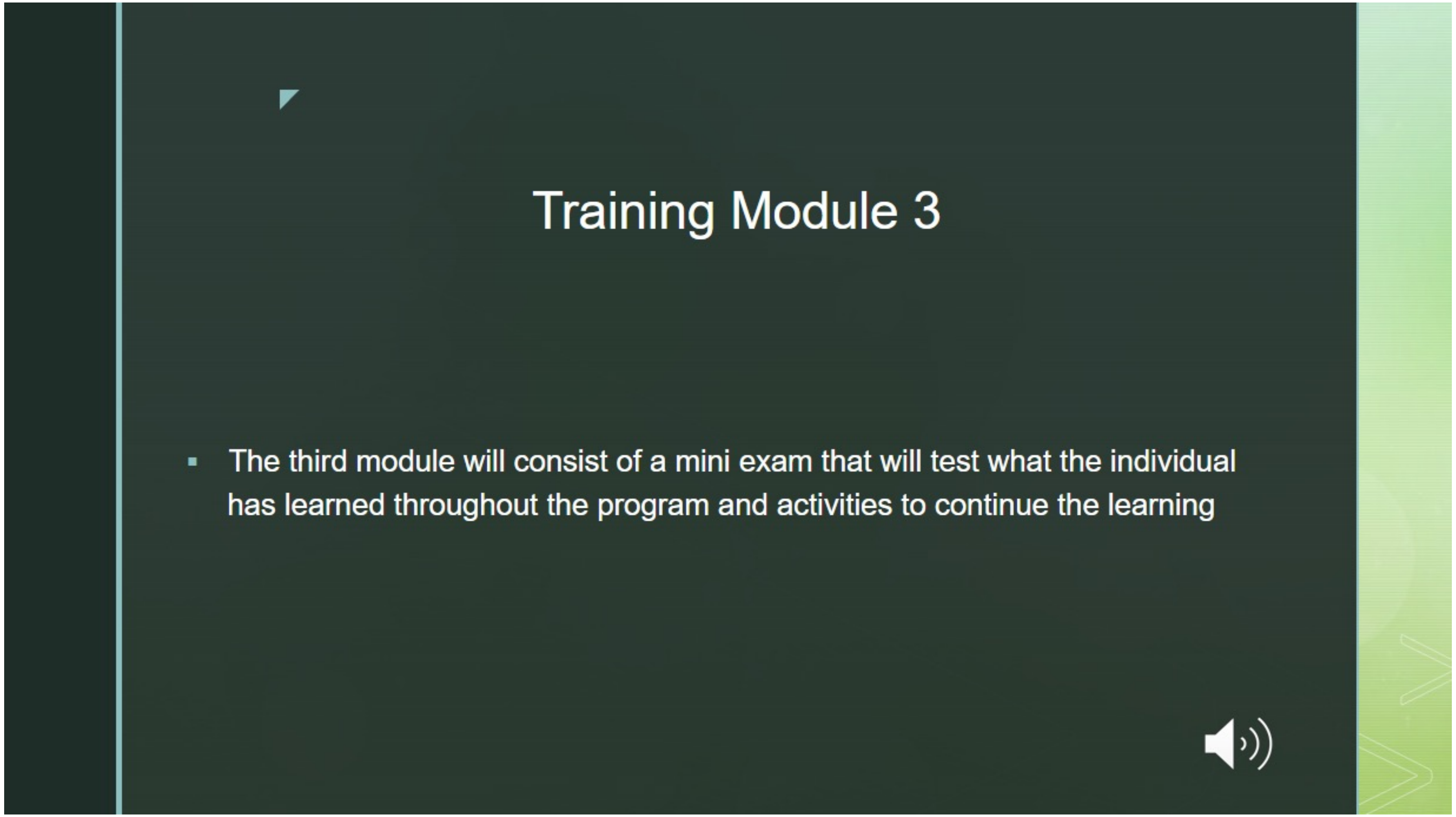
Security protocols must be in place

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

Owner: Stephanie Aguirre

Release Cyber Awareness Training Client Offering into Production



Training Module 3

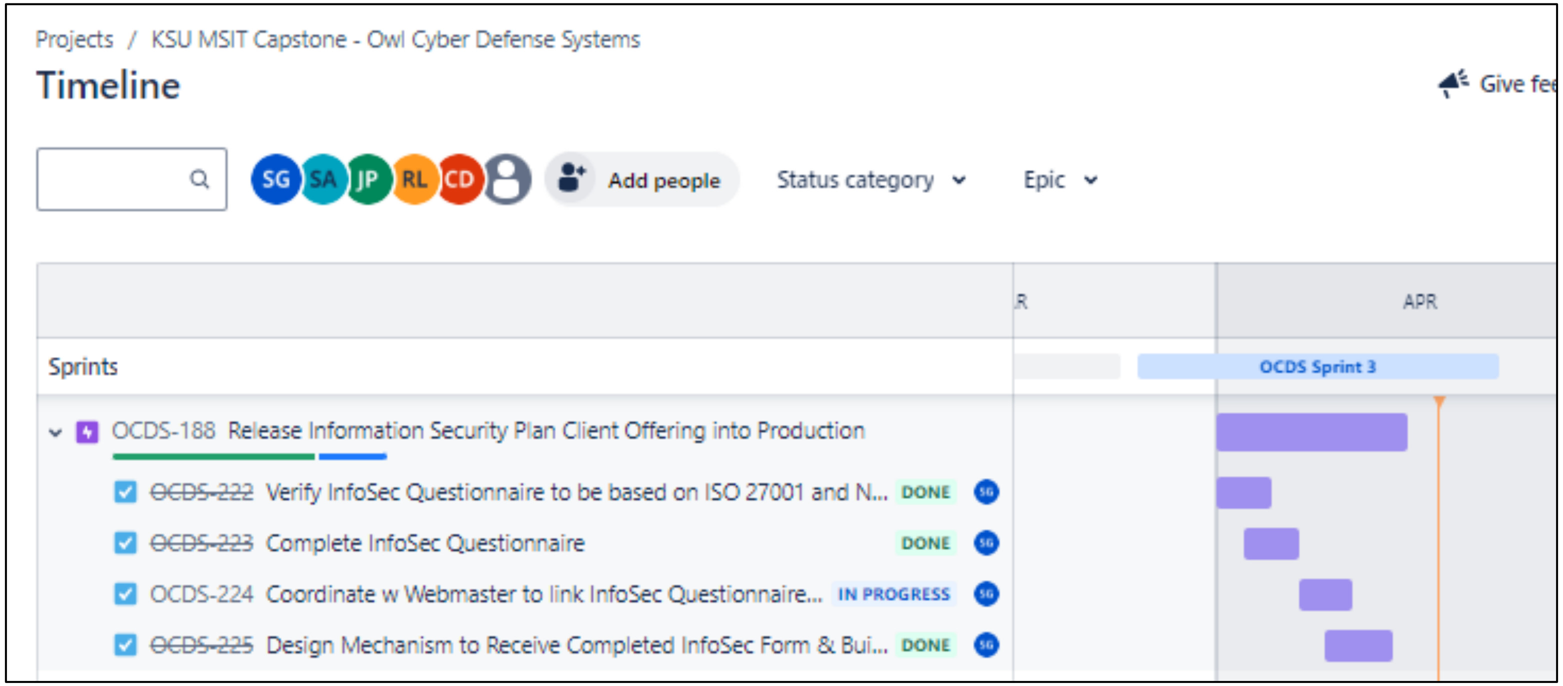
- The third module will consist of a mini exam that will test what the individual has learned throughout the program and activities to continue the learning

Owner: Stephanie Aguirre

Epic: Release Information Security Plan Client Offering into Production

Scott Gilstrap

Release Information Security Plan Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

OCDS-188 Release Information Security Plan Client Offering into Production

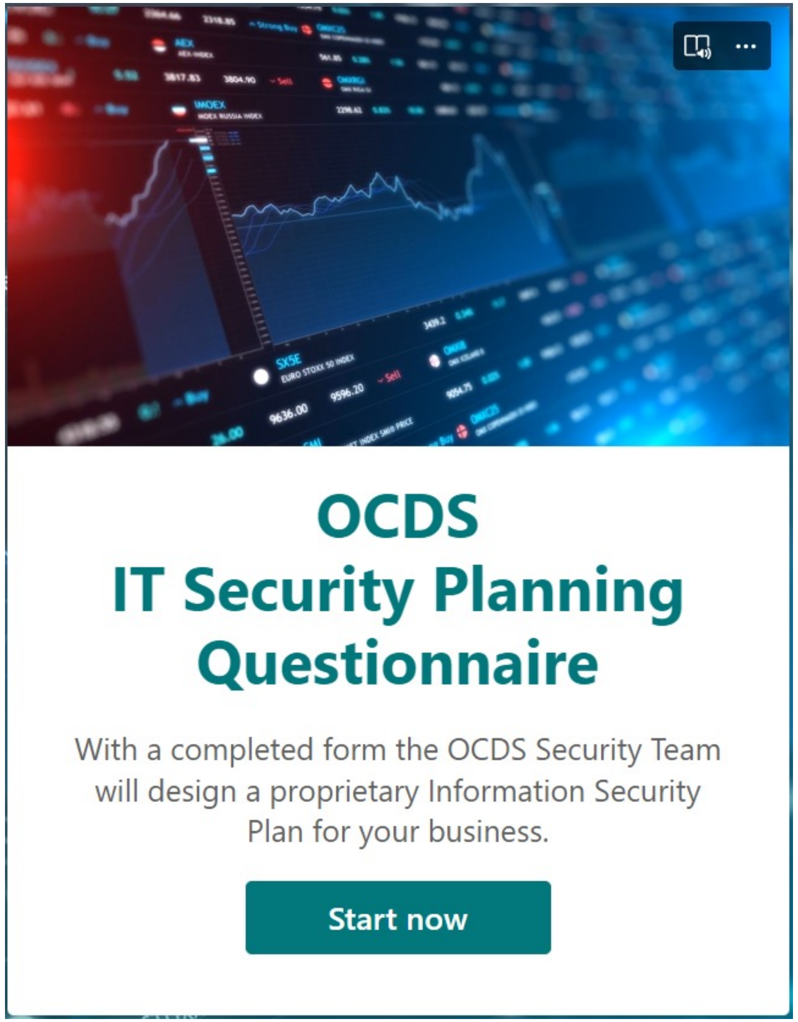
- ☑ ~~OCDS-222~~ Verify InfoSec Questionnaire to be based on ISO 27001 and N... DONE SG
- ☑ ~~OCDS-223~~ Complete InfoSec Questionnaire DONE SG
- ☑ OCDS-224 Coordinate w Webmaster to link InfoSec Questionnaire... IN PROGRESS SG
- ☑ ~~OCDS-225~~ Design Mechanism to Receive Completed InfoSec Form & Bui... DONE SG

Complete/On Track

Release Information Security Plan Client Offering into Production

- Completed and deployed the IT Security Planning Questionnaire into Production
- Based questions and data collection on two primary information security standards
  - **NIST 800-53** – Standards for Security and Privacy Controls
  - **ISO 27001** – Information Security Management System (ISMS)
- 17 Sections
- 27 Questions
- 10 File Upload Points
  - Supporting Documentation

OCDS IT Security Planning Questionnaire



OCDS IT Security Planning Questionnaire

With a completed form the OCDS Security Team will design a proprietary Information Security Plan for your business.

- https://forms.office.com/r/6jnRL8eX8j?origin=lprLink

Owner: Scott Gilstrap

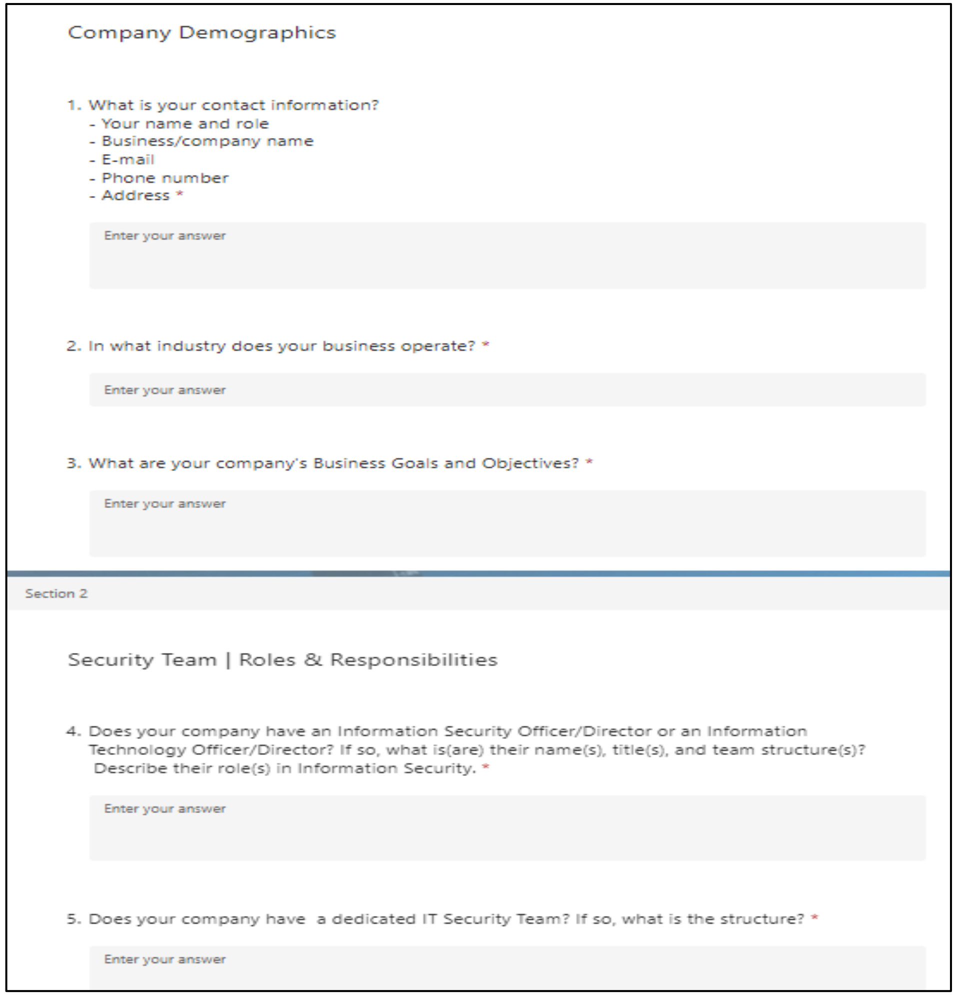
Release Information Security Plan Client Offering into Production

- Overall Process
  - **Determine all company Assets**
  - **Identify vulnerabilities with each asset**
  - Threat analysis
    - Identify threats to each vulnerability
    - Assess threat impact to company if vulnerability is exploited
    - Assess the likelihood of the threat exploiting each vulnerability
  - Calculate the Level of Risk
  - Determine acceptability of Risk
  - If not acceptable identify treatment options using security controls to mitigate the Risk
  - Create Risk Assessment & Treatment Plan
  - Create Statement of Acceptance
    - Addressing residual risks

- OCDS process details of IT Security Planning Process
  - This part is the asset identification stage
  - Client completes initial IT Security Planning Questionnaire
  - OCDS Receives and logs response
  - Using the detailed asset identifications OCDS creates a proprietary Risk Assessment Questionnaire for client to complete

Owner: Scott Gilstrap

Release Information Security Plan Client Offering into Production



Company Demographics

1. What is your contact information?
   - Your name and role
   - Business/company name
   - E-mail
   - Phone number
   - Address *

Enter your answer

2. In what industry does your business operate? *

Enter your answer

3. What are your company's Business Goals and Objectives? *

Enter your answer

Section 2

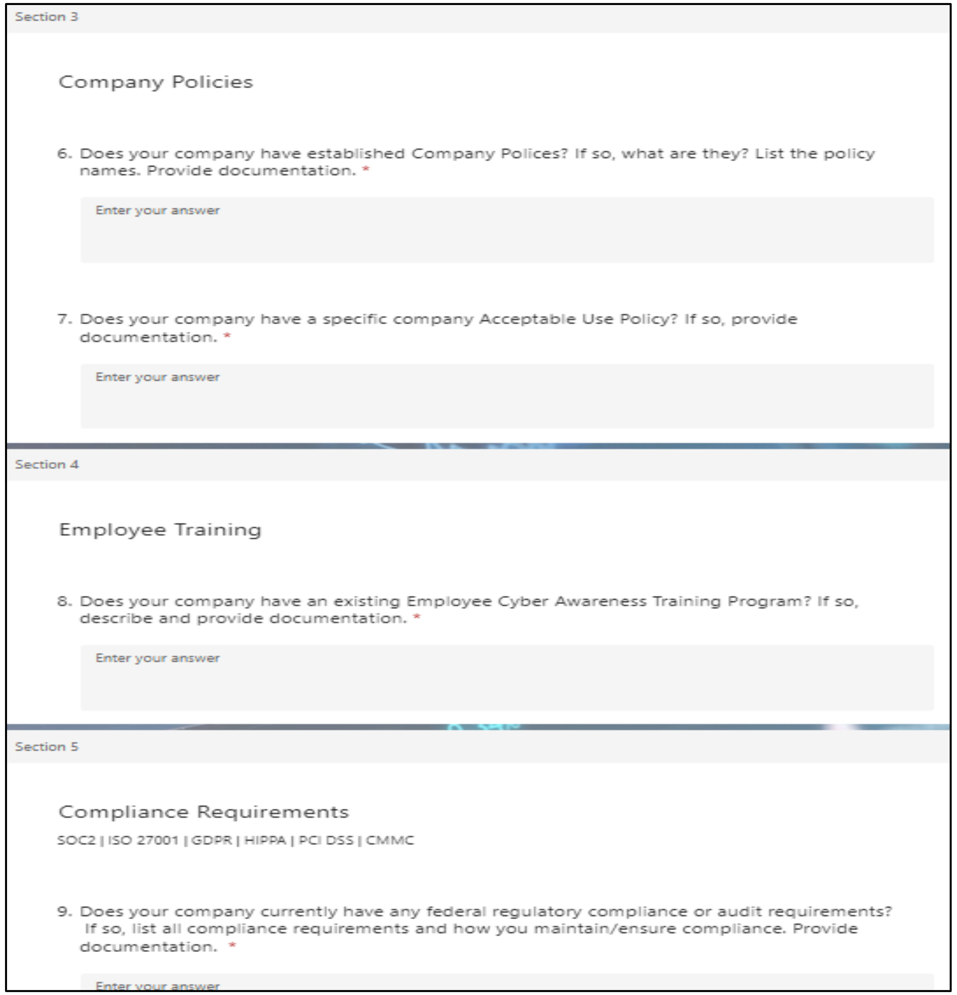
Security Team | Roles & Responsibilities

4. Does your company have an Information Security Officer/Director or an Information Technology Officer/Director? If so, what is(are) their name(s), title(s), and team structure(s)? Describe their role(s) in Information Security. *

Enter your answer

5. Does your company have a dedicated IT Security Team? If so, what is the structure? *

Enter your answer



Section 3

Company Policies

6. Does your company have established Company Polices? If so, what are they? List the policy names. Provide documentation. *

Enter your answer

7. Does your company have a specific company Acceptable Use Policy? If so, provide documentation. *

Enter your answer

Section 4

Employee Training

8. Does your company have an existing Employee Cyber Awareness Training Program? If so, describe and provide documentation. *

Enter your answer

Section 5

Compliance Requirements

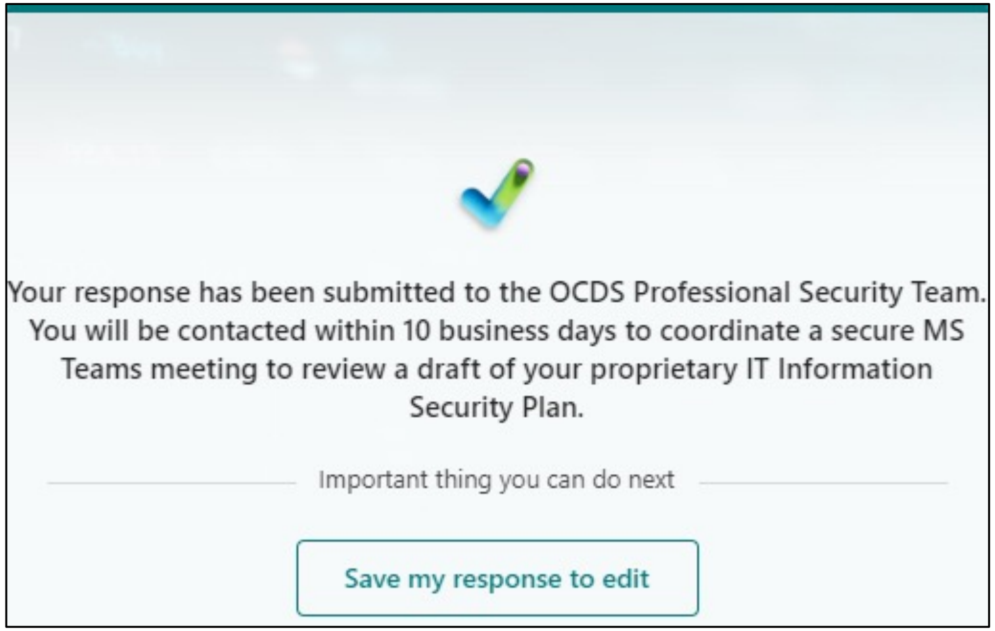
SOC2 | ISO 27001 | GDPR | HIPPA | PCI DSS | CMMC

