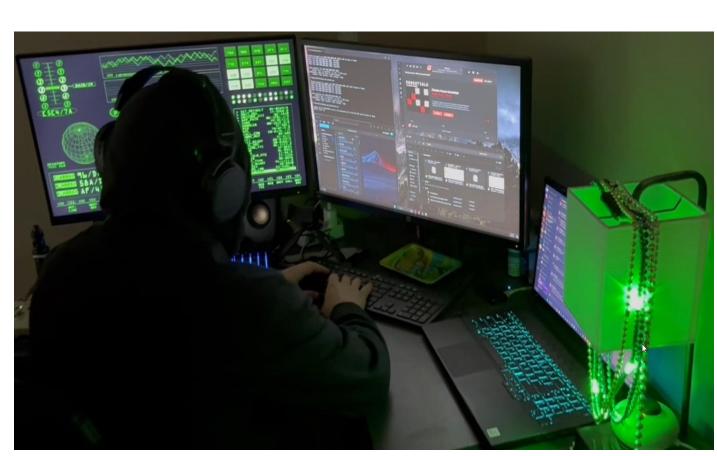
**GC-84** 

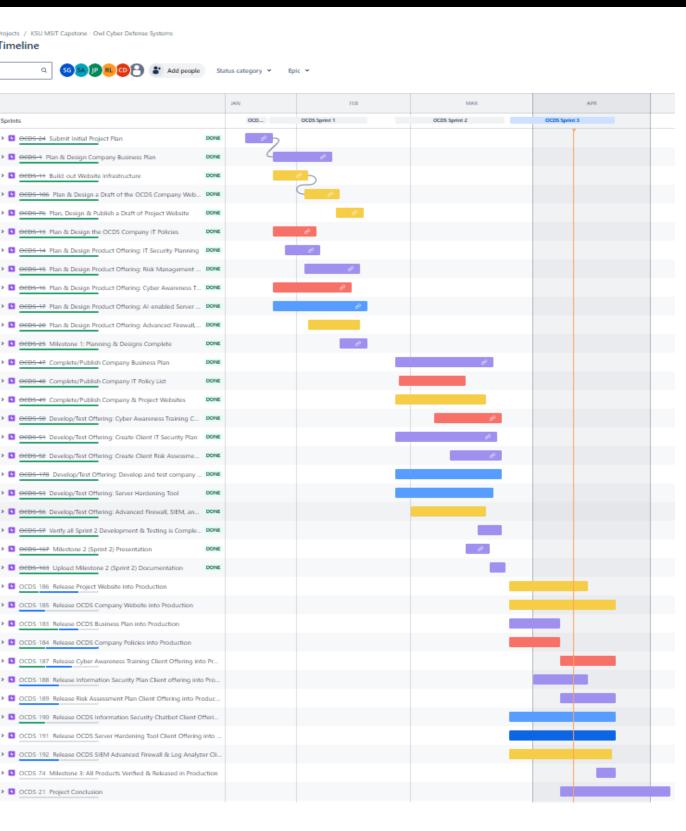
## Introduction

Half of all cyber breaches impact small businesses (SMBs) with less than 1,000 employees. 61% of SMBs were the target of a cyberattack in 2023. Most SMBs do not have an adequate cybersecurity posture due to insufficient education and funding. As cybercriminals increasingly target smaller companies, it's crucial SMBs take proactive measures to protect



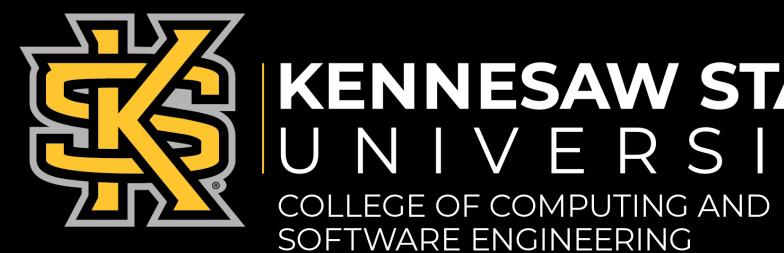
sensitive data and systems. This project addresses this need by chronicling the startup and tool development of a cybersecurity firm offering affordable security assessments, employee cyber awareness training, an AI-enabled hardening tool in association with an OCDS AI chatbot, as well as deployment of a SIEM tool for firewall and log analysis assisting small businesses with protecting their assets at an affordable cost.

