KENNESAW STATE
UNIVERSITY

IT-7993
IT Capstone Project

Owl Cyber Defense Systems

https://project.ocds.tech

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

KENNESAW STATE
UNIVERSITY

Milestone-2 Presentation

March 20, 2024

What Will Be Covered in This Presentation?

- Team Introduction
- Sprint 2 Milestone Goals and Objectives
- Sprint 2 Milestone Progress Summary
  - One-page Dashboard
  - Overall WBS: Timeline / Gantt Chart
- Sprint 2 Weekly Scrum Updates
- Sprint 2 Task Discussions
  - Overall WBS: Timeline / Gantt Chart
  - Team member presentation
  - Per Epic WBS: Timeline / Gantt Chart
  - Discussion with Empirical Evidence / Artifacts
- Time Tracking: Team and individual effort via person-hour burn-up pivot tables / charts / graphs for Sprint 2
- Sprint 2 Recap/Review to include Project Experience

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

Sprint 2 Goals & Objectives

Development & Testing Phase

Milestone 2
Goals & Objectives

Sprint 2
Feb 26 – Mar 24, 2024

- Complete & Publish OCDS Business Plan
- Complete & Publish OCDS Company Policies
- Publish the OCDS Company and Project Websites
- Develop & Test the Cyber Awareness Training Curriculum Client Offering
- Develop & Test the Proprietary IT Security Plan Client Offering
- Develop & Test the Risk Management Plan Client Offering
- Develop & Test the OCDS AI-enabled Chatbot with Hardening Content
- Develop & Test the OCDS Server Hardening Tool Client Offering
- Develop & Test the Advanced Firewall, SEIM, and Log Analyzer Client Offering

Sprint 2 Milestone Progress Summary

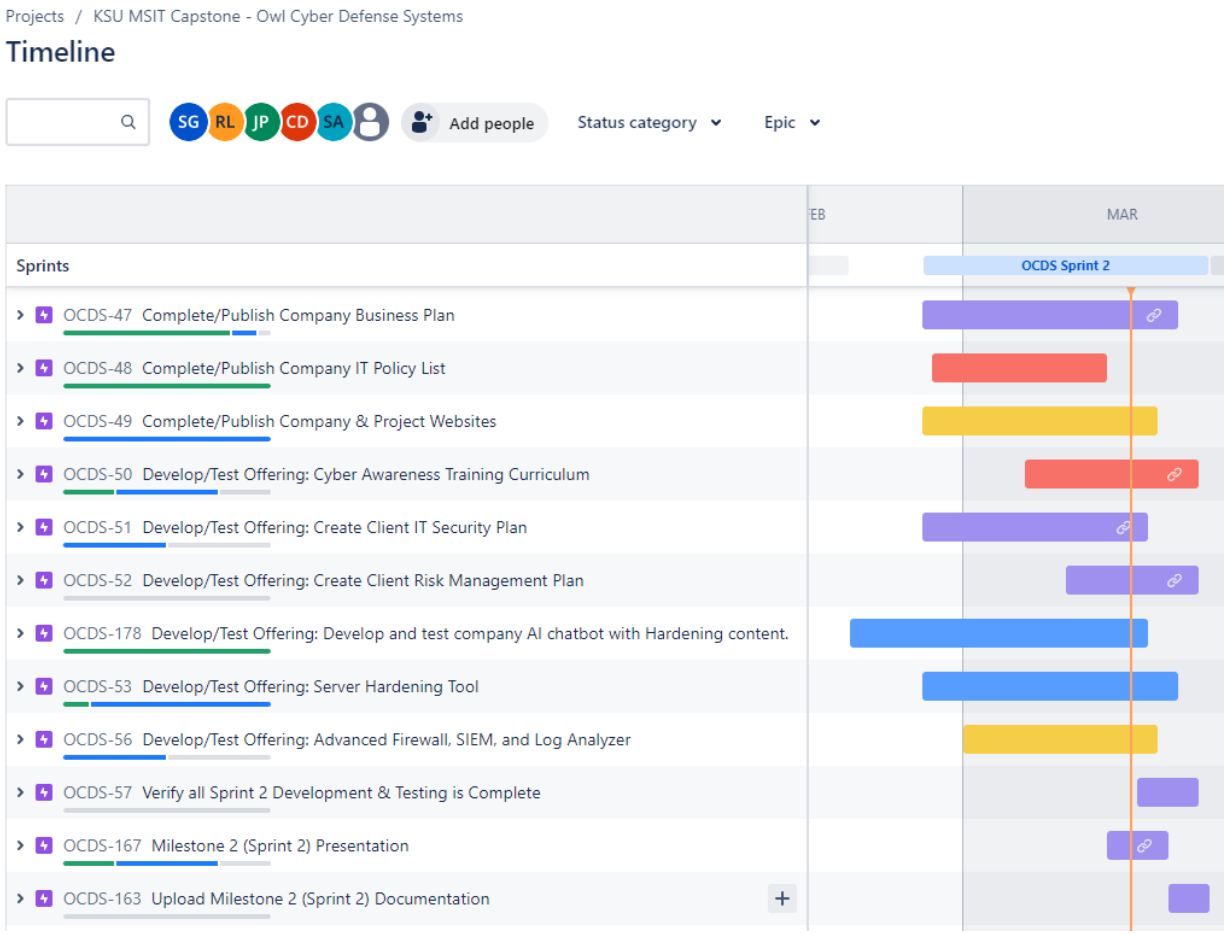
Sprint 1 Milestone Progress One-Slide Dashboard

Epic / Objective	Health	Target Date	Progress	Key Issues & Risks	GTG Action Plan	Leadership Assistance Requested
Complete & Publish OCDS Business Plan	B	21-Mar-24	• Successfully completed Business Plan ahead of time. • The Business Plan is on target to be published on website by 21-Mar.	NA	NA	NA
Publish OCDS Company Policy List	B	14-Mar-24	• Completed OCDS Company Policy List. • Incorporated into the Business Plan and the OCDS Company website.	NA	NA	NA
Complete & Publish OCDS Company & Project Websites	B	19-Mar-24	• Using input from all team members configured and published the OCDS company and project websites.	NA	NA	NA
Develop & Test the OCDS IT Security Plan Client Offering	B	18-Mar-24	• Completed the IT Security Plan Form Questionnaire • Worked with webmaster to incorporate form into the website	NA	NA	NA
Develop & Test the OCDS Risk Management Plan Client Offering	B	23-Mar-24	• Building the Risk Assessment Plan based on IT Security Plan form. • The RA Plan is on target to be completed by deadline, March 23rd. • Issue w RM Plan resolved by incorporating into InfoSec Plan.	Separate Risk Assessment from IT InfoSec Plan	Incorporate outcome w IT Security Plan	No
Develop & Test the OCDS AI-enabled Chatbot with Server Hardening Content	B	18-Mar-24	• Completed entry of all the various datasets (WinServer 19 & 22, Win10, Red Hat Enterprise Linux, Ubuntu, etc. and Chatbot testing.	NA	NA	NA
Develop & Test the OCDS Server Hardening Tool Client Offering	B	21-Mar-24	• Created the VM Infrastructure to support hardening tool and demo. • Completed PowerShell & Bash scripts. Testing now. On target.	NA	NA	NA
Develop & Test the OCDS Advanced Firewall, SEIM & Log Analyzer Client Offering	B	19-Mar-24	• Completed SEIM tool configuration (Security Onion). • Established network traffic for monitoring. On target.	SEIM network traffic flow	-Move cable -Software reinstall	No

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

Sprint 1 Milestone Progress Summary

- All Sprint 2 Epics are completed or on target for successful completion and submission by Mar 24, 2024.
- 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.
- Two issues were noted with the Risk Management Plan & SEIM Epics
    - RA needed to be incorporated into the over IT Security Plan
    - SEIM network traffic flow required mitigation efforts
- Issues did not become an impediment or risk
- No change request was required



Weekly Scrum Updates

Project – Owl Cyber Defense Systems – Sprint 2

Data as of: 03/02/24

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
✓ Sprint 1 Review & Retrospective ✓ Sprint 2 Planning & appropriate Project task updates ✓ Completed Company Business Plan ✓ Added data to AI dataset for further learning & accuracy ✓ Reached STIG PowerShell script for server scanning ✓ Started writing scripts for server hardening content ✓ Installed/configured NVIDIA Chat w RTX for STIG trng data ✓ Company website additions: Navbar, menus for client offerings (product catalog), new automation code. ✓ Started investigating CMS for Project website ✓ Upgraded Company IT Policy list; added to Business Plan ✓ Completed Company Legal Structure & added to the Business plan	✓ Create dataset tasks of documentation for company, so the chatbot can provide information to customers ✓ Add datasets to feed NIST 2.0 information ✓ Troubleshoot website public access config ✓ Publish Business Plan to Company website ✓ Start work to create IT Security Plan website form ✓ Collapse Risk Mngmnt Plan into IT Security Plan task ✓ Research, install, configure STIG Manager ✓ Create scripts to assist customer with STIG systems ✓ Publish draft of Company website ✓ Resolve issue with or rebuild SEIM server (not impediment issue at this time) ✓ Implement monitoring of live network traffic ✓ Investigate Nvidia's Chat w RTX AI application for possible integration with company website for live demos

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	15%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

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: 25 Feb – 02 Mar 2024

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

Project – Owl Cyber Defense Systems – Sprint 2

Data as of: 03/02/24

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
✓ Completed the Legal Structure & included in the OCDS Final Business Plan ✓ Completed all aspects of the OCS Business Plan and delivered it to the team for Publishing to the Websites ✓ OCDS AI security chatbot is now accessible over the internet without going through gradio ✓ Added datasets to incorporate NIST 2.0 data ✓ Incorporated STIG Manager and appropriate scripts to AI ✓ Published draft of Company website ✓ Rebuilt SEIM server successfully to avoid impediment ✓ Completed troubleshooting and fixed issues with Chatbot interface – no issue or risk to the Project Plan	✓ Complete the Cyber Awareness Training Curriculum ✓ Incorporate Training into the website ✓ Add datasets to feed NIST 2.0 information ✓ Create script to give report on system compliance (Windows and Linux) ✓ Configure/join ubuntu client-server domain. ✓ Create scripts to harden Windows and Linux systems. ✓ Create form to support the IT Security Plan client offering ✓ Incorporate IT Security plan with the website ✓ Configure the Risk Management Plan client offering into the IT Security Plan.

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	35%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

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: 03 – 09 Mar 2024

LEGEND

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

Project – Owl Cyber Defense Systems – Sprint 2

Data as of: 03/02/24

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
✓ Incorporated the Business Plan with the OCDS website ✓ Began incorporation of the OCDS IT Security Plan Questionnaire Form on the OCDS company website. ✓ Experienced issue w Risk Assessment flow. Avoided risk & impediment by deciding to incorporate w InfoSec Plan ✓ Completed the Training Curriculum and began work to incorporate on the OCDS company website. ✓ Published updates on Project & OCDS Company websites ✓ Conducted troubleshooting on SEIM network issues ✓ Added datasets to feed NIST 2.0 information ✓ Created the initial scripts to provide reports on system compliance (Windows and Linux) ✓ Configured/joined a ubuntu client-server domain	✓ Update scripts to give report on system compliance. ✓ Update configuration for scripts for hardening content. ✓ Completed integration of the IT Security Plan and Risk Assessment questionnaires w the OCDS company website. ✓ Complete the last section of Cyber Security Awareness Training in its entirety. ✓ Publish additional child webpages of websites ✓ Complete Website Training page & Team page w bios. ✓ Visit data center again to fix network issue ✓ Complete scripts for applying STIGs via NIST 2.0 ✓ Configure the systems to prevent certain applications from being blocked. ✓ Test scripts as they progress on demo systems to ensure they work and are not blocked.

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	75%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

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

ID	Key Issue(s)	Description	Mitigation / Action Plan
001 002	Risk Assessment SEIM Network	Overall flow of data and deliverable. Physical flow of data impeded.	Incorporate w IT Security Plan. Visit data center, move cable.

Week 3: 10 – 16 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 2

Data as of: 03/02/24

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
✓ Updated scripts to give report on system compliance. ✓ Updated configuration for hardening content scripts. ✓ Completed integration of the IT Security Plan and Risk Assessment questionnaires w the company website. ✓ Completed the last section of Cyber Security Awareness Training in its entirety. ✓ Published additional child webpages of websites. ✓ Completed Website Training page & Team page w bios. ✓ Traveled to the data center again to fix network issue ✓ Completed scripts to apply STIGs via NIST 2.0 ✓ Configured systems to prevent application blocking. ✓ Tested scripts as they progress on demo systems to ensure they work and are not blocked.	✓ Sprint 2 Review Meeting ✓ Sprint 2 Retrospective Meeting. ✓ Sprint 3 Planning Session. ✓ Review lessons learned and discuss improvements for Sprint 3 and project completion. ✓ Register for and discuss preparation for C-Day. ✓ Make final plan for all tasks to be completed and in production to start testing and preparation for project finalization.

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	0%

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

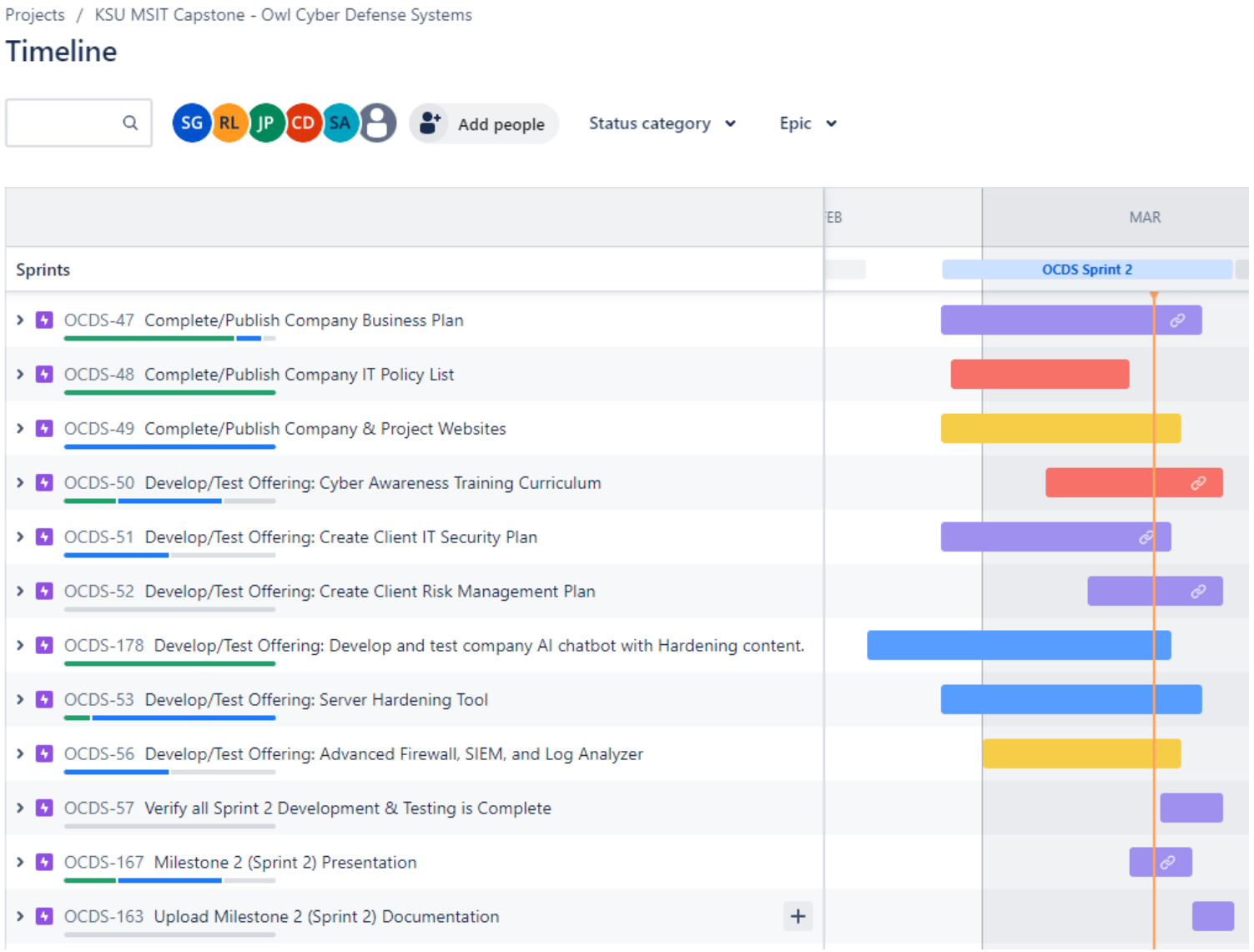
Week 4: 17 – 23 Mar 2024

LEGEND

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

Sprint 2 Task Discussions

Overall WBS Epic Timeline for Sprint 2 Milestones



Complete

Epic: Complete & Publish the OCDS Business Plan

Scott Gilstrap

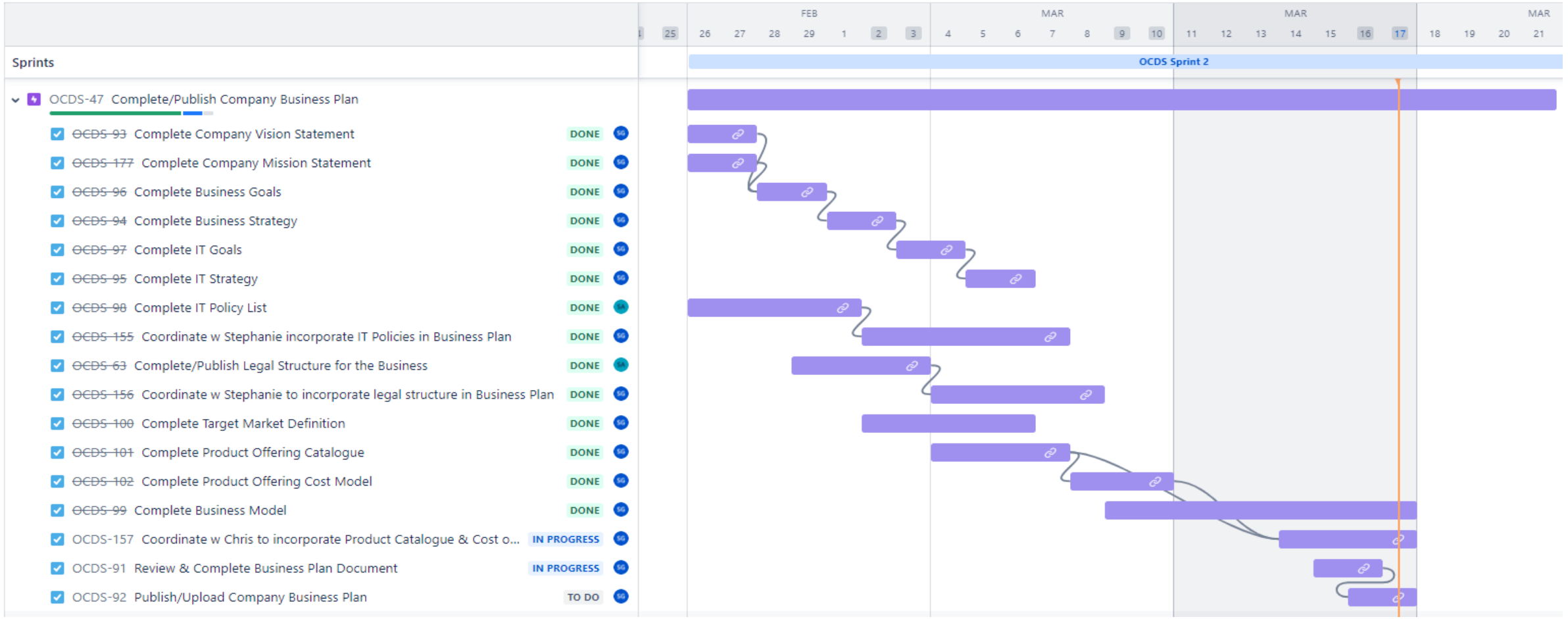
Complete & Publish the OCDS Business Plan

Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Give feedback | Share | Export

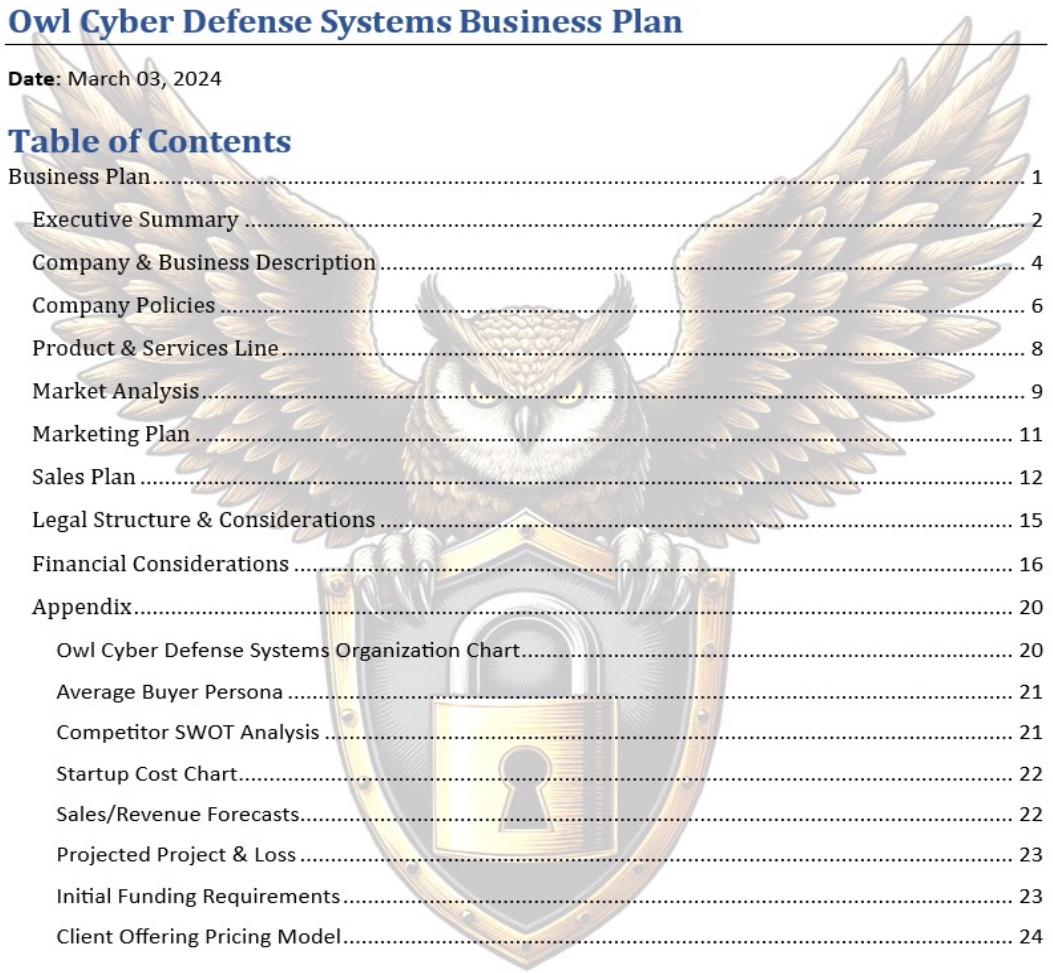
SG RL JP CD SA | Add people | Status category | Epic | View set



Complete/On Track

Complete & Publish the OCDS Business Plan

- Conducted multiple hours of research to obtain details for each section with very specific, true and realistic data to produce a very realistic Business Plan
- Verified content via team member collaboration
- Completed the specific details for OCDS company specific Business Plan entries
    - See TOC screenshot for all specific detailed sections
- Uploaded completed OCDS Business Plan to the MS Teams collaboration site
- Deliverable artifact attached and included in the appendix
- Coordinated with Webmaster to upload to websites



Owl Cyber Defense Systems Business Plan

Date: March 03, 2024

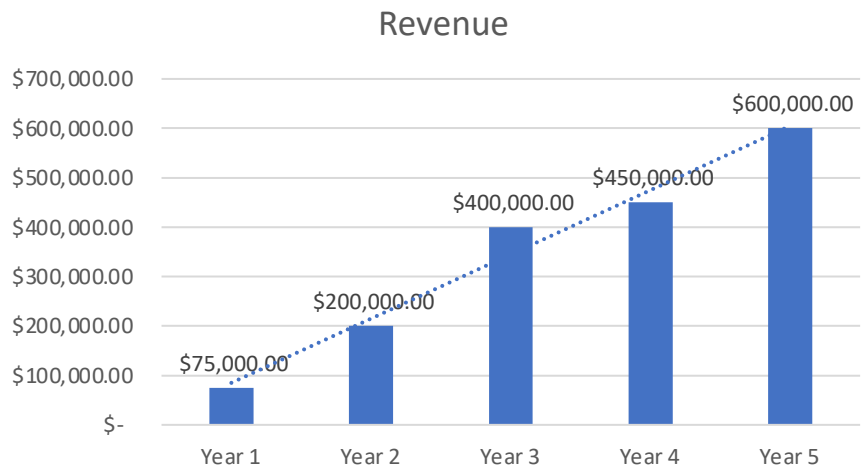
Table of Contents

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

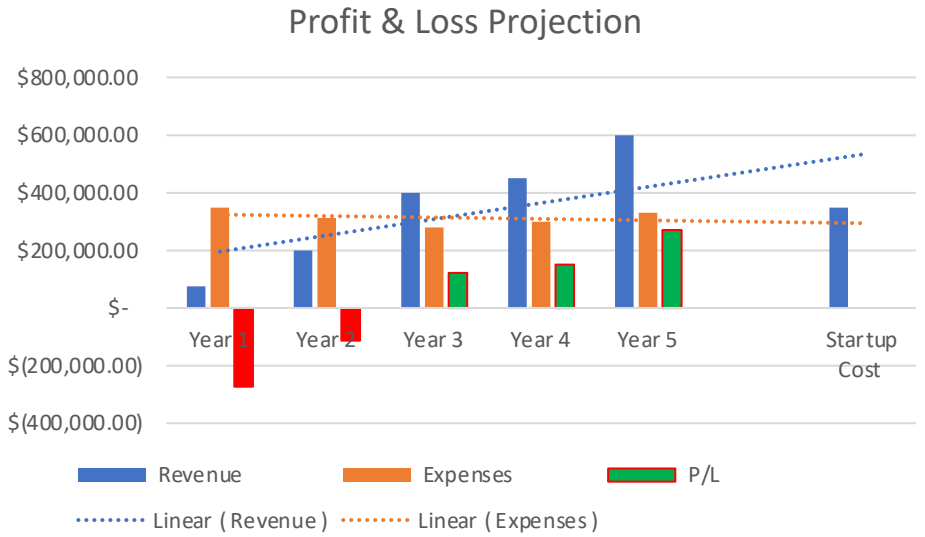
Owner: Scott Gilstrap

Complete & Publish the OCDS Business Plan

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		



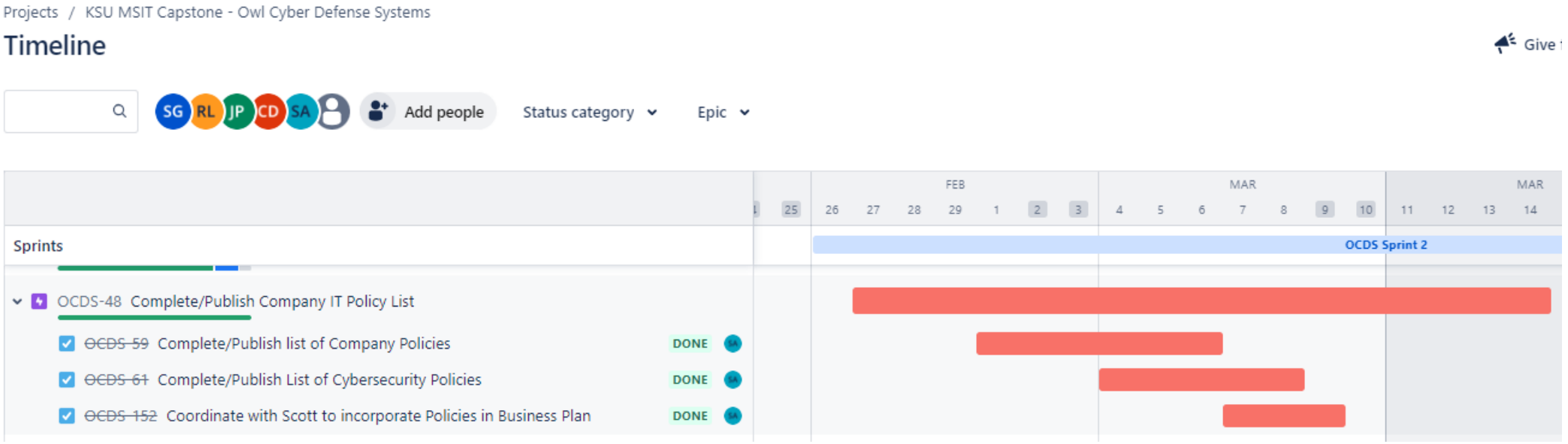
OCDS Client Offering	Retail Cost
Proprietary IT Security Plan	$699.99
Proprietary Risk Management & Assessment Plan	$499.99
AI-enabled Security Chatbot Tool	$1499.99
SIEM Tool	$999.99
Cyber Awareness Training	$399.99 per course

Owner: Scott Gilstrap

Epic: Complete & Publish the OCDS Company Policies

Stephanie Aguirre

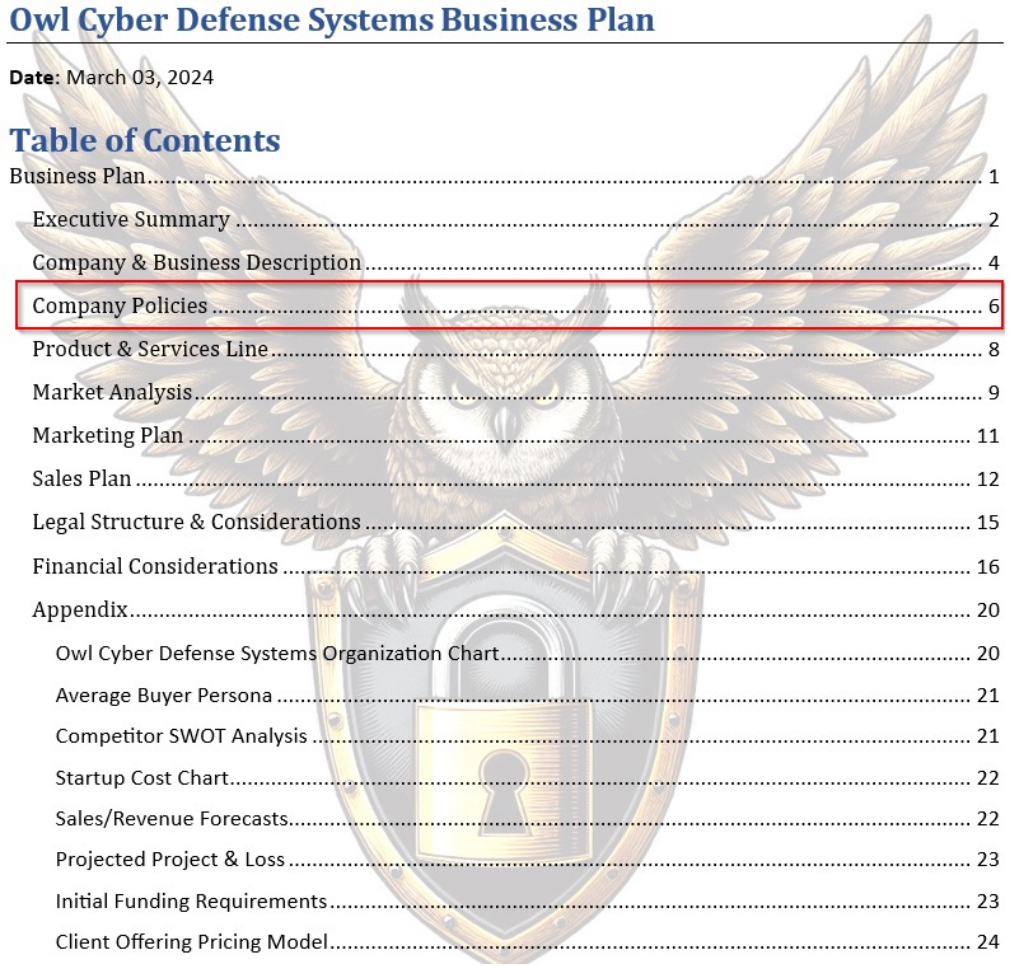
Complete & Publish the OCDS Company Policies



Complete

Complete & Publish the OCDS Company Policies

- Completed detailed research of multiple sites and companies for Company Policy concepts and ideas.
- Completed research on specific policies for Company Policy List as well as specific IT Polices and decided which policies to use as OCDS Policy List.
- Completed final version of OCDS Company and IT Policies.
- Coordinated with the Scott Gilstrap to incorporate the completed version of the OCDS Company Policies into the OCDS Business Plan.
- Screenshot of Table of Contents to the right and more to follow on next three slides



Owl Cyber Defense Systems Business Plan

Date: March 03, 2024

Table of Contents

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

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: Complete & Publish OCDS Company & Project Website

Chris Dunbar

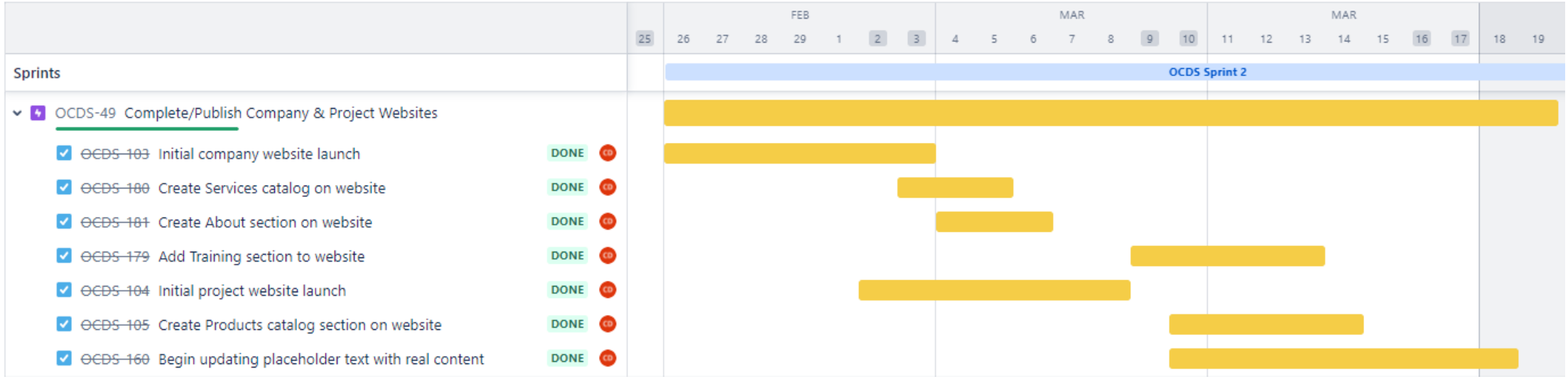
Complete & Publish OCDS Company & Project Website

Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline

Give feedback

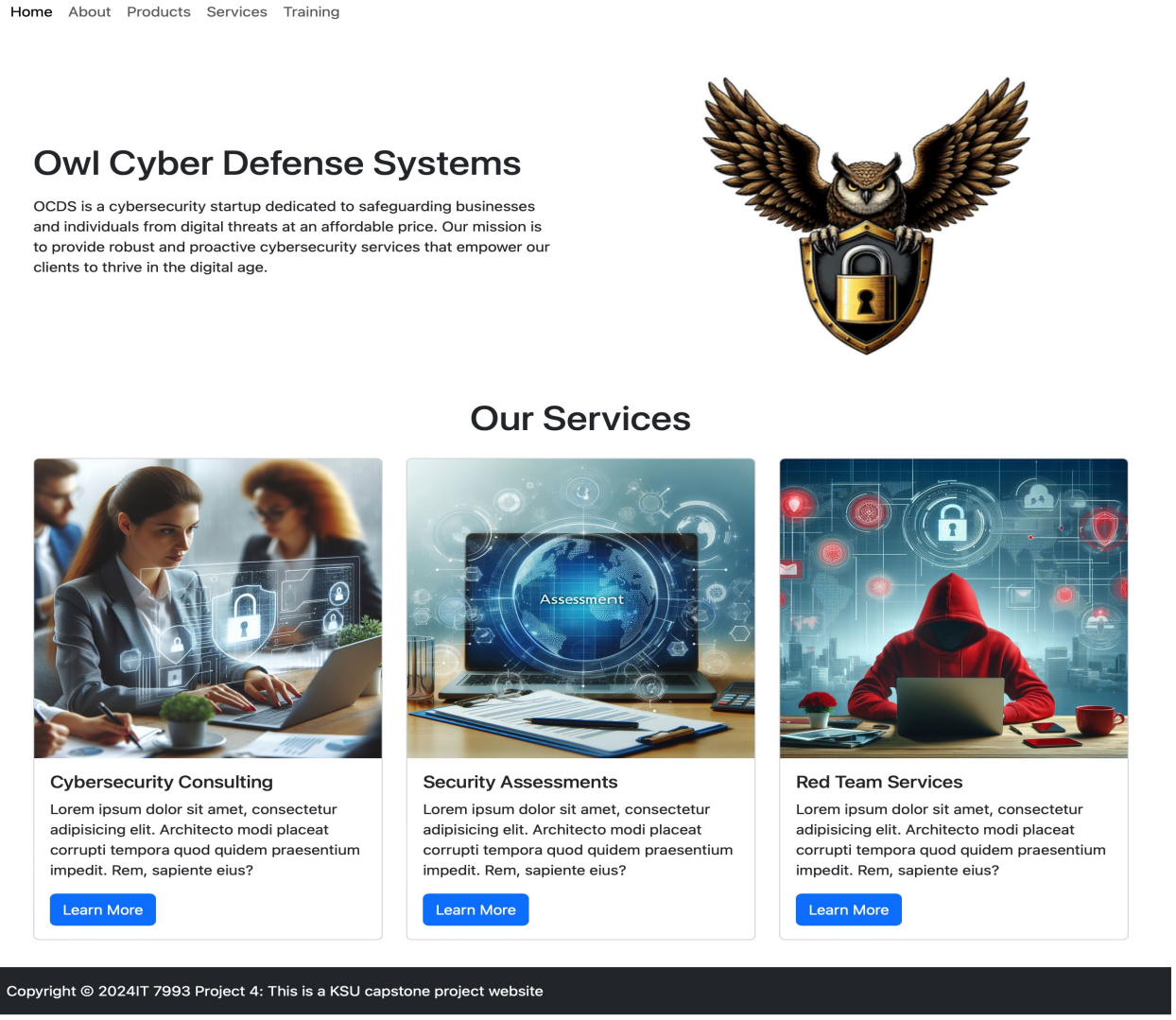
SG RL JP CD SA Add people Status category Epic



Complete/On Track

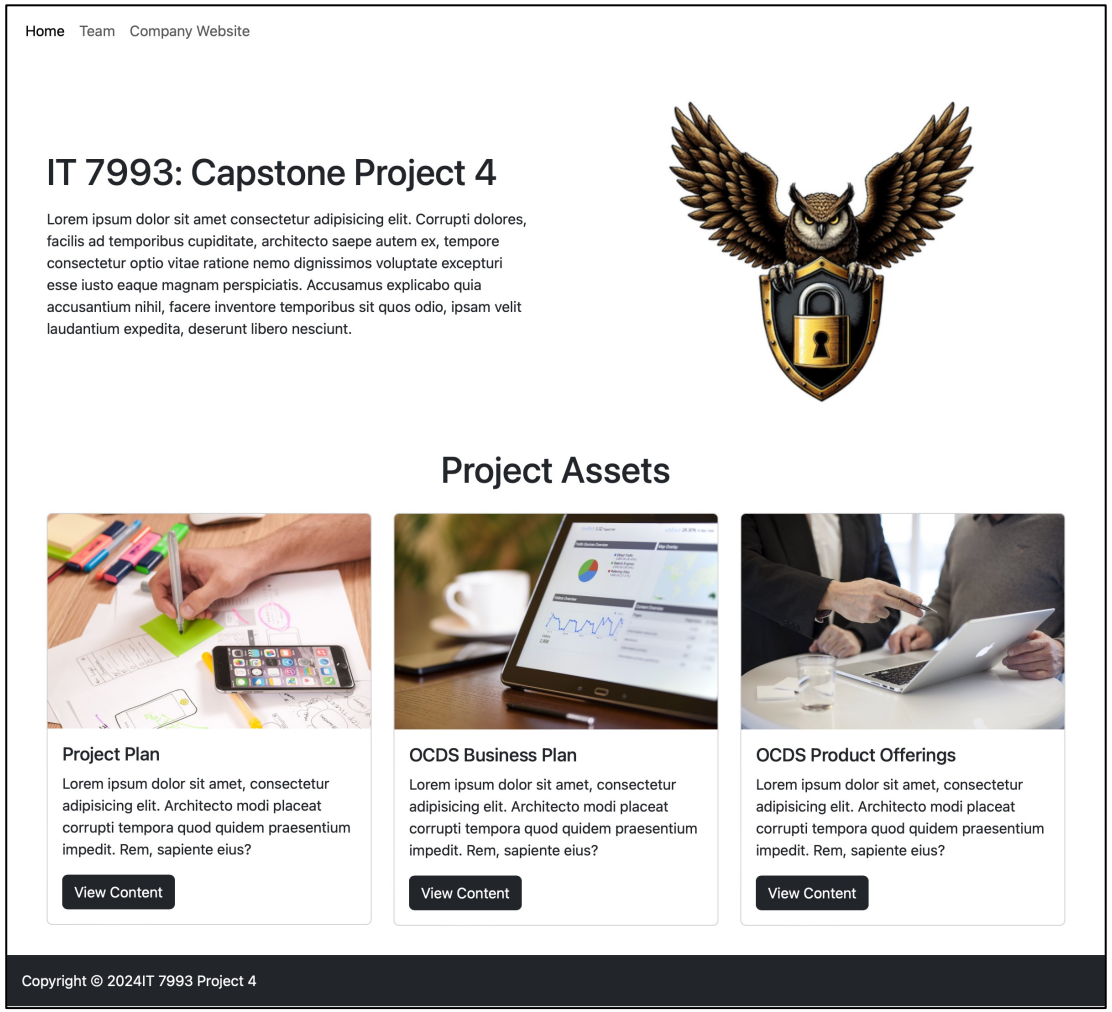
Complete & Publish OCDS Company & Project Website

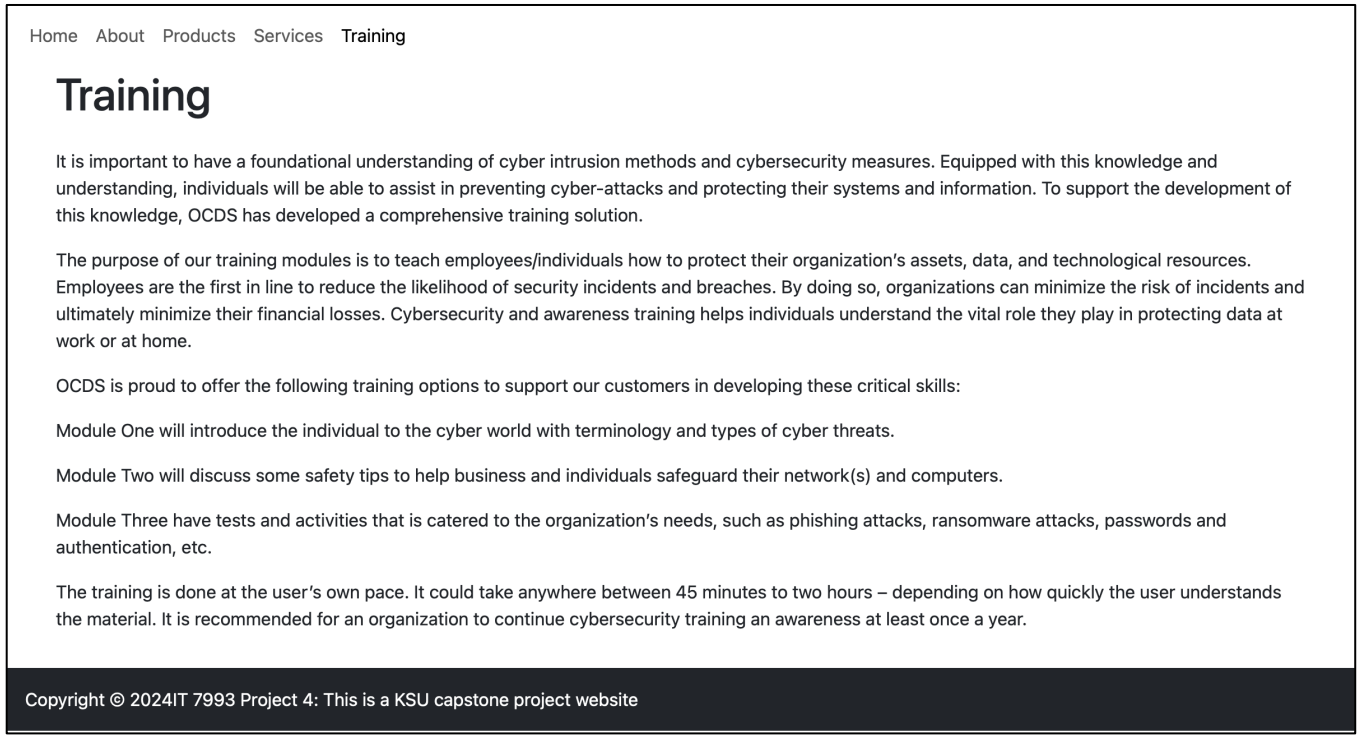
- Conducted multiple lines of research for hosting capabilities to support the websites
- Published drafts of both the Project and the OCDS Company Websites
- Navigation bar, drop down menus, & automation
- Added content to both websites
- Company website
  - Updated Products page layout
  - Updated Services page layout
  - Added Training page
- Project website
  - Updated placeholder text with content from project documents (e.g., Business Plan).
  - Added Team page (need team input)
  - Added completed Business Plan in PDF format.



Owner: Chris Dunbar

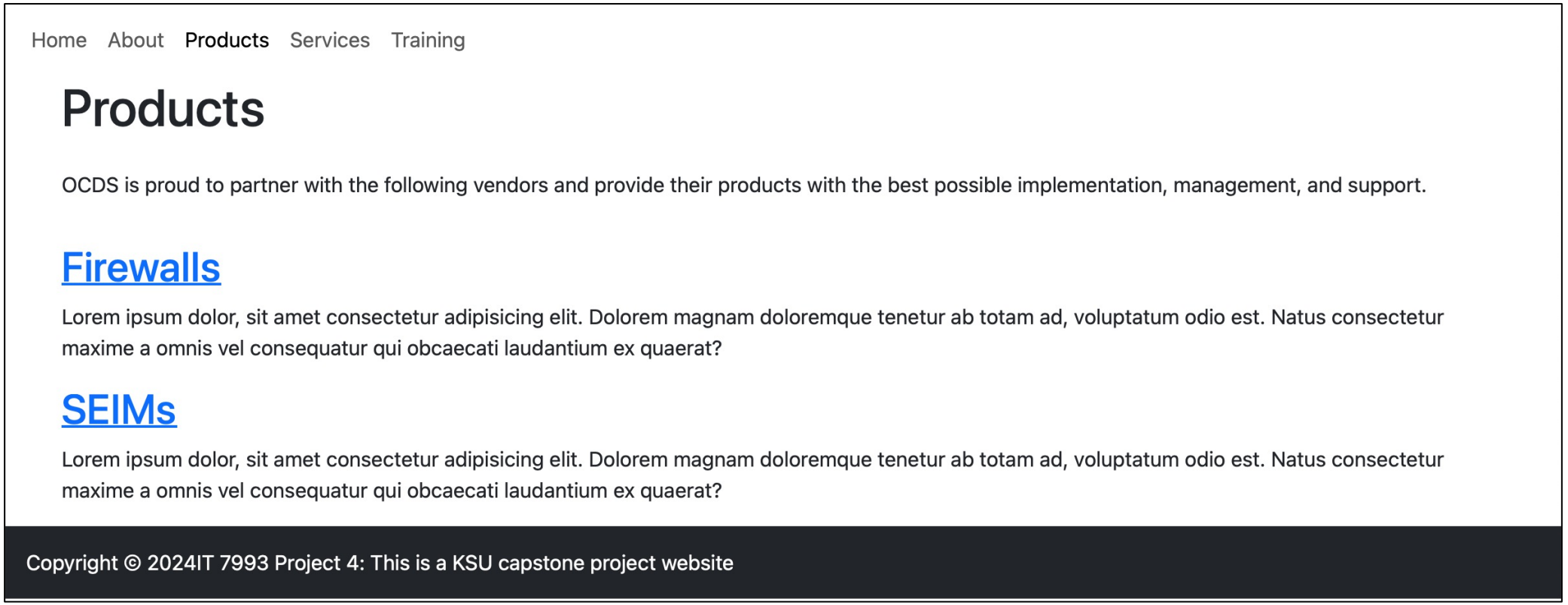
Complete & Publish OCDS Company & Project Website





Owner: Chris Dunbar

Complete & Publish OCDS Company & Project Website

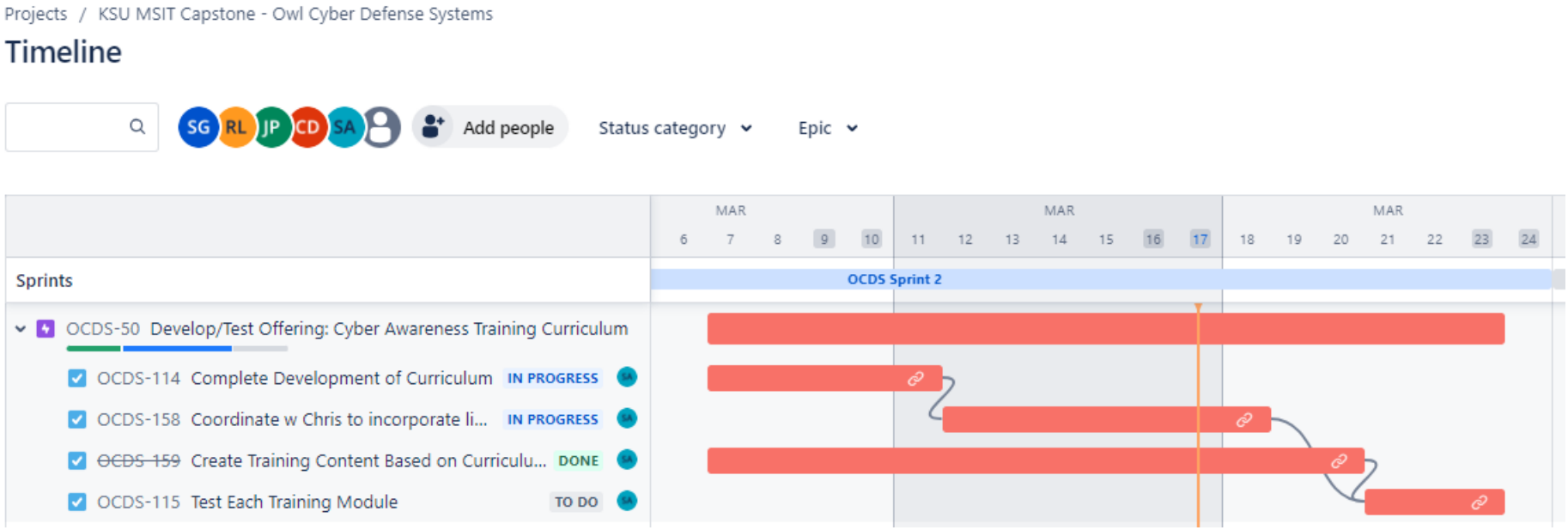


Owner: Chris Dunbar

Epic: Develop & Test Cyber Awareness Training Client Offering

Stephanie Aguirre

Develop & Test Cyber Awareness Training Client Offering



On Track – no risks

Develop & Test Cyber Awareness Training Client Offering

- Took the Cyber Awareness Training design drafted in Sprint 1 and added content to Publish.
- Working with Webmaster to incorporate with the Training section of website.
- Researched several cyber awareness training experts to develop a proprietary OCDS training program.
- Following are screenshots and artifact evidence of…
  - Our Cyber Awareness Training statement
  - The Cyber Awareness Training Curriculum Client Offering
  - AN actual training module

Cybersecurity Training and Awareness

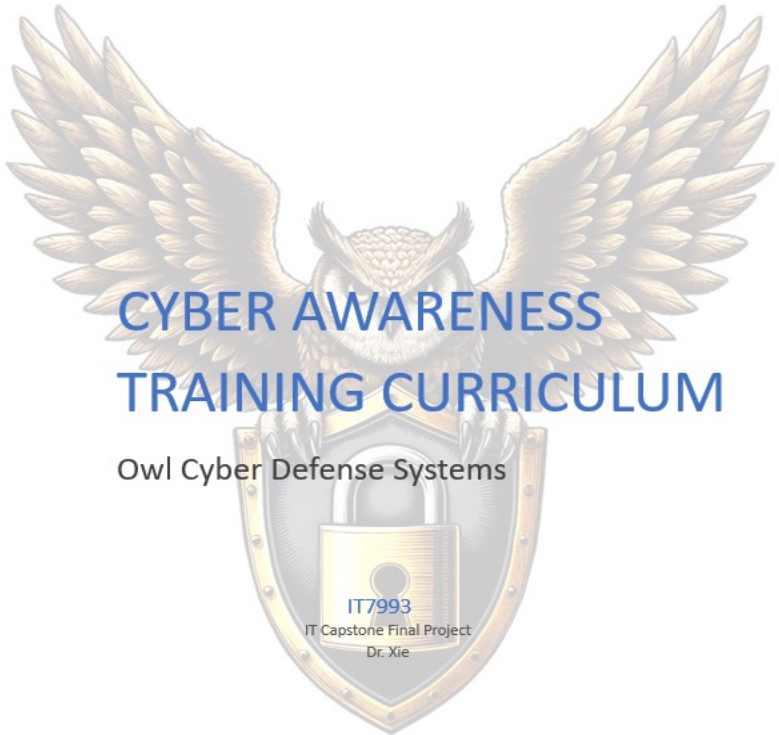
It is important to have a foundational understanding of cyber intrusion methods and cybersecurity measures. By having this knowledge and understanding, individuals will be able to assist in preventing cyber-attacks and protecting their systems and information.

Purpose:
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.

What Does it Cover:
Cybersecurity training and awareness will cover three (3) modules. The first two modules are standard, while the last module is organization specific.

1. *Module One will introduce the individual to the cyber world with terminology and types of cyber threats.*
2. *Module Two will discuss some safety tips to help business and individuals safeguard their network(s) and computers.*
3. *Module Three have tests and activities that is catered to the organization's needs, such as phishing attacks, ransomware attacks, passwords and authentication, etc.*

How Long is the Training:
The training is done at the user's own pace. It could take anywhere between 45 minutes to 2 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.



Author: Stephanie Aguirre
saguirr5@students.kennesaw.edu

Cyber Awareness Training Curriculum Client Offering

Date: February 21, 2024

Cybersecurity Awareness Training Curriculum (Design)

This will outline clear expectations, rules, and approach that our organization will use to maintain the confidentiality, integrity, and availability of sensitive information obtained.

Protecting confidential data such as:

- Unreleased and classified information
- Customer, supplier, and shareholder information
- Patents and business processes
- New technology and software
- Employees' passwords, tasks, and personal information
- Contracts and legal records for the organization

Organization's use on device security:

- Keep all passwords and issued devices protected
- Secure company devices before leaving work area
- Obtain authorization from manager/supervisor before removing devices from organization premise
- **Regularly** update devices with the latest patches and security software

Organization on transferring data:

- Employees should not transfer classified information to outside parties
- Only transfer classified data over the organization's networks
- Any authorization needed must be obtained by manager/supervisor

- Verify the recipient of the information always, and ensure that the security measures are in place
- Immediately alert the IT department if any breaches or malicious software are found

Cybersecurity Training for employees

- Training helps minimize the risks that could potentially stem from user error. An organization can have all the technology in the world, but no technology solution will help stop all cyber-attacks if the end user is not prepared to help prevent it.

Cybersecurity response plan

Preparing for an incident, identifying incident and reporting it, containing it, eradication, recovery, and learning from the incident:

- Preparation: prepare users for a potential attack/incident
- Identifying: attempting to identify all details of the attack , and figure out why/how it occurred and what it has impacted
- Containment: containing the attack that occurred to make sure it does not affect other parts of the network and/or losing evidence of the attack.
- Eradication: eradicate the malware and patching any vulnerabilities
- Recovery: bringing the systems and networks back up and running – making sure it is all running smoothly again.
- Learning from Incident: Think about how the attack was contained and handled, and attempting to fix the gaps that caused the attack in the first place.

Legal Compliance

- HIPAA compliant: Compliance with the U.S. Health Insurance Portability and Accountability Act that requires companies and organizations that worth with protected health information (PHI) to implement and follow physical and network security measures.
- Export Administration Regulation: regulates the export, reexport and transfer of military items, commercial items, and purely commercial items without obvious military use.
- PCI Security Standards: The global data security standard that is primarily adopted and used by payment card brands that stores or transmits cardholder data and/or sensitive data.

Consistently test run cybersecurity policy and IT security policy

- By consistently test running policies, it will inform the organization of the cyber risk exposure and encourage them to address the identified issues to be able to improve their security.

End of document

Develop & Test Cyber Awareness Training Client Offering

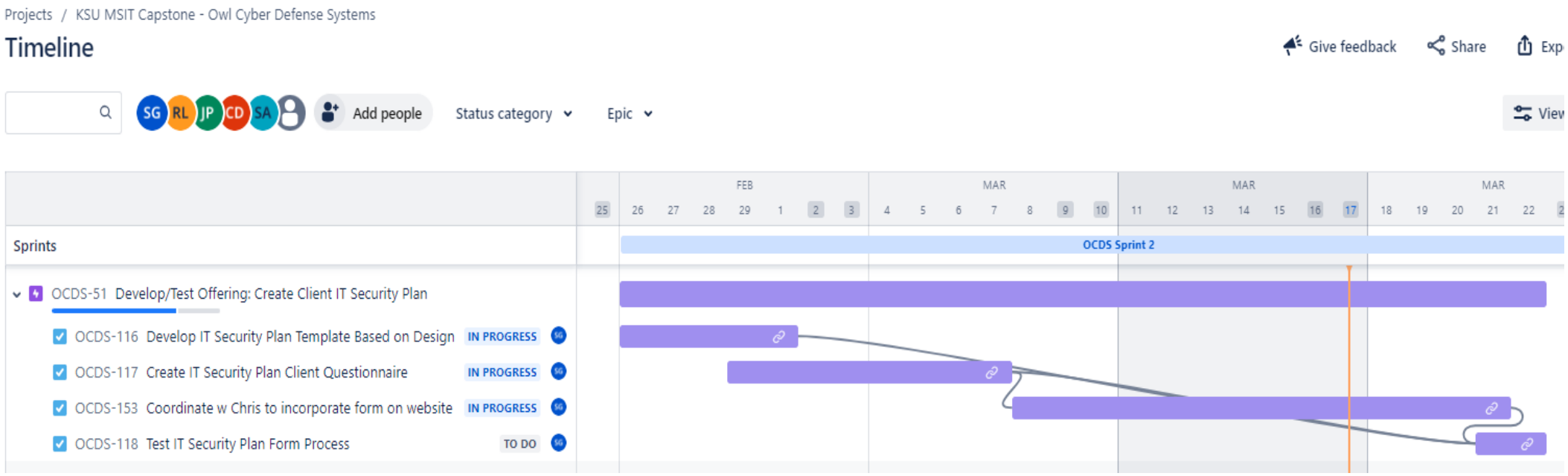
Owner: Stephanie Aguirre

Epic: Develop & Test OCDS IT Security Planning Client Offering

Epic: Complete & Test the Risk Assessment Plan Client Offering

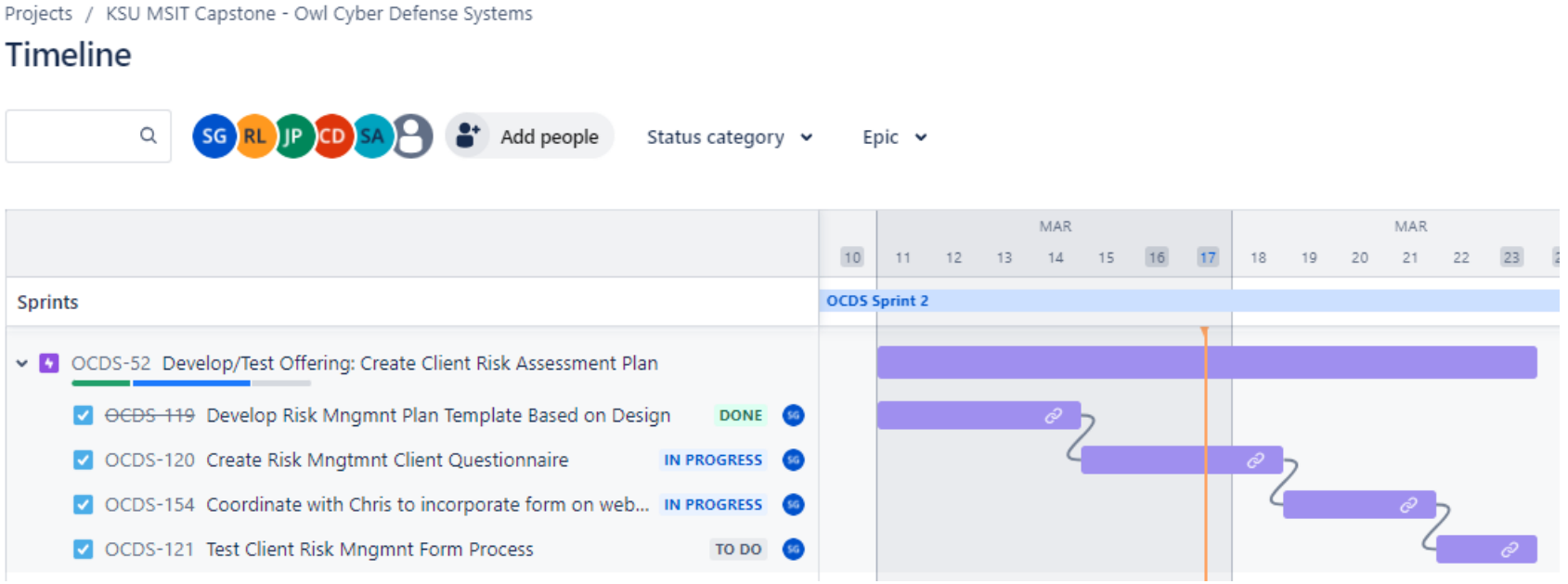
Scott Gilstrap

Develop & Test OCDS IT Security Planning Client Offering



Complete/On Track

Complete & Test the Risk Assessment Plan Client Offering



On Track – no risks

Develop & Test OCDS IT Security Planning Client Offering

- Complete research on multiple aspects of an appropriate detailed IT Information Security Plan
- Took the initial concept/design and converted it into a 25-question IT Cybersecurity Plan Questionnaire Form
- Coordinated with the Webmaster to incorporate the IT Security Plan Form on the Website Client Service Offerings section
- Tested form submission
- Began work to build out an actual IT Security Plan for a client

Process:

- http://www.ocds.tech
- Navigate to **Products/Services Catalog**
- Introductory/About page available for the **Proprietary IT Security Planning** client offering
  - What is an IT Security Plan
  - Benefits of a well written IT Security Plan
  - How to get started
- Click **Get Started**
- Prompt to log in if not logged in already
- Start 25-question questionnaire
- Submit questionnaire upon completion.

Owner: Scott Gilstrap

Develop & Test OCDS IT Security Planning Client Offering

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

Owner: Scott Gilstrap

Complete & Test the Risk Assessment Plan Client Offering

- Issue: Research indicated the best option is to incorporate the Risk Assessment into the IT Security Plan.
- This did **not** result in an impediment or a risk. No *change request* was required.
- Completed research on the various aspects of an appropriate detailed Risk Assessment and Management Plan.
- Incorporated appropriate Risk Assessment questions into the IT Security Planning tool.
- Worked with the webmaster to design the IT Security/Risk Assessment Form on the OCDS website.
- Began work to create an actual IT Security Plan to include a Risk Assessment section.

- Risk Assessment Questionnaire:
  - What are your company's most important IT assets?
  - What kind of data breach would have a major impact on your business?
    - Malware, cyber attack, human error?
    - Think effect on customer information.
  - Can all threat sources be identified?
  - What is the level of the potential impact of each identified threat?
  - What are the internal and external vulnerabilities?
  - What is the impact if those vulnerabilities are exploited?
  - What is the likelihood of exploitation?
  - What cyber attacks, cyber threats, or security incidents could impact affect
  - the ability of the business to function?
  - What is the level of risk my organization is comfortable taking?
- Next, determine remediation method for each Risk
  - Determine risks to reduce.
  - Determine the highest priority security risk hierarchy?
  - Reduce the risk in the most cost-effective way.

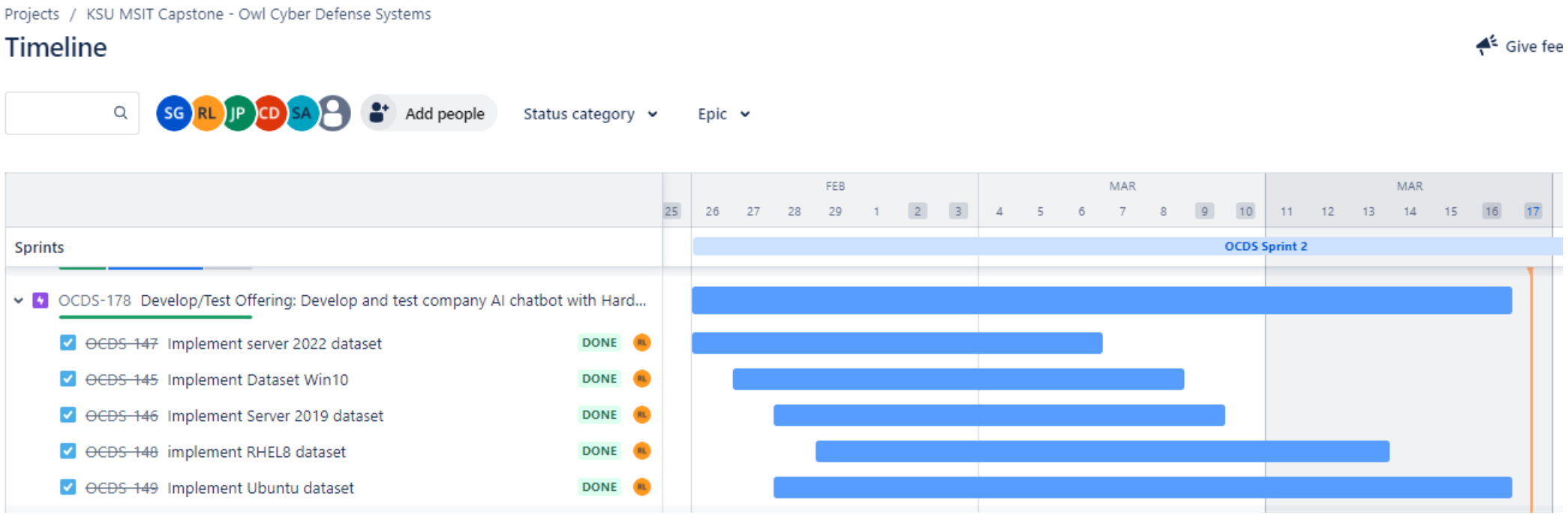
Owner: Scott Gilstrap

Epic: Develop & Test OCDS AI-enable Chatbot with Server Hardening Client Offering

Epic: Develop & Test Server Hardening Tool Client Offering

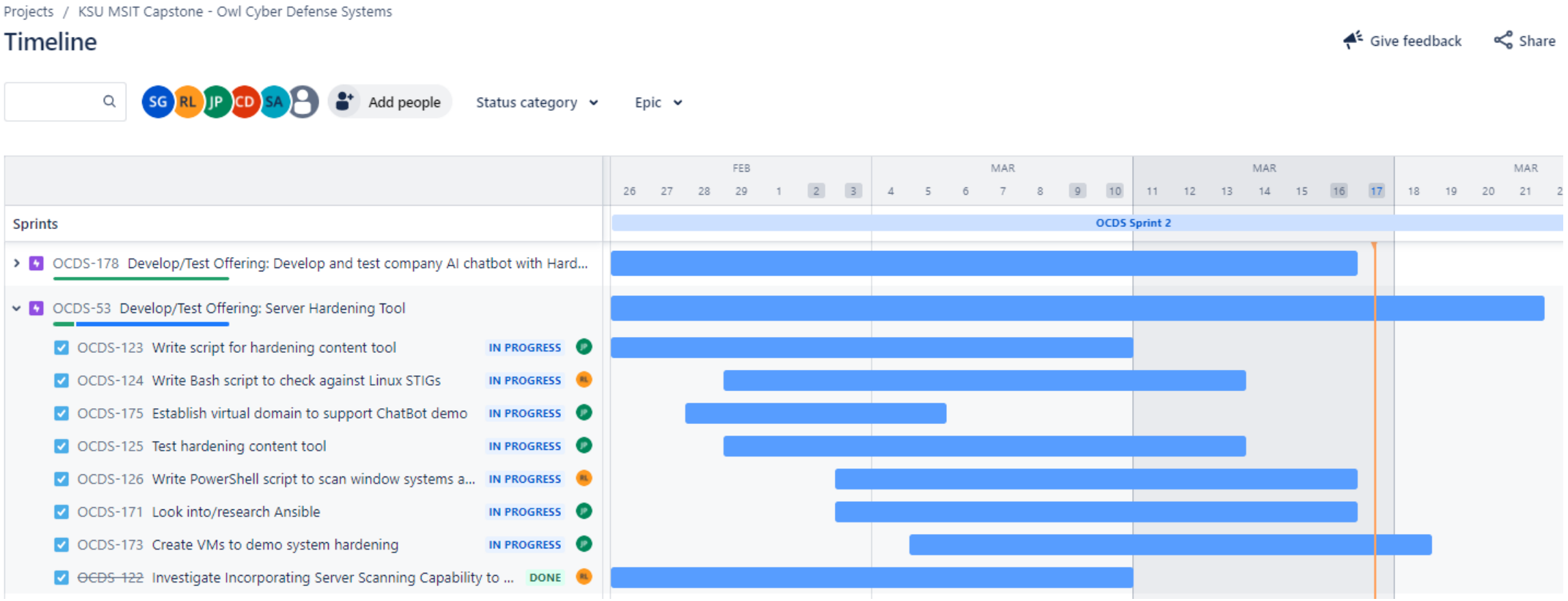
Ryan LeBlanc & Justin Place

Develop & Test OCDS AI-enable Chatbot with Server Hardening Client Offering



Complete

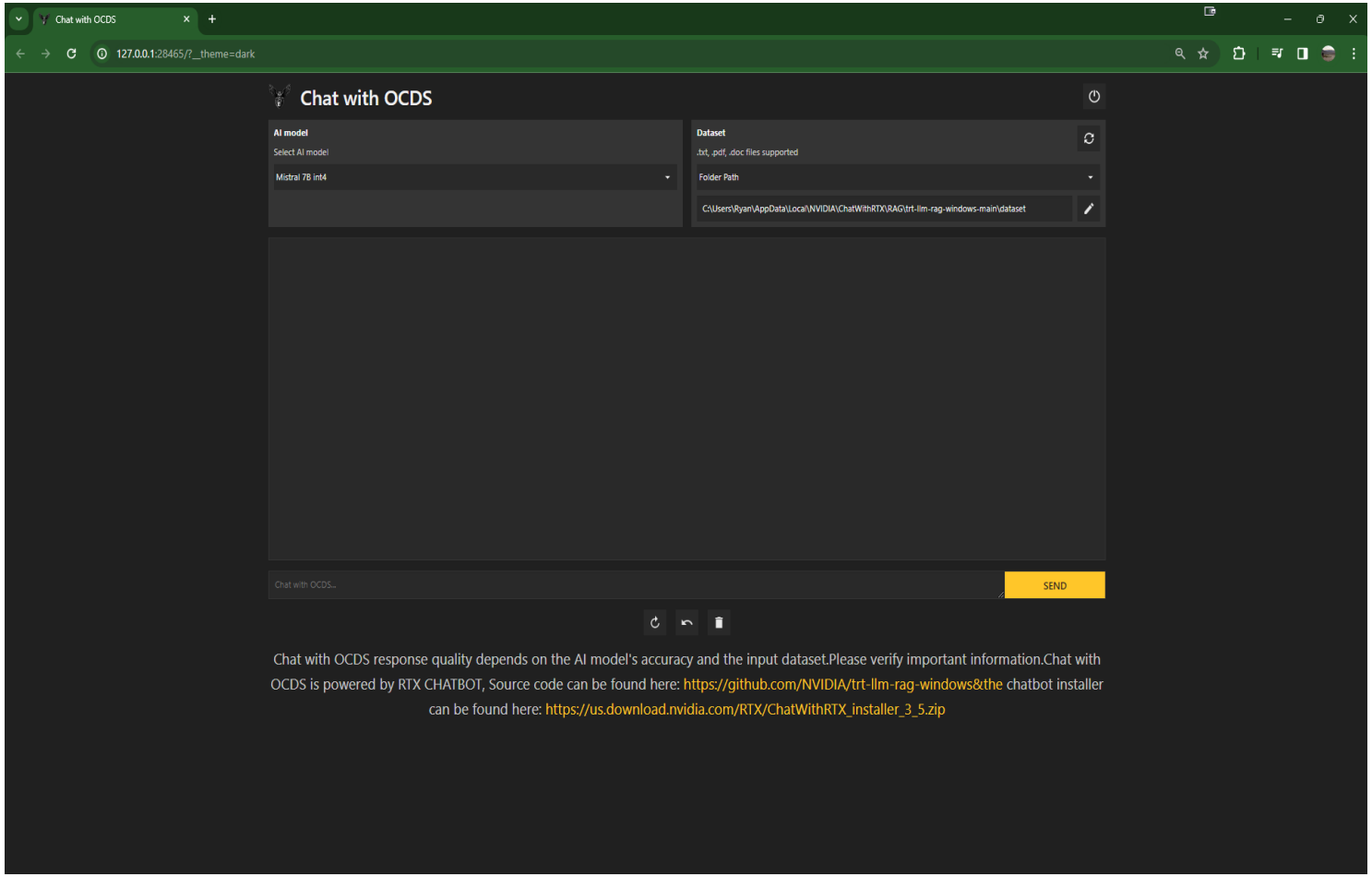
Develop & Test Server Hardening Tool Client Offering



Complete/On Track

Develop & Test OCDS AI-enable Chatbot with Server Hardening Client Offering

- Developed and tested chatbot with datasets.
- Researched scripting for automated server scanning capability.
- Started writing bash script to check Linux STIGs.
- Installed NVIDIA Chat with RTX and configured to use previously created training data for providing STIG information.
- Implemented Server 2022, Windows 10, RHEL8, & Ubuntu datasets.
- Investigated server AI scanning capabilities.
- Configured OCDA Chatbot to be accessible over internet without going through gradio.
- Implemented security controls.
- Researched Ansible for system hardening.

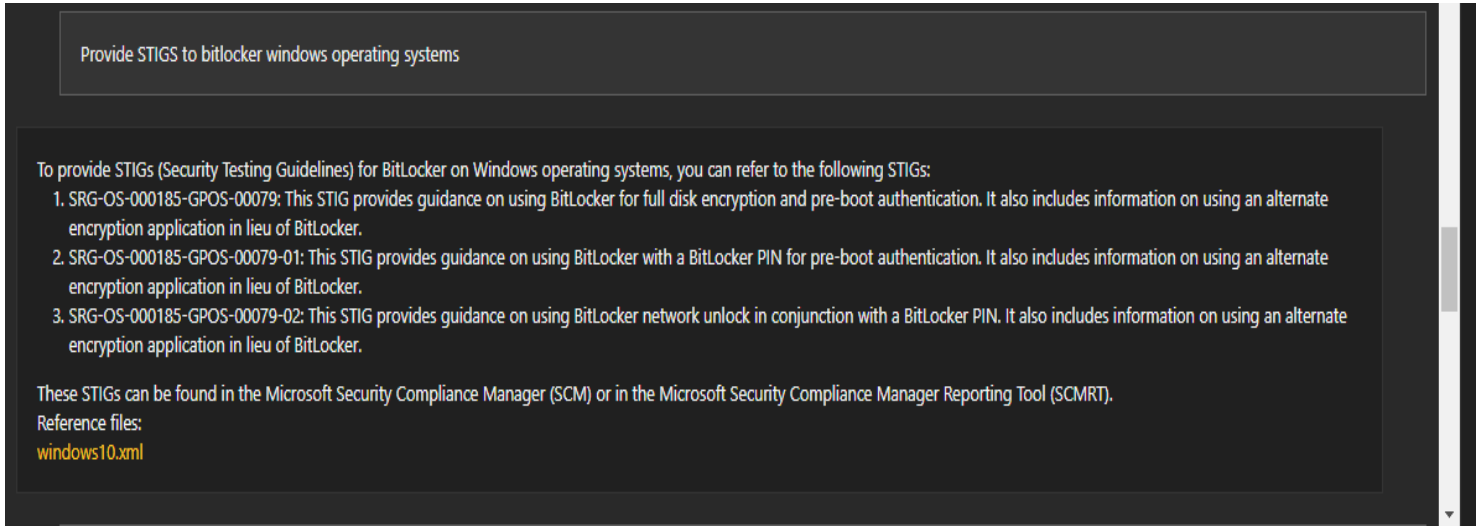


OCDS Chatbot

Owner: Ryan LeBlanc & Justin Place

Develop & Test Server Hardening Tool Client Offering

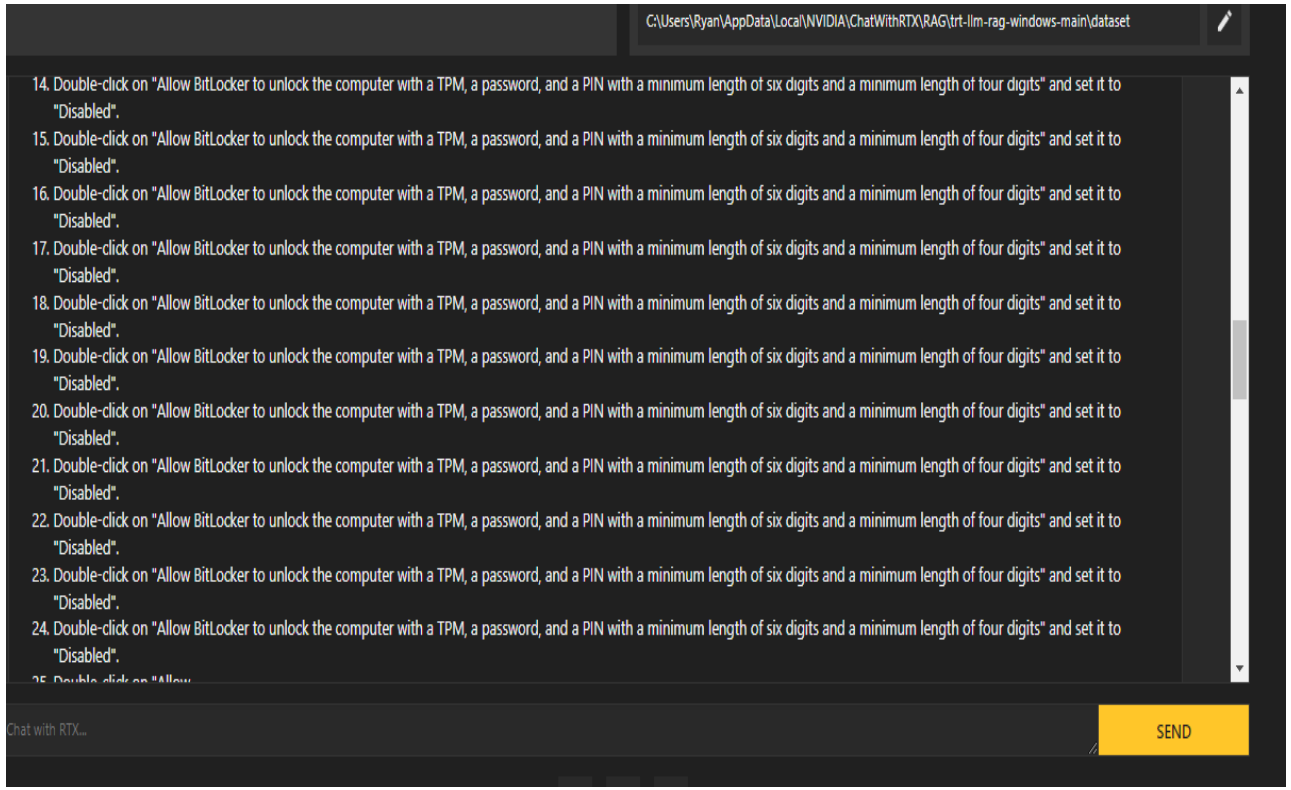
- Creating virtual domain environment (domain controller, management server, windows 10 client created, and domain joined.
- Created Ubuntu client and server.
- Complete configuration of all Ubuntu, RHEL8, Windows 10, and Server 2019 & 2022 dataset configurations.
- Configured PowerShell and Bash scripts scan the Windows systems against the NIST STIGs.
- Configured VM environment for demo & established virtualized domain infrastructure.
- Management server connects to all systems on domain.
- Installed vulnerability scanner for identifying vulnerabilities (Windows and Ubuntu) in which the AI chat bot can be used for remediation.

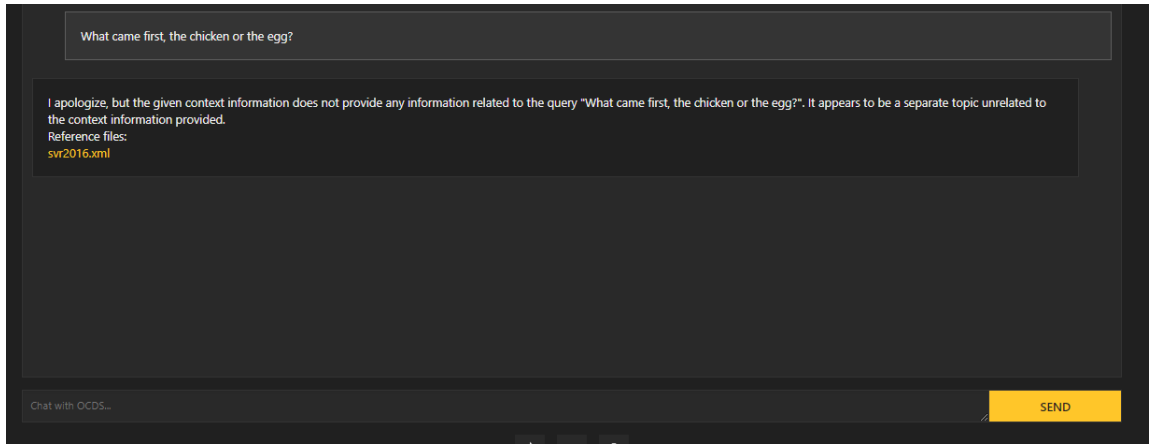


STIG Reference examples

Owner: Ryan LeBlanc & Justin Place

Develop & Test OCDS AI-enable Chatbot with Server Hardening Client Offering





Owner: Ryan LeBlanc & Justin Place

SCC 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_STIG-2.4.4.html]

Navigation: Back | Forward | Reload

Search: find in report | < | > | Match Case | Whole Words | 0 of 0

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

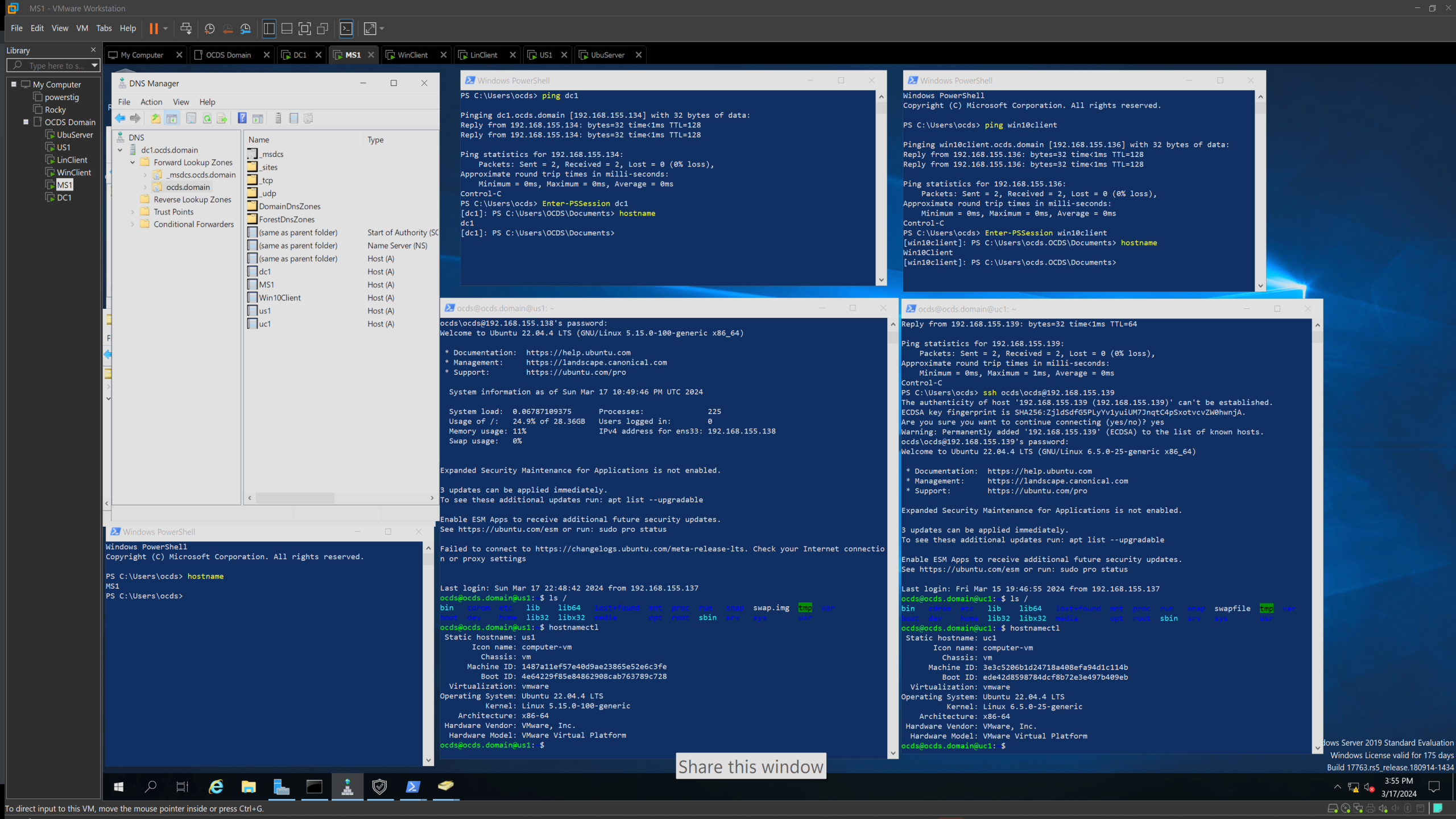
- V-205711 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-205724 - Windows Server 2019 must not allow anonymous enumeration 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

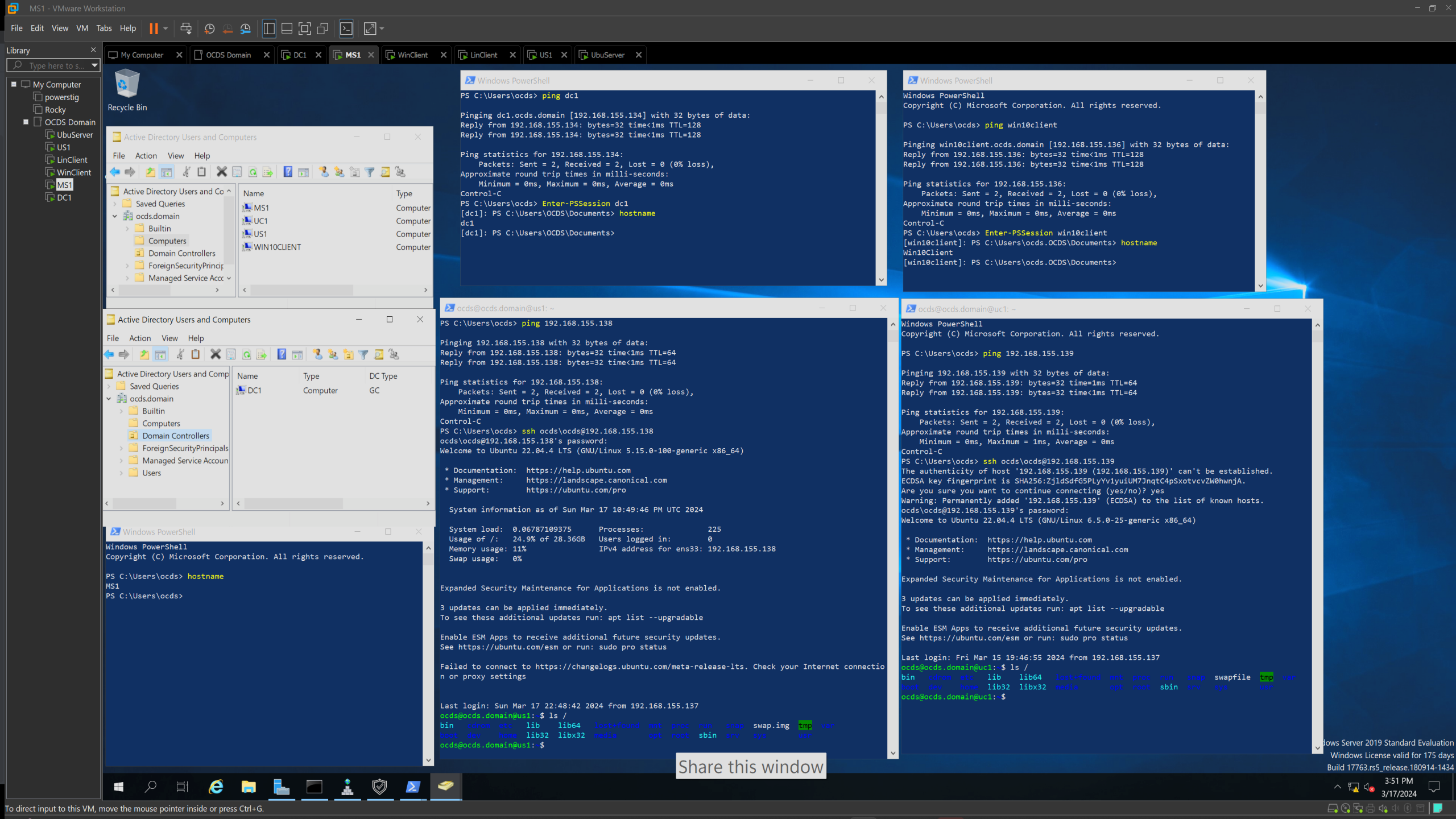
Manual Checks

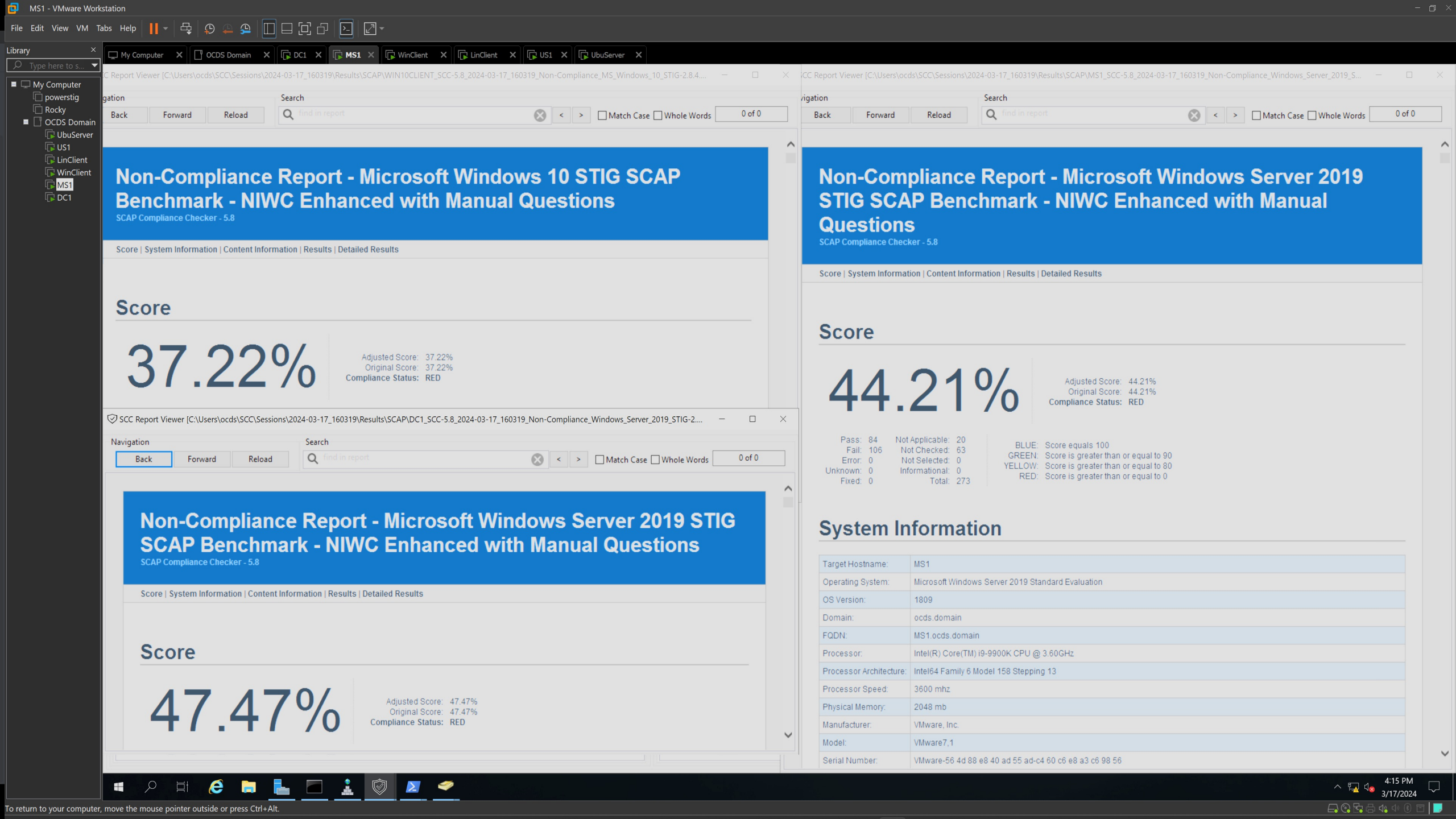
Results: Medium Severity (CAT II)

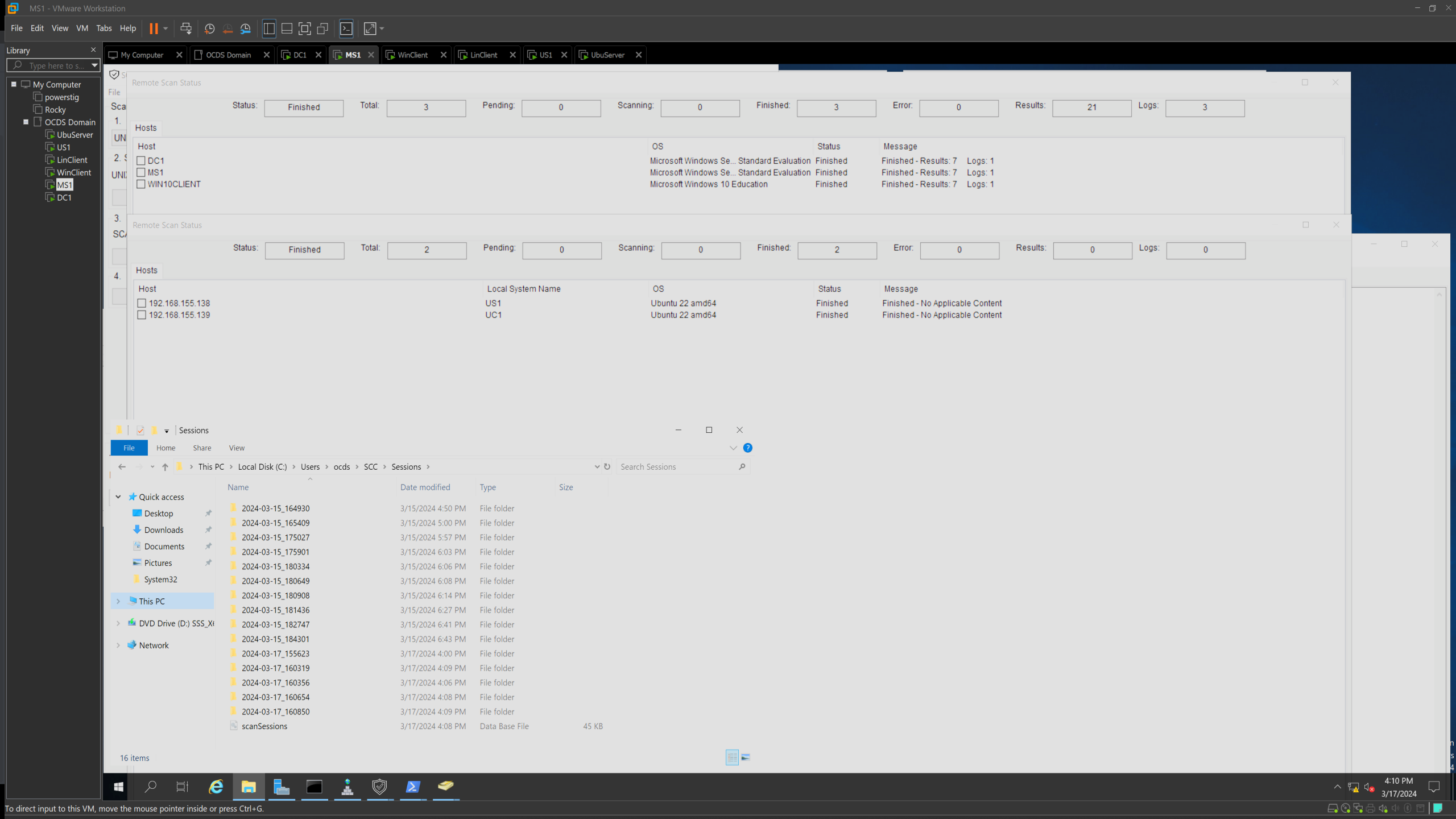
Automated Checks

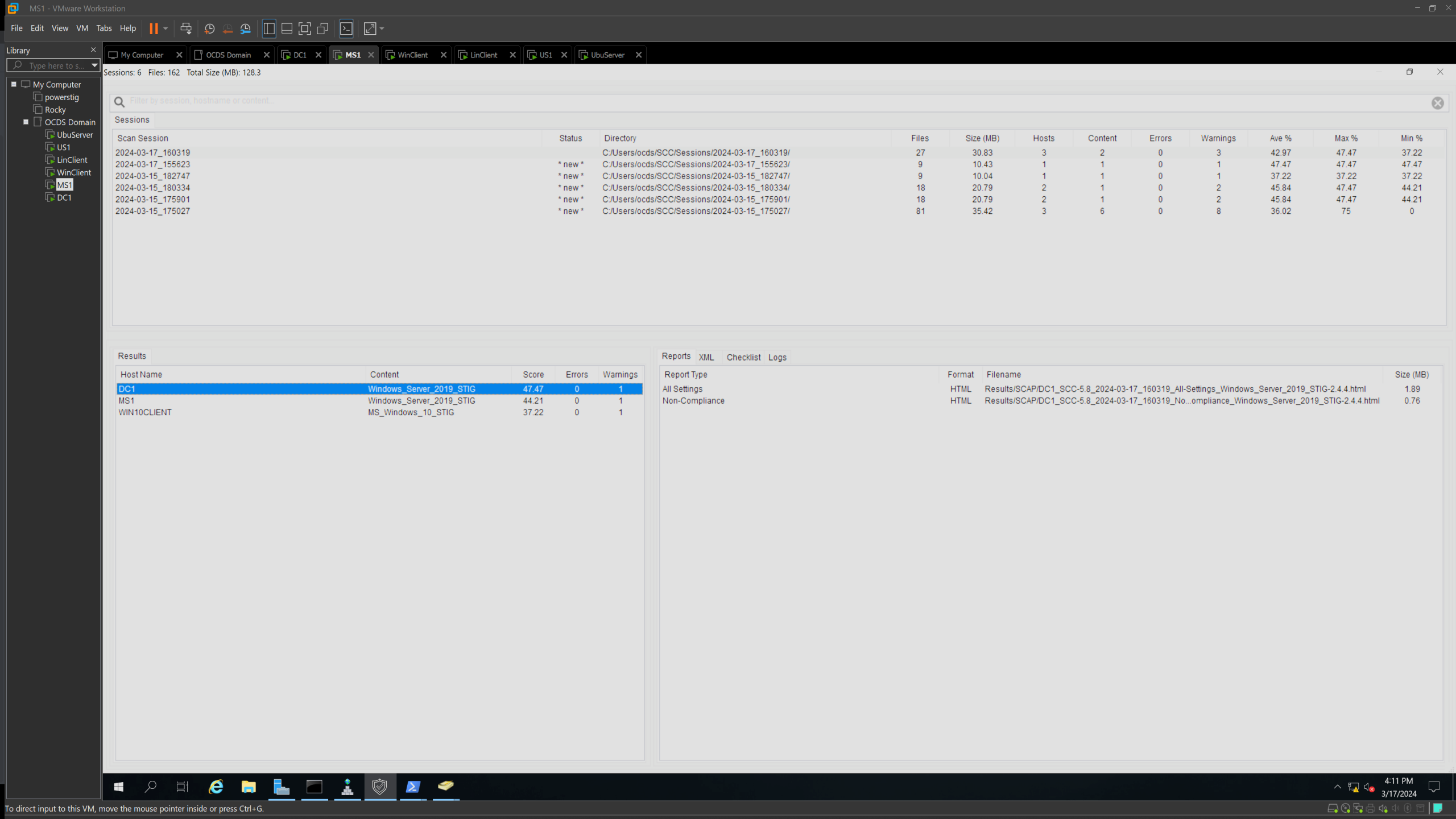
- V-205627 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures. - Fail
- V-205629 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less. - Fail
- V-205630 - Windows Server 2019 must have the period of time 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


MS1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
powerstig
Rocky
OCDS Domain
UbuServer
US1
LinClient
WinClient
MS1
DC1
My Computer
OCDS Domain
DC1
MS1
WinClient
LinClient
US1
UbuServer
DNS Manager
File Action View Help
DNS
dc1.ocds.domain
Forward Lookup Zones
_msdcs.ocds.domain
ocds.domain
Reverse Lookup Zones
Trust Points
Conditional Forwarders
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)
Windows PowerShell
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
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
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\ocds> hostname
MS1
PS C:\Users\ocds>
ocds@ocds.domain@us1: ~
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 connection or proxy settings
Last login: Sun Mar 17 22:48:42 2024 from 192.168.155.137
ocds@ocds.domain@us1:~$ ls /
bin boot cdrom dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv snap swap.img sys tmp usr var
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:~$
ocds@ocds.domain@uc1: ~
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 boot cdrom dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv snap swapfile sys tmp usr var
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:~$
Share this window
Windows Server 2019 Standard Evaluation
Windows License valid for 175 days
Build 17763.rs5_release.180914-1434
3:55 PM
3/17/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


MS1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to s...
My Computer
powerstig
Rocky
OCDS Domain
UbuServer
US1
LinClient
WinClient
MS1
DC1
My Computer
OCDS Domain
DC1
MS1
WinClient
LinClient
US1
UbuServer
Recycle Bin
Active Directory Users and Computers
File Action View Help
Active Directory Users and Co
Saved Queries
ocds.domain
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Acc
Name
Type
MS1
Computer
UC1
Computer
US1
Computer
WIN10CLIENT
Computer
Windows PowerShell
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
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>
Active Directory Users and Computers
File Action View Help
Active Directory Users and Comp
Saved Queries
ocds.domain
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accoun
Users
Name
Type
DC Type
DC1
Computer
GC
ocds@ocds.domain@us1: ~
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 connection or proxy settings
Last login: Sun Mar 17 22:48:42 2024 from 192.168.155.137
ocds@ocds.domain@us1:~$ ls /
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv swap.img sys tmp usr var
ocds@ocds.domain@us1:~$
ocds@ocds.domain@uc1: ~
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 boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv swapfile sys tmp usr var
ocds@ocds.domain@uc1:~$
Share this window
Windows Server 2019 Standard Evaluation
Windows License valid for 175 days
Build 17763.rs5_release.180914-1434
3:51 PM
3/17/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


MS1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
powerstig
Rocky
OCDS Domain
UbuServer
US1
LinClient
WinClient
MS1
DC1
My Computer
OCDS Domain
DC1
MS1
WinClient
LinClient
US1
UbuServer
Back
Forward
Reload
Search
Match Case
Whole Words
0 of 0
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
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
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
Fail: 106
Error: 0
Unknown: 0
Fixed: 0
Not Applicable: 20
Not Checked: 63
Not Selected: 0
Informational: 0
Total: 273
BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0
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
4:15 PM
3/17/2024
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

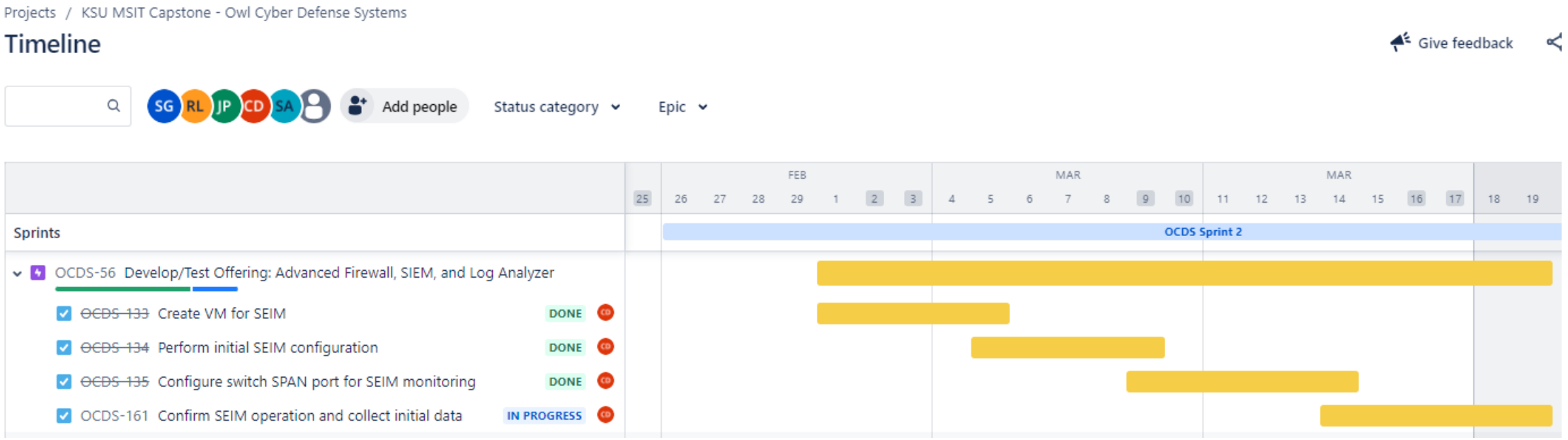

MS1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
powerstig
Rocky
OCDS Domain
UbuServer
US1
LinClient
WinClient
MS1
DC1
My Computer
OCDS Domain
DC1
MS1
WinClient
LinClient
US1
UbuServer
Remote Scan Status
Status: Finished
Total: 3
Pending: 0
Scanning: 0
Finished: 3
Error: 0
Results: 21
Logs: 3
Hosts
Host
OS
Status
Message
DC1
MS1
WIN10CLIENT
Microsoft Windows Se... Standard Evaluation
Microsoft Windows Se... Standard Evaluation
Microsoft Windows 10 Education
Finished
Finished
Finished
Finished - Results: 7 Logs: 1
Finished - Results: 7 Logs: 1
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
192.168.155.139
US1
UC1
Ubuntu 22 amd64
Ubuntu 22 amd64
Finished
Finished
Finished - No Applicable Content
Finished - No Applicable Content
Sessions
File Home Share View
This PC › Local Disk (C:) › Users › ocds › SCC › Sessions ›
Search Sessions
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
DVD Drive (D:) SSS_X
Network
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
4:10 PM
3/17/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


MS1 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to s...
My Computer
powerstig
Rocky
OCDS Domain
UbuServer
US1
LinClient
WinClient
MS1
DC1
My Computer
OCDS Domain
DC1
MS1
WinClient
LinClient
US1
UbuServer
Sessions: 6 Files: 162 Total Size (MB): 128.3
Filter by session, hostname or content...
Sessions
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
Results
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
Reports XML Checklist Logs
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
4:11 PM
3/17/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Epic: Develop & Test the Advanced Firewall, SIEM, & Log Analyzer Client Offering

Chris Dunbar

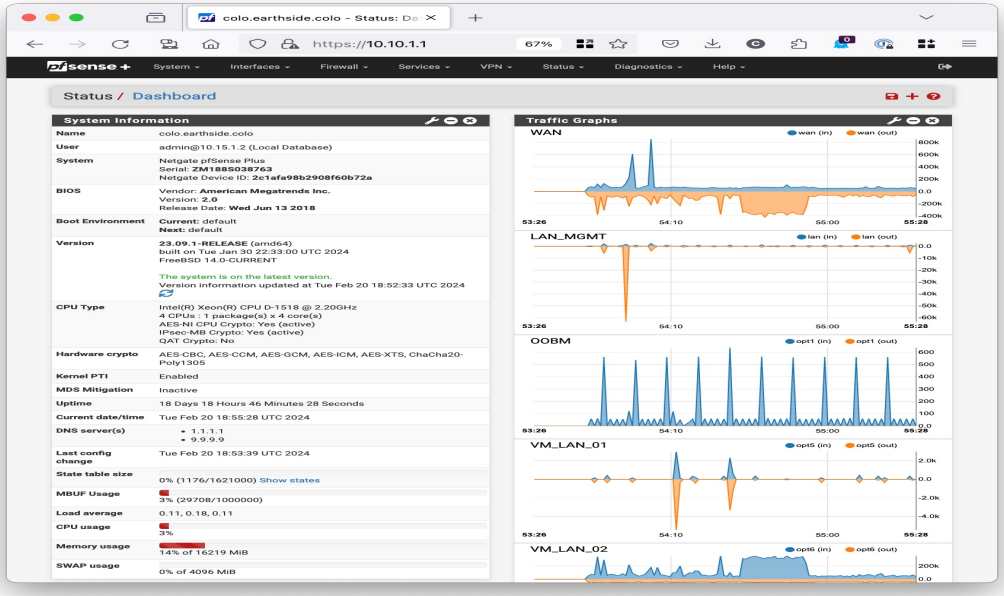
Develop & Test the Advanced Firewall, SIEM, & Log Analyzer Client Offering



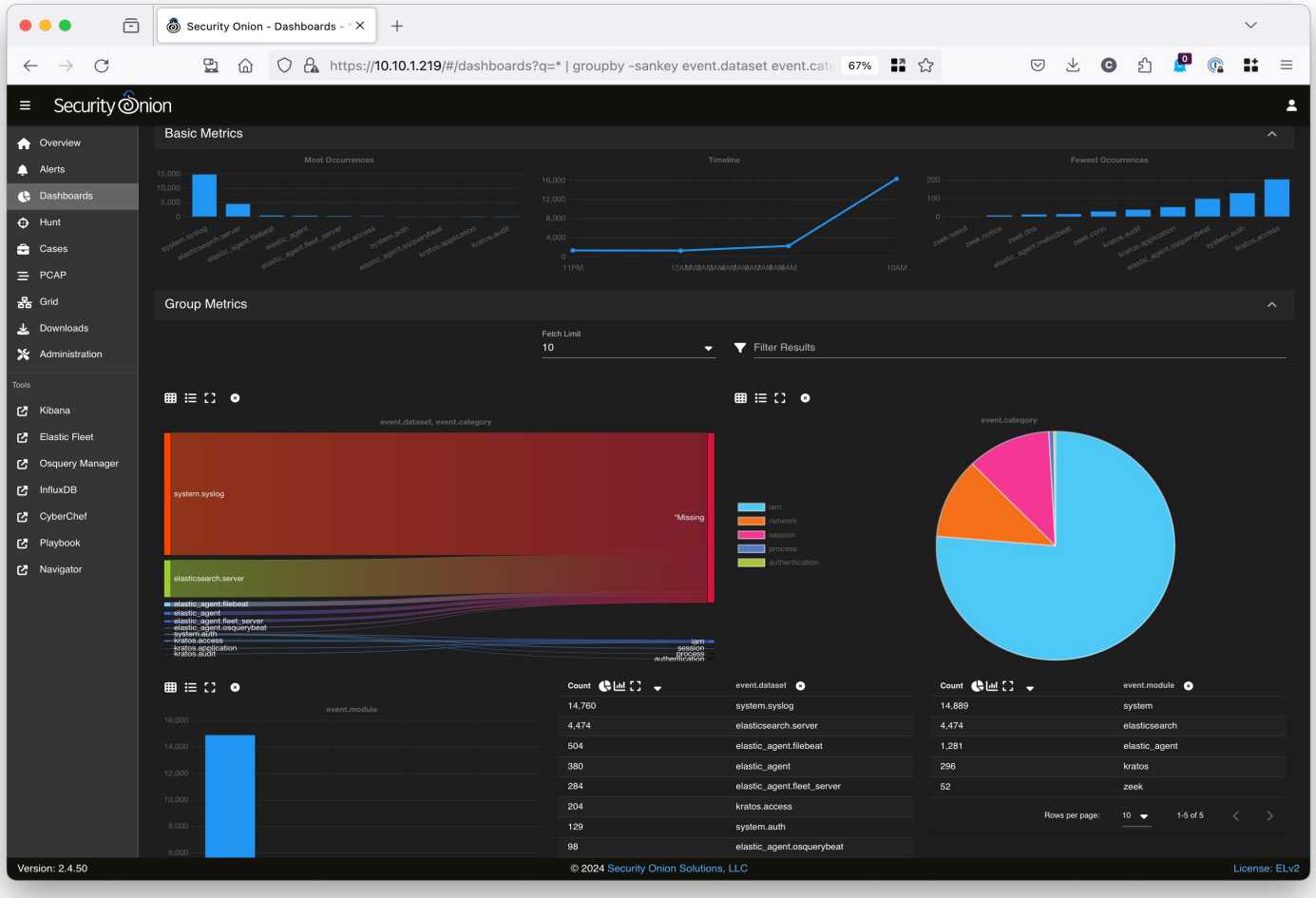
Complete/On Track

Plan & Design the Advanced Firewall, SIEM, & Log Analyzer Client Offering

- Configured Security Onion VM and open source SEIM network & security monitoring tool for client offering.
- Visited data center to connect demo SEIM server to SPAN port for data collection
    - Identified issue with SEIM server that may require reinstallation of software.
- Researched options for more hosting capabilities.
- Configured a detailed design for the OCDS Advanced Firewall, SIEM & Log Analyzer
- Tested end to end monitoring



Develop & Test the Advanced Firewall, SIEM, & Log Analyzer Client Offering



Owner: Chris Dunbar

Sprint 2 Time Tracking

Sprint 2 Person-hour Time Tracking (Real-time Jira project export)

Person-hours — Edited Save Details

Share Ex

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

Sprint: OCDS Sprint 2

1–50 of 64

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

Person-hours Automated Report: 25Feb-02Mar24

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	25Feb-2Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	16
⊞ Justin Place	5
⊞ Ryan LeBlanc	5
⊞ Scott Gilstrap	12
⊞ Stephanie Aguirre	3
Grand Total	41

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	25Feb-2Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊟ Chris Dunbar	16
Complete configuration of SEIM	3
Initial company website launch	3
Research & Select Firewall	4
Research & Select Log Analyzer	3
Research & Select SIEM	3
⊟ Justin Place	5
Test hardening content tool	2
Write script for hardening content tool	3
⊟ Ryan LeBlanc	5
Implement Ubuntu dataset	1
Investigate Incorporating Server Scanning Capability to Produce Vuln Report	2
Write Bash script to check against Linux STIGs	1
Write PowerShell script to scan window systems against STIG & show results	1
⊟ Scott Gilstrap	12
Complete Business Goals	2
Complete Business Strategy	2
Complete Company Mission Statement	3
Complete Company Vision Statement	2.5
Develop IT Security Plan Template Based on Design	1
Sprint 2 Project Management	1.5
⊟ Stephanie Aguirre	3
Complete IT Policy List	3
Grand Total	41

Person-hours Automated Report: 03-09Mar24

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	03-09Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
Chris Dunbar	**6.0**
Justin Place	**6.5**
Ryan LeBlanc	**5.0**
Scott Gilstrap	**10.7**
Stephanie Aguirre	**6.0**
Grand Total	**34.2**

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	03-09Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
Chris Dunbar	**6.0**
Complete configuration of SEIM	1.0
Initial project website launch	1.0
Configure Company Website	2.0
Security Onion SIEM VM - fix interfaces	1.0
Research/investigate hosting possibilities	1.0
Justin Place	**6.5**
Write script for hardening content tool	2.0
Create VMs to demo system hardening	2.5
Establish virtual domain to support ChatBot demo	2.0
Ryan LeBlanc	**5.0**
Implement Dataset Win10	1.0
Implement Server 2019 dataset	2.0
Implement server 2022 dataset	2.0
Scott Gilstrap	**10.7**
Complete IT Goals	1.4
Complete IT Strategy	1.3
Complete Product Offering Catalogue	1.4
Complete Target Market Definition	1.4
Coordinate w Stephanie incorporate IT Policies in Business Plan	0.8
Coordinate w Stephanie to incorporate legal structure in Business Plan	0.8
Create IT Security Plan Client Questionnaire	1.4
Project Management	2.2
Stephanie Aguirre	**6.0**
Complete/Publish Legal Structure for the Business	3.0
Complete/Publish list of IT Security Policies	3.0
Grand Total	**34.2**

Person-hours Automated Report: 10-16Mar24

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	10-16Mar2024
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊞ **Chris Dunbar**	**8.0**
⊞ **Justin Place**	**6.0**
⊞ **Ryan LeBlanc**	**10.0**
⊞ **Scott Gilstrap**	**9.9**
⊞ **Stephanie Aguirre**	**5.0**
Grand Total	**38.9**

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	10-16Mar2024
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊟ **Chris Dunbar**	**8.0**
Configure switch SPAN port for SEIM monitoring	4.0
Create Products catalog section on website	4.0
⊟ **Justin Place**	**6.0**
Test hardening content tool	2.0
Write script for hardening content tool	2.0
Look into/research Ansible	2.0
⊟ **Ryan LeBlanc**	**10.0**
implement RHEL8 dataset	1.0
Implement Ubuntu dataset	2.0
Investigate Incorporating Server Scanning Capability to Produce Vuln Report	5.0
Write Bash script to check against Linux STIGs	1.0
Write PowerShell script to scan windows systems against STIG & show results	1.0
⊟ **Scott Gilstrap**	**9.9**
Complete Product Offering Cost Model	2.0
Develop Risk Mngmnt Plan Template Based on Design	2.9
Review & Complete Business Plan Document	4.0
Ensure Milestone 2 presentation is scheduled	1.0
⊟ **Stephanie Aguirre**	**5.0**
Complete Development of Curriculum	2.0
Complete/Publish List of Cybersecurity Policies	2.0
Coordinate w Chris to incorporate links on website	1.0
Grand Total	**38.9**

Person-hours Automated Report: 17-23Mar24

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	17-23Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊞ Chris Dunbar	10.3
⊞ Justin Place	10.8
⊞ Ryan LeBlanc	10.0
⊞ Scott Gilstrap	10.7
⊞ Stephanie Aguirre	9.4
Grand Total	51.2

Sprint	OCDS Sprint 2
Issue Type	Task
Week of	17-23Mar24
Updated	(All)

Row Labels	Sum of Time Spent Calc
⊟ Chris Dunbar	10.3
Confirm SEIM operation and collect initial data	4.2
Begin updating placeholder text with real content	2.2
Create Products catalog section on website	3.9
⊟ Justin Place	10.8
Test hardening content tool	3.3
Write script for hardening content tool	4.4
Create VMs to demo system hardening	3.0
⊟ Ryan LeBlanc	10.0
Implement Dataset Win10	1.0
implement RHEL8 dataset	2.0
Implement Server 2019 dataset	2.0
Implement server 2022 dataset	2.0
Implement Ubuntu dataset	1.0
Write PowerShell script to scan windows systems against STIG & show results	2.0
⊟ Scott Gilstrap	10.7
Coordinate w Chris to incorporate form on website	1.0
Coordinate w Chris to incorporate Product Catalogue & Cost on website	1.0
Coordinate with Chris to incorporate form on website	1.0
Review & Complete Business Plan Document	1.0
Test IT Security Plan Form Process	1.1
Test Client Risk Mngmnt Form Process	1.4
Make Milestone 2 Presentation to Sponsor/Instructor	1.0
Upload all documentation to D2L	0.0
Verify all documentation for upload	1.3
Prepare all documentation for Milestone 2 Presentation	1.0
Create Milestone 2 PPT Presentation	1.0
⊟ Stephanie Aguirre	9.4
Coordinate w Chris to incorporate links on website	3.3
Create Training Content Based on Curriculum	3.1
Test Each Training Module	3.1
Grand Total	51.2

Sprint 2 Person-hour Time Tracking (Team Totals)

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

Sprint	OCDS Sprint 2
Week of	(All)

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

Recap/Review

Sprint 2 Project Experience

- Accomplishments
  - Everyone became more familiar with Jira project management software
  - Got the Chatbot working across the network as opposed to just locally
  - Successful scanning and producing a STIG related resultant set
  - Automated team member time-tracking using Jira
- Challenges
  - It is still challenging to work together so closely with such a demanding project, but this team continues to pull it off
  - Creating a stand-alone Risk Assessment Plan – ended up incorporating with IT Security Plan
  - Proper network connectivity at the data center – a couple of physical trips and a software reinstall fixed this challenge
  - Establishing an appropriate work/school/life balance
  - Writing the scripts to run against the STIGs
- Lessons Learned
  - Stay ahead of the curve by maintaining the weekly updates
  - Consistent communications via MS Teams can produce good daily/weekly Scrum input
  - Automate as much as possible
- Opportunities for Improvement
  - Better time management to complete tasks with less stress
  - Team Lead to make contact each morning

Milestone 2
Goals & Objectives

Sprint 2
Feb 26 – Mar 24, 2024

- Complete & Publish OCDS Business Plan
- Complete & Publish OCDS Company Policies
- Publish the OCDS Company and Project Websites
- Develop & Test the Cyber Awareness Training Curriculum Client Offering
- Develop & Test the Proprietary IT Security Plan Client Offering
- Develop & Test the Risk Management Plan Client Offering
- Develop & Test the OCDS AI-enabled Chatbot with Hardening Content
- Develop & Test the OCDS Server Hardening Tool Client Offering
- Develop & Test the Advanced Firewall, SEIM, and Log Analyzer Client Offering

Next Phase: Sprint 3

Milestone 3
Goals & Objectives

Sprint 3
Mar 25 – Apr 21, 2024

- Sprint 2 Review & Retrospective and
- Sprint 3 Planning Meeting scheduled for February 25, 2024
- Sprint 3 Potential Goals & Objectives
  - Review finalized Deliverables
  - Business Plan
  - Company Policies
  - Project & Company website
  - Client Offerings
    - Cyber Awareness Training Curriculum
    - IT Security Planning & Risk Assessment
    - AI-enable Server Hardening Tool
    - Adv F/W, SIEM, & Log Analyzer

Thank You!