9. Does your company currently have any federal regulatory compliance or audit requirements? If so, list all compliance requirements and how you maintain/ensure compliance. Provide documentation. *

Enter your answer

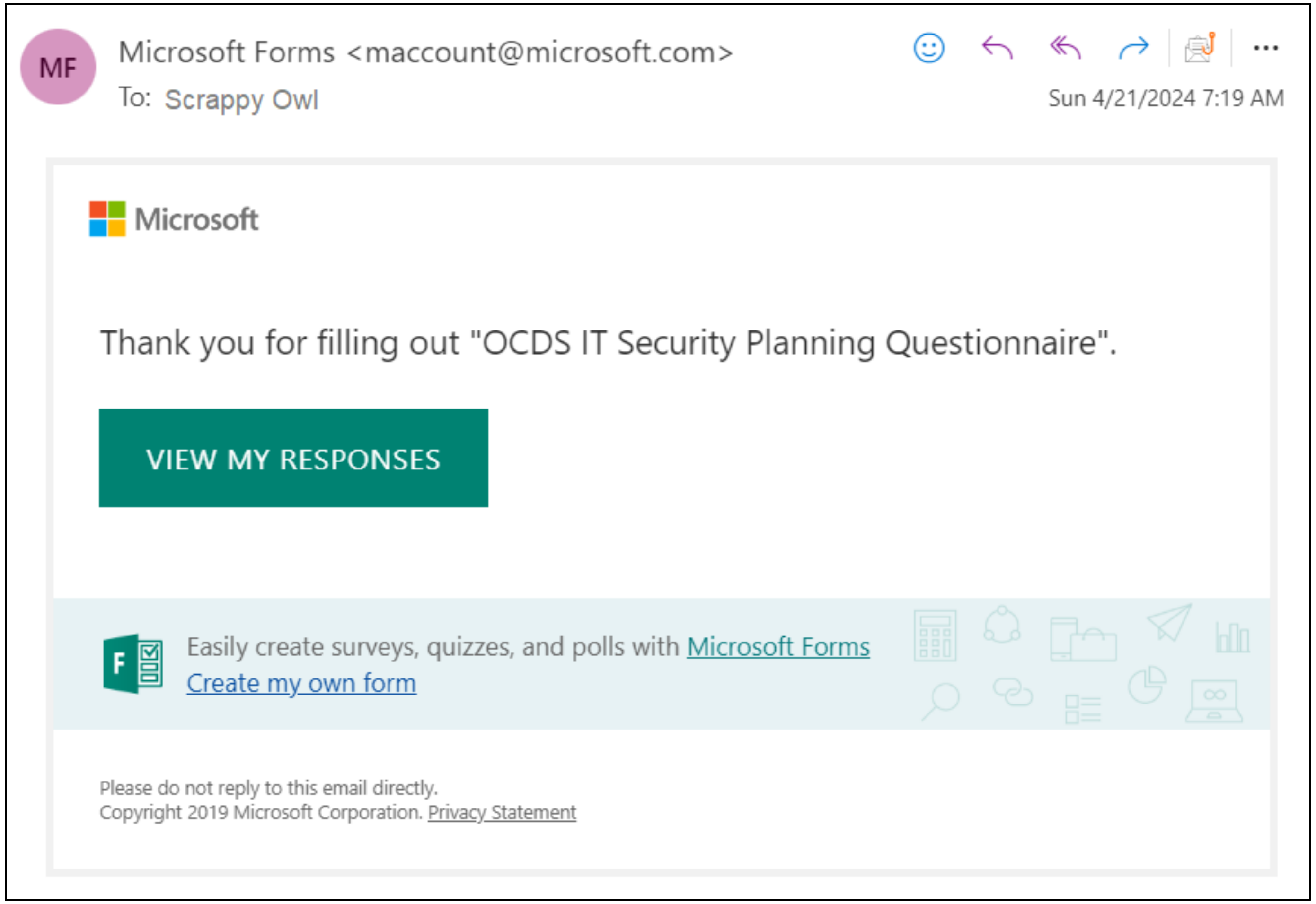
Owner: Scott Gilstrap

Release Information Security Plan Client Offering into Production



Your response has been submitted to the OCDS Professional Security Team. You will be contacted within 10 business days to coordinate a secure MS Teams meeting to review a draft of your proprietary IT Information Security Plan.

Important thing you can do next



Microsoft Forms <maccount@microsoft.com>
To: Scrappy Owl
Sun 4/21/2024 7:19 AM

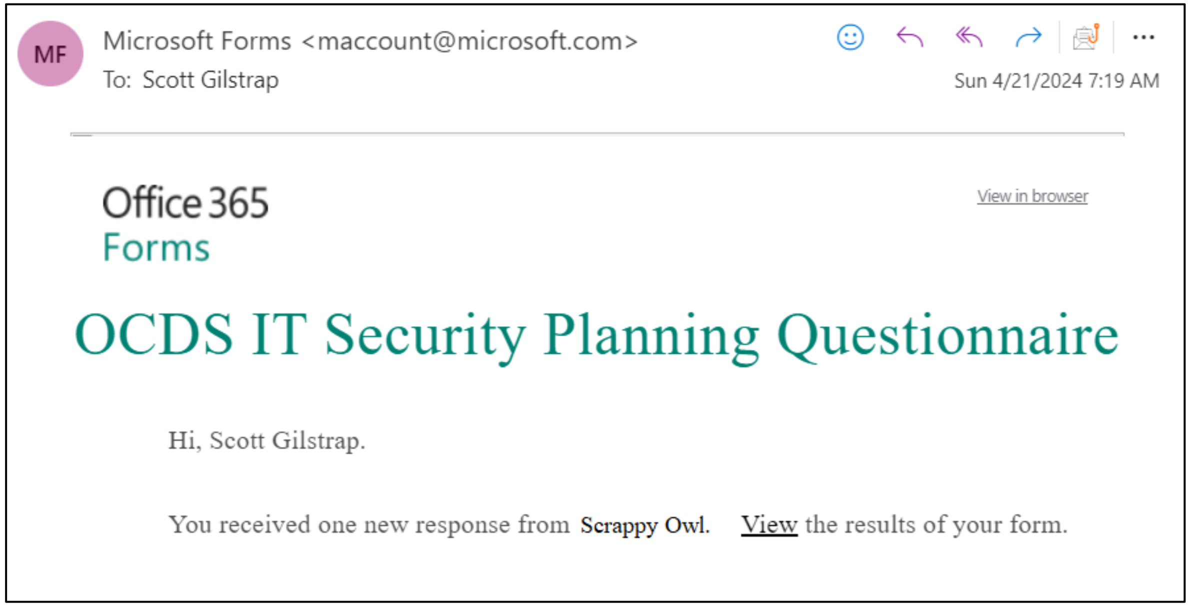
Thank you for filling out "OCDS IT Security Planning Questionnaire".

Easily create surveys, quizzes, and polls with Microsoft Forms
Create my own form

Please do not reply to this email directly.
Copyright 2019 Microsoft Corporation. Privacy Statement

Owner: Scott Gilstrap

Release Information Security Plan Client Offering into Production



MF Microsoft Forms <maccount@microsoft.com>

To: Scott Gilstrap

Sun 4/21/2024 7:19 AM

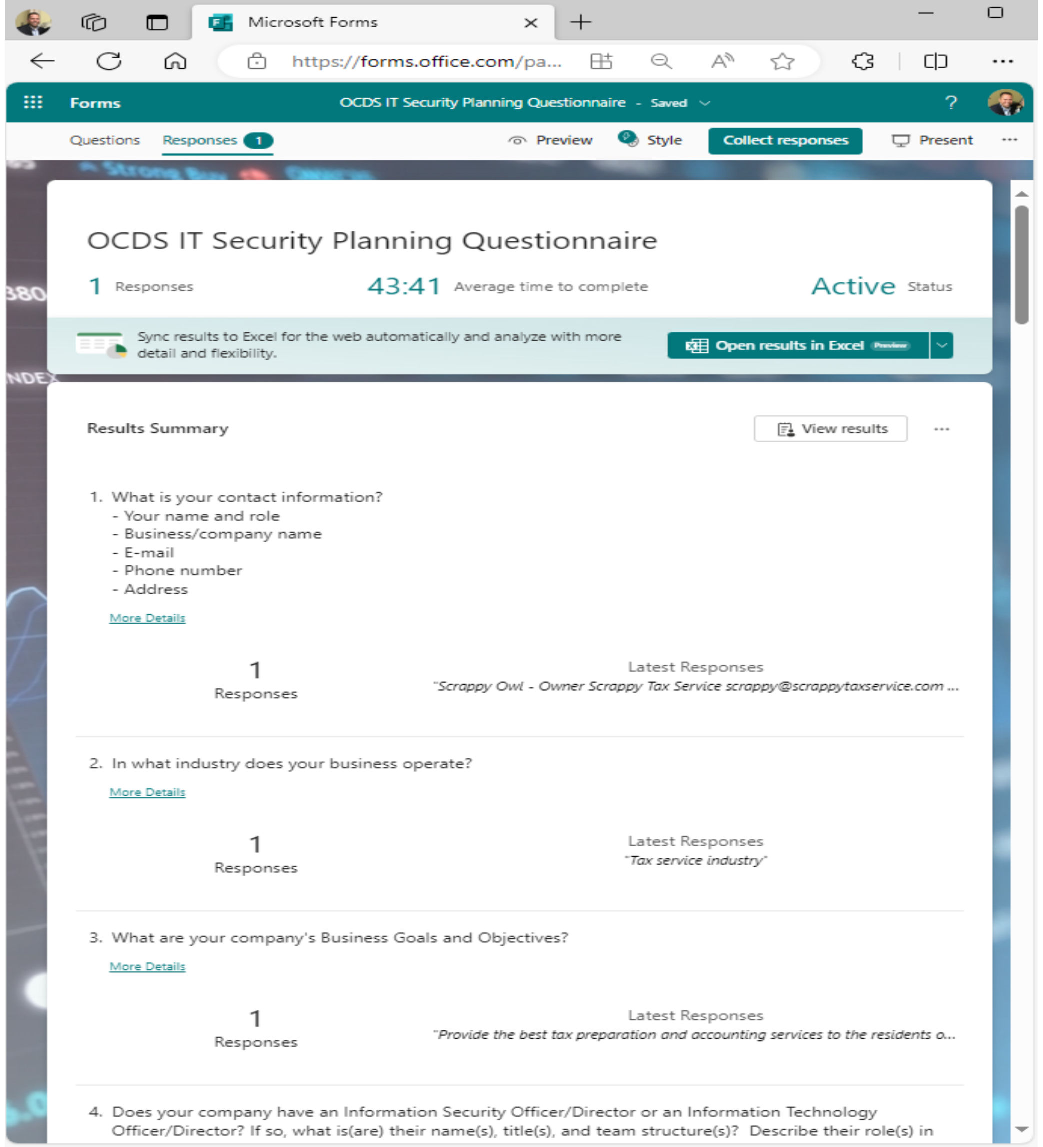
Office 365
Forms

View in browser

OCDS IT Security Planning Questionnaire

Hi, Scott Gilstrap.

You received one new response from Scrappy Owl. View the results of your form.



Microsoft Forms
https://forms.office.com/pa...
Forms
OCDS IT Security Planning Questionnaire - Saved
Questions
Responses 1
Preview
Style
Collect responses
Present

OCDS IT Security Planning Questionnaire

1 Responses 43:41 Average time to complete Active Status

Sync results to Excel for the web automatically and analyze with more detail and flexibility.

Open results in Excel

Results Summary

View results

1. What is your contact information?
   - Your name and role
   - Business/company name
   - E-mail
   - Phone number
   - Address

More Details

1 Responses

Latest Responses
"Scrappy Owl - Owner Scrappy Tax Service scrappy@scrappytaxservice.com ...

2. In what industry does your business operate?

More Details

1 Responses

Latest Responses
"Tax service industry"

3. What are your company's Business Goals and Objectives?

More Details

1 Responses

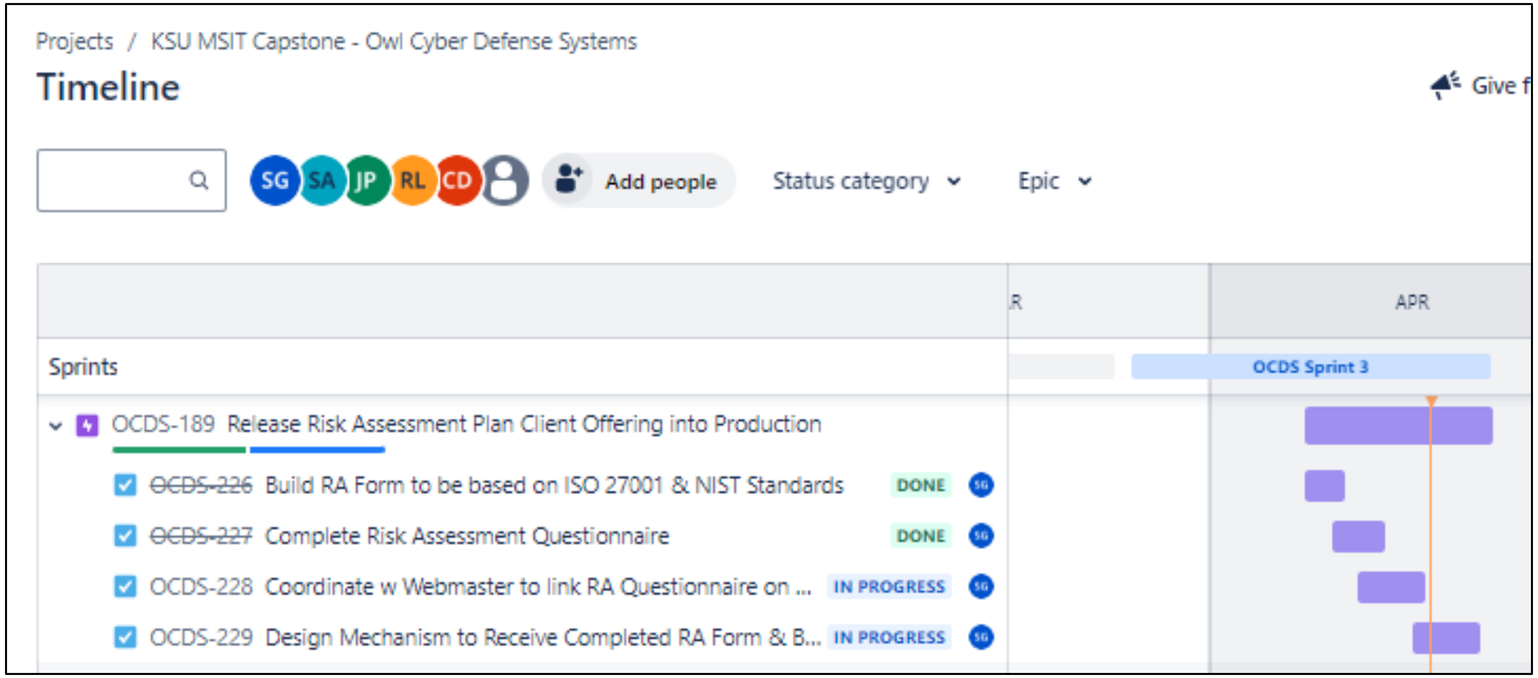
Latest Responses
"Provide the best tax preparation and accounting services to the residents o...

4. Does your company have an Information Security Officer/Director or an Information Technology Officer/Director? If so, what is(are) their name(s), title(s), and team structure(s)? Describe their role(s) in

Epic: Release Risk Assessment Plan Client Offering into Production

Scott Gilstrap

Release Risk Assessment Plan Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Sprints

OCDS-189 Release Risk Assessment Plan Client Offering into Production

☑ ~~OCDS-226~~	Build RA Form to be based on ISO 27001 & NIST Standards	DONE	SG
☑ ~~OCDS-227~~	Complete Risk Assessment Questionnaire	DONE	SG
☑ OCDS-228	Coordinate w Webmaster to link RA Questionnaire on ...	IN PROGRESS	SG
☑ OCDS-229	Design Mechanism to Receive Completed RA Form & B...	IN PROGRESS	SG

On Track – no risks

Release Risk Assessment Plan Client Offering into Production

- Overall Process
  - Determine all company Assets
  - Identify vulnerabilities with each asset
  - **Threat analysis**
    - Identify threats to each vulnerability
    - Assess threat impact to company if vulnerability is exploited
    - Assess the likelihood of the threat exploiting each vulnerability
  - **Calculate the Level of Risk**
  - **Determine acceptability of Risk**
  - **If not acceptable identify treatment options using security controls to mitigate the Risk**
  - **Create Risk Assessment & Treatment Plan**
  - **Create Statement of Acceptance**
    - Addressing residual risks

- OCDS process details of Risk Assessment Pan
  - This section is the Risk Assessment and Management stage
  - OCDS creates a proprietary Risk Assessment Questionnaire for client to complete
  - Client completes the multi-form, detailed Risk Assessment Questionnaire
  - OCDS creates a Risk Assessment Treatment Plan
  - Client reviews the Risk Assessment Treatment Plan and accepts
  - Documentation is recorded and all parties sign/agree to the developed IT Security and Risk Management Plan

Owner: Scott Gilstrap

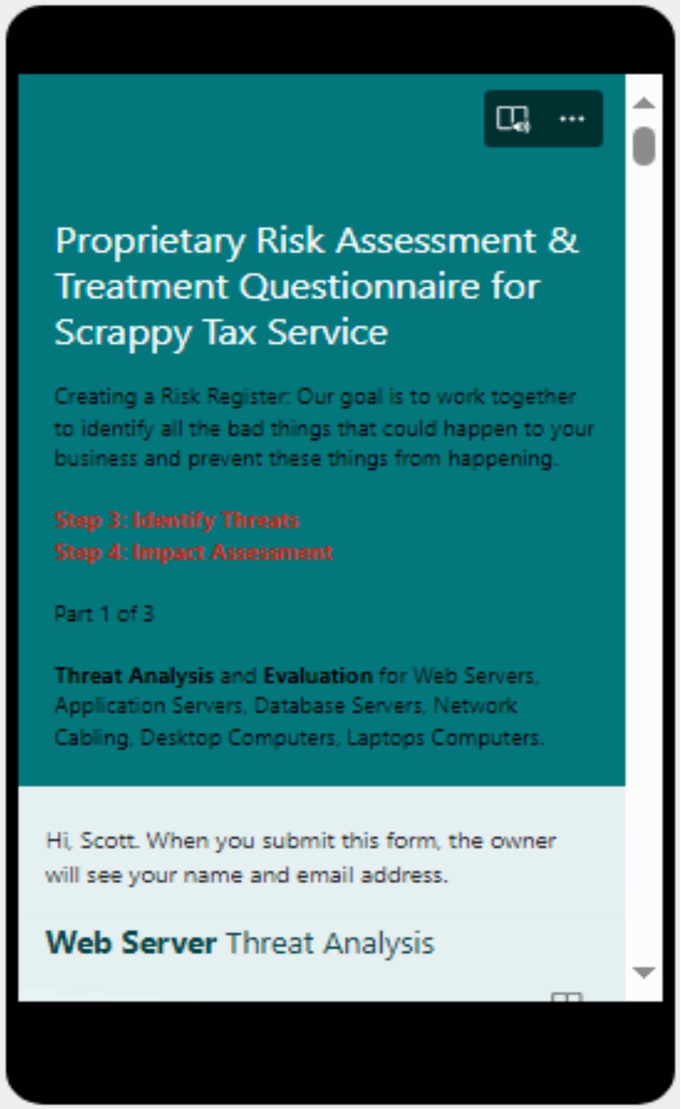
Release Risk Assessment Plan Client Offering into Production

NIST 800-53 – Standards for Security and Privacy Controls

ISO 27001 – Information Security Management System

This a multi-form process designed specifically for each client

- Threat Identification and Impact Analysis (Impact & Likelihood Assessment):
  - Step 1 of 3: https://forms.office.com/r/eaZpRaMDH9?origin=lprLink
  - Step 2 of 3: https://forms.office.com/r/UQdQsCCSZg?origin=lprLink
  - Step 3 of 3: https://forms.office.com/r/bj2kaz9nkS?origin=lprLink
- Based on the answers to the above questionnaires OCDS calculates Risk Levels:
- Client accepts Risks that are of an appropriate level
- OCDS identifies treatment options using appropriate security controls to mitigate each risk to an acceptable level
- Client accepts treatment options and Risk Treatment Plan
- OCDS generates two reports:
  1) Risk Assessment and Treatment
  2) Statement of acceptance of residual risks



Proprietary Risk Assessment & Treatment Questionnaire for Scrappy 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

Release Risk Assessment Plan Client Offering into Production

Risk Treatment Options:

- **Decrease** the risk using safeguards
- **Avoid** the risk
- **Accept** the risk
- **Transfer** the risk to a third party