- Strategic Goal: Establish the OCDS cybersecurity business providing SMBs cost effective tools to increase their cybersecurity protection posture
- **Operational Goals:** Build Project & Company Websites, Business Plan, and Client Offerings: 1) IT Security Planning & Risk Assessment, 2) Cyber Awareness Training, 3) Alenabled Server Hardening Tool, 4) AI Security Chatbot, & 5) SIEM tool
- Sprint 1 Plan & Design
- Sprint 2 Development & Testing
- Sprint 3 Production Deployment



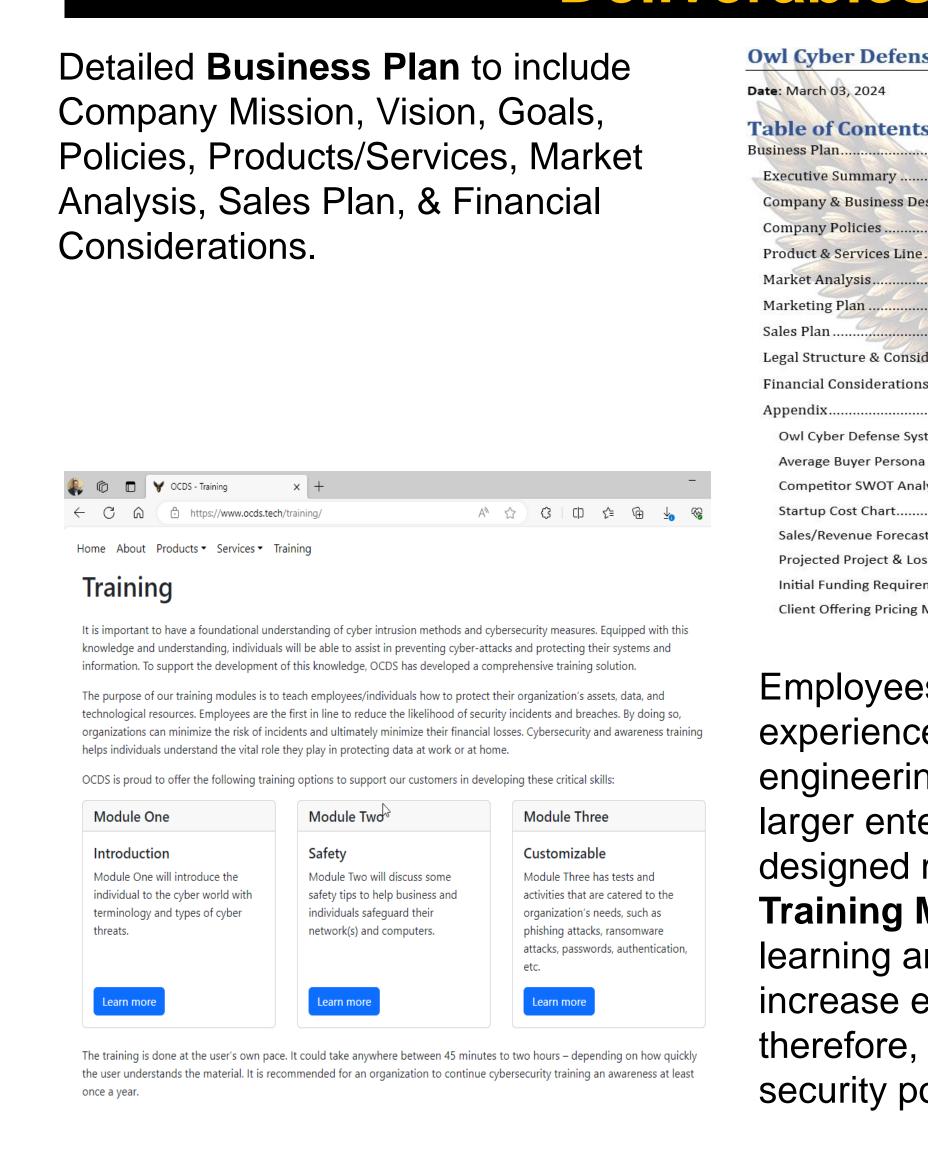
### Tools, Technology & Methods

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

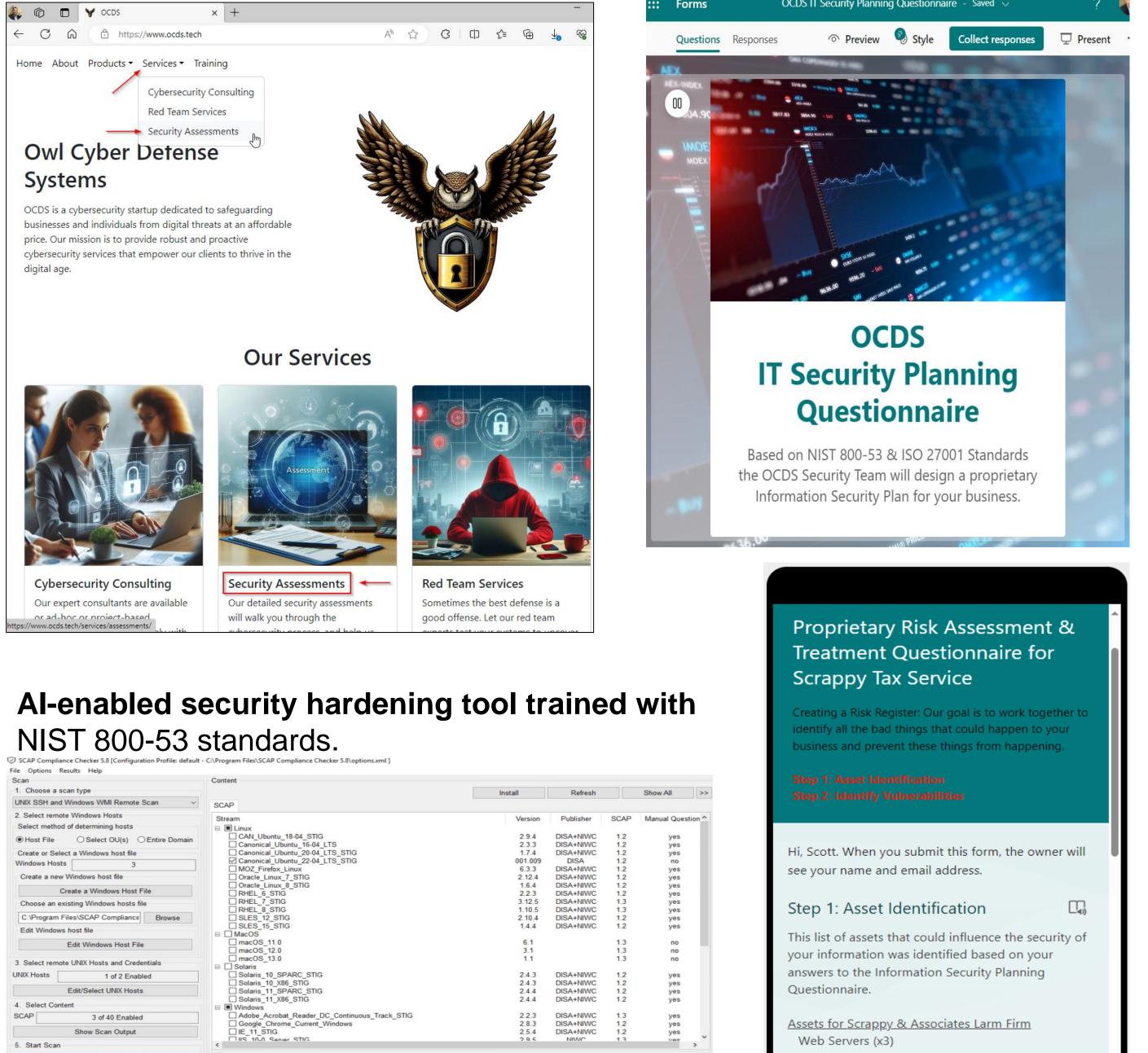




# **OWL CYBER DEFENSE SYSTEMS [OCDS]**

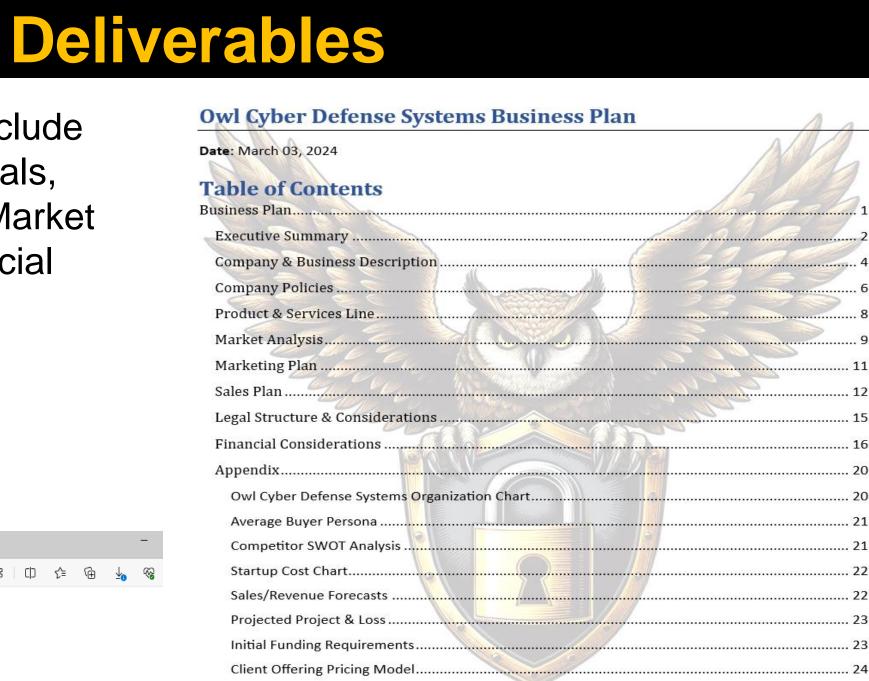


**Security Assessments:** The IT Security Planning Questionnaire collects client feedback. OCDS creates a client **IT Security Plan**. With a completed IT Security Plan, a proprietary **Risk Assessment & Treatment Plan** is created.



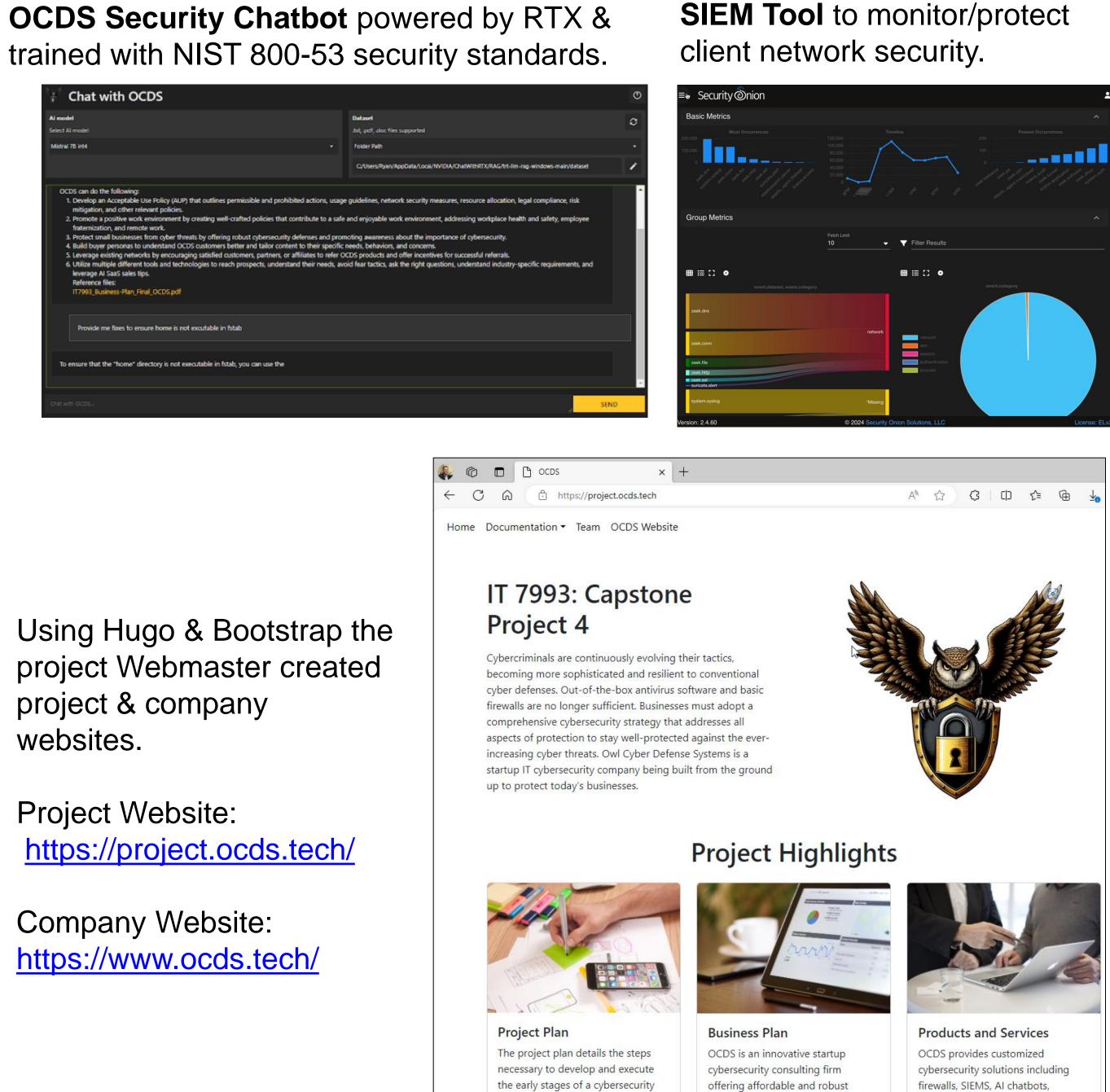
Scan		Content							
1. Choose a scan	type				Install	Refresh		Show All	>>
UNIX SSH and Wi	ndows WMI Remote Scan ~	SCAP							
2. Select remote \	Vindows Hosts	Stream			Version	Publisher	SCAP	Manual Que	stion ^
Select method of determining hosts					