



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-1 Presentation

February 21, 2024

What Will Be Covered in This Presentation?

- Team Introduction
- Sprint 1 Milestone Progress Summary
- Sprint 1 Milestone Goals and Objectives
- WBS: Timeline / Gantt Chart view of all Sprint 1 Epics and Tasks showing assignee and progress
- Sprint 1 weekly scrum updates
- Sprint 1 Task Discussions with empirical evidence/artifacts
- Time Tracking: Team and individual effort via person-hour burn-up pivot tables / charts / graphs
- Sprint 1 Recap/Review to include Project Experience

OCDS Team

-  • Scott Gilstrap
 - Project Manager / Team Leader / Scrum Master
-  • Stephanie Aguirre
 - Technical Writer / Instructor
-  • Chris Dunbar
 - Systems Administrator / Web Master
-  • Justin Place
 - Senior Architect / Developer
-  • Ryan LeBlanc
 - Senior Architect / Developer

Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline



Sprint 1 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
Plan & Design OCDS Business Plan	G	09-Feb-24	<ul style="list-style-type: none"> Completed successful design of OCDS Business Plan after researching multiple options/possibilities. 	NA	NA	NA
Build-out Website Infrastructure	G	03-Feb-24	<ul style="list-style-type: none"> Complete. Used actual data center infrastructure as host systems. Built and configured VMs using VMware and configured firewall. 	NA	NA	NA
Plan & Design the OCDS Company Website	G	11-Feb-24	<ul style="list-style-type: none"> In Progress. On Track. Installed all server packages and encryption certificates. Created web page templates using team input. 	NA	NA	NA
Plan, Design & Publish draft of Project Website	G	25-Feb-24	<ul style="list-style-type: none"> Complete. Configured proper web template using requirements document for project folders and content 	NA	NA	NA
Plan & Design the OCDS IT Policies	G	17-Feb-24	<ul style="list-style-type: none"> Completed the list of IT Policies for the OCDS Business Plan. Coordinated with Scott to preparation incorporation into the plan. 	NA	NA	NA
Plan & Design the IT Security Planning Client Offering	G	06-Feb-24	<ul style="list-style-type: none"> Complete. Compared multiple cybersecurity plan options. Designed the baseline for IT cybersecurity planning tool. 	NA	NA	NA
Plan & Design the Risk Management Planning Client Offering	G	16-Feb-24	<ul style="list-style-type: none"> Complete. Based on the design of the OCDS cybersecurity planning tool created a form design to develop proprietary risk mgmt. plan 	NA	NA	NA
Plan & Design the Cyber Awareness Training Client Offering	G	14-Feb-24	<ul style="list-style-type: none"> Complete. Created employee cybersecurity educational curriculum. Listed certs & skills required and designed a training plan 	NA	NA	NA
Plan & Design the AI-enabled Server Hardening Client Offering	G	18-Feb-24	<ul style="list-style-type: none"> Complete. Designed website layout, researched NIST 800-53 & AI toolsets. Configured dataset. Trained AI. Improved design accuracy. 	NA	NA	NA
Plan & Design the Advanced Firewall, SIEM, & Log Analysis Client Offering	G	16-Feb-24	<ul style="list-style-type: none"> Complete. Researched multiple firewalls & selected pfSense. Selected SecurityOnion to by the SIEM & Log Analyzer. 	NA	NA	NA

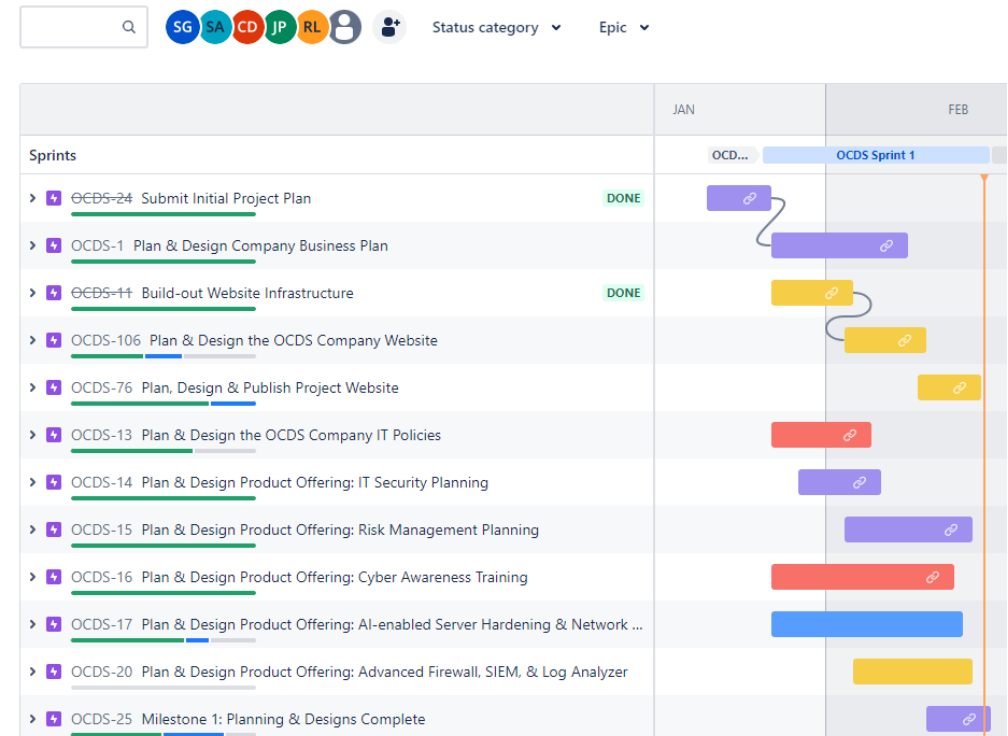
LEGEND B Complete G On Track Y At Risk R Delayed H On-Hold/ Canceled N Not Started

Sprint 1 Milestone Progress Summary

- Sprint 1 is on target for successful completion and submission by Feb 25, 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 contributing appropriately
- There have been no risks, issues nor impediments to log/track
- No change requests were required
- Details addressed in following slides

Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline



Sprint 1 Goals & Objectives

Milestone 1

Goals & Objectives

Sprint 1
Jan 25 – Feb 25, 2024

- Plan & Design the OCDS Business Plan
- Build-out Website Infrastructure
- Plan & Design the OCDS Company Website
- Plan, Design & Publish draft of Project Website
- Plan & Design the OCDS IT Policies
- Plan & Design the IT Security Planning Client Offering
- Plan & Design the Risk Management Planning Client Offering
- Plan & Design the Cyber Awareness Training Client Offering
- Plan & Design the AI-enabled Server Hardening Client Offering
- Plan & Design the Advanced Firewall, SIEM, & Log Analysis Client Offering

Work Breakdown Structure

Overall WBS Epic Timeline for Sprint 1 Milestones

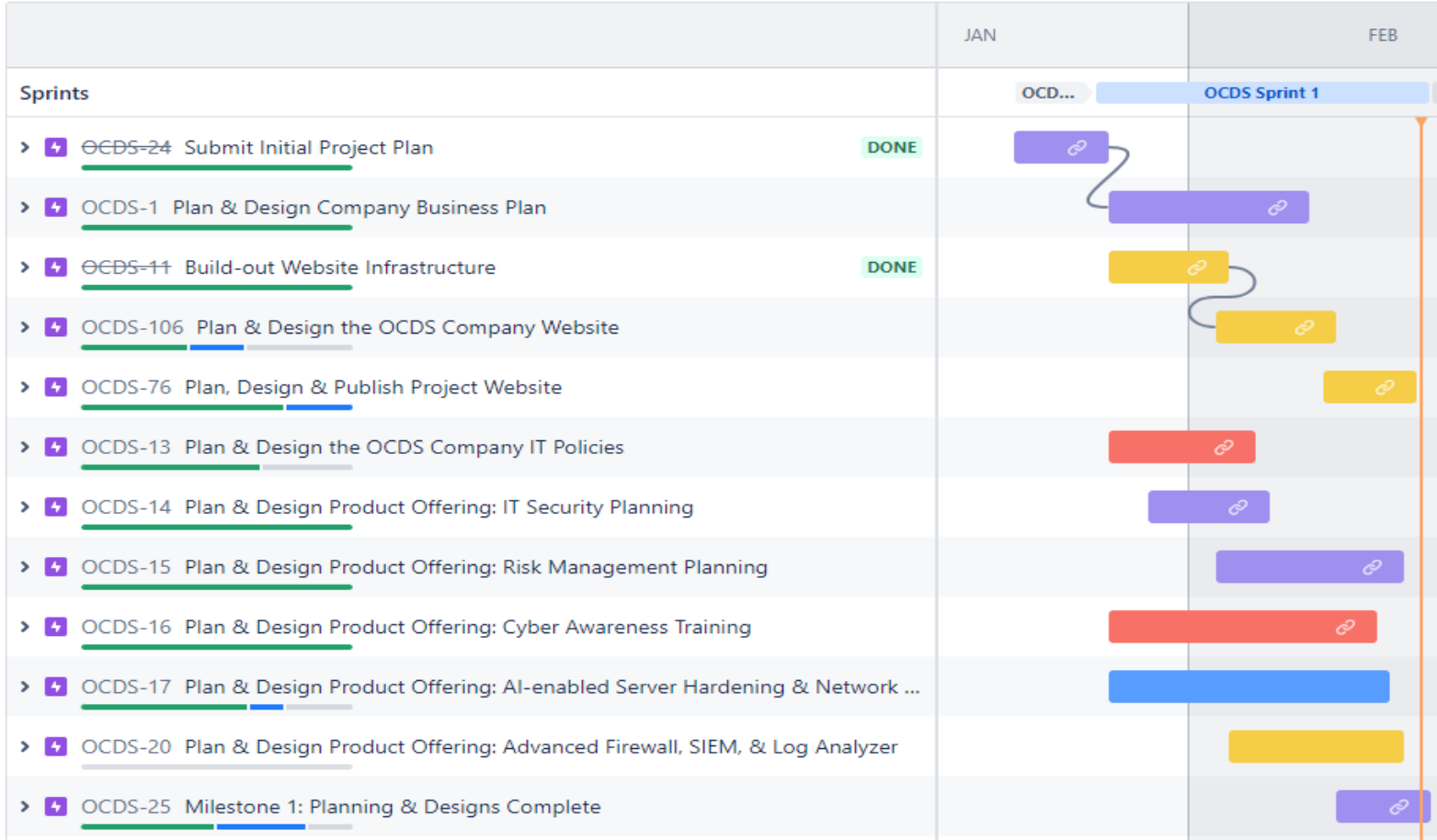
Projects / KSU MSIT Capstone - Owl Cyber Defense Systems