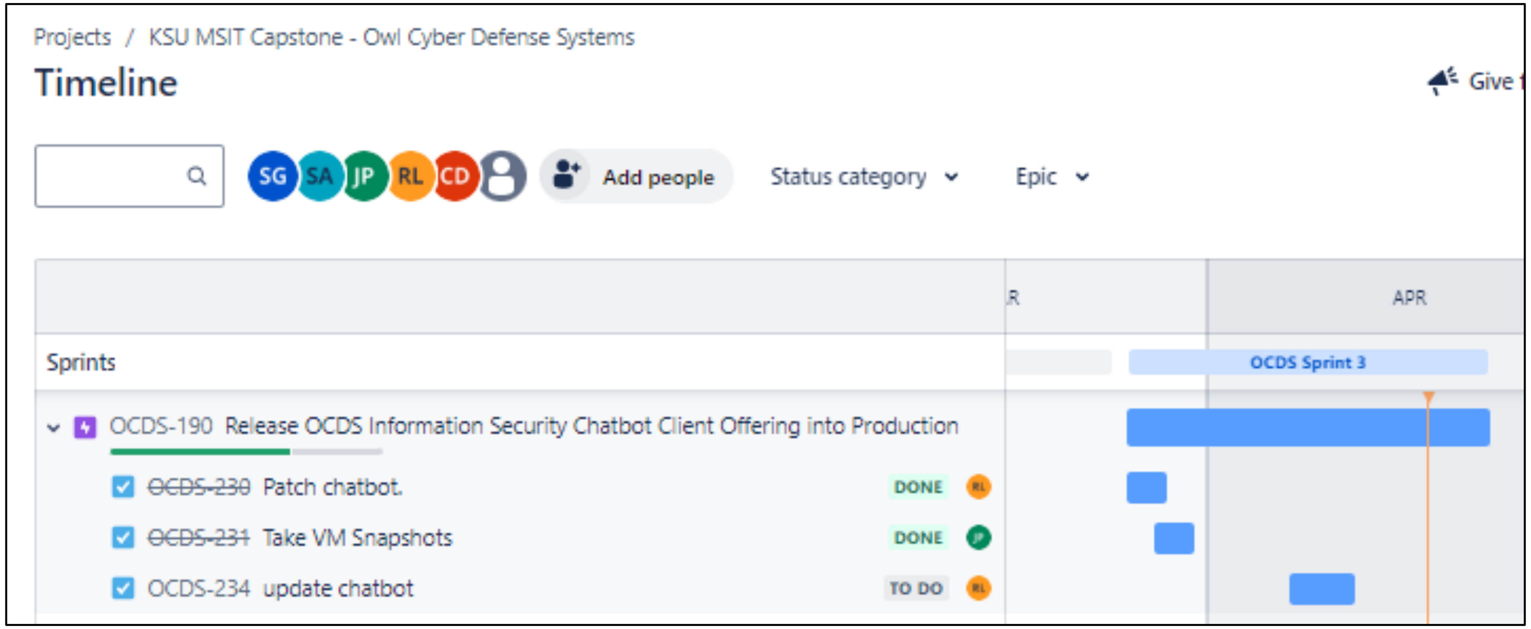
Example of a Risk Register

Asset Area	Vulnerability	Threat	Impact	Likelihood	Level	Risk Owner
Remote workspace	Lack of access to facilities, rooms or offices	Unauthorized entry into facilities, rooms or offices	1 – Medium	2 – High	3 Not Acceptable	Scrappy Owl
Remote workspace	Lack of access to facilities, rooms or offices	Unauthorized entry into facilities, rooms or offices	1 – Medium	1 – Medium	2 Acceptable	Scrappy Owl
ScrappyWebSrvr1	Inadequate / incompatible equipment	Interruption of power supply from public network	0 – Low	2 - High	2 Acceptable	Feisty Nightjar
ScrappyWebSrvr1	Inadequate / incompatible equipment	Equipment failure	1 – Medium	1 – Medium	2 Acceptable	Feisty Nightjar
ScrappyWebSrvr1	Test & prod environments not separated	Unauthorized Access: Employee	1 – Medium	2 – High	3 Not Acceptable	Feisty Nightjar
ScrappyWebSrvr1	Test & prod environments not separated	Unauthorized Access: Attacker	2 – High	1 – Medium	3 Not Acceptable	Feisty Nightjar

Epic: Release OCDS Information Security Chatbot Client Offering into Production

Ryan LeBlanc

Release OCDS Information Security Chatbot Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Sprints

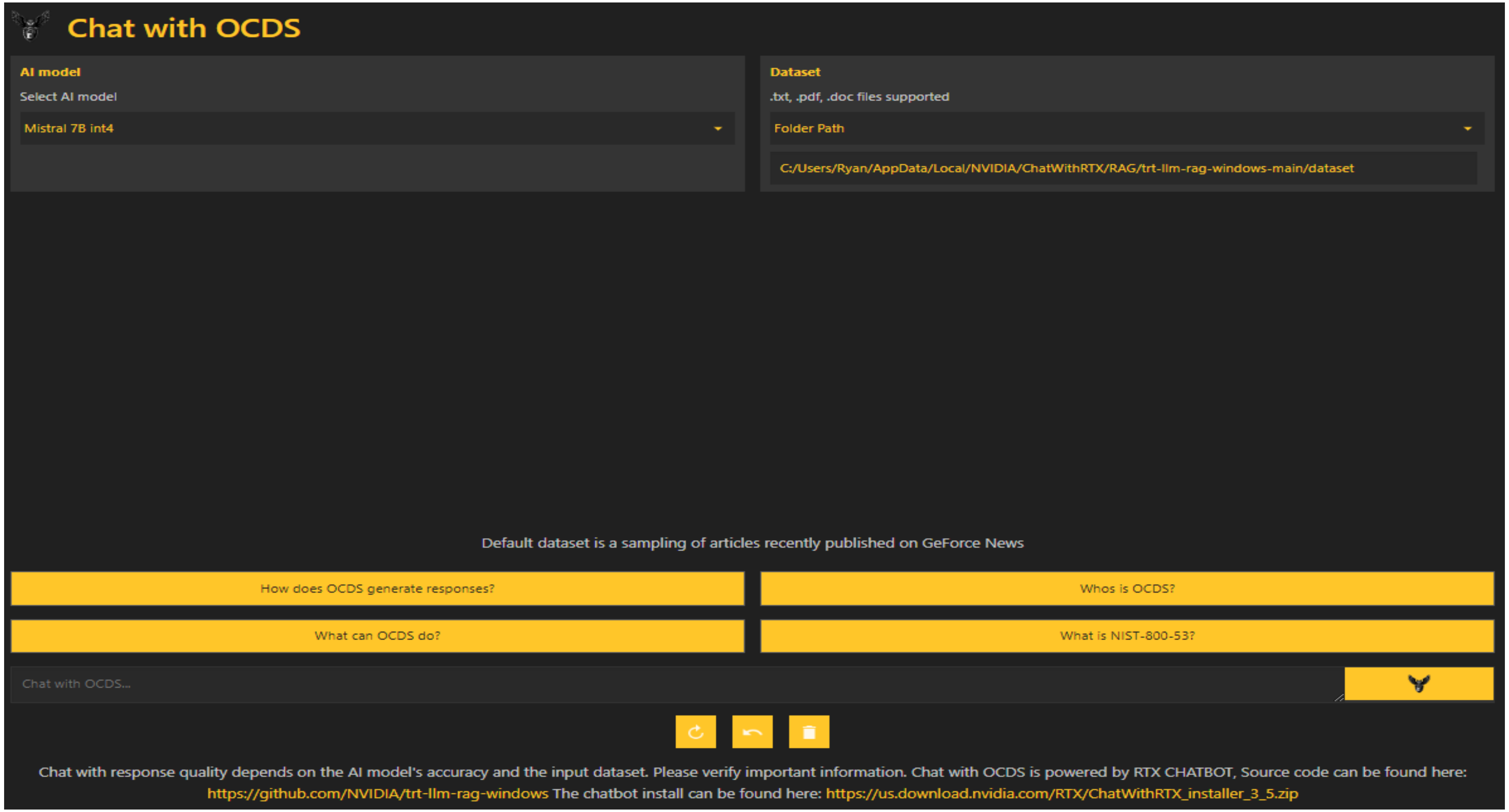
OCDS-190 Release OCDS Information Security Chatbot Client Offering into Production

- ☑ ~~OCDS-230~~ Patch chatbot. DONE RL
- ☑ ~~OCDS-231~~ Take VM Snapshots DONE JP
- ☑ OCDS-234 update chatbot TO DO RL

Complete

Release OCDS Information Security Chatbot Client Offering into Production

- Powered by RTX
- Used **NIST 800-53** information security controls and standards to populate datasets to teach the OCDS Chatbot
- Used PyCharm and Visual Studio Code scripting to modify RTX Chatbot source code
- OCDS Chatbot utilized NIST standards to appropriately answer client security questions providing security advice based on NIST standards
- This enables our clients to ask IT security questions and receive the appropriate answer to properly secure their environment



Chat with OCDS

AI model

Select AI model

Mistral 7B int4

Dataset

.txt, .pdf, .doc files supported

Folder Path

C:/Users/Ryan/AppData/Local/NVIDIA/ChatWithRTX/RAG/trt-llm-rag-windows-main/dataset

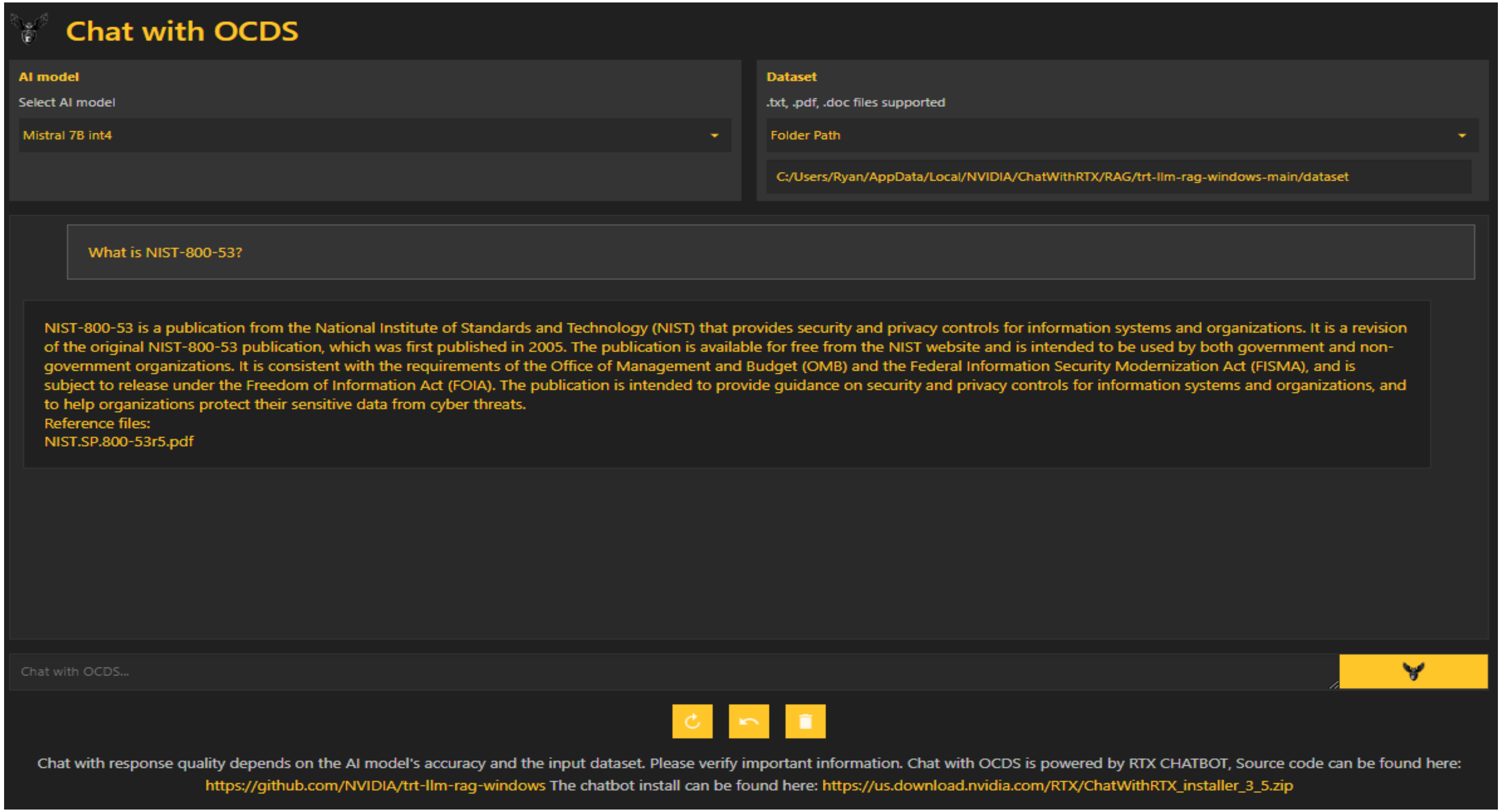
Default dataset is a sampling of articles recently published on GeForce News

Chat with response quality depends on the AI model's accuracy and the input dataset. Please verify important information. Chat with OCDS is powered by RTX CHATBOT, Source code can be found here: https://github.com/NVIDIA/trt-llm-rag-windows The chatbot install can be found here: https://us.download.nvidia.com/RTX/ChatWithRTX_installer_3_5.zip

Owner: Ryan LeBlanc

Release OCDS Information Security Chatbot Client Offering into Production

- Default dataset – STIG xml & business proposal file.
- OCDS Security Chatbot provides appropriate answers to security questions and an output file for the clients.
- Examples:
  - What is NIST 800-53?



Chat with OCDS

AI model

Select AI model

Mistral 7B int4

Dataset

.txt, .pdf, .doc files supported

Folder Path

C:/Users/Ryan/AppData/Local/NVIDIA/ChatWithRTX/RAG/trt-llm-rag-windows-main/dataset

What is NIST-800-53?

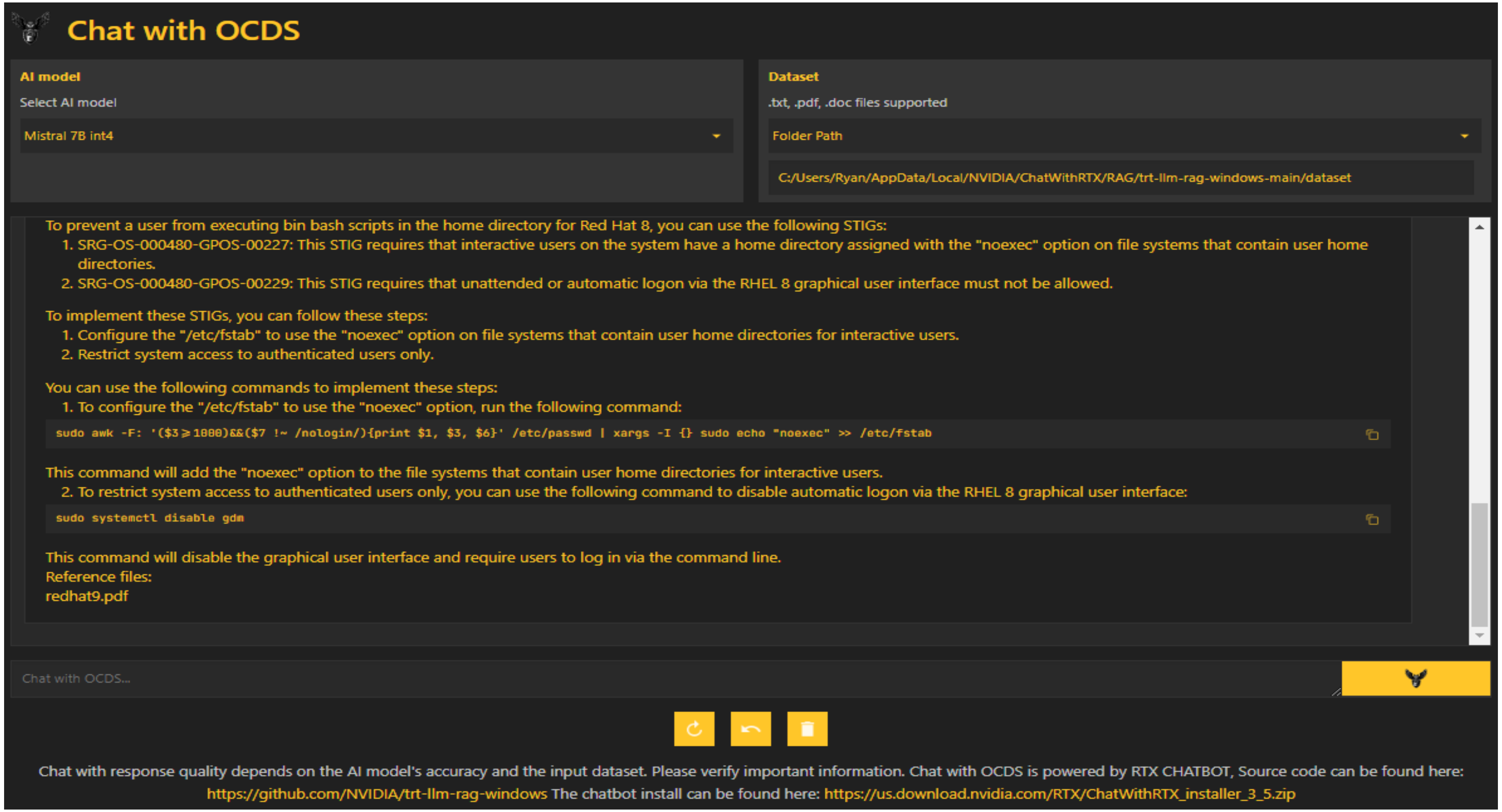
NIST-800-53 is a publication from the National Institute of Standards and Technology (NIST) that provides security and privacy controls for information systems and organizations. It is a revision of the original NIST-800-53 publication, which was first published in 2005. The publication is available for free from the NIST website and is intended to be used by both government and non-government organizations. It is consistent with the requirements of the Office of Management and Budget (OMB) and the Federal Information Security Modernization Act (FISMA), and is subject to release under the Freedom of Information Act (FOIA). The publication is intended to provide guidance on security and privacy controls for information systems and organizations, and to help organizations protect their sensitive data from cyber threats.
Reference files:
NIST.SP.800-53r5.pdf

Chat with response quality depends on the AI model's accuracy and the input dataset. Please verify important information. Chat with OCDS is powered by RTX CHATBOT, Source code can be found here: https://github.com/NVIDIA/trt-llm-rag-windows The chatbot install can be found here: https://us.download.nvidia.com/RTX/ChatWithRTX_installer_3_5.zip

Owner: Ryan LeBlanc

Release OCDS Information Security Chatbot Client Offering into Production

- Default dataset – STIG xml & business proposal file.
- OCDS Security Chatbot provides appropriate answers to security questions and an output file for the clients.
- Examples:
  - STIG implementation



Chat with OCDS

Mistral 7B int4

Folder Path

C:/Users/Ryan/AppData/Local/NVIDIA/ChatWithRTX/RAG/trt-llm-rag-windows-main/dataset

To prevent a user from executing bin bash scripts in the home directory for Red Hat 8, you can use the following STIGs:

1. SRG-OS-000480-GPOS-00227: This STIG requires that interactive users on the system have a home directory assigned with the "noexec" option on file systems that contain user home directories.
2. SRG-OS-000480-GPOS-00229: This STIG requires that unattended or automatic logon via the RHEL 8 graphical user interface must not be allowed.

To implement these STIGs, you can follow these steps:

1. Configure the "/etc/fstab" to use the "noexec" option on file systems that contain user home directories for interactive users.
2. Restrict system access to authenticated users only.

You can use the following commands to implement these steps:

1. To configure the "/etc/fstab" to use the "noexec" option, run the following command:

```
sudo awk -F: '($3≥1000)&&($7 !~ /nologin/){print $1, $3, $6}' /etc/passwd | xargs -I {} sudo echo "noexec" >> /etc/fstab
```

This command will add the "noexec" option to the file systems that contain user home directories for interactive users.

2. To restrict system access to authenticated users only, you can use the following command to disable automatic logon via the RHEL 8 graphical user interface:

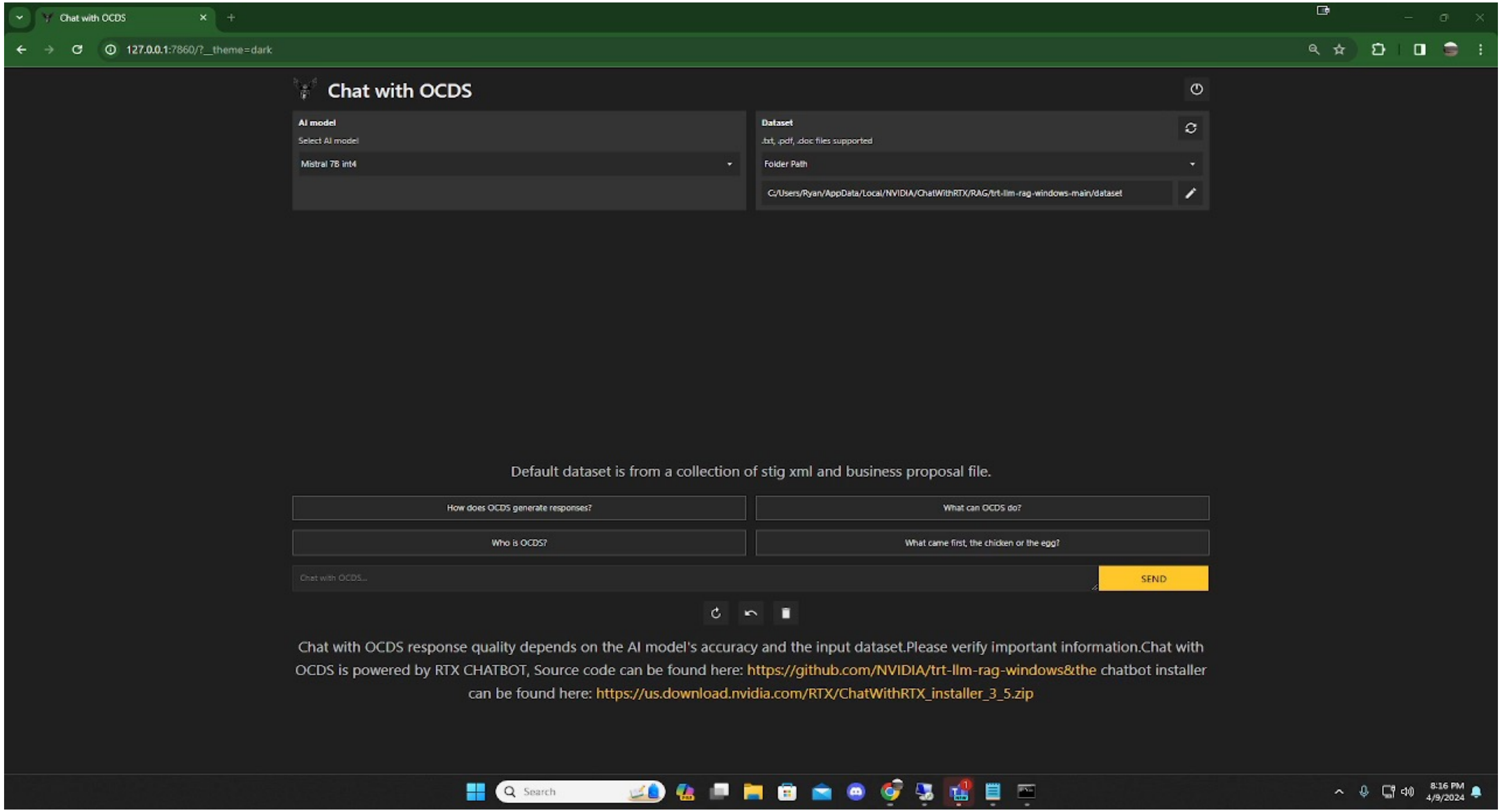
```
sudo systemctl disable gdm
```

This command will disable the graphical user interface and require users to log in via the command line.
Reference files:
redhat9.pdf

Chat with response quality depends on the AI model's accuracy and the input dataset. Please verify important information. Chat with OCDS is powered by RTX CHATBOT, Source code can be found here: https://github.com/NVIDIA/trt-llm-rag-windows The chatbot install can be found here: https://us.download.nvidia.com/RTX/ChatWithRTX_installer_3_5.zip

Release OCDS Information Security Chatbot Client Offering into Production

- Click image to play video (older color scheme)
- Default dataset – STIG xml & business proposal file.
- OCDS Security Chatbot provides appropriate answers to security questions and an output file for the clients.
- Examples:
  - What can OCDS do?
  - Provide me fixes to ensure home is not executable in FSTAB.
  - In Ubuntu provide me fixes to make sure password history is on compliance with STIGs.



Chat with OCDS
127.0.0.1:7860/?__theme=dark
Search
8:16 PM
4/9/2024

Chat with OCDS

AI model

Select AI model

Mistral 7B int4

Dataset

.txt, .pdf, .doc files supported

Folder Path

C:/Users/Ryan/AppData/Local/NVIDIA/ChatWithRTX/RAG/trt-llm-rag-windows-main/dataset

Default dataset is from a collection of stig xml and business proposal file.

How does OCDS generate responses?
What can OCDS do?
Who is OCDS?
What came first, the chicken or the egg?
Chat with OCDS...
SEND

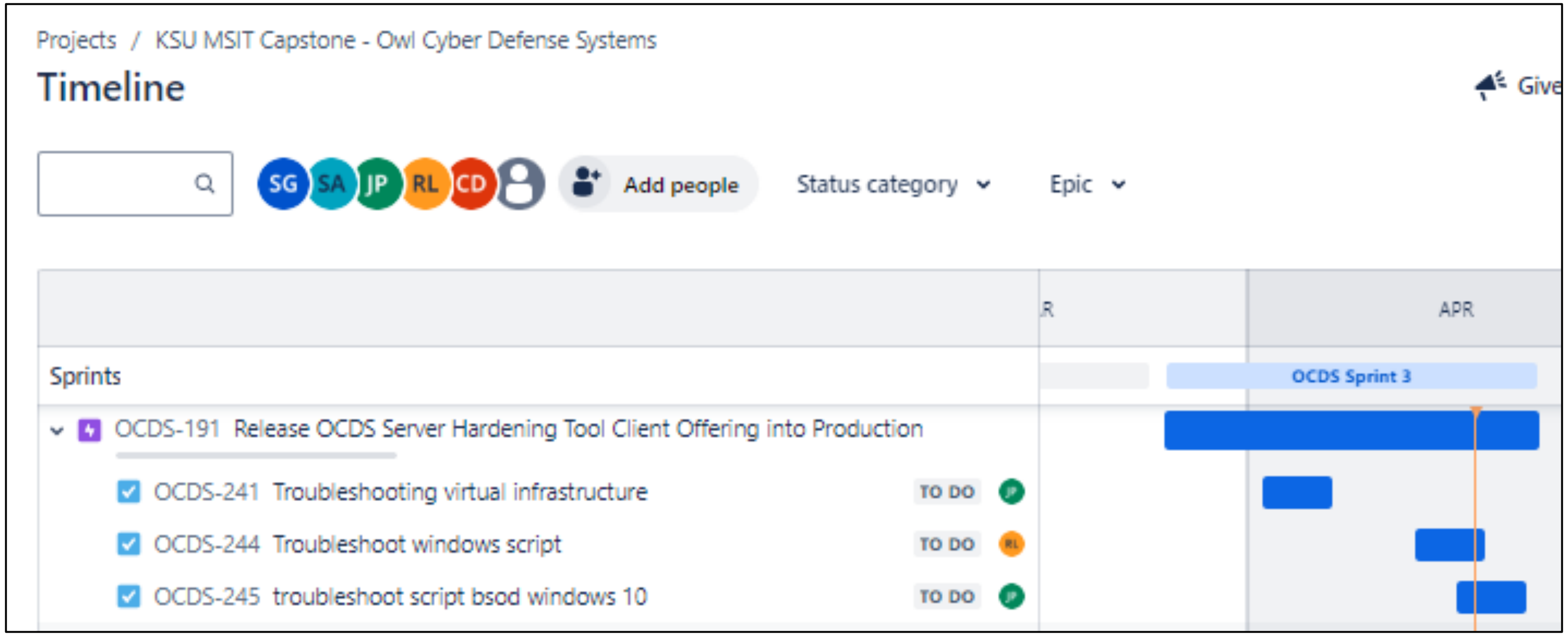
Chat with OCDS response quality depends on the AI model's accuracy and the input dataset.Please verify important information.Chat with OCDS is powered by RTX CHATBOT, Source code can be found here: https://github.com/NVIDIA/trt-llm-rag-windows&the chatbot installer can be found here: https://us.download.nvidia.com/RTX/ChatWithRTX_installer_3_5.zip

Owner: Ryan LeBlanc

Epic: Release OCDS Server Hardening Tool Client Offering into Production

Justin Place

Release OCDS Server Hardening Tool Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

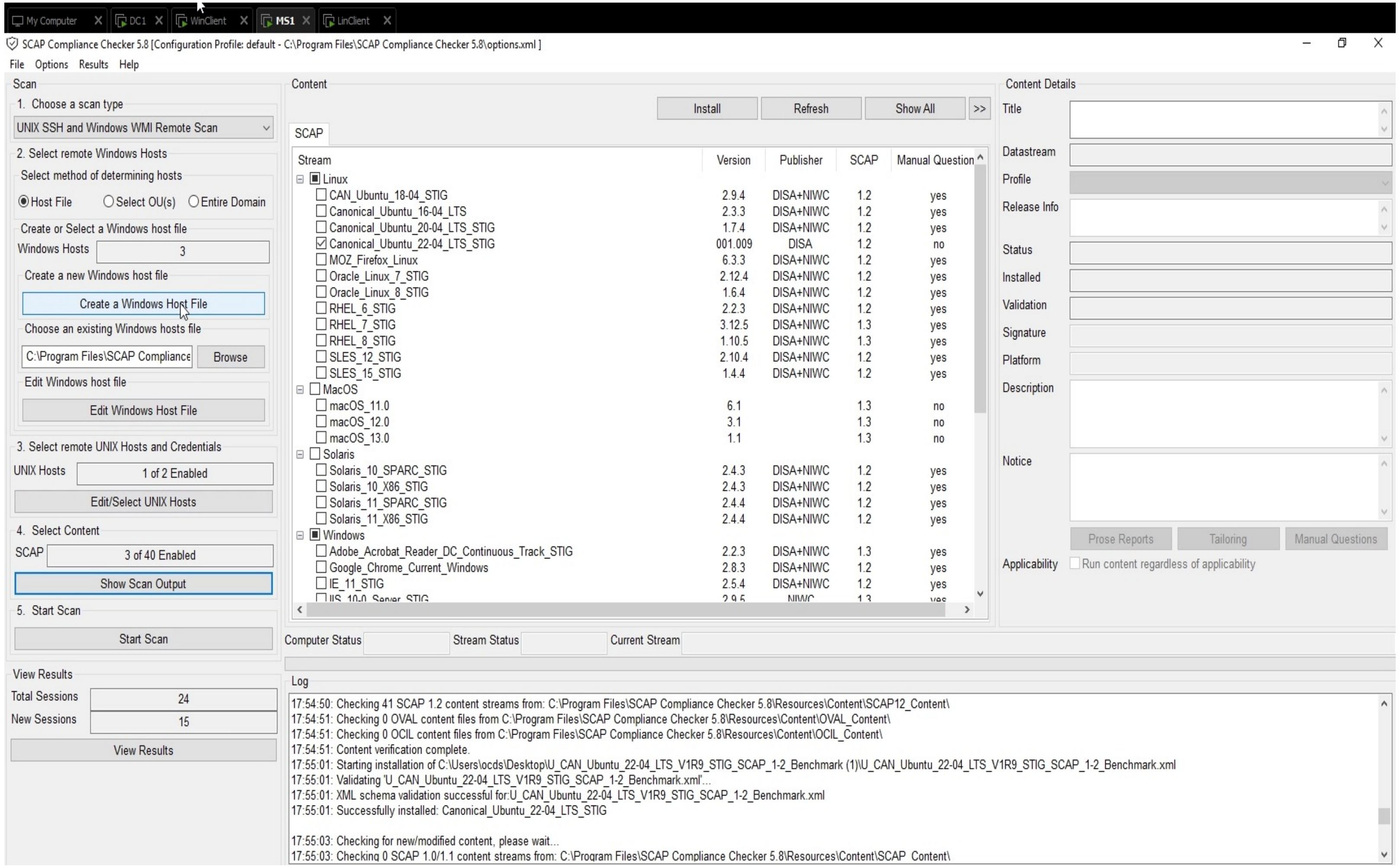
OCDS-191 Release OCDS Server Hardening Tool Client Offering into Production		
☑ OCDS-241 Troubleshooting virtual infrastructure	TO DO	JP
☑ OCDS-244 Troubleshoot windows script	TO DO	RL
☑ OCDS-245 troubleshoot script bsod windows 10	TO DO	JP

Complete/On Track

Release OCDS Server Hardening Tool Client Offering into Production

JP
RL

- Completely built out and hosting entire virtual infrastructure on VMWare Workstation
    - DC1
    - Win10Client (Windows 10)
    - UC1 (Ubuntu client)
    - MS1
- PSSession
- PowerShell / SSH
- STIG – Security Technical Implementation Guide
- SCAP – Security Content Automation Protocol
- Pre-STIG scan / Post-STIG scan



SCAP Compliance Checker 5.8 [Configuration Profile: default - C:\Program Files\SCAP Compliance Checker 5.8\options.xml]

Scan

1. Choose a scan type
UNIX SSH and Windows WMI Remote Scan

2. Select remote Windows Hosts
Select method of determining hosts
● Host File ○ Select OU(s) ○ Entire Domain
Create or Select a Windows host file
Windows Hosts: 3
Create a new Windows host file
Choose an existing Windows hosts file
C:\Program Files\SCAP Compliance
Edit Windows host file

3. Select remote UNIX Hosts and Credentials
UNIX Hosts: 1 of 2 Enabled

4. Select Content
SCAP: 3 of 40 Enabled

5. Start Scan

View Results
Total Sessions: 24
New Sessions: 15

Content

SCAP

Stream	Version	Publisher	SCAP	Manual Question
⊟ ▣ Linux				
□ CAN_Ubuntu_18-04_STIG	2.9.4	DISA+NIWC	1.2	yes
□ Canonical_Ubuntu_16-04_LTS	2.3.3	DISA+NIWC	1.2	yes
□ Canonical_Ubuntu_20-04_LTS_STIG	1.7.4	DISA+NIWC	1.2	yes
☑ Canonical_Ubuntu_22-04_LTS_STIG	001.009	DISA	1.2	no
□ MOZ_Firefox_Linux	6.3.3	DISA+NIWC	1.2	yes
□ Oracle_Linux_7_STIG	2.12.4	DISA+NIWC	1.2	yes
□ Oracle_Linux_8_STIG	1.6.4	DISA+NIWC	1.2	yes
□ RHEL_6_STIG	2.2.3	DISA+NIWC	1.2	yes
□ RHEL_7_STIG	3.12.5	DISA+NIWC	1.3	yes
□ RHEL_8_STIG	1.10.5	DISA+NIWC	1.3	yes
□ SLES_12_STIG	2.10.4	DISA+NIWC	1.2	yes
□ SLES_15_STIG	1.4.4	DISA+NIWC	1.2	yes
⊟ □ MacOS				
□ macOS_11.0	6.1		1.3	no
□ macOS_12.0	3.1		1.3	no
□ macOS_13.0	1.1		1.3	no
⊟ □ Solaris				
□ Solaris_10_SPARC_STIG	2.4.3	DISA+NIWC	1.2	yes
□ Solaris_10_X86_STIG	2.4.3	DISA+NIWC	1.2	yes
□ Solaris_11_SPARC_STIG	2.4.4	DISA+NIWC	1.2	yes
□ Solaris_11_X86_STIG	2.4.4	DISA+NIWC	1.2	yes
⊟ ▣ Windows				
□ Adobe_Acrobat_Reader_DC_Continuous_Track_STIG	2.2.3	DISA+NIWC	1.3	yes
□ Google_Chrome_Current_Windows	2.8.3	DISA+NIWC	1.2	yes
□ IE_11_STIG	2.5.4	DISA+NIWC	1.2	yes
□ IIS_10-0_Server_STIG	2.9.5	NIWC	1.3	yes

Content Details
Title
Datastream
Profile
Release Info
Status
Installed
Validation
Signature
Platform
Description
Notice
Applicability □ Run content regardless of applicability

Computer Status
Stream Status
Current Stream

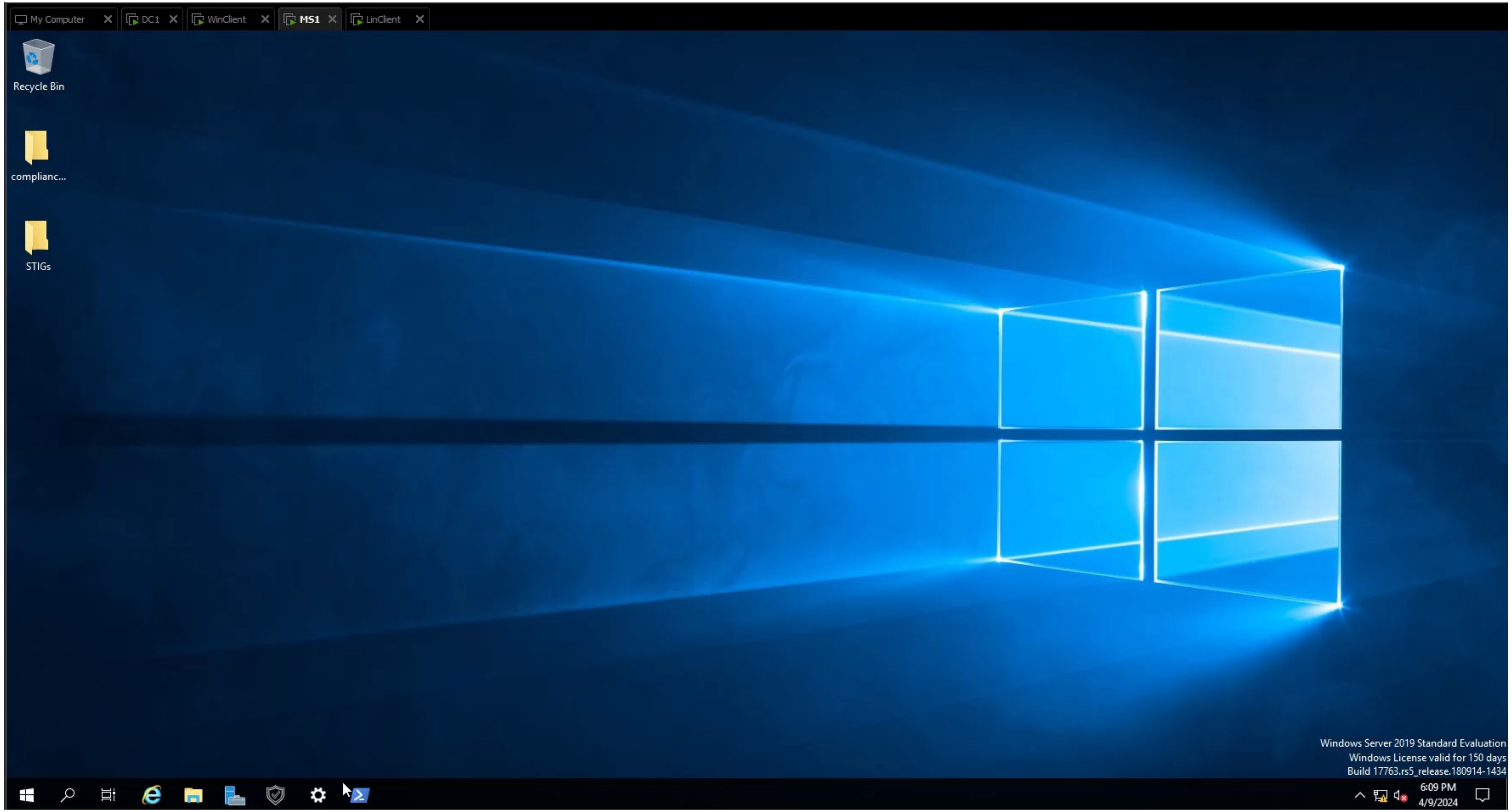
Log

```
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\ocds\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\
```

Owner: Justin Place

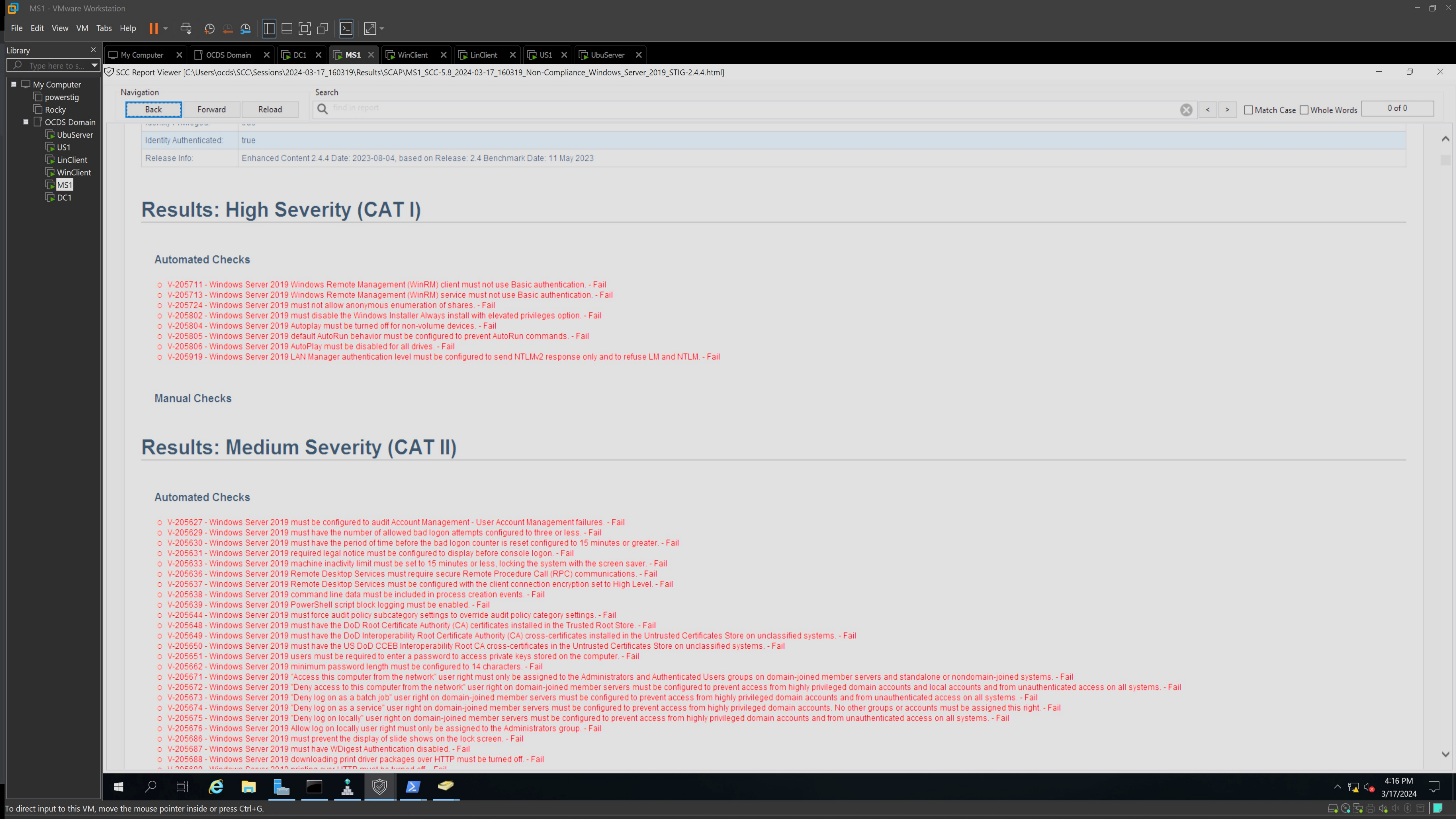
Release OCDS Server Hardening Tool Client Offering into Production

- Click image to play video
- Hardening process based on NIST guidelines and appropriate STIGs
- Pings all VMs from MS1 showing connectivity
- Enter PSSession to show STIG & run script – changes registry
- SSH to Ubuntu client
- Launch SCAP
- Host files
- Run scans
- Scores



Windows Server 2019 Standard Evaluation
Windows License valid for 150 days
Build 17763.rs5_release.180914-1434

Owner: Justin Place



Identity Privileged:	true
Identity Authenticated:	true
Release Info:	Enhanced Content 2.4.4 Date: 2023-08-04, based on Release: 2.4 Benchmark Date: 11 May 2023

Results: High Severity (CAT I)

Automated Checks

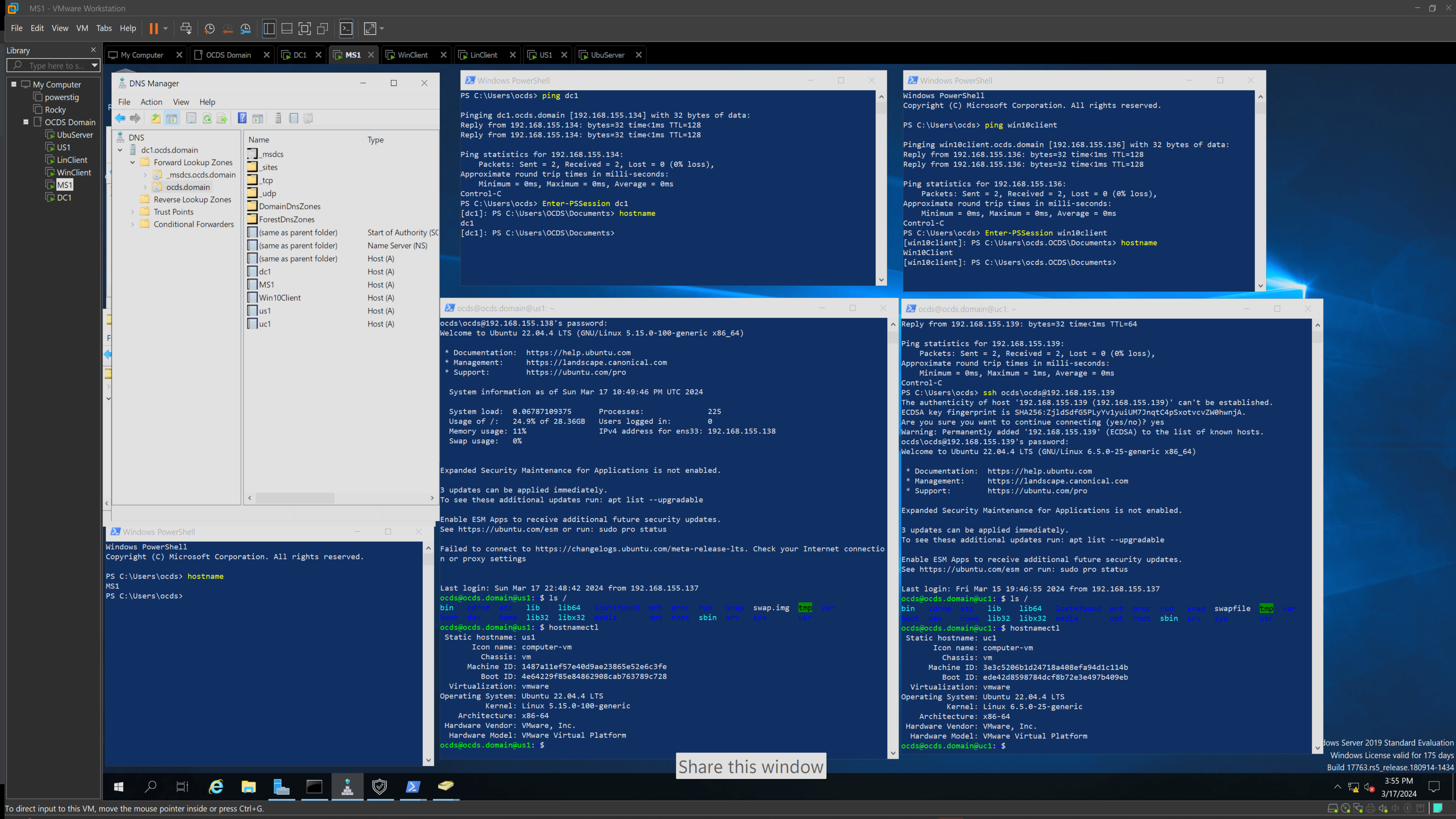
- V-205711 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-205724 - Windows Server 2019 must not allow anonymous enumeration of shares. - Fail
- V-205802 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option. - Fail
- V-205804 - Windows Server 2019 Autoplay must be turned off for non-volume devices. - Fail
- V-205805 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands. - Fail
- V-205806 - Windows Server 2019 AutoPlay must be disabled for all drives. - Fail
- V-205919 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. - Fail

Manual Checks

Results: Medium Severity (CAT II)

Automated Checks

- V-205627 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures. - Fail
- V-205629 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less. - Fail
- V-205630 - Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater. - Fail
- V-205631 - Windows Server 2019 required legal notice must be configured to display before console logon. - Fail
- V-205633 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver. - Fail
- V-205636 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications. - Fail
- V-205637 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High Level. - Fail
- V-205638 - Windows Server 2019 command line data must be included in process creation events. - Fail
- V-205639 - Windows Server 2019 PowerShell script block logging must be enabled. - Fail
- V-205644 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings. - Fail
- V-205648 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store. - Fail
- V-205649 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205650 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205651 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer. - Fail
- V-205662 - Windows Server 2019 minimum password length must be configured to 14 characters. - Fail
- V-205671 - Windows Server 2019 "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems. - Fail
- V-205672 - Windows Server 2019 "Deny access to this computer from the network" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems. - Fail
- V-205673 - Windows Server 2019 "Deny log on as a batch job" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems. - Fail
- V-205674 - Windows Server 2019 "Deny log on as a service" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts. No other groups or accounts must be assigned this right. - Fail
- V-205675 - Windows Server 2019 "Deny log on locally" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems. - Fail
- V-205676 - Windows Server 2019 Allow log on locally user right must only be assigned to the Administrators group. - Fail
- V-205686 - Windows Server 2019 must prevent the display of slide shows on the lock screen. - Fail
- V-205687 - Windows Server 2019 must have WDigest Authentication disabled. - Fail
- V-205688 - Windows Server 2019 downloading print driver packages over HTTP must be turned off. - Fail
- V-205689 - Windows Server 2019 printing over HTTP must be turned off. - Fail



Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SC
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
dc1	Host (A)
MS1	Host (A)
Win10Client	Host (A)
us1	Host (A)
uc1	Host (A)

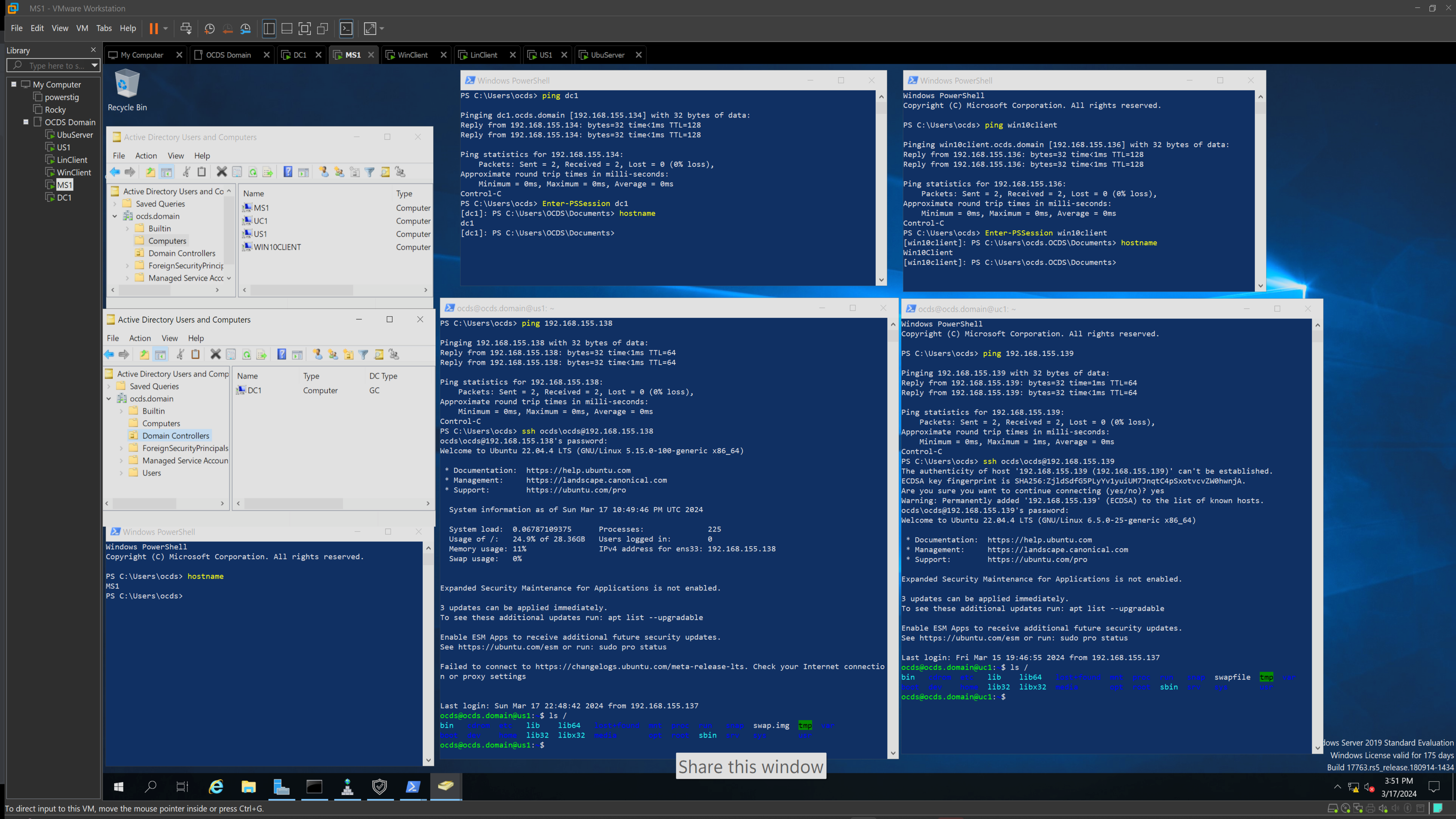
```
PS C:\Users\ocds> ping dc1

Pinging dc1.ocds.domain [192.168.155.134] with 32 bytes of data:
Reply from 192.168.155.134: bytes=32 time<1ms TTL=128
Reply from 192.168.155.134: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.155.134:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\ocds> Enter-PSSession dc1
[dc1]: PS C:\Users\OCDS\Documents> hostname
dc1
[dc1]: PS C:\Users\OCDS\Documents>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ocds> ping win10client

Pinging win10client.ocds.domain [192.168.155.136] with 32 bytes of data:
Reply from 192.168.155.136: bytes=32 time<1ms TTL=128
Reply from 192.168.155.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.155.136:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\ocds> Enter-PSSession win10client
[win10client]: PS C:\Users\ocds.OCDS\Documents> hostname
Win10Client
[win10client]: PS C:\Users\ocds.OCDS\Documents>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ocds> hostname
MS1
PS C:\Users\ocds>
```

```
ocds\ocds@192.168.155.138's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sun Mar 17 10:49:46 PM UTC 2024

  System load:  0.06787109375      Processes:             225
  Usage of /:   24.9% of 28.36GB   Users logged in:       0
  Memory usage: 11%                IPv4 address for ens33: 192.168.155.138
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connectio
n or proxy settings


Last login: Sun Mar 17 22:48:42 2024 from 192.168.155.137
ocds@ocds.domain@us1:~$ ls /
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swap.img  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
ocds@ocds.domain@us1:~$ hostnamectl
 Static hostname: us1
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 1487a11ef57e40d9ae23865e52e6c3fe
         Boot ID: 4e64229f85e84862908cab763789c728
  Virtualization: vmware
Operating System: Ubuntu 22.04.4 LTS
          Kernel: Linux 5.15.0-100-generic
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
ocds@ocds.domain@us1:~$
```

```
Reply from 192.168.155.139: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.155.139:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\ocds> ssh ocds\ocds@192.168.155.139
The authenticity of host '192.168.155.139 (192.168.155.139)' can't be established.
ECDSA key fingerprint is SHA256:ZjldSdfG5PLyYv1yuiUM7JnqtC4pSxotvcvZW0hwnjA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.155.139' (ECDSA) to the list of known hosts.
ocds\ocds@192.168.155.139's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Mar 15 19:46:55 2024 from 192.168.155.137
ocds@ocds.domain@uc1:~$ ls /
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swapfile  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
ocds@ocds.domain@uc1:~$ hostnamectl
 Static hostname: uc1
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 3e3c5206b1d24718a408efa94d1c114b
         Boot ID: ede42d8598784dcf8b72e3e497b409eb
  Virtualization: vmware
Operating System: Ubuntu 22.04.4 LTS
          Kernel: Linux 6.5.0-25-generic
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
ocds@ocds.domain@uc1:~$
```



Active Directory Users and Computers

File Action View Help

	Name	Type
Active Directory Users and Co	MS1	Computer
Saved Queries	UC1	Computer
ocds.domain	US1	Computer
Builtin	WIN10CLIENT	Computer
Computers		
Domain Controllers		
ForeignSecurityPrincip		
Managed Service Acc		

Active Directory Users and Computers

File Action View Help

	Name	Type	DC Type
Active Directory Users and Comp	DC1	Computer	GC
Saved Queries			
ocds.domain			
Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipals			
Managed Service Accoun			
Users			

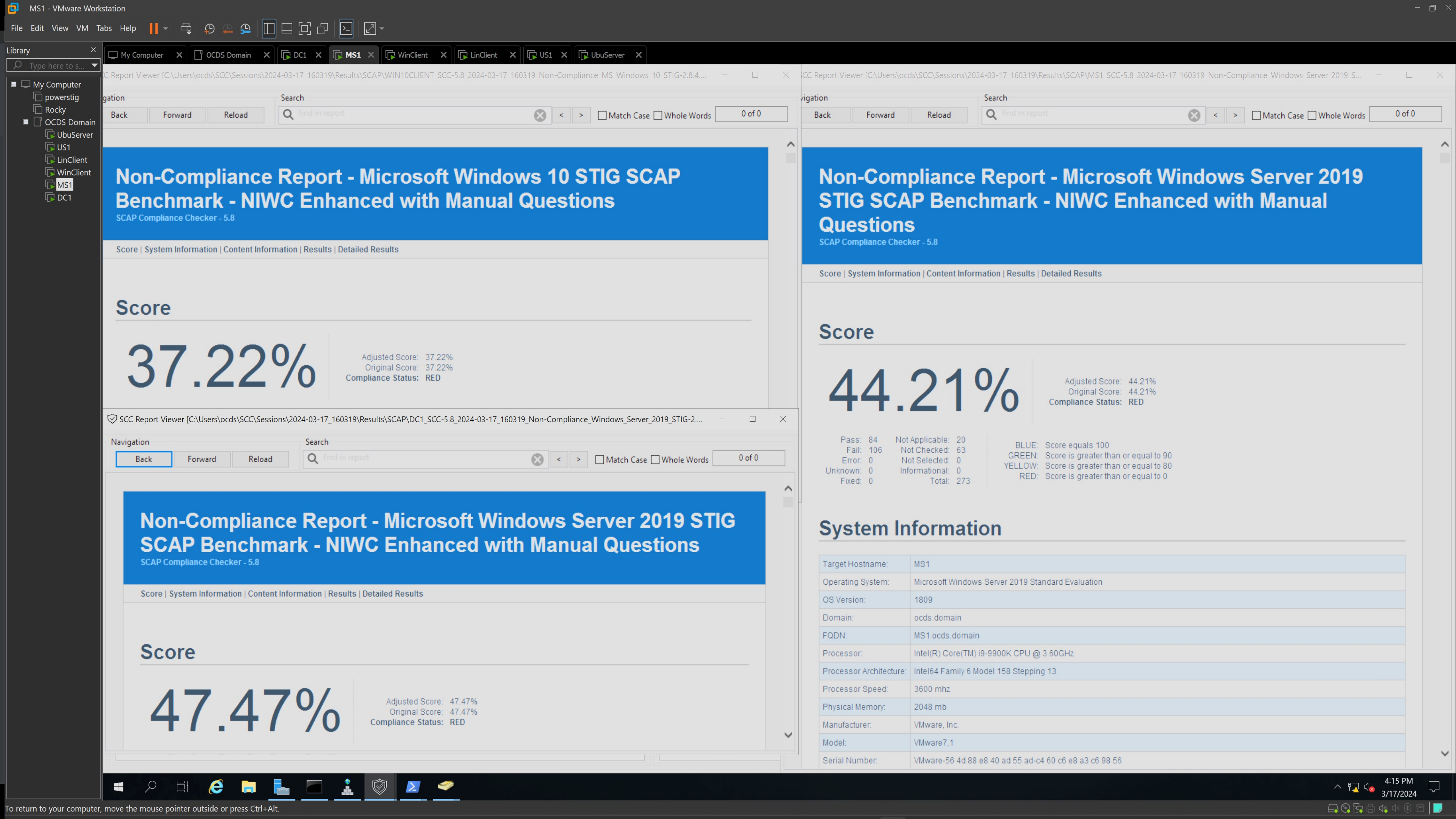
```
PS C:\Users\ocds> ping dc1

Pinging dc1.ocds.domain [192.168.155.134] with 32 bytes of data:
Reply from 192.168.155.134: bytes=32 time<1ms TTL=128
Reply from 192.168.155.134: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.155.134:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\ocds> Enter-PSSession dc1
[dc1]: PS C:\Users\OCDS\Documents> hostname
dc1
[dc1]: PS C:\Users\OCDS\Documents>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ocds> ping win10client

Pinging win10client.ocds.domain [192.168.155.136] with 32 bytes of data:
Reply from 192.168.155.136: bytes=32 time<1ms TTL=128
Reply from 192.168.155.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.155.136:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\ocds> Enter-PSSession win10client
[win10client]: PS C:\Users\ocds.OCDS\Documents> hostname
Win10Client
[win10client]: PS C:\Users\ocds.OCDS\Documents>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ocds> hostname
MS1
PS C:\Users\ocds>
```

```
PS C:\Users\ocds> ping 192.168.155.138

Pinging 192.168.155.138 with 32 bytes of data:
Reply from 192.168.155.138: bytes=32 time<1ms TTL=64
Reply from 192.168.155.138: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.155.138:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\ocds> ssh ocds\ocds@192.168.155.138
ocds\ocds@192.168.155.138's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sun Mar 17 10:49:46 PM UTC 2024

  System load:  0.06787109375      Processes:             225
  Usage of /:   24.9% of 28.36GB   Users logged in:       0
  Memory usage: 11%                IPv4 address for ens33: 192.168.155.138
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connectio
n or proxy settings


Last login: Sun Mar 17 22:48:42 2024 from 192.168.155.137
ocds@ocds.domain@us1:~$ ls /
bin   cdrom  etc   lib    lib64   lost+found  mnt   proc  run   snap  swap.img  tmp  var
boot  dev    home  lib32  libx32  media       opt   root  sbin  srv   sys       usr
ocds@ocds.domain@us1:~$
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ocds> ping 192.168.155.139

Pinging 192.168.155.139 with 32 bytes of data:
Reply from 192.168.155.139: bytes=32 time=1ms TTL=64
Reply from 192.168.155.139: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.155.139:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\ocds> ssh ocds\ocds@192.168.155.139
The authenticity of host '192.168.155.139 (192.168.155.139)' can't be established.
ECDSA key fingerprint is SHA256:ZjldSdfG5PLyYv1yuiUM7JnqtC4pSxotvcvZW0hwnjA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.155.139' (ECDSA) to the list of known hosts.
ocds\ocds@192.168.155.139's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Mar 15 19:46:55 2024 from 192.168.155.137
ocds@ocds.domain@uc1:~$ ls /
bin   cdrom  etc   lib    lib64   lost+found  mnt   proc  run   snap  swapfile  tmp  var
boot  dev    home  lib32  libx32  media       opt   root  sbin  srv   sys       usr
ocds@ocds.domain@uc1:~$
```



C Report Viewer [C:\Users\ocds\SCC\Sessions\2024-03-17_160319\Results\SCAP\WIN10CLIENT_SCC-5.8_2024-03-17_160319_Non-Compliance_MS_Windows_10_STIG-2.8.4....

Non-Compliance Report - Microsoft Windows 10 STIG SCAP Benchmark - NIWC Enhanced with Manual Questions

SCAP Compliance Checker - 5.8

Score | System Information | Content Information | Results | Detailed Results

Score

37.22%

Adjusted Score: 37.22%
Original Score: 37.22%
Compliance Status: RED

SCC Report Viewer [C:\Users\ocds\SCC\Sessions\2024-03-17_160319\Results\SCAP\DC1_SCC-5.8_2024-03-17_160319_Non-Compliance_Windows_Server_2019_STIG-2....

Non-Compliance Report - Microsoft Windows Server 2019 STIG SCAP Benchmark - NIWC Enhanced with Manual Questions

SCAP Compliance Checker - 5.8

Score | System Information | Content Information | Results | Detailed Results

Score

47.47%

Adjusted Score: 47.47%
Original Score: 47.47%
Compliance Status: RED

CC Report Viewer [C:\Users\ocds\SCC\Sessions\2024-03-17_160319\Results\SCAP\MS1_SCC-5.8_2024-03-17_160319_Non-Compliance_Windows_Server_2019_S...

Non-Compliance Report - Microsoft Windows Server 2019 STIG SCAP Benchmark - NIWC Enhanced with Manual Questions

SCAP Compliance Checker - 5.8

Score | System Information | Content Information | Results | Detailed Results

Score

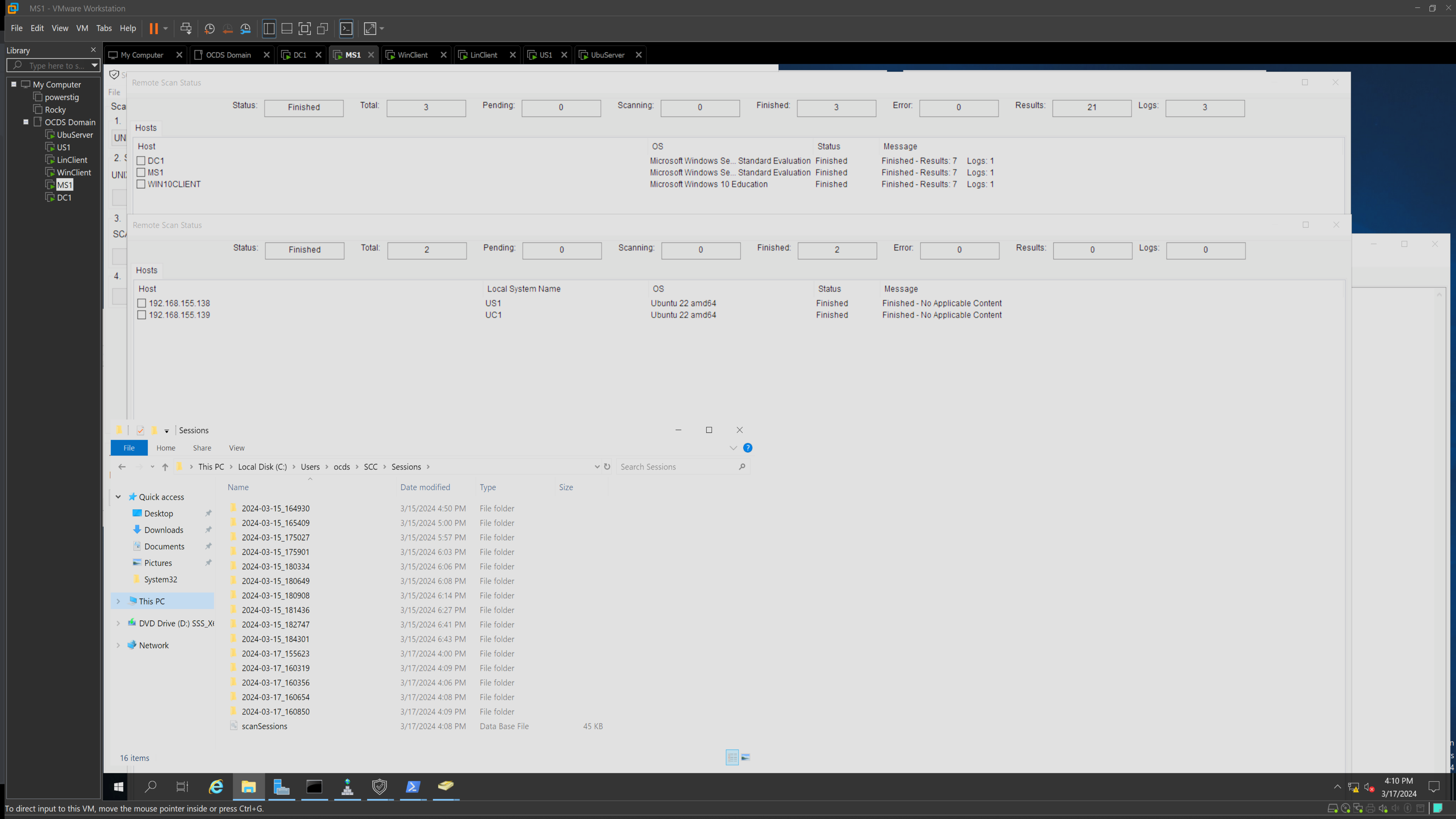
44.21%

Adjusted Score: 44.21%
Original Score: 44.21%
Compliance Status: RED

```
   Pass:  84     Not Applicable:  20        BLUE:  Score equals 100
   Fail:  106       Not Checked:  63       GREEN:  Score is greater than or equal to 90
  Error:  0        Not Selected:  0       YELLOW:  Score is greater than or equal to 80
Unknown:  0       Informational:  0          RED:  Score is greater than or equal to 0
  Fixed:  0               Total:  273
```

System Information

Target Hostname:	MS1
Operating System:	Microsoft Windows Server 2019 Standard Evaluation
OS Version:	1809
Domain:	ocds.domain
FQDN:	MS1.ocds.domain
Processor:	Intel(R) Core(TM) i9-9900K CPU @ 3.60GHz
Processor Architecture:	Intel64 Family 6 Model 158 Stepping 13
Processor Speed:	3600 mhz
Physical Memory:	2048 mb
Manufacturer:	VMware, Inc.
Model:	VMware7,1
Serial Number:	VMware-56 4d 88 e8 40 ad 55 ad-c4 60 c6 e8 a3 c6 98 56



Remote Scan Status

Status: Finished Total: 3 Pending: 0 Scanning: 0 Finished: 3 Error: 0 Results: 21 Logs: 3

Hosts

Host	OS	Status	Message
□ DC1	Microsoft Windows Se... Standard Evaluation	Finished	Finished - Results: 7 Logs: 1
□ MS1	Microsoft Windows Se... Standard Evaluation	Finished	Finished - Results: 7 Logs: 1
□ WIN10CLIENT	Microsoft Windows 10 Education	Finished	Finished - Results: 7 Logs: 1

Remote Scan Status

Status: Finished Total: 2 Pending: 0 Scanning: 0 Finished: 2 Error: 0 Results: 0 Logs: 0

Hosts

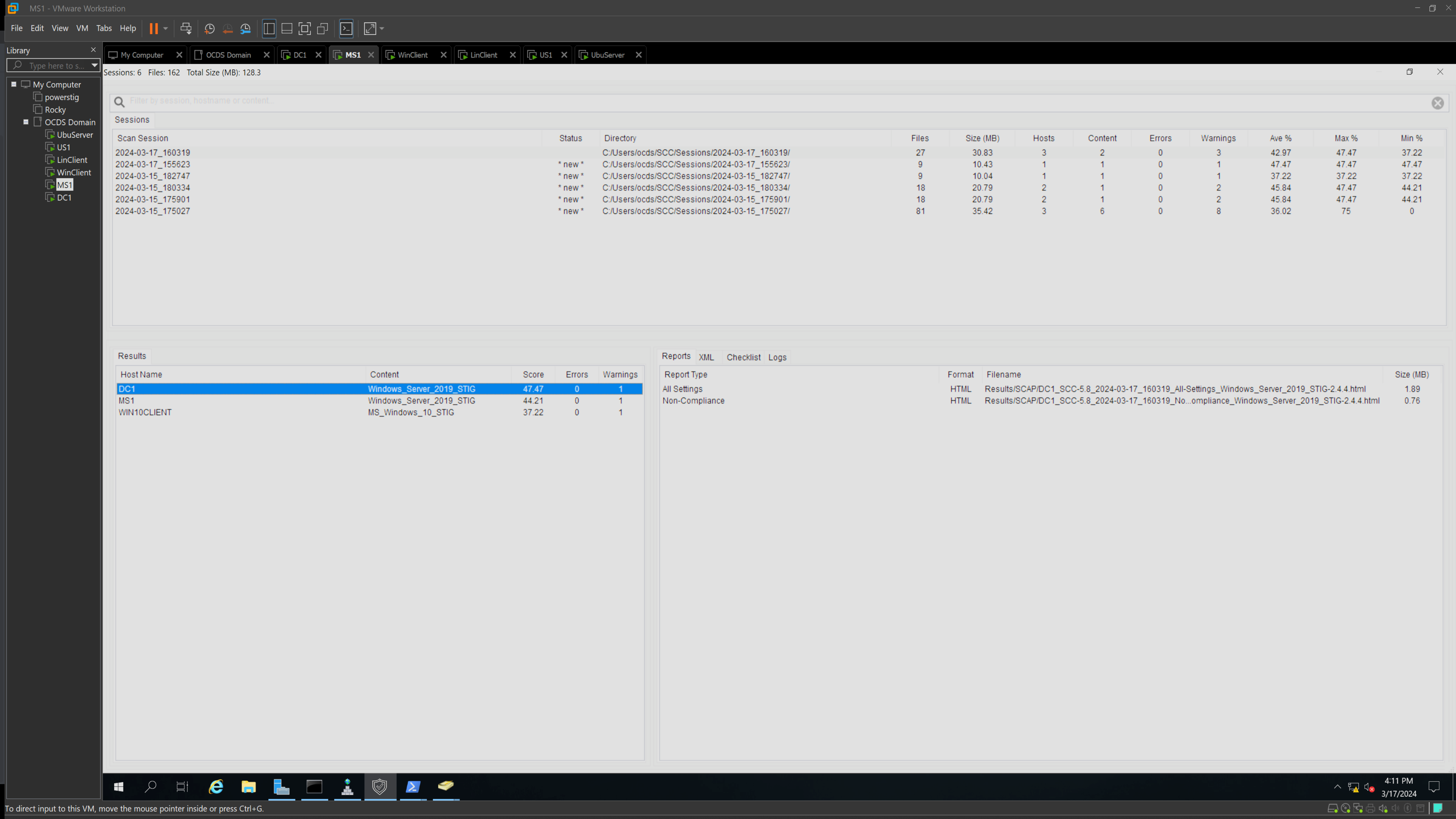
Host	Local System Name	OS	Status	Message
□ 192.168.155.138	US1	Ubuntu 22 amd64	Finished	Finished - No Applicable Content
□ 192.168.155.139	UC1	Ubuntu 22 amd64	Finished	Finished - No Applicable Content

Sessions

Name	Date modified	Type	Size
2024-03-15_164930	3/15/2024 4:50 PM	File folder	
2024-03-15_165409	3/15/2024 5:00 PM	File folder	
2024-03-15_175027	3/15/2024 5:57 PM	File folder	
2024-03-15_175901	3/15/2024 6:03 PM	File folder	
2024-03-15_180334	3/15/2024 6:06 PM	File folder	
2024-03-15_180649	3/15/2024 6:08 PM	File folder	
2024-03-15_180908	3/15/2024 6:14 PM	File folder	
2024-03-15_181436	3/15/2024 6:27 PM	File folder	
2024-03-15_182747	3/15/2024 6:41 PM	File folder	
2024-03-15_184301	3/15/2024 6:43 PM	File folder	
2024-03-17_155623	3/17/2024 4:00 PM	File folder	
2024-03-17_160319	3/17/2024 4:09 PM	File folder	
2024-03-17_160356	3/17/2024 4:06 PM	File folder	
2024-03-17_160654	3/17/2024 4:08 PM	File folder	
2024-03-17_160850	3/17/2024 4:09 PM	File folder	
scanSessions	3/17/2024 4:08 PM	Data Base File	45 KB

16 items

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Sessions: 6   Files: 162   Total Size (MB): 128.3

Scan Session	Status	Directory	Files	Size (MB)	Hosts	Content	Errors	Warnings	Ave %	Max %	Min %
2024-03-17_160319		C:/Users/ocds/SCC/Sessions/2024-03-17_160319/	27	30.83	3	2	0	3	42.97	47.47	37.22
2024-03-17_155623	* new *	C:/Users/ocds/SCC/Sessions/2024-03-17_155623/	9	10.43	1	1	0	1	47.47	47.47	47.47
2024-03-15_182747	* new *	C:/Users/ocds/SCC/Sessions/2024-03-15_182747/	9	10.04	1	1	0	1	37.22	37.22	37.22
2024-03-15_180334	* new *	C:/Users/ocds/SCC/Sessions/2024-03-15_180334/	18	20.79	2	1	0	2	45.84	47.47	44.21
2024-03-15_175901	* new *	C:/Users/ocds/SCC/Sessions/2024-03-15_175901/	18	20.79	2	1	0	2	45.84	47.47	44.21
2024-03-15_175027	* new *	C:/Users/ocds/SCC/Sessions/2024-03-15_175027/	81	35.42	3	6	0	8	36.02	75	0

Host Name	Content	Score	Errors	Warnings
DC1	Windows_Server_2019_STIG	47.47	0	1
MS1	Windows_Server_2019_STIG	44.21	0	1
WIN10CLIENT	MS_Windows_10_STIG	37.22	0	1

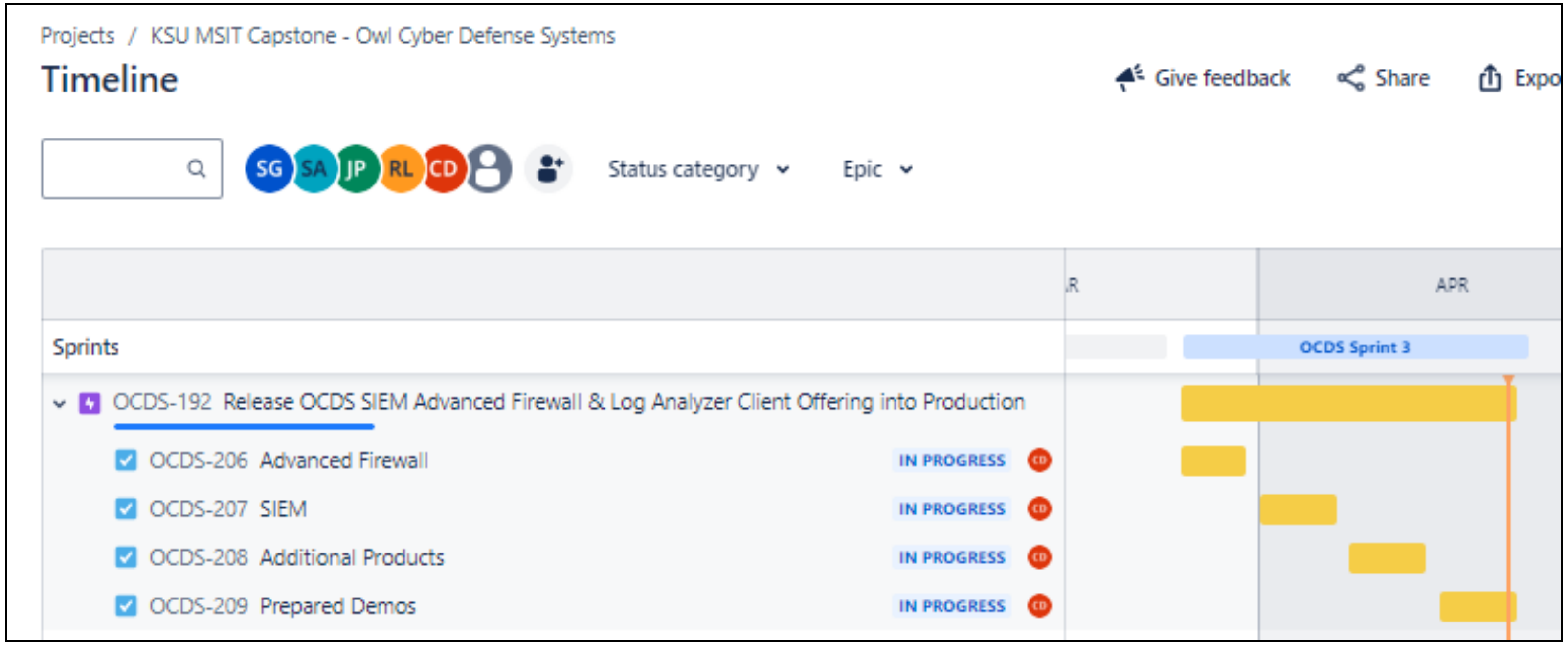
Report Type	Format	Filename	Size (MB)
All Settings	HTML	Results/SCAP/DC1_SCC-5.8_2024-03-17_160319_All-Settings_Windows_Server_2019_STIG-2.4.4.html	1.89
Non-Compliance	HTML	Results/SCAP/DC1_SCC-5.8_2024-03-17_160319_No...ompliance_Windows_Server_2019_STIG-2.4.4.html	0.76

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Epic: Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production

Chris Dunbar

Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production



Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

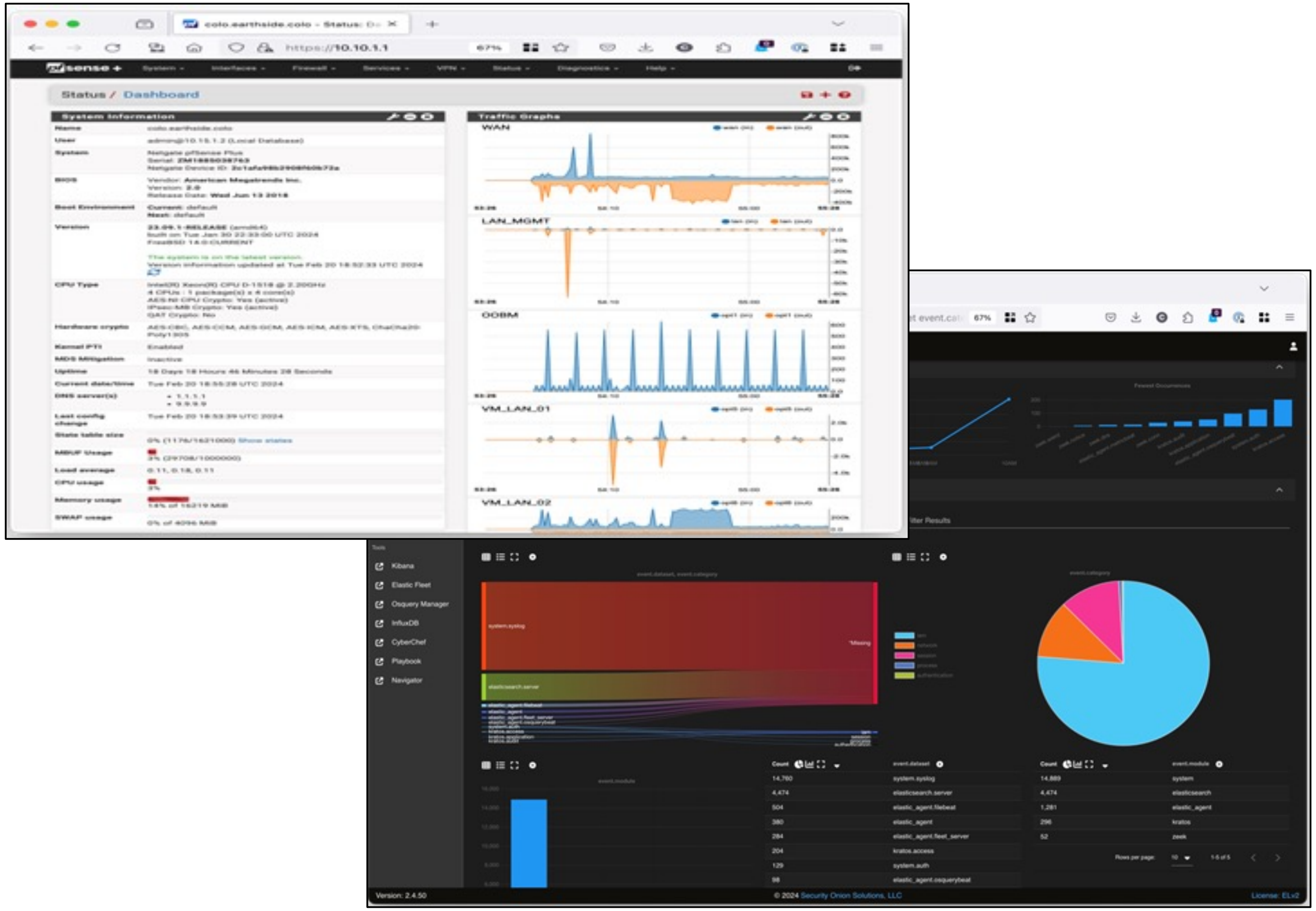
OCDS-192 Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production

☑ OCDS-206	Advanced Firewall	IN PROGRESS
☑ OCDS-207	SIEM	IN PROGRESS
☑ OCDS-208	Additional Products	IN PROGRESS
☑ OCDS-209	Prepared Demos	IN PROGRESS

Complete/On Track

Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production

- Configured Security Onion VM and open source SEIM network & security monitoring tool for client offering.
- Configured SPAN port at data center
- Self-hosted on VMWare ESXi virtual infrastructure



System Information

Name	colo.earthside.colo
User	admin@10.15.1.2 (Local Database)
System	Netgate pfSense Plus Serial: ZM1885038763 Netgate Device ID: 2c1afa98b2908f60b72a
BIOS	Vendor: American Megatrends Inc. Version: 2.0 Release Date: Wed Jun 13 2018
Boot Environment	Current: default Next: default
Version	23.09.1-RELEASE (amd64) built on Tue Jan 30 22:33:00 UTC 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 18:52:33 UTC 2024
CPU Type	Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz 4 CPUs : 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (active) IPsec-MB Crypto: Yes (active) QAT Crypto: No
Hardware crypto	AES-CBC, AES-CCM, AES-GCM, AES-ICM, AES-XTS, ChaCha20-Poly1305
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	18 Days 18 Hours 46 Minutes 28 Seconds
Current date/time	Tue Feb 20 18:55:28 UTC 2024
DNS server(s)	• 1.1.1.1 • 9.9.9.9
Last config change	Tue Feb 20 18:53:39 UTC 2024
State table size	0% (1176/1621000) Show states
MBUF Usage	3% (29708/1000000)
Load average	0.11, 0.18, 0.11
CPU usage	3%
Memory usage	14% of 16219 MiB
SWAP usage	0% of 4096 MiB

Count	event.dataset
14,760	system.syslog
4,474	elasticsearch.server
504	elastic_agent.filebeat
380	elastic_agent
284	elastic_agent.fleet_server
204	kratos.access
129	system.auth
98	elastic_agent.osquerybeat

Count	event.module
14,889	system
4,474	elasticsearch
1,281	elastic_agent
296	kratos
52	zeek

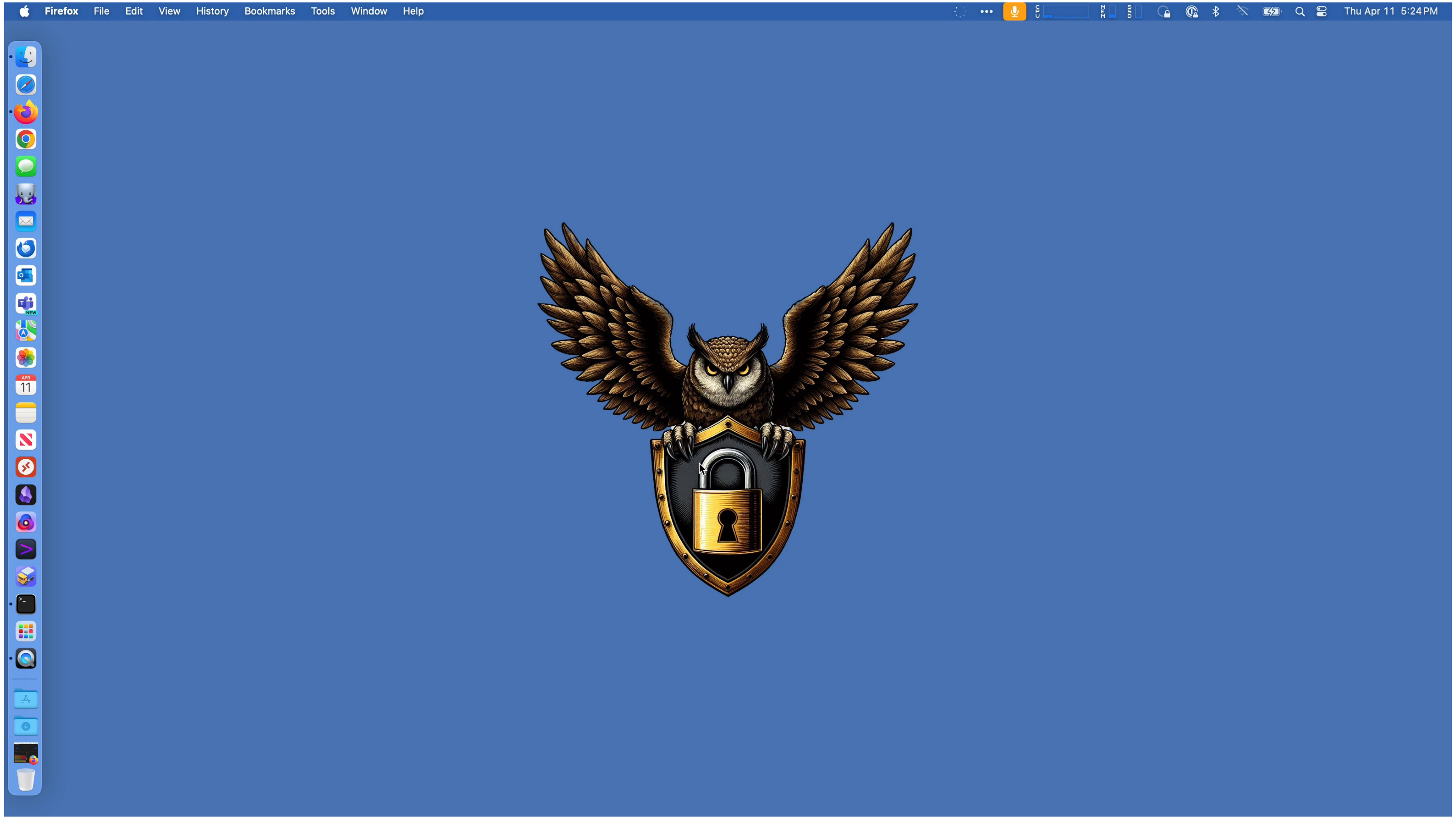
Rows per page: 10 1-5 of 5

Version: 2.4.50 © 2024 Security Onion Solutions, LLC License: ELv2

Chris Dunbar

Release OCDS SIEM Advanced Firewall & Log Analyzer Client Offering into Production

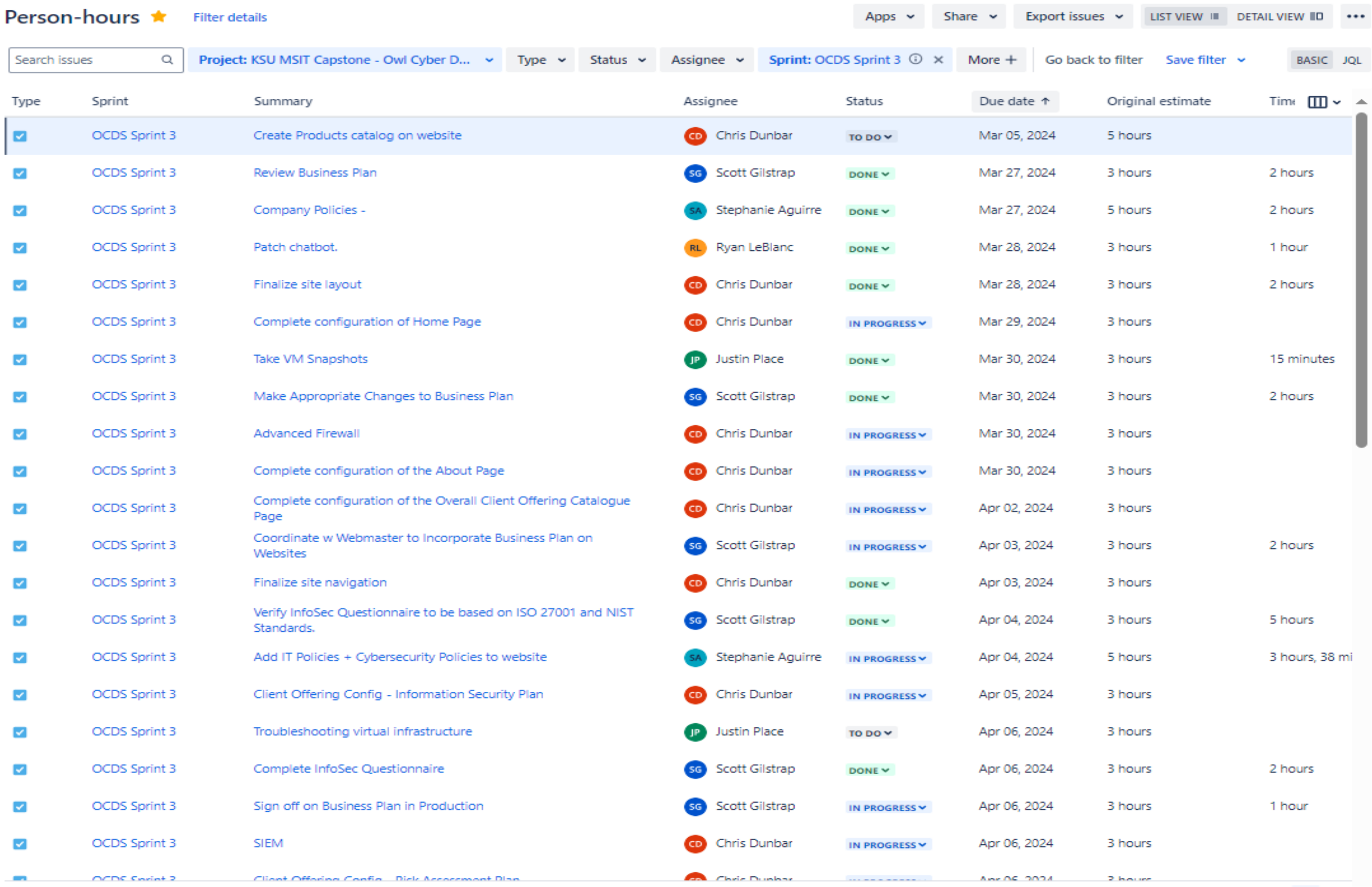
- Click to play video
- Hardening process based on NIST guidelines and appropriate STIGs
- Pings all VMs from MS1 showing connectivity
- Enter PSSession to show STIG & run script – changes registry
- SSH to Ubuntu client
- Launch SCAP
- Host files
- Run scans
- Scores



Owner: Chris Dunbar

Sprint 3 Time Tracking

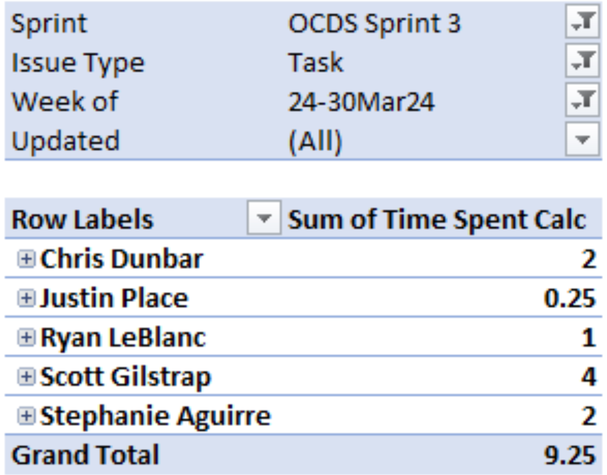
Sprint 3 Person-hour Time Tracking (Real-time Jira project export)



Person-hours ★ Filter details

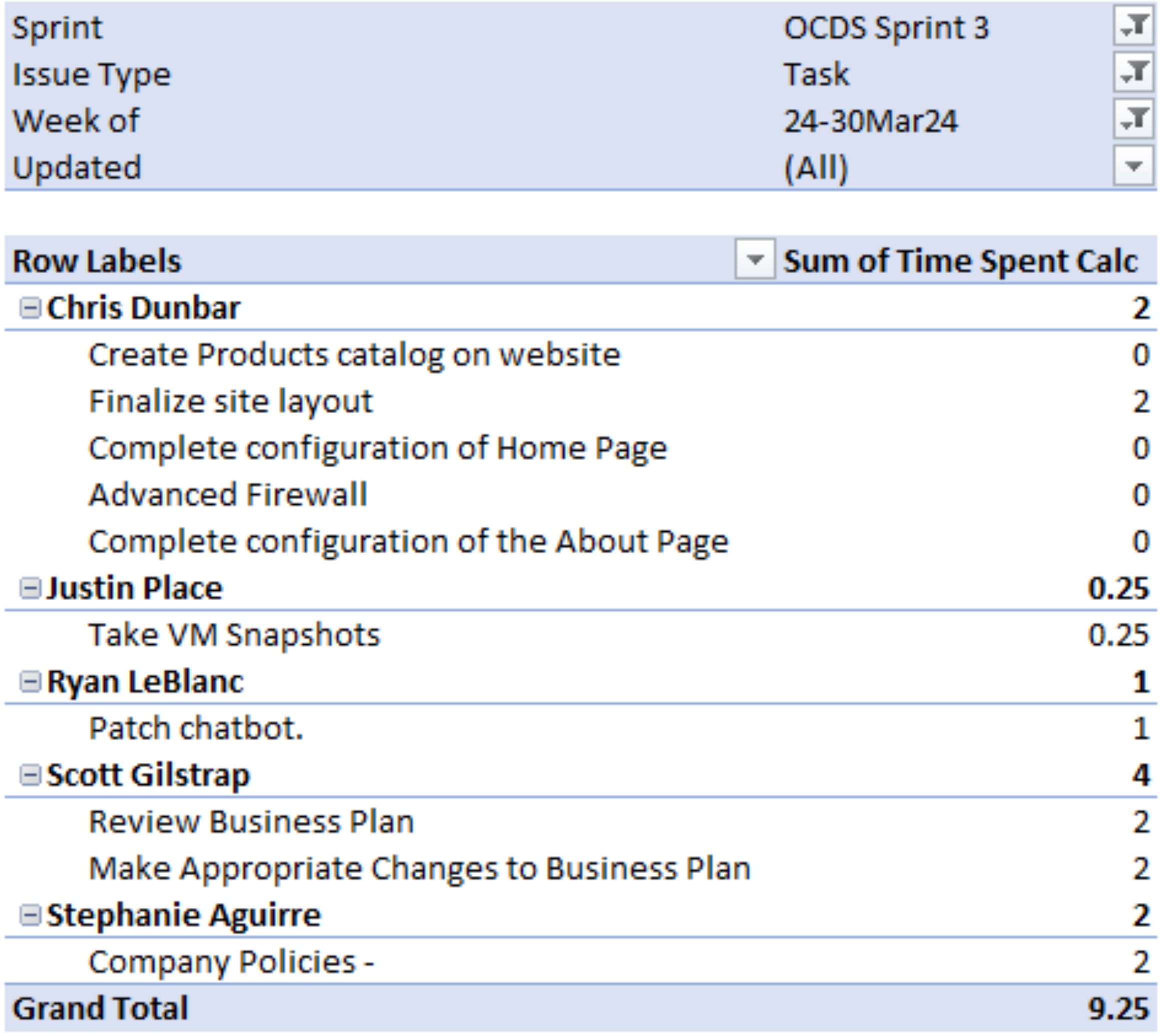
Type	Sprint	Summary	Assignee	Status	Due date ↑	Original estimate	Tim
☑	OCDS Sprint 3	Create Products catalog on website	CD Chris Dunbar	TO DO	Mar 05, 2024	5 hours	
☑	OCDS Sprint 3	Review Business Plan	SG Scott Gilstrap	DONE	Mar 27, 2024	3 hours	2 hours
☑	OCDS Sprint 3	Company Policies -	SA Stephanie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

Person-hours Automated Report: Week-1 24-30Mar24



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	24-30Mar24
Updated	(All)

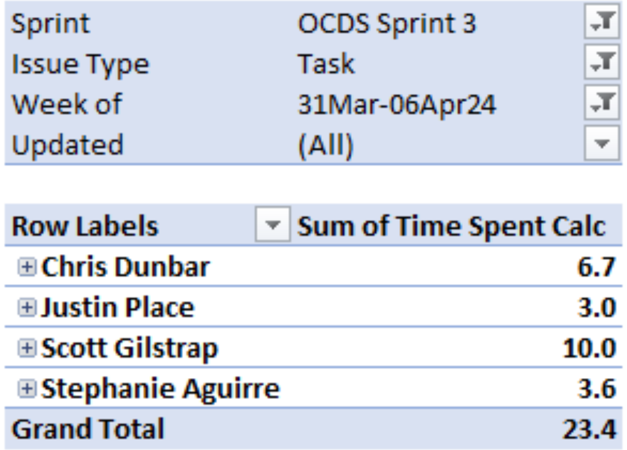
Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	2
⊞ Justin Place	0.25
⊞ Ryan LeBlanc	1
⊞ Scott Gilstrap	4
⊞ Stephanie Aguirre	2
Grand Total	9.25



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	24-30Mar24
Updated	(All)

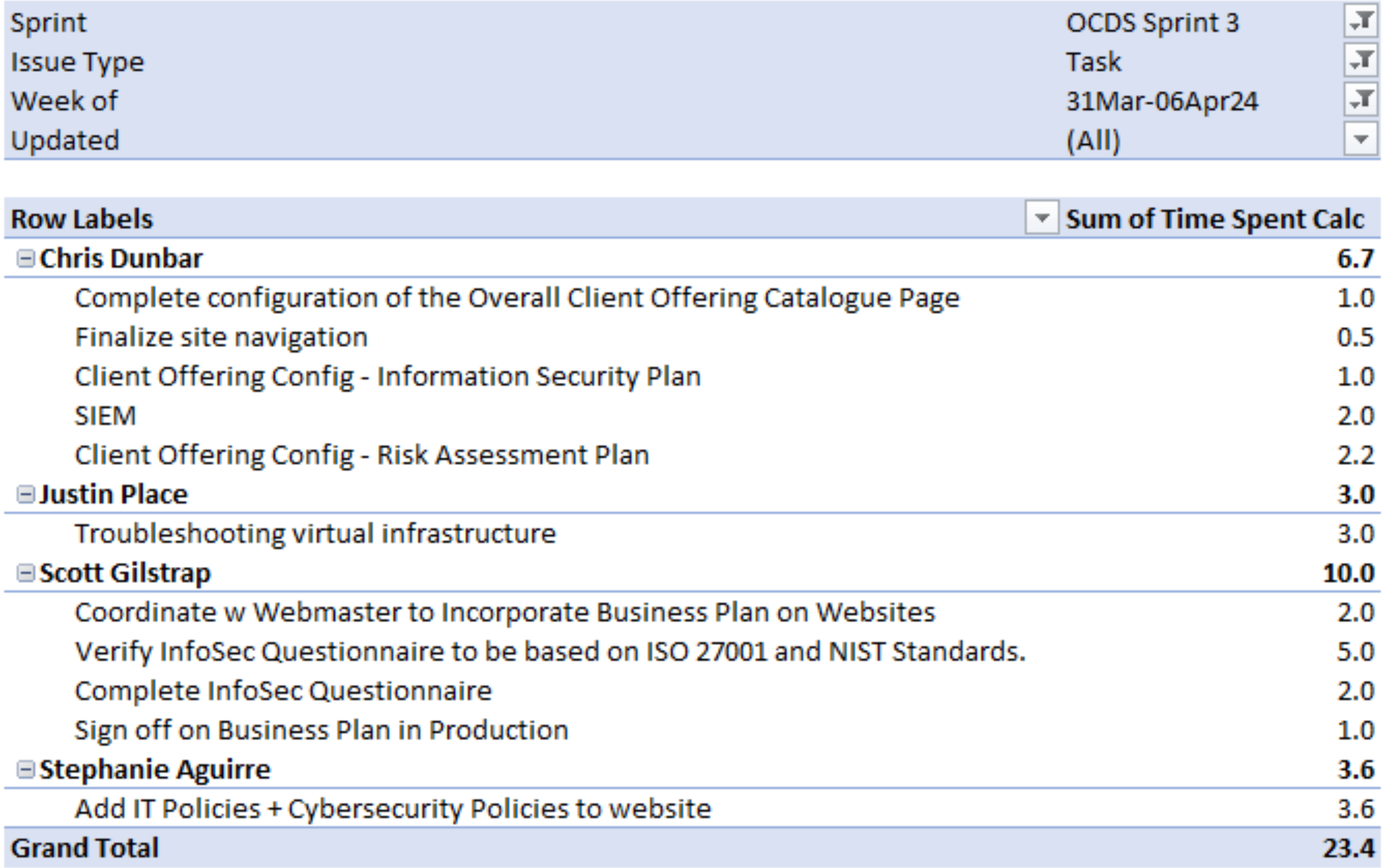
Row Labels	Sum of Time Spent Calc
⊟ **Chris Dunbar**	**2**
Create Products catalog on website	0
Finalize site layout	2
Complete configuration of Home Page	0
Advanced Firewall	0
Complete configuration of the About Page	0
⊟ **Justin Place**	**0.25**
Take VM Snapshots	0.25
⊟ **Ryan LeBlanc**	**1**
Patch chatbot.	1
⊟ **Scott Gilstrap**	**4**
Review Business Plan	2
Make Appropriate Changes to Business Plan	2
⊟ **Stephanie Aguirre**	**2**
Company Policies -	2
Grand Total	**9.25**

Person-hours Automated Report: Week-2 31Mar-06Apr24



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	31Mar-06Apr24
Updated	(All)

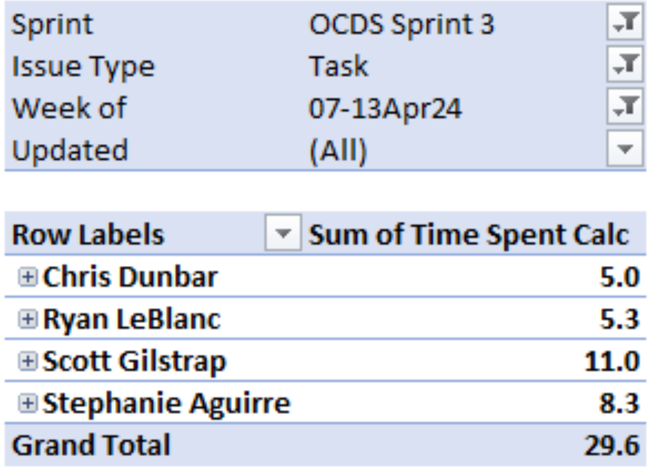
Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	6.7
⊞ Justin Place	3.0
⊞ Scott Gilstrap	10.0
⊞ Stephanie Aguirre	3.6
Grand Total	**23.4**



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	31Mar-06Apr24
Updated	(All)

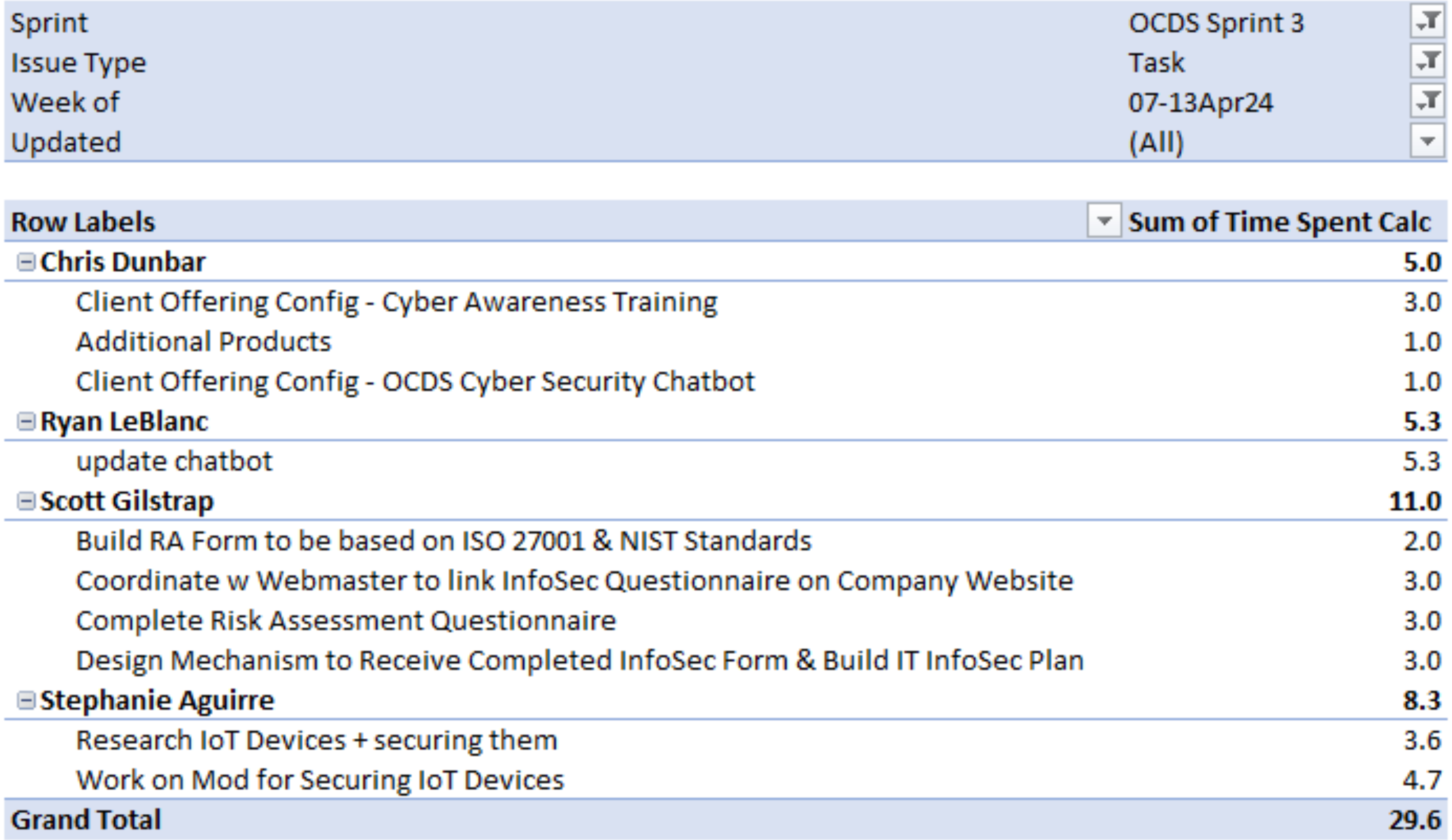
Row Labels	Sum of Time Spent Calc
⊟ Chris Dunbar	**6.7**
Complete configuration of the Overall Client Offering Catalogue Page	1.0
Finalize site navigation	0.5
Client Offering Config - Information Security Plan	1.0
SIEM	2.0
Client Offering Config - Risk Assessment Plan	2.2
⊟ Justin Place	**3.0**
Troubleshooting virtual infrastructure	3.0
⊟ Scott Gilstrap	**10.0**
Coordinate w Webmaster to Incorporate Business Plan on Websites	2.0
Verify InfoSec Questionnaire to be based on ISO 27001 and NIST Standards.	5.0
Complete InfoSec Questionnaire	2.0
Sign off on Business Plan in Production	1.0
⊟ Stephanie Aguirre	**3.6**
Add IT Policies + Cybersecurity Policies to website	3.6
Grand Total	**23.4**

Person-hours Automated Report: Week-3 07-13Apr24



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	07-13Apr24
Updated	(All)

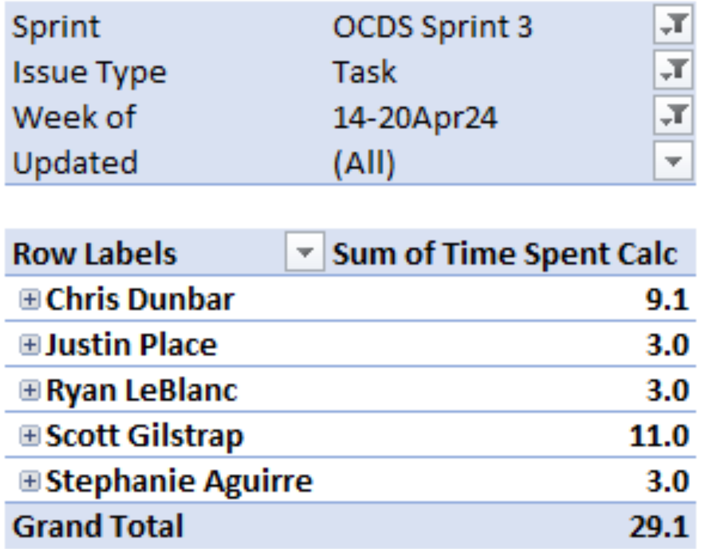
Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	5.0
⊞ Ryan LeBlanc	5.3
⊞ Scott Gilstrap	11.0
⊞ Stephanie Aguirre	8.3
Grand Total	**29.6**



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	07-13Apr24
Updated	(All)

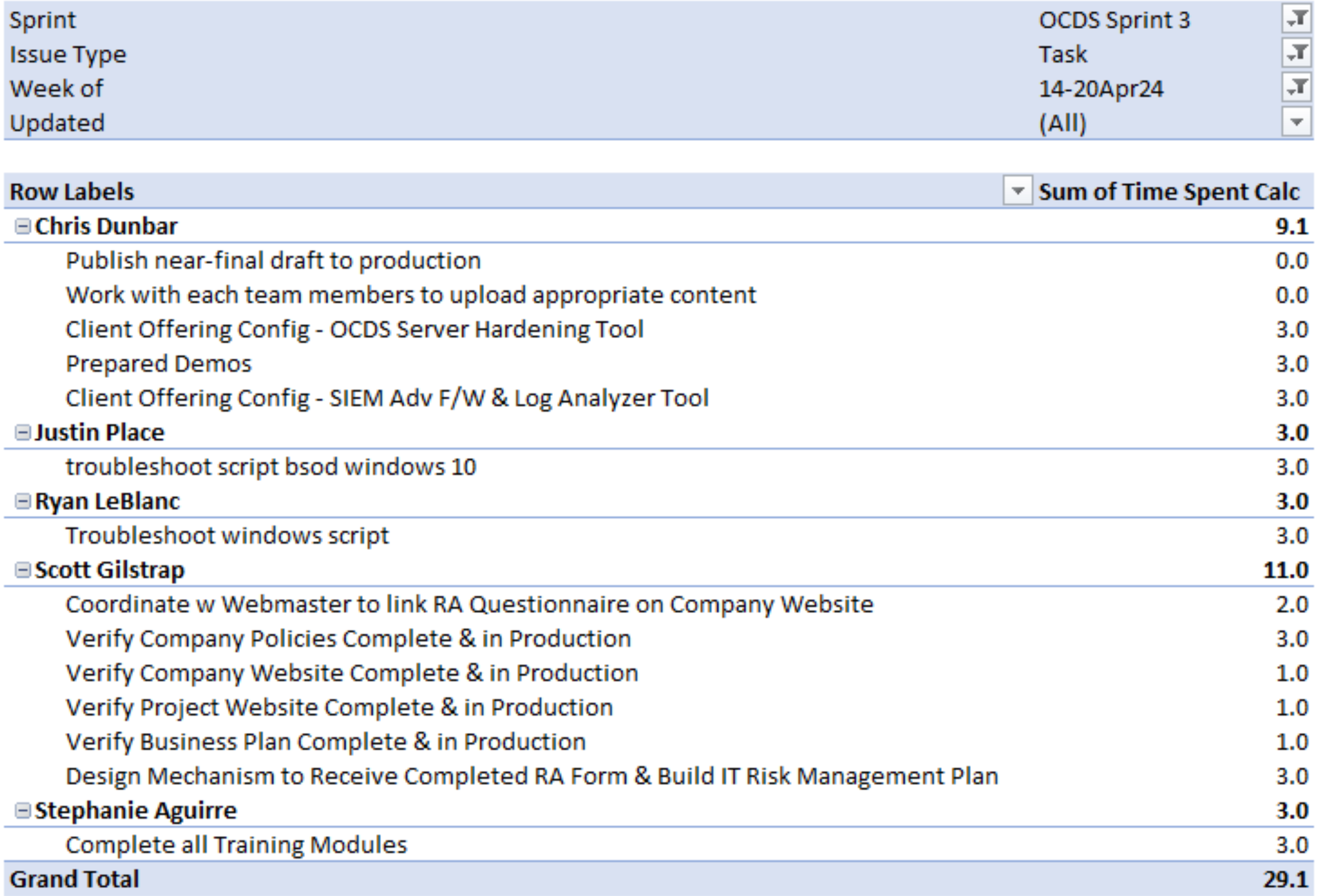
Row Labels	Sum of Time Spent Calc
⊟ **Chris Dunbar**	**5.0**
Client Offering Config - Cyber Awareness Training	3.0
Additional Products	1.0
Client Offering Config - OCDS Cyber Security Chatbot	1.0
⊟ **Ryan LeBlanc**	**5.3**
update chatbot	5.3
⊟ **Scott Gilstrap**	**11.0**
Build RA Form to be based on ISO 27001 & NIST Standards	2.0
Coordinate w Webmaster to link InfoSec Questionnaire on Company Website	3.0
Complete Risk Assessment Questionnaire	3.0
Design Mechanism to Receive Completed InfoSec Form & Build IT InfoSec Plan	3.0
⊟ **Stephanie Aguirre**	**8.3**
Research IoT Devices + securing them	3.6
Work on Mod for Securing IoT Devices	4.7
Grand Total	**29.6**

Person-hours Automated Report: Week-4 14-20Apr24



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	14-20Apr24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	9.1
⊞ Justin Place	3.0
⊞ Ryan LeBlanc	3.0
⊞ Scott Gilstrap	11.0
⊞ Stephanie Aguirre	3.0
Grand Total	29.1

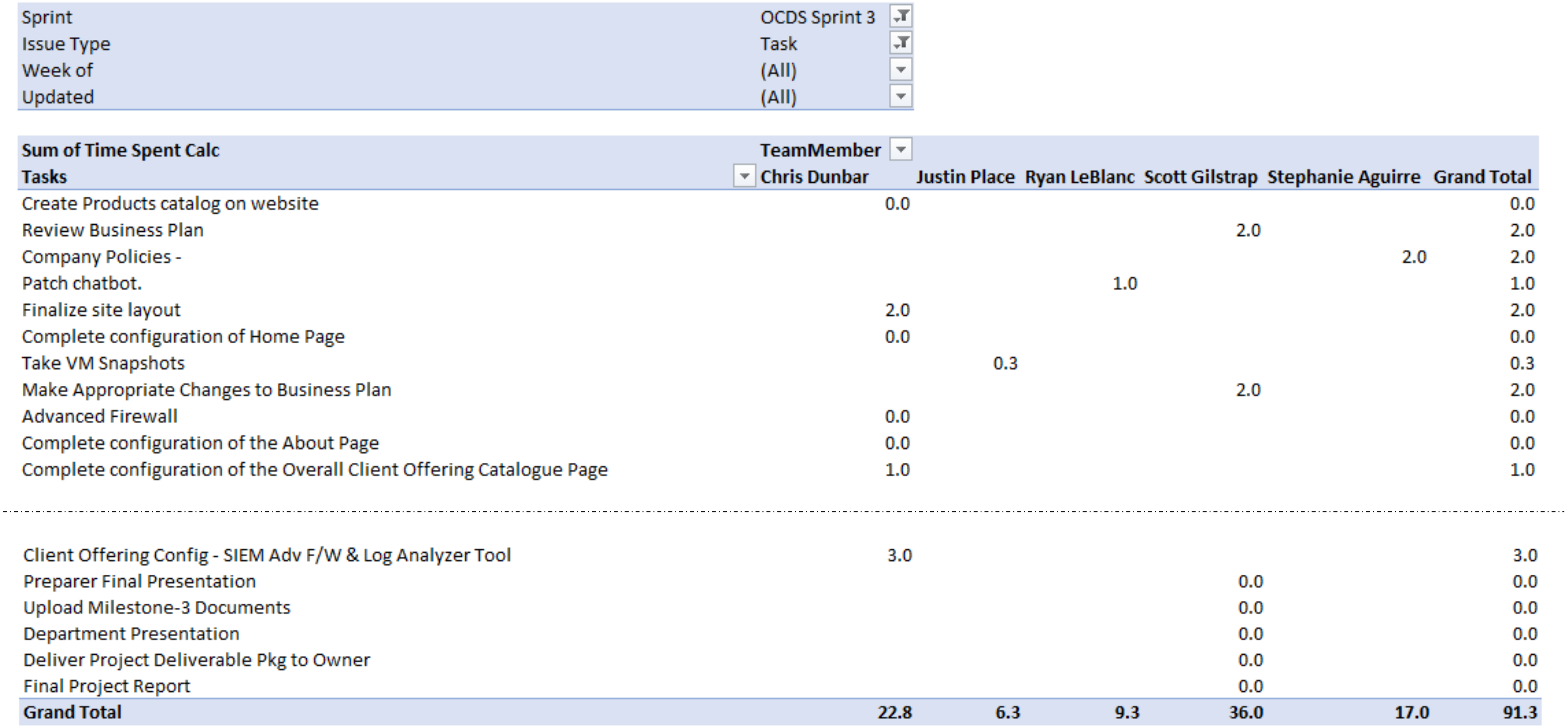


Sprint	OCDS Sprint 3
Issue Type	Task
Week of	14-20Apr24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊟ **Chris Dunbar**	**9.1**
Publish near-final draft to production	0.0
Work with each team members to upload appropriate content	0.0
Client Offering Config - OCDS Server Hardening Tool	3.0
Prepared Demos	3.0
Client Offering Config - SIEM Adv F/W & Log Analyzer Tool	3.0
⊟ **Justin Place**	**3.0**
troubleshoot script bsod windows 10	3.0
⊟ **Ryan LeBlanc**	**3.0**
Troubleshoot windows script	3.0
⊟ **Scott Gilstrap**	**11.0**
Coordinate w Webmaster to link RA Questionnaire on Company Website	2.0
Verify Company Policies Complete & in Production	3.0
Verify Company Website Complete & in Production	1.0
Verify Project Website Complete & in Production	1.0
Verify Business Plan Complete & in Production	1.0
Design Mechanism to Receive Completed RA Form & Build IT Risk Management Plan	3.0
⊟ **Stephanie Aguirre**	**3.0**
Complete all Training Modules	3.0
Grand Total	**29.1**

Sprint 3 Person-hour Time Tracking (Team Totals)

- Chris Dunbar
- Justin Place
- Ryan LeBlanc
- Scott Gilstrap
- Stephanie Aguirre



Sprint	OCDS Sprint 3
Issue Type	Task
Week of	(All)
Updated	(All)

Sum of Time Spent Calc	**TeamMember**					
Tasks	**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
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
Grand Total	**22.8**	**6.3**	**9.3**	**36.0**	**17.0**	**91.3**

Project Performance & Experience

Recap/Review/Reflection

Milestone 3 Goals

Strategic Objective:

Establish the OCDS cybersecurity business providing small businesses cost effective tools to increase their cybersecurity protection posture at an affordable rate

Sprint 3

Mar 26 – Apr 21, 2024

Operational Objectives

- Business Plan fully completed and published
- Company Policies published in Business Plan
- Project Website deployed and released into production with all documentation
- Company Website deployed and released into production
- Cyber Awareness Training Modules deployed and released into production on website
- IT Security Plan deployed and released into production on the website
- Proprietary Risk Assessment deployed and released into production on the website
- AI Security Chatbot deployed and released into production on the website
- Server Hardening Tool deployed and released into production
- SIEM Advanced Firewall and Log Analyzer deployed and released into production

Project Performance & Experience

- Accomplishments
  - Staying on track to complete each milestone task in a timely matter. Creating the cyber security training and awareness training modules.
  - Getting a mixture of code working to initially create a chatbot and create python scrips to format datasets so the chatbot could learn.
  - Implemented and adjusted the RTX chatbot to be more OCDS specific/proprietary.
  - Created a Windows 10, two Ubuntu (desktop and server) systems and two Server 2019 VM's. Created virtualized domain infrastructure to include three Windows OS's and two Linux OS's. Assisted in the development of AI training model data used for chat bot.
  - Used Jira for a complete project for the first time and created the automated Person-hour export. Used Microsoft Forms to create the IT Security Planning Tool as well as the proprietary Client Risk Assessment tool. Also created the detailed and robust company Business Plan.
- Challenges
  - Deciding on the presentation format of our cyber security training and awareness for this project. Researched a lot of different trainings to get an idea on what to do for ours and the look & feel.
  - Learning and becoming efficient at Python coding. There was also an ML/AI learning curve.
  - A few challenges faced were joining Linux machines to the virtualized domain. Editing AI training model data for accuracy. Training original AI bot for optimal accuracy. Creating PowerShell script to automate STIG process.
  - Trying to figure out how to get AI to collect all the data from the client and generate an automated Risk Assessment. I ended up with some automation, but I still had some manual effort as well to generate the proprietary Risk Assessment Plan for the client.
  - Time management was a big challenge. With a fulltime career being on the verge of a promotion to Director, taking Scrum Master certification courses, being in the Navy Reserves in the process of transferring to the Army National Guard as a Cyber Warrant Officer, and managing a family all while taking this Capstone class and working this project has proven to be very taxing and time consuming.
  - Configuring the Span Port correct in the data center for the SIEM data collection.

Project Performance & Experience

- Lessons Learned
  - Time goes by fast when researching information for a project and applying all the information learned. You think you have all the time in the world, but before you know it — it's time to submit the final project.
  - ML/AI is only as good as the dataset that is prepared, and ML/AI can be created to be bias as the dataset is what it builds from.
  - Over the course of the semester, I learned a lot regarding AI. I learned about the different models and methods that could be used in creating and training an AI. How to trim the AI dataset for increased accuracy.
  - Good, detailed planning and adherence to that plan is always required when a lot is going on.
  - Thorough research is key to collecting data, developing a good plan, and executing on that plan.
  - Communication is extremely important for a multifaceted project – always keep everyone informed. Meet and/or exchange information often. Adherence to the scrum meeting methodology is important to good project tracking and a successful project.
- Opportunities for Improvement
  - Time management is still something to work on. Hold ourselves accountable every day instead of tackling all tasks in one day and having one day of research/working on the project.
  - Python coding experience and better understanding of ML/AI language models, and the intricate networks that are designed to make them self learn.
  - More precise datasets for AI model. Learn more about how the different AI datasets work and how to optimize model used for optimal performance. Increase PowerShell scripting knowledge.
  - Stay focused on my current topic at hand. Finish a thought or a task before trying to multi-task too much and get too much going at one time causing a lose of focus and losing track of current task status. If multi-tasking is required keep good notes and log everything.
  - Execute on the plan. Learn to be concise in my delivery. Stay focused on short, deliberate, well-worded and informative speaking points.

Next Steps

What’s next for OCDS

- OCDS at C-Day! – April 25, 2024
- Department presentation of OCDS project – April 28, 2024
- Final Project Report by May 5, 2024
- Each member to conduct…
  - End Term Peer Evaluation by May 1, 2024
  - Capstone Self Reflection by May 1, 2024
  - Career Profile (LinkedIn) by April 28, 2024
- Celebrate success!
  - A good project manager/scrum master will drive a project team and pull out the teams’ best during a project
  - It’s important to celebrate success at the end of a successful project!

Thank You!

KENNESAW STATE
UNIVERSITY

https://project.ocds.tech

IT-7993 IT Capstone Project

ID: G01/W01-P4

Title: Owl Cyber Defense Systems

Sponsor: Dr. Ying Xie

April 23, 2024

Team Members: Scott Gilstrap, Stephanie Aguirre, Chris Dunbar, Justin Place, Ryan LeBlanc