Timeline



Status category ▾

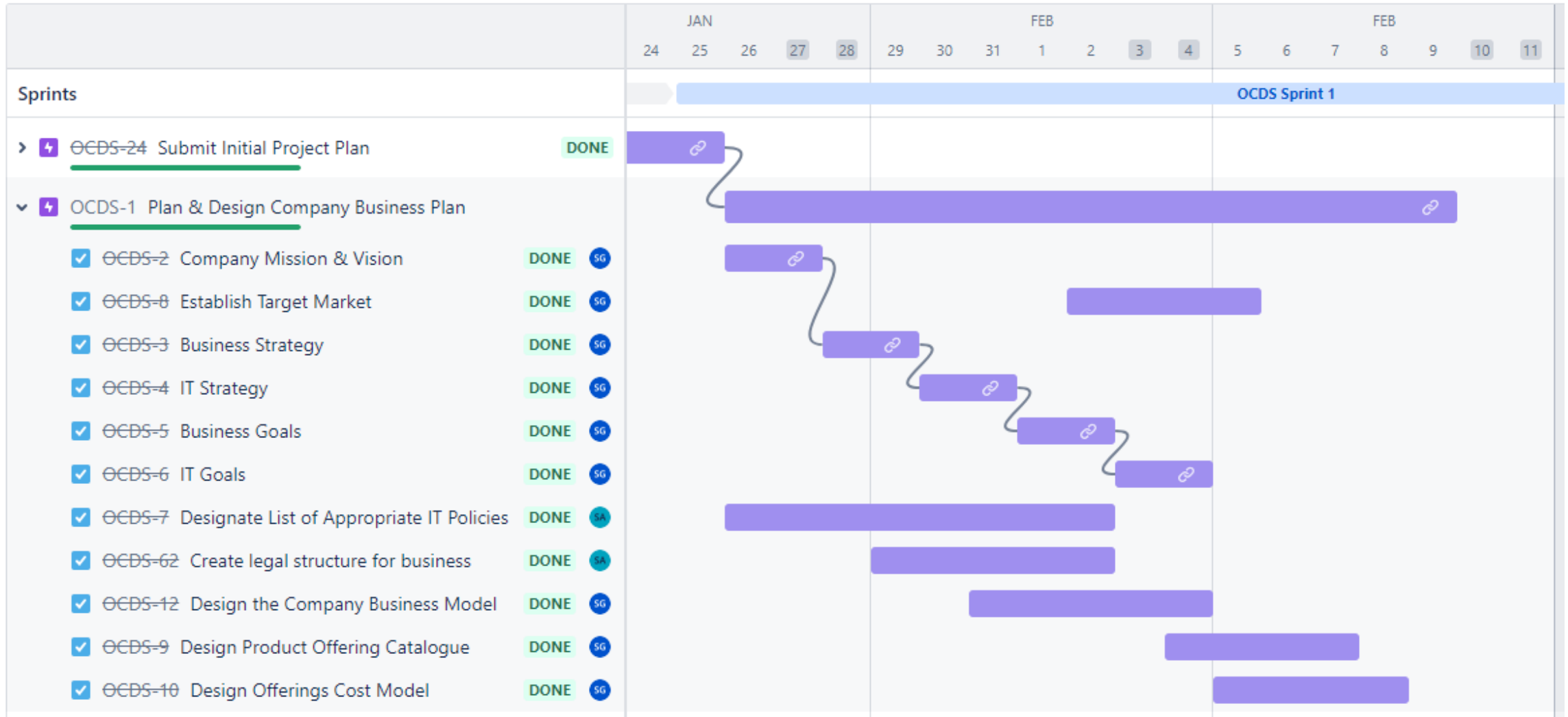
Epic ▾



Complete



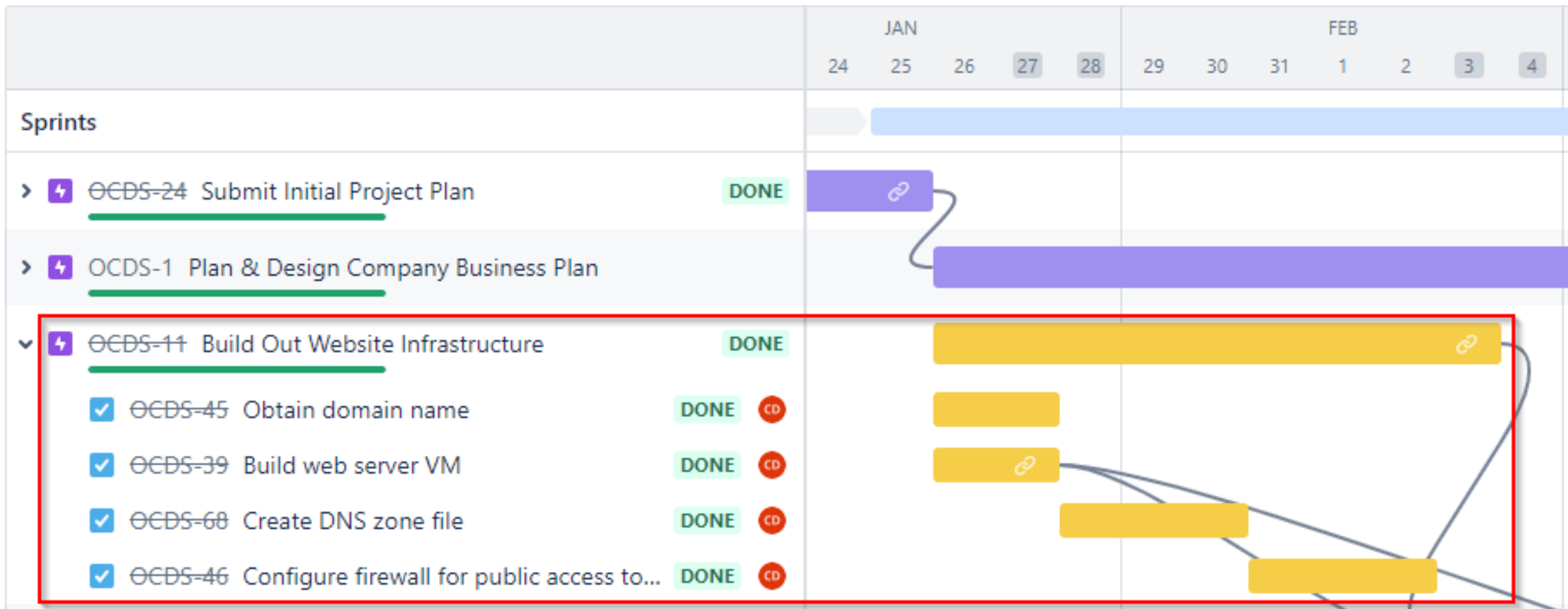
Plan & Design the OCDS Business Plan



Complete



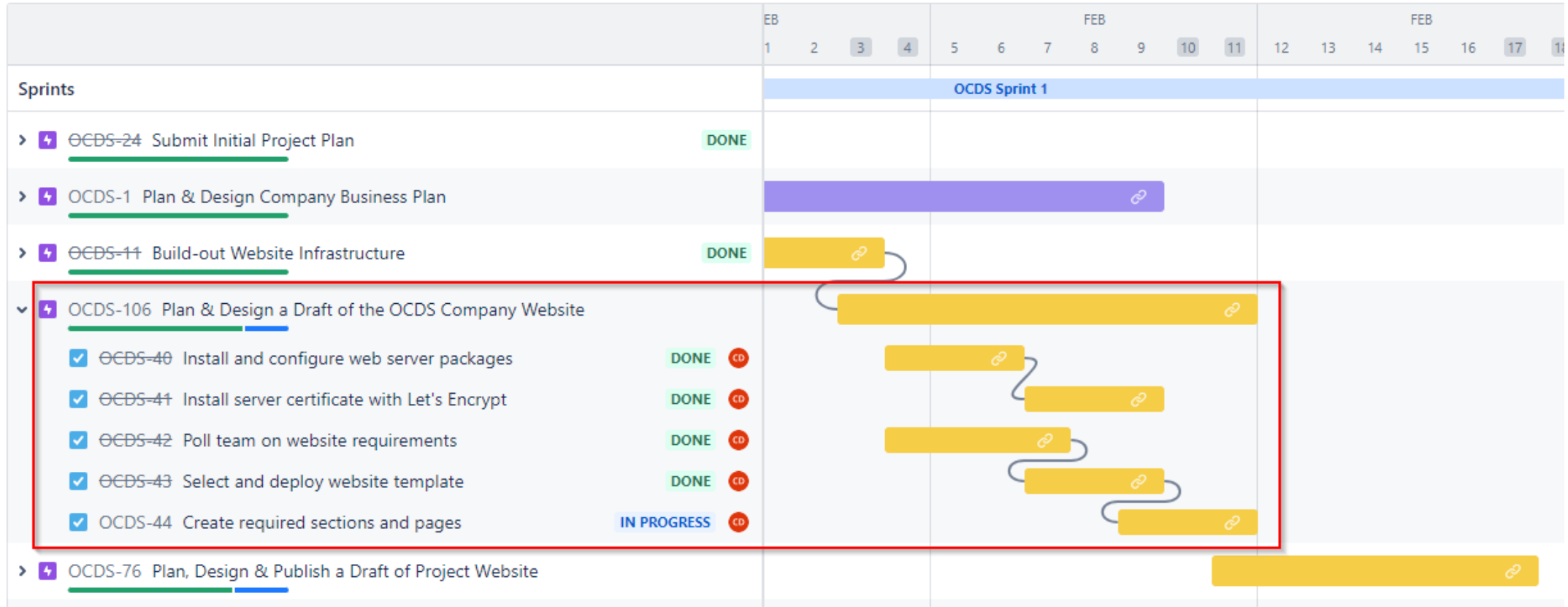
Build Out Website Infrastructure



Complete



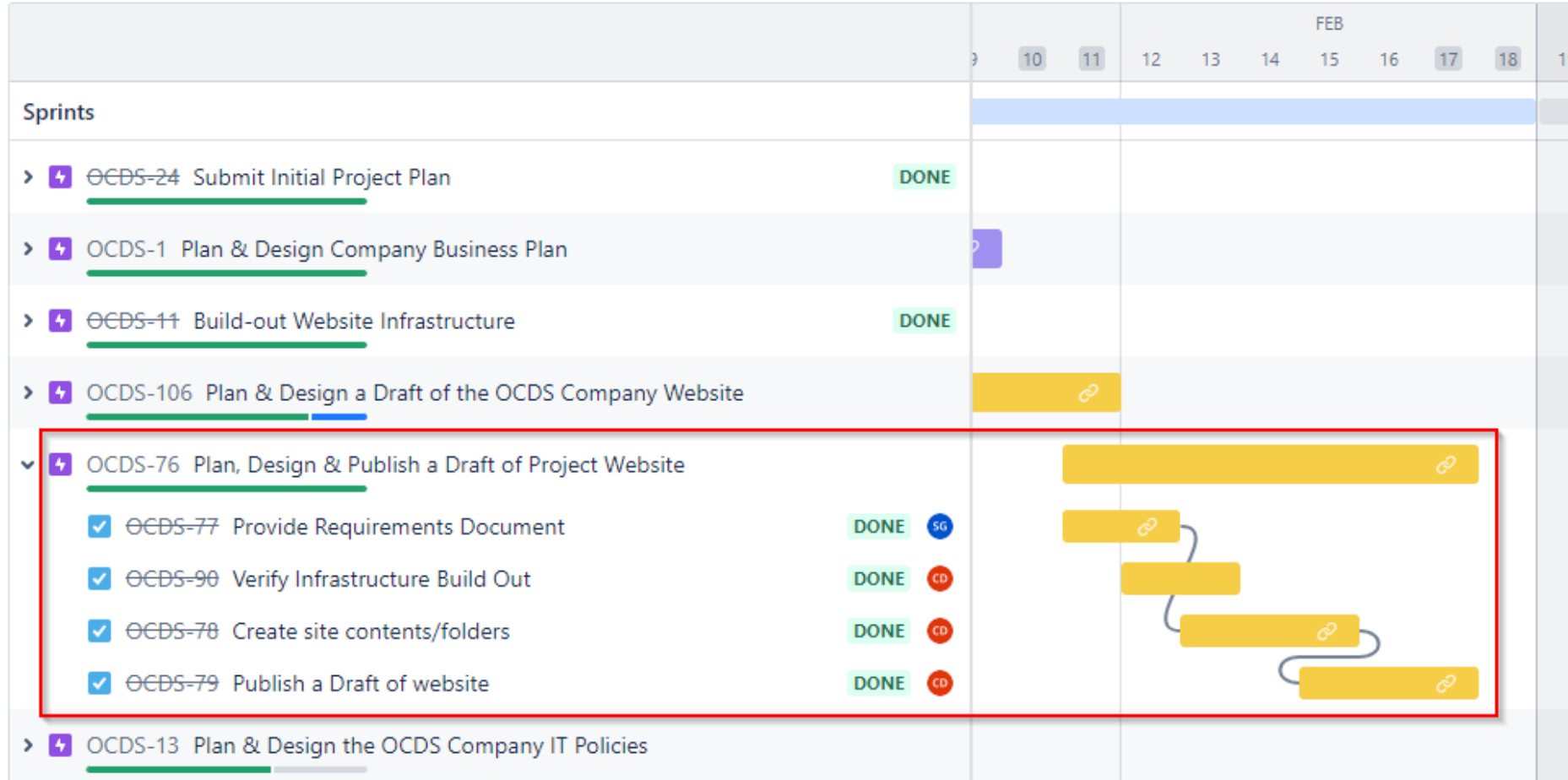
Plan & Design a Draft of the OCDS Company Website



In Progress & On Target to be Completed in Sprint 1 – requirements expanded as needs were discussed with team.



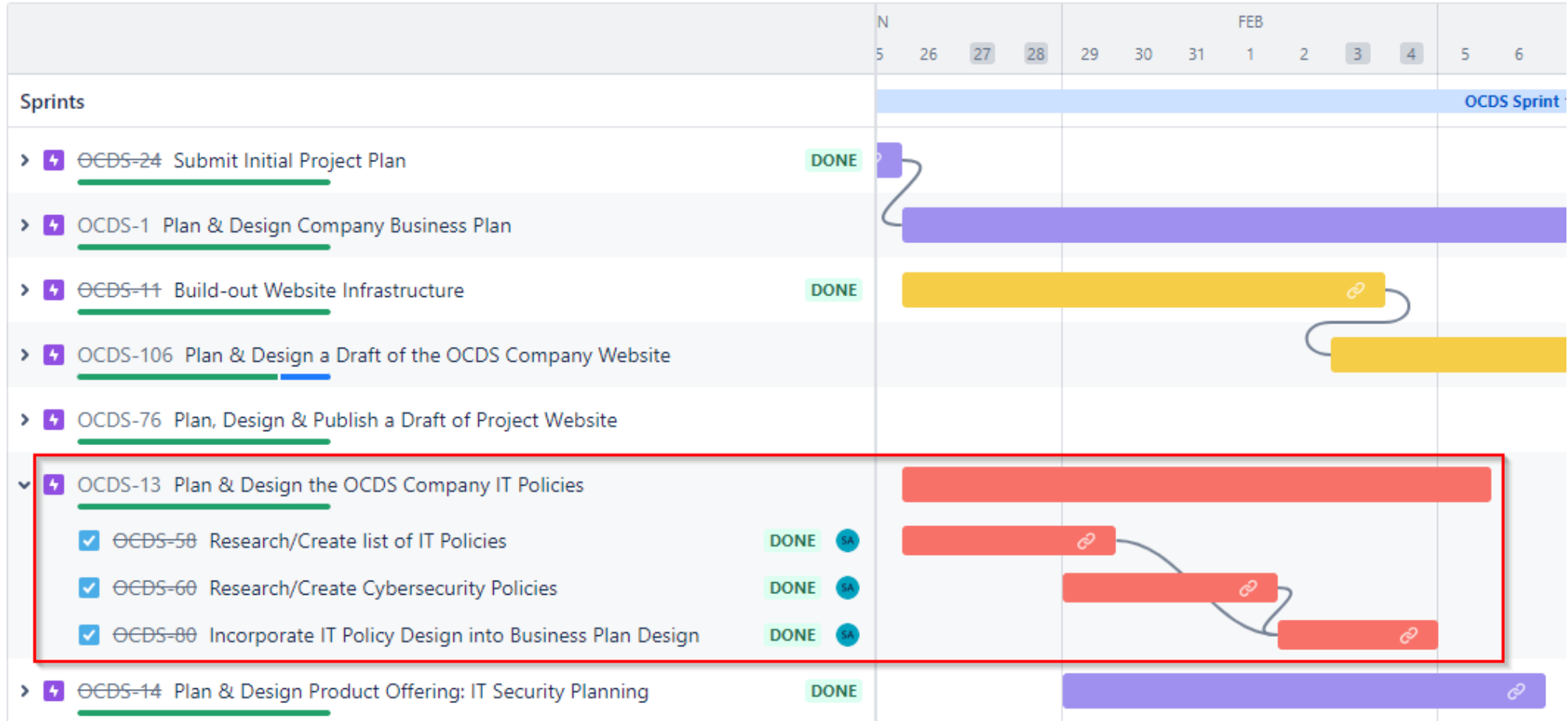
Plan, Design & Publish a Draft of the Project Website



Complete



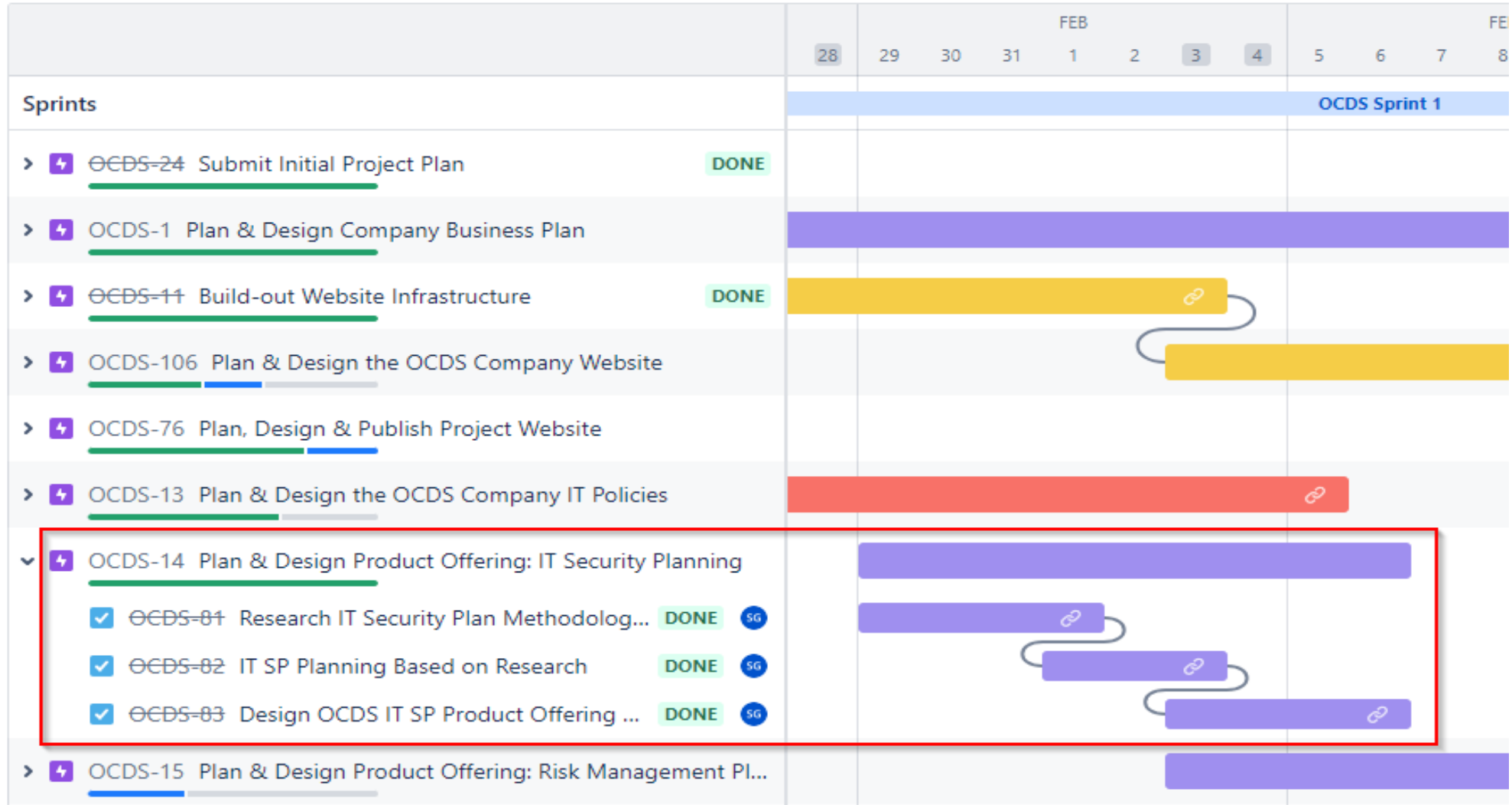
Plan & Design the OCDS Company IT Policies



Complete



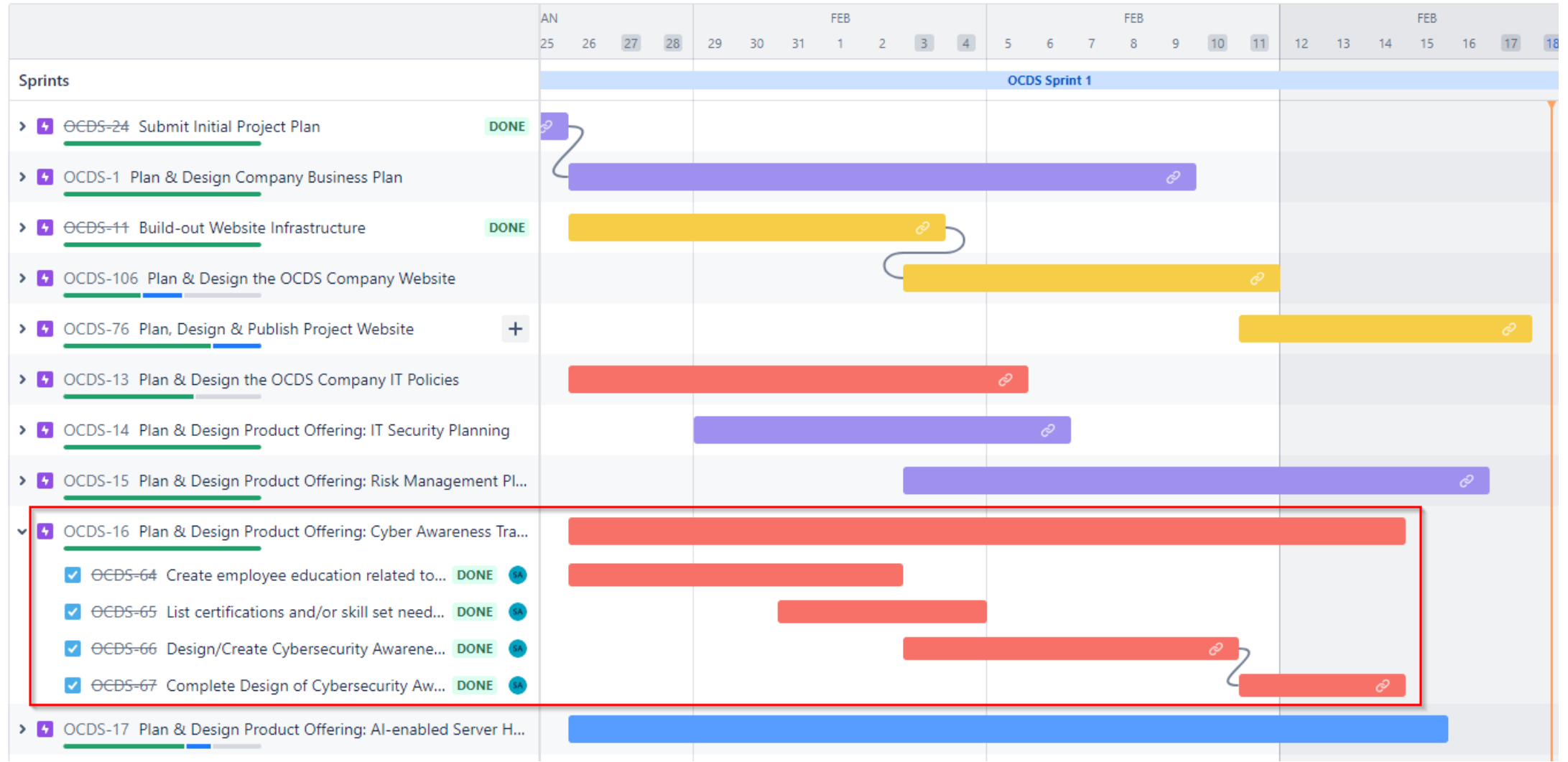
Plan & Design the IT Security Planning Client Offering



Complete



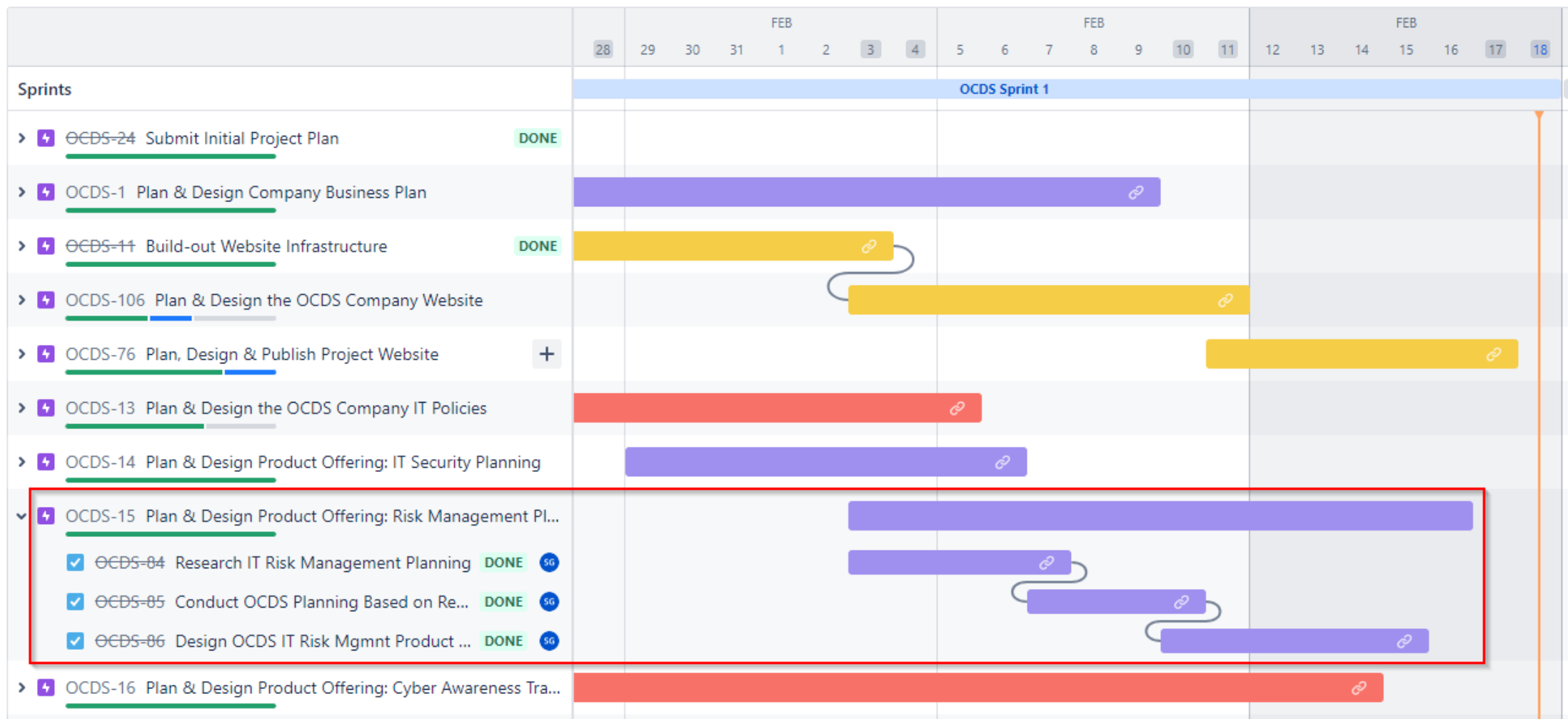
Plan & Design Cyber Awareness Training Client Offering



Complete



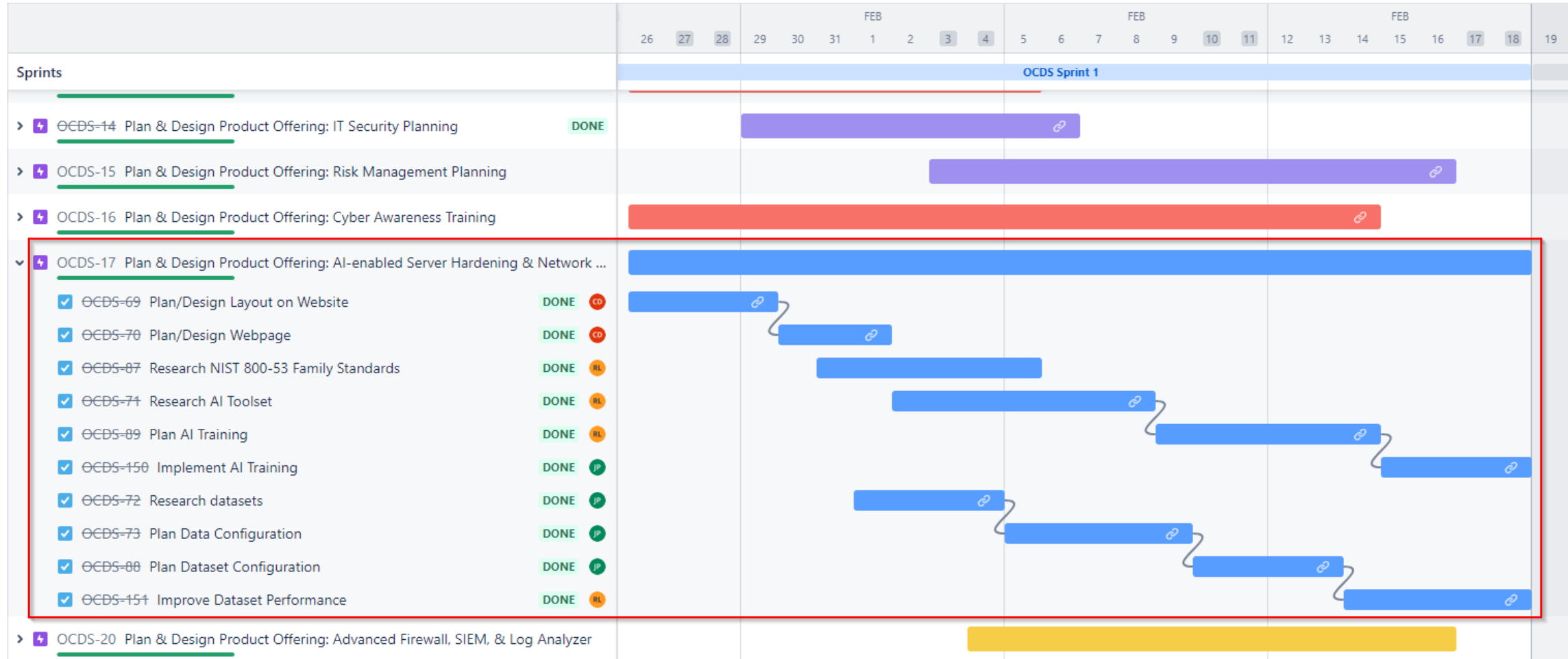
Plan & Design the Risk Management Plan Client Offering



Complete



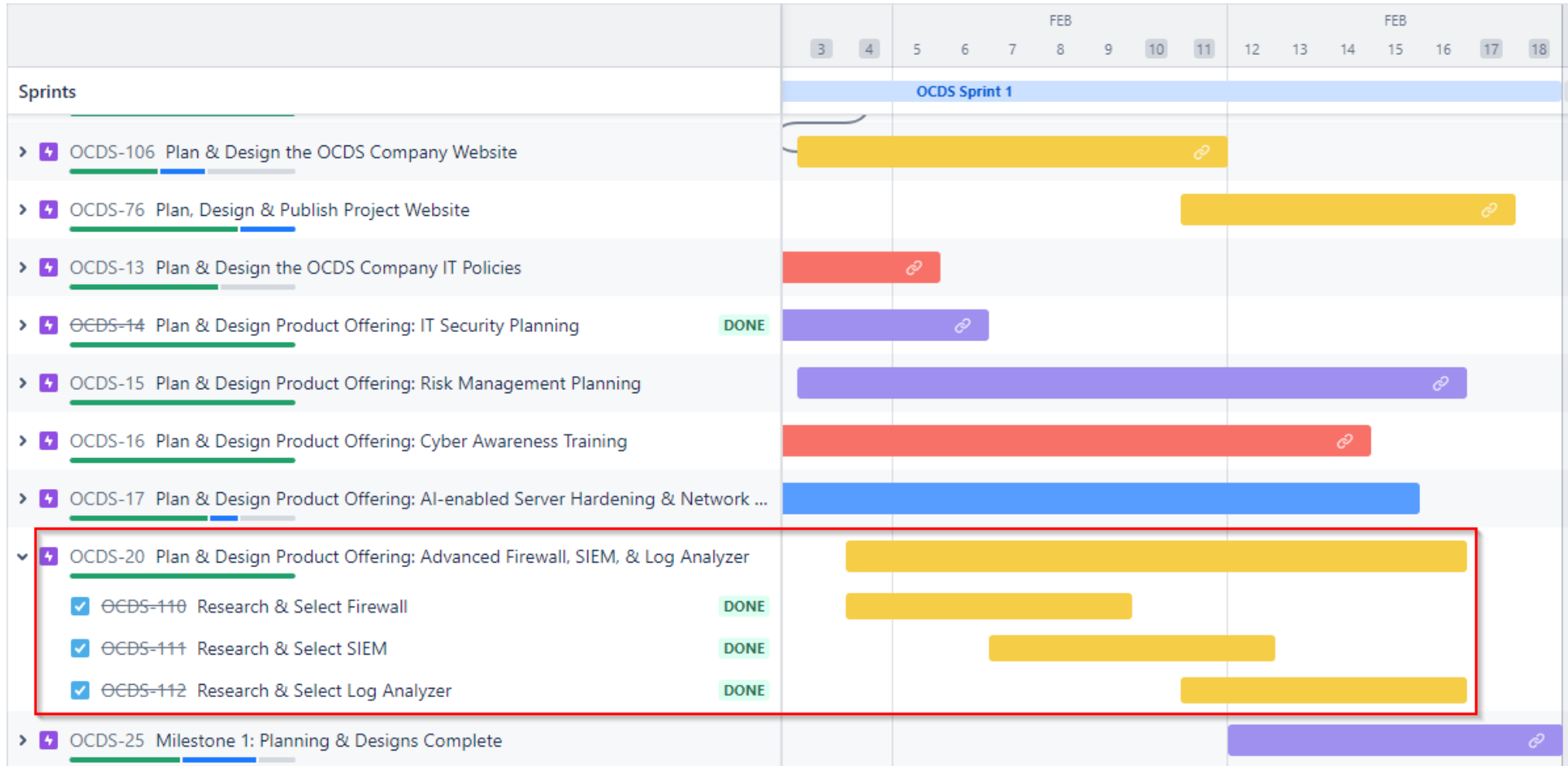
Plan & Design the AI-enabled Server Client Offering



Complete



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



Complete

Weekly Scrum Updates

Project – Owl Cyber Defense Systems

Data as of: 01/21/24

Project Manager	Project Objective	Start Date	End Date	Overall	Schedule	Budget	Scope	Resource
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	●	●	●	●	●

Key Accomplishments/Activities	Next Steps
<ul style="list-style-type: none"> ✓ Created/Submitted Project Proposal ✓ Template for Project created in Jira ✓ Researched IT Policies & cyber awareness training ✓ Researched company and project website infrastructure required ✓ Purchased company website domain name (ocds.tech) ✓ Researched AI coding 	<ul style="list-style-type: none"> ✓ Obtain Project Proposal Approval ✓ Complete Project planning via Jira ✓ Submit and obtain Project Plan documentation ✓ Continue research and start planning & designing <ul style="list-style-type: none"> ✓ Business Plan ✓ IT Policies ✓ Cyber Awareness Training Curriculum ✓ Website structure ✓ AI coding for network analysis and hardening

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	50%
Planning & Designs Complete (Sprint 1)	01/26/24	02/18/24	5%
Development & Testing Complete (Sprint 2)	02/19/24	03/17/24	0%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

Key Risks/Issues

ID	Risk(s)	Description	Mitigation / Action Plan	ID	Issue(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A	No Data	N/A	N/A	N/A



Week of 14-20 Jan 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

Data as of: 01/28/24

Project Manager	Project Objective	Start Date	End Date	Overall	Schedule	Budget	Scope	Resource
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	●	●	●	●	●

Key Accomplishments/Activities	Next Steps
<ul style="list-style-type: none"> ✓ Acquired Instructure project approval to move forward ✓ Conducted Kickoff Meeting ✓ Designated Team Lead / Project Manager ✓ Conducted Sprint 0 Retrospective –no issues ✓ Conducted Sprint 1 Planning Meeting – Planning & Design ✓ Completed Jira project entries (Epics, Tasks, Reports) ✓ Researched specific policies for Company IT Policy List ✓ Capacity planning for website infrastructure build ✓ Researched AI-enable data sets for NIST 800-53 ✓ Created OCDS company logo 	<ul style="list-style-type: none"> ✓ Research Business and IT Planning <ul style="list-style-type: none"> ✓ Vision, Strategies, Goals ✓ Plan/Design company IT Policy structure ✓ Plan/Design client product cyber awareness videos ✓ Research Business legal structures ✓ Plan/Design company's product offering catalogue and target market ✓ Research appropriate Business Models ✓ Build out website infrastructure ✓ Design company & project websites ✓ Continue research into AI coding for product offerings

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/26/24	02/18/24	15%
Development & Testing Complete (Sprint 2)	02/19/24	03/17/24	0%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

Key Risks/Issues

ID	Risk(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A

ID	Issue(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A



Week of 21-27 Jan 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

Data as of: 02/04/24

Project Manager	Project Objective	Start Date	End Date	Overall	Schedule	Budget	Scope	Resource
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	●	●	●	●	●

Key Accomplishments/Activities	Next Steps
<ul style="list-style-type: none"> ✓ Completed Sprint 0 & started Sprint 1 ✓ Began research on OCDS Business Plan. ✓ Completed initial design of OCDS IT Policies & legal ✓ Began website infrastructure and server build outs ✓ Initiated DNS configurations for both OCDS websites ✓ Discovered multiple tools for AI Bot research ✓ Initiated NIST STIG server hardening research ✓ Began research to identified tools, methods, & datasets to create & train AI chat bot ✓ Researched applicable types of AI applications 	<ul style="list-style-type: none"> ✓ Milestone 3 & associated Project Plan task assignments. ✓ Design OCDS Business & IT Goals & Objectives. ✓ AI application research & create initial AI environment. ✓ Create initial data set & train w/ Win10 STIGs. ✓ Refine training dataset to improve AI responses. ✓ Convert full STIG checklists to JSON for AI training. ✓ Design cybersecurity resources list & awareness training. ✓ Incorporate OCDS IT policy design w/ Business Plan. ✓ Static HTML site generator package research. ✓ Select website templates & created initial website pages. ✓ Research open-source security packages to support Zero Trust Security client offerings & AI server hardening

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/26/24	02/18/24	25%
Development & Testing Complete (Sprint 2)	02/19/24	03/17/24	0%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

Key Risks/Issues

ID	Risk(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A

ID	Issue(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A



Week of 28 Jan - 03 Feb 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

Data as of: 02/11/24

Project Manager	Project Objective	Start Date	End Date	Overall	Schedule	Budget	Scope	Resource
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	●	●	●	●	●

Key Accomplishments/Activities	Next Steps
<ul style="list-style-type: none"> ✓ Completed planning for the overall Business Plan Design ✓ Established the employee cybersecurity resource list ✓ Completed early stages of Cybersecurity Awareness Training client offering ✓ Decided on Hugo as HTML website generator and created initial development website – polled team on site content ✓ Completed research on AI language models and implemented baseline dataset for AI learning ✓ Designed AI Chatbot based on JSON 	<ul style="list-style-type: none"> ✓ Focus on the company's product catalogue & cost model ✓ Plan design of client offerings... <ul style="list-style-type: none"> ✓ IT Securing & Risk Management Planning ✓ Make final decision on website templates & themes ✓ Publish initial draft of company website ✓ Design Capstone project website ✓ Complete research on open-source security packages to support the Zero Trust Security offering ✓ Implement multiple responses from the Chatbot by increasing AI data set & implement openAI API ✓ Convert JSON items to intents for AI training and increase the dat set.

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/26/24	02/18/24	75%
Development & Testing Complete (Sprint 2)	02/19/24	03/17/24	0%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

Key Risks/Issues

ID	Risk(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A

ID	Issue(s)	Description	Mitigation / Action Plan
No Data	N/A	N/A	N/A



Week of 04-10 Feb 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

Data as of: 02/18/24

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
<ul style="list-style-type: none"> ✓ Installed Hugo site generator and dependent packages ✓ Created initial development website using site generator ✓ Researched open-source security packages to support our Zero Trust Security offerings ✓ Researched AI on Language models and algorithms ✓ Implement code to take dataset and learn ✓ Created Chatbot to answer questions based on learning ✓ Windows 10 dataset configuration completed ✓ Formatted dataset to be ingested by learning model ✓ Adjusted batch sizes & epochs for better accuracy results ✓ Created intents for AI training ✓ Worked patterns for better AI bot conversation accuracy ✓ Linux checklist in JSON format & added to training model ✓ Completed initial Security Planning client offering ✓ Completed adjustments to the initial OCDS Business Plan 	<ul style="list-style-type: none"> ✓ Final decision website templates & themes selection ✓ Publish draft of company website / start Project website ✓ Conclude research into open-source security packages to support our Zero Trust Security offerings ✓ Implement multiple responses from bot ✓ increase data set with other OS ✓ Implement OpenAI API to assist if answer not in dataset ✓ Modify intents to get better results from chatbot ✓ Research NVIDIA RAG ✓ Investigate adding OpenAI to chatbot to increase functionality ✓ Complete Risk Assessment client offering design ✓ Conduct adjustments to the Security Planning client offering design ✓ Incorporate the final OCDS IT Policies into the Business Plan & complete the design of Cyber Awareness Training client offering

Key Milestones	Start Date	End Date	% Complete
Planning & Designs Complete (Sprint 0)	01/19/24	01/25/24	100%
Planning & Designs Complete (Sprint 1)	01/26/24	02/18/24	95%
Development & Testing Complete (Sprint 2)	02/19/24	03/17/24	0%
Business Plan & Products Released to Production (Sprint 3)	03/18/24	04/21/24	0%

No Key Risks/Issues to log



Week of 11-17 Feb 2024

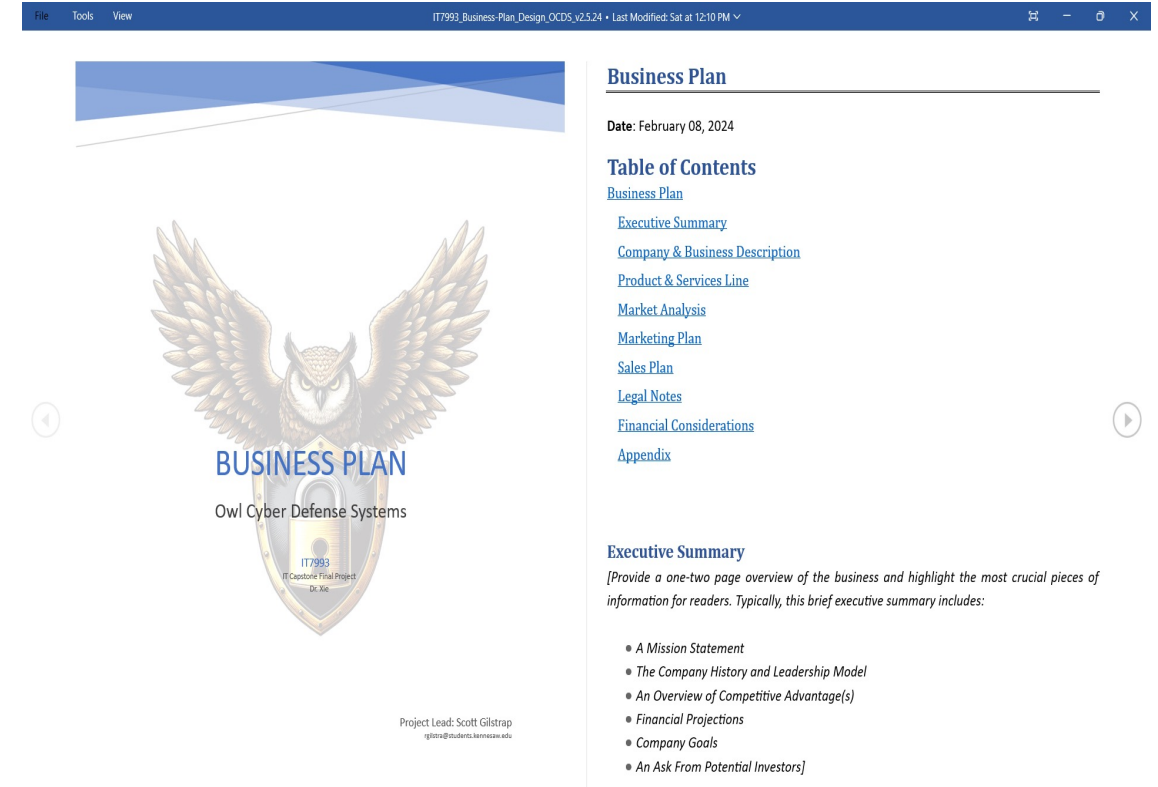
LEGEND

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

Sprint 1 Task Discussions

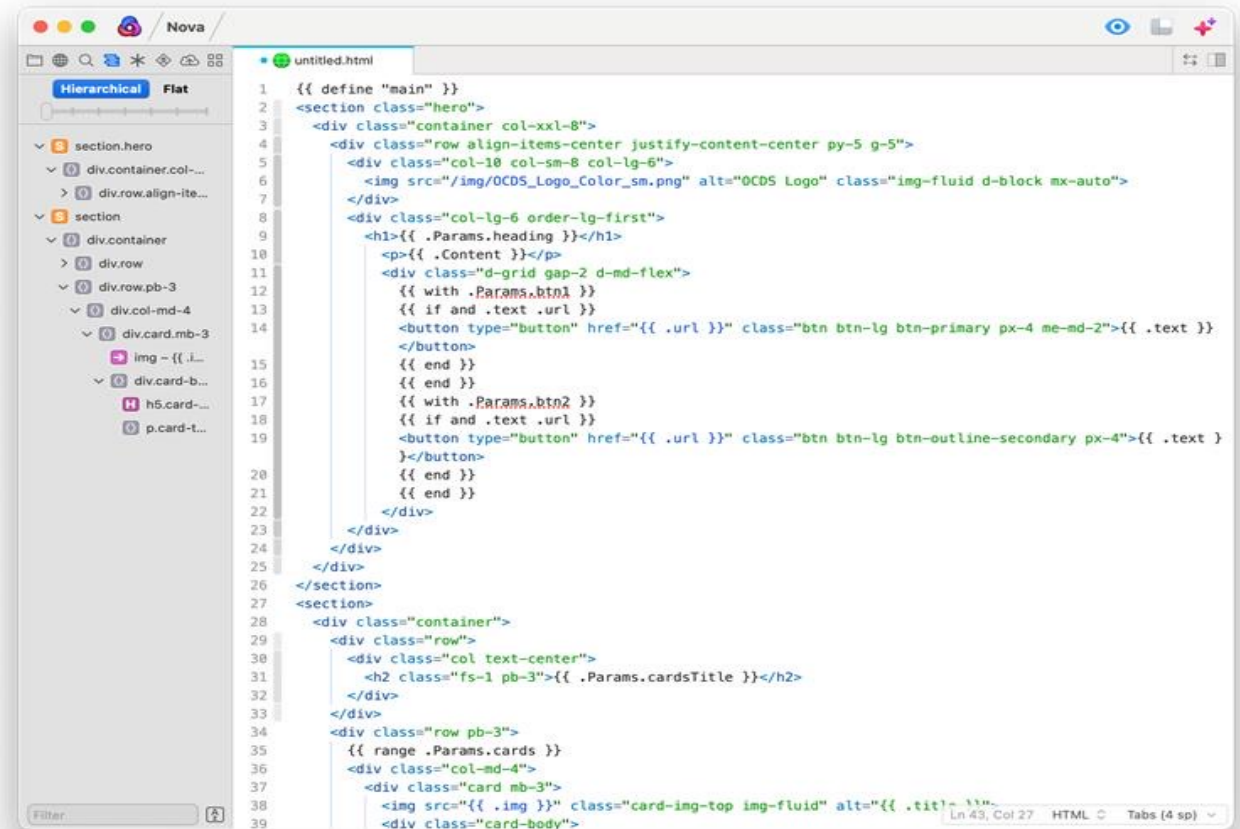
Plan & Design the OCDS Business Plan

- Conducted multiple hours of research into multiple different Business Plan designs
- Planned out and created the design for the OCDS company Business Plan
 - Mission & Vision
 - Business Strategies & Goals
 - IT Strategies & Goals
 - Company IT Policies
 - Business Model
 - Product Offering Catalogue
 - Cost Model
- Uploaded design to the OCDS MS Teams collaboration site
- Deliverable artifact attached and included in the appendix



Plan & Design the OCDS Company & Project Website (1 of 3)

- Purchased company website domain name (ocds.tech)
- Completed DNS configurations for both OCDS websites
- Used Hugo as HTML website generator to create initial development website
- Polled team on site content
- Completed draft of the OCDS company website as well as the project website



The screenshot shows a code editor window titled "Nova" with a file named "untitled.html". The editor displays HTML code using Tailwind CSS classes and Hugo templating syntax. The code is organized into sections and rows, with a sidebar on the left showing a hierarchical view of the document structure. The code includes a hero section with a container, a row of columns, and a section with a heading, content, and buttons. The buttons are defined with parameters like ".Params.btn1" and ".Params.btn2". The code also includes a section for cards, with a row of columns and a card body.

```
1  {{ define "main" }}
2  <section class="hero">
3    <div class="container col-xxl-8">
4      <div class="row align-items-center justify-content-center py-5 g-5">
5        <div class="col-10 col-sm-8 col-lg-6">
6          
7        </div>
8        <div class="col-lg-6 order-lg-first">
9          <h1>{{ .Params.heading }}</h1>
10         <p>{{ .Content }}</p>
11         <div class="d-grid gap-2 d-md-flex">
12           {{ with .Params.btn1 }}
13             {{ if and .text .url }}
14             <button type="button" href="{{ .url }}" class="btn btn-lg btn-primary px-4 me-md-2">{{ .text }}
15             </button>
16           {{ end }}
17           {{ with .Params.btn2 }}
18             {{ if and .text .url }}
19             <button type="button" href="{{ .url }}" class="btn btn-lg btn-outline-secondary px-4">{{ .text }}
20             </button>
21           {{ end }}
22         </div>
23       </div>
24     </div>
25   </section>
26 </section>
27 <section>
28   <div class="container">
29     <div class="row">
30       <div class="col text-center">
31         <h2 class="fs-1 pb-3">{{ .Params.cardsTitle }}</h2>
32       </div>
33     </div>
34     <div class="row pb-3">
35       {{ range .Params.cards }}
36       <div class="col-md-4">
37         <div class="card mb-3">
38           
39           <div class="card-body">
```

Plan & Design the OCDS Company & Project Website (2 of 3)

Owl Cyber Defense Systems

Lorem ipsum dolor sit amet consectetur adipisicing elit. Corrupti dolores, facilis ad temporibus cupiditate, architecto saepe autem ex, tempore consectetur optio vitae ratione nemo dignissimos voluptate excepturi esse iusto eaque magnam perspiciatis. Accusamus explicabo quia accusantium nihil, facere inventore temporibus sit quos odio, ipsam velit laudantium expedita, deserunt libero nesciunt.

Our Services

Cybersecurity Consulting

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[Learn More](#)

Security Assessments

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[Learn More](#)

Red Team Services

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[Learn More](#)

Copyright © 2024 IT 7993 Project 4

OCDS Home Team Members Company

IT7993 Capstone Project 4

Lorem ipsum dolor sit amet consectetur adipisicing elit. Corrupti dolores, facilis ad temporibus cupiditate, architecto saepe autem ex, tempore consectetur optio vitae ratione nemo dignissimos voluptate excepturi esse iusto eaque magnam perspiciatis. Accusamus explicabo quia accusantium nihil, facere inventore temporibus sit quos odio, ipsam velit laudantium expedita, deserunt libero nesciunt.

Project Assets

Project Plan

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[View Content](#)

OCDS Business Plan

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[View Content](#)

OCDS Product Offerings

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto modi placeat corrupti tempora quod quidem praesentium impedit. Rem, sapiente eius?

[View Content](#)

Copyright © 2024 IT 7993 Project 4

Plan & Design the OCDS Company & Project Website (3 of 3)

- DNS zone file
- Completed DNS configurations for both OCDS websites
 - <https://ocds.tech>
 - <https://project.ocds.tech>
- Start Of Authority
 - ns1.dunabr.net
 - hostmaster.dunabr.net
- Name Servers
 - ns1.dunabr.net
 - ns2.dunabr.net
 - ns3.dunbar.net
- Public IP
 - 38.110.15.77

```
cdunbar — ssh cdunbar@10.11.12.53 — 80x26
$TTL 300 ; Defines the default Time To Live in seconds
@      IN      SOA     ns1.dunbar.net. hostmaster.dunbar.net. (
                          2024020101
                          3600
                          3600
                          604800
                          3600 )
;
; Name Servers authoritative for this domain
;
;              IN NS      ns1.dunbar.net.
;              IN NS      ns2.dunbar.net.
;              IN NS      ns3.dunbar.net.
;
; Mail Servers
;
;              IN MX      10 mail-example.ocds.tech.
;
; Public Addresses
;
;              IN A       38.110.15.77
www      IN A       38.110.15.77
project  IN A       38.110.15.77
;
```

Plan & Design the OCDS Company IT Policies

- Researched various sites and companies for IT Policy concepts and ideas
- Researched specific policies for Company IT Policy List and narrowed down potential policies to use as OCDS IT Policies
- Completed initial design of OCDS IT Policies
- Converted design into a Word document for presentation and record keeping

The screenshot shows a Microsoft Word document titled "Cybersecurity Policies" in a read-only state. The document content is as follows:

Cybersecurity Policies

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 work 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.

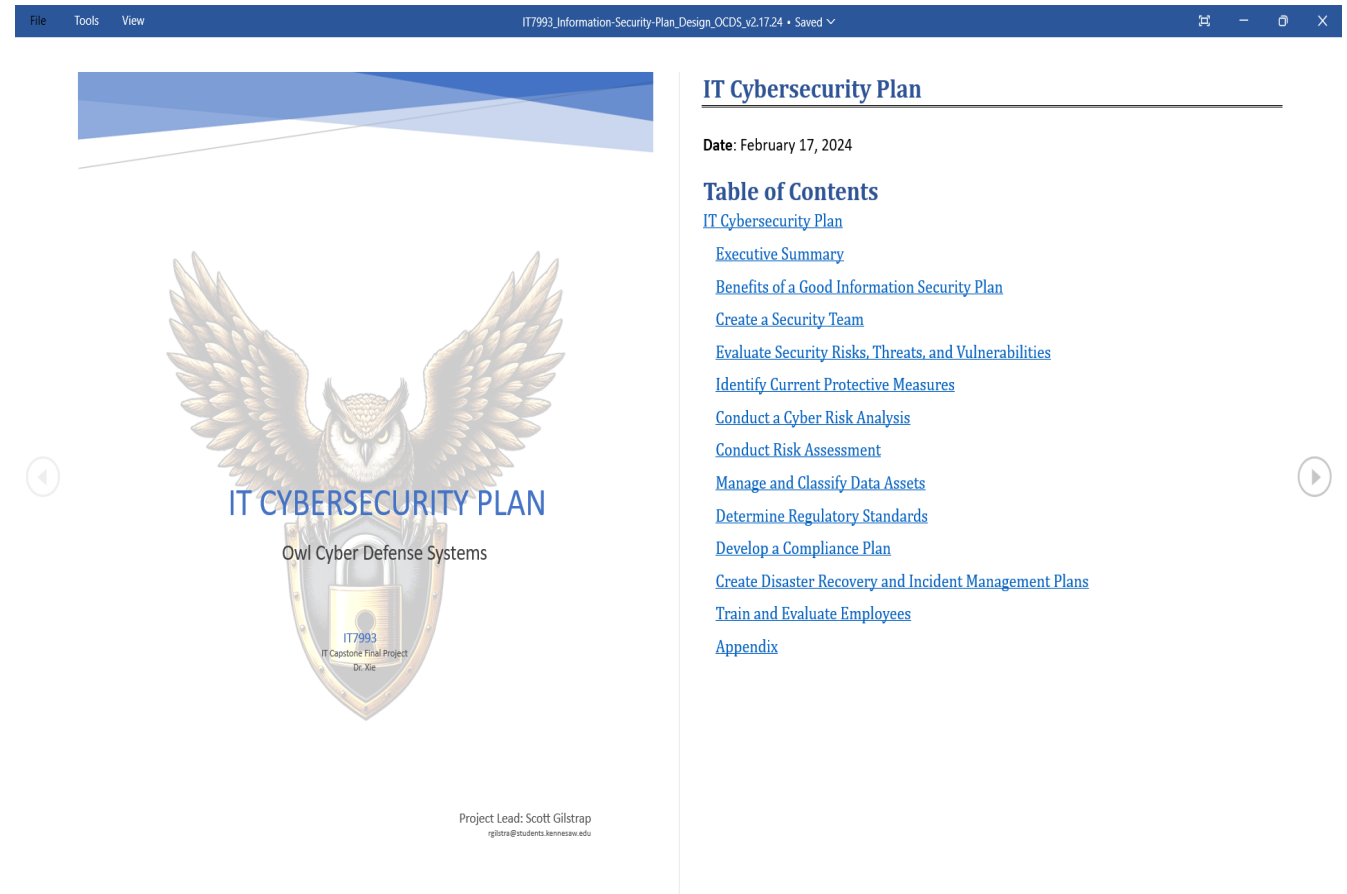
Consistently test run cybersecurity policy and IT security policy

- 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

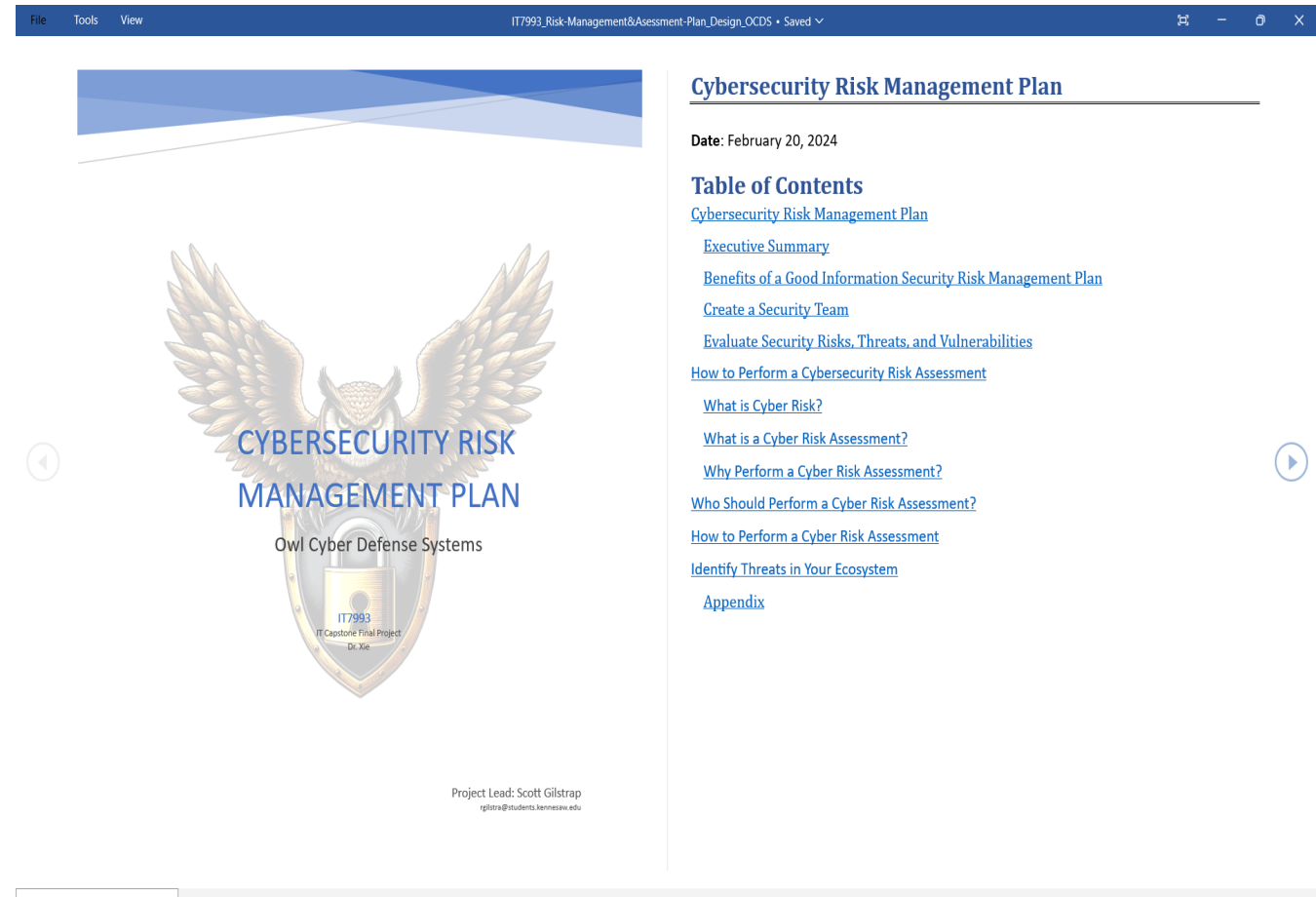
Plan & Design the IT Security Planning Client Offering

- Researched various aspects of an appropriate detailed IT Cybersecurity Plan
- Designed an initial concept of an IT Cybersecurity Plan
- Converted conceptional design into a client offering to establish a client's proprietary IT Cybersecurity Plan
- Prepared the design for conversion into a testable format
- Converted the design into a Word document for presentation and record keeping



Plan & Design the Risk Management Plan Client Offering

- Researched various aspects of an appropriate detailed Risk Assessment and Management Plan
- Designed an initial concept of a Risk Assessment and Management Plan
- Converted conceptional design into a client offering to establish a client's proprietary Risk Assessment and Management Plan
- Prepared the design for conversion into a testable format
- Converted the design into a Word document for presentation and record keeping



Plan & Design Cybersecurity Awareness Training Offering

- Research various sites and business for ideas to design an IT Cybersecurity Awareness Training curriculum and policies
- Established the employee cybersecurity resource list
- Completed early stages of Cybersecurity Awareness Training client offering
- Converted the Cybersecurity Awareness Training into a Word document showing Cybersecurity Polices for presentation and project record keeping

The screenshot shows a Microsoft Word document titled "Cybersecurity Policies". The document content is as follows:

Cybersecurity Policies

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

Plan & Design the AI-enable Server Client Offering (1 of 3)

- Researched the concept of AI coding
- Researched AI-enable data sets for the NIST 800-53 family
- Discovered multiple tools for AI Bot research
- NIST STIG server hardening research
- Researched identified tools, methods, & datasets to create & train AI chat bot
- Researched applicable types of AI applications
- Researched AI language models and implemented baseline dataset for AI learning
- Designed AI Chatbot based on JSON
- Researched AI on Language models and algorithms

```
1 import json
2
3 1 usage
4 def format_json(input_file, output_file):
5     try:
6         with open(input_file, 'r') as file:
7             input_data = json.load(file)
8
9             formatted_data = {"intents": []}
10
11             for item in input_data["intents"]:
12                 intent = {
13                     "tag": item["VulnID"],
14                     "patterns": [item["RuleID"], item["VulnID"], item["RuleTitle"]],
15                     "responses": [item["FixText"]]
16                 }
17                 formatted_data["intents"].append(intent)
18
19             with open(output_file, 'w') as output_file:
20                 formatted_json = json.dumps(formatted_data, indent=2)
21                 output_file.writelines(formatted_json)
22
23                 print("Conversion successful. Output written to", output_file)
24
25             except Exception as e:
26                 print("Error:", e)
27
28             # Replace 'input.json' and 'output.json' with the actual file names
29
30
31 format_json(input_file: 'rh8.json', output_file: 'rhel8.json')
```

Plan & Design the AI-enable Server Client Offering (2 of 3)

- Implement code to take dataset and learn
- Created Chatbot to answer questions based on learning
- Windows 10 dataset configuration completed
- Formatted dataset to be ingested by learning model
- Adjusted batch sizes & epochs for better accuracy results
- Created intents for AI training
- Worked patterns for better AI bot conversation accuracy
- Linux checklist in JSON format & added to training model

```
1 # LOAD PYTHON MODULE
2 from stig_parser import convert_stig, generate_stig_json
3
4
5 ## PARSE STIG ZIP FILE
6 # ASSUMES ZIP FILE IS IN CURRENT WORKING DIRECTORY
7 json_results = convert_stig('./U_RHEL_8_V1R13_STIG.zip')
8 generate_stig_json(json_results, EXPORT_FILE: './rh8.json')
```

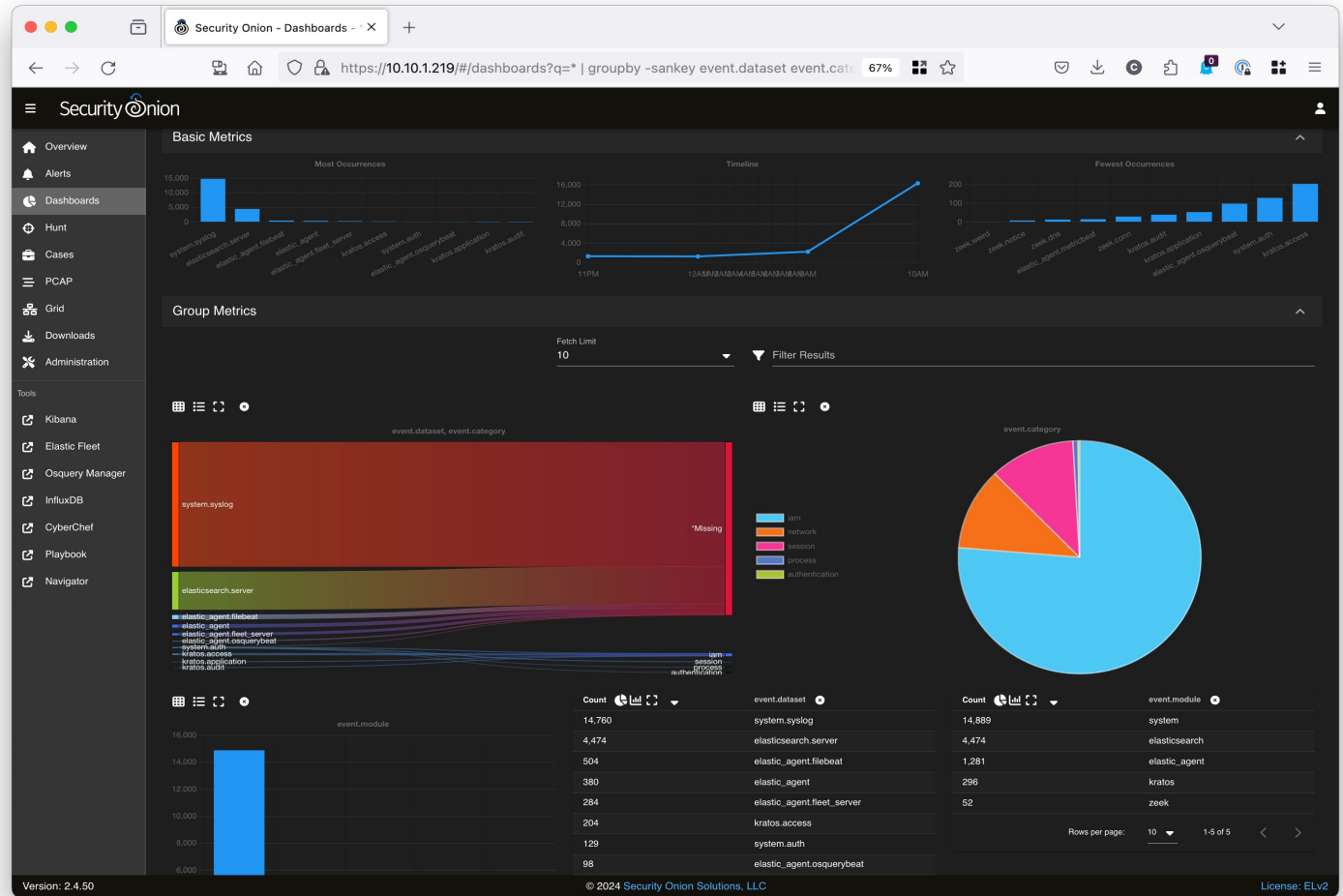
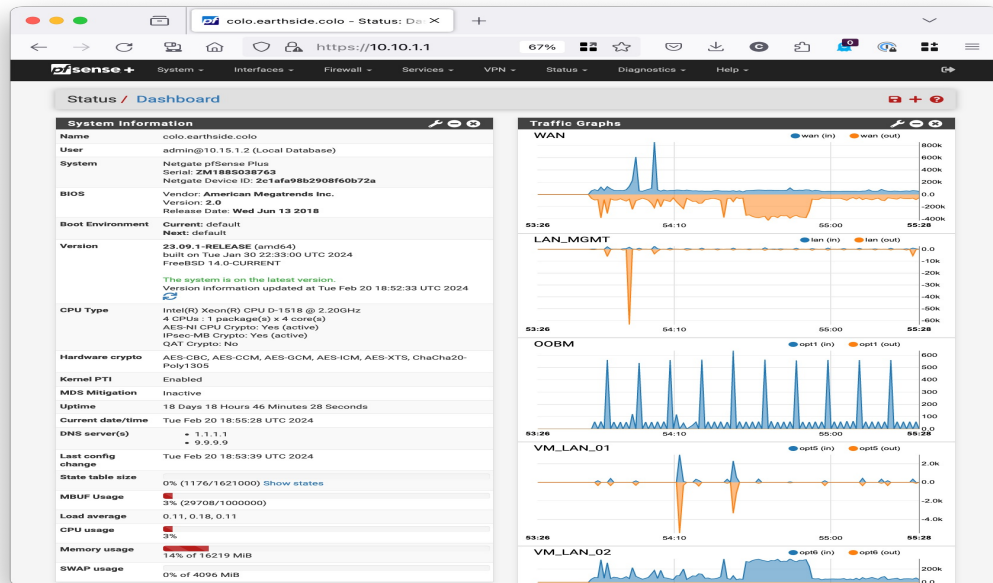
Plan & Design the AI-enable Server Client Offering (3 of 3)

```
Epoch 15061/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0077 - accuracy: 0.6881
Epoch 15062/30000
37/37 [=====] - 0s 4ms/step - loss: 0.9851 - accuracy: 0.6984
Epoch 15063/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0319 - accuracy: 0.6770
Epoch 15064/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0190 - accuracy: 0.6807
Epoch 15065/30000
37/37 [=====] - 0s 4ms/step - loss: 0.9936 - accuracy: 0.6826
Epoch 15066/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0224 - accuracy: 0.6704
Epoch 15067/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0307 - accuracy: 0.6783
Epoch 15068/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0319 - accuracy: 0.6713
Epoch 15069/30000
37/37 [=====] - 0s 4ms/step - loss: 0.9965 - accuracy: 0.6881
Epoch 15070/30000
37/37 [=====] - 0s 4ms/step - loss: 0.9852 - accuracy: 0.6861
Epoch 15071/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0075 - accuracy: 0.6826
Epoch 15072/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0117 - accuracy: 0.6840
Epoch 15073/30000
37/37 [=====] - 0s 4ms/step - loss: 0.9900 - accuracy: 0.6811
Epoch 15074/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0280 - accuracy: 0.6811
Epoch 15075/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0183 - accuracy: 0.6822
Epoch 15076/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0098 - accuracy: 0.6778
Epoch 15077/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0006 - accuracy: 0.6833
Epoch 15078/30000
37/37 [=====] - 0s 4ms/step - loss: 1.0034 - accuracy: 0.6907
Epoch 15079/30000
```

```
"responses": [
  "Configure the audit log to be protected from unauthorized read access, by setting the correct owner as \"root\" with the following command:\n\n$ sudo chown root:root /var/log/audit/audit.log"
],
},
{
  "tag": "V-230398",
  "patterns": [
    "SV-230398r627750_rule",
    "V-230398",
    "RHEL 8 audit logs must be group-owned by root to prevent unauthorized read access."
  ],
  "responses": [
    "Configure the audit log to be owned by root by configuring the log group in the /etc/audit/auditd.conf file:\n\nlog_group = root"
  ]
},
{
  "tag": "V-230399",
  "patterns": [
    "SV-230399r627750_rule",
    "V-230399",
    "RHEL 8 audit log directory must be owned by root to prevent unauthorized read access."
  ],
  "responses": [
    "Configure the audit log to be protected from unauthorized read access, by setting the correct owner as \"root\" with the following command:\n\n$ sudo chown root:root /var/log/audit/audit.log"
  ]
},
{
  "tag": "V-230400",
  "patterns": [
    "SV-230400r627750_rule",
    "V-230400",
    "RHEL 8 audit log directory must be group-owned by root to prevent unauthorized read access."
  ],
  "responses": [
    "Configure the audit log to be protected from unauthorized read access by setting the correct group-owner as \"root\" with the following command:\n\n$ sudo chown root:root /var/log/audit/audit.log"
  ]
}
```


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

- Researched open-source security packages to support our Zero Trust Security offerings
- Planned out an initial design for the OCDS Advanced Firewall, SIEM & Log Analyzer
- Security Onion SIEM dashboard (Elasticsearch)
- pfSense firewall dashboard



Sprint 1 Time Tracking

Sprint 1 Person-hour Time Tracking (Real-time Jira project export)

Person-hours — Edited Save Details

★ 📄 📄 📄 Share Export

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

Sprint: OCDS Sprint 1

1-50 of 54

Color

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

Sprint 0 Person-hour Time Tracking (Week 0)

- Scott Gilstrap
- Chris Dunbar

Sprint	OCDS Sprint 0		
Week of	21-27 Jan 24		
Sum of Time Spent Calc		Column Labels	
Row Labels	Chris Dunbar	Scott Gilstrap	Grand Total
Create Dependencies		4.0	4.0
Create Epics		6.0	6.0
Create Plan Document		5.0	5.0
Create Tasks		4.0	4.0
Generate Team Logo	2.0		2.0
Get Plan Document Approved by Team Members		1.5	1.5
Interview team members		1.5	1.5
Upload Project Plan Document		0.3	0.3
Grand Total	2.0	22.3	24.3

Sprint 1 Person-hour Time Tracking (Week 1)

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

Sum of Time Spent Calc		Column Labels					
Row Labels	Chris Dunbar	Justin Place	Ryan LeBlanc	Scott Gilstrap	Stephanie Aguirre	Grand Total	
Build-out Website Infrastructure	5.0					5.0	
Business Goals				1.5		1.5	
Business Strategy				1.0		1.0	
Configure firewall for public access to website	0.3					0.3	
Create DNS zone file	1.0					1.0	
Create employee education related to cybersecurity (i.e. cybersecurity resources)					3.4	3.4	
Create legal structure for business					2.5	2.5	
Designate List of Appropriate IT Policies					1.5	1.5	
IT SP Planning Based on Research				2.0		2.0	
IT Strategy				1.5		1.5	
Plan/Design Layout on Website	1.5					1.5	
Plan/Design Webpage	1.5					1.5	
Research AI Toolset		7.0	7.0			14.1	
Research IT Security Plan Methodologies				3.0		3.0	
Research/Create Cybersecurity Policies					3.0	3.0	
Research/Create list of IT Policies					3.2	3.2	
Grand Total	9.3	7.0	7.0	9.0	13.6	45.9	

Sprint 1 Person-hour Time Tracking (Week 2)

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

Sprint		OCDS Sprint 1				
Week of		04-10 Feb 24				
Sum of Time Spent Calc		Column Labels				
Row Labels	Chris Dunbar	Justin Place	Ryan LeBlanc	Scott Gilstrap	Stephanie Aguirre	Grand Total
Conduct OCDS Planning Based on Reseach				2.5		2.5
Design Data Configuration		2.0	1.0			3.0
Design Dataset Configuration		3.0	1.5			4.5
Design OCDS IT SP Product Offering Documentation				2.0		2.0
Design Offerings Cost Model				2.0		2.0
Design Product Offering Catalogue				2.0		2.0
Design the Company Business Model				2.0		2.0
Design/Create Cybersecurity Awareness Training					4.8	4.8
Establish Target Market				1.0		1.0
Incorporate IT Policy Design into Business Plan Design					1.0	1.0
Install and configure web server packages	2.0					2.0
Install server certificate with Let's Encrypt	1.0					1.0
IT Goals				1.0		1.0
List certifications and/or skill set needed					1.4	1.4
Plan Data Configuration		3.0	1.5			4.5
Plan Dataset Configuration		4.0				4.0
Poll team on website requirements	1.5					1.5
Research datasets		3.5	3.5			7.0
Research IT Risk Management Planning				3.0		3.0
Research NIST 800-53 Family Standards			4.5			4.5
Select and deploy website template	1.0					1.0
Grand Total	5.5	15.5	12.0	15.5	7.2	55.7

Sprint 1 Person-hour Time Tracking (Week 3)

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

Sprint		OCDS Sprint 1				
Week of		11-17 Feb 24				
Sum of Time Spent Calc	Column Labels					
Row Labels	Chris Dunbar	Justin Place	Ryan LeBlanc	Scott Gilstrap	Stephanie Aguirre	Grand Total
Complete Design of Cybersecurity Awareness Training					3.0	3.0
Create site contents/folders	3.0					3.0
Design AI Training		4.0				4.0
Design OCDS IT Risk Mgmt Product Offering				3.5		3.5
Plan & Design Product Offering: Advanced Firewall, SIEM, & Log Analyzer	1.0					1.0
Plan & Design Product Offering: Cyber Awareness Training					2.0	2.0
Plan & Design Product Offering: Risk Management Planning				0.0		0.0
Plan & Design the OCDS Company Website	3.6					3.6
Plan AI Training		4.2				4.2
Plan, Design & Publish Project Website	3.6					3.6
Provide Requirements Document				1.5		1.5
Research AI Toolset			4.2			4.2
Verify Infrastructure Build Out	2.0					2.0
Verify Initial Business Plan Design is Complete				1.0		1.0
Verify Initial Policy List is Complete					1.0	1.0
Verify Planning & Design of all Client Offerings are Complete				1.0		1.0
Plan & Design Dataset Accuracy Improvement			4.0			4.0
Grand Total	13.2	8.2	8.2	7.0	6.0	42.6

Sprint 1 Person-hour Time Tracking (Week 4)

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

Sum of Time Spent Calc		Column Labels					
Row Labels	Chris Dunbar	Justin Place	Ryan LeBlanc	Scott Gilstrap	Stephanie Aguirre	Grand Total	
Complete Development of Curriculum					3.0	3.0	
Complete IT Policy List					3.6	3.6	
Complete Milestone 1 Report Documentation				5.0		5.0	
Create required sections and pages	2.5					2.5	
Milestone 1: Planning & Designs Complete				3.0		3.0	
Upload Milestone 1 Report Documentation				0.0		0.0	
Implement AI Toolset		5.0				5.0	
Implement Dataset Accuracy Improvement		5.0				5.0	
Implement AI Training			8.0			8.0	
Publish site contents/folders	3.0					3.0	
Publish draft site/go live	3.6					3.6	
Grand Total	9.1	10.0	8.0	8.0	6.6	41.7	

Sprint 1 Person-hour Time Tracking (Team Totals)

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

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

Recap/Review

Sprint 1 Project Experience

- **Accomplishments**

- Established a good, robust Jira project model
- Overcoming multiple scheduling conflicts to complete tasks on time
- Learn HTML generator tool & technical VM configurations for website as well SIEM infosec security offerings
- Built a JSON training data-based Python AI ChatBot

- **Challenges**

- Meeting consistently as a team when all members have full time jobs but this team did it well
- Creating design for the cyber awareness training
- The Hugo tool was more involved than originally estimated & required a lot of time investment to learn
- Establishing an appropriate work/school/life balance
- Python code was complex & accomplishing better accuracy was difficult but eventually accomplished

- **Lessons Learned**

- Concentrate on better time management between Capstone and work tasks
- Hugo (static HTML generator) is very robust and complicated
- Consistent communications via MS Teams can produce good daily/weekly Scrum input

- **Opportunities for Improvement**

- Better time management in order to complete tasks with less stress
- Spend a little more time on website folder & content to make for a better website presentation of client offerings

Milestone 1

Goals & Objectives

Sprint 1
Jan 25 – Feb 25, 2024

- Plan & Design the OCDS Business Plan
- Build-out Website Infrastructure
- Plan & Design the OCDS Company Website
- Plan, Design & Publish draft of Project Website
- Plan & Design the OCDS IT Policies
- Plan & Design the IT Security Planning Client Offering
- Plan & Design the Risk Management Planning Client Offering
- Plan & Design the Cyber Awareness Training Client Offering
- Plan & Design the AI-enabled Server Hardening Client Offering
- Plan & Design the Advanced Firewall, SIEM, & Log Analysis Client Offering

Next Phase: Sprint 2

Milestone 2

Goals & Objectives

Sprint 2
Feb 26 – Mar 24, 2024

- Sprint 1 Review & Retrospective and
- Sprint 2 Planning Meeting scheduled for February 25, 2024
- Sprint 2 Potential Goals & Objectives
 - Complete & Publish Business Plan
 - Complete & Publish IT Policies
 - Publish Websites
 - Develop & Test Client Offerings
 - Cyber Awareness Training Curriculum
 - IT Security Planning
 - Risk Management & Assessment
 - AI-enable Server Hardening Tool
 - Adv F/W, SIEM, & Log Analyzer

The background of the slide is a repeating geometric pattern of interlocking shapes in various shades of yellow and gold. The pattern is symmetrical and creates a sense of depth and movement. A solid black horizontal band runs across the middle of the slide, providing a high-contrast background for the text.

Thank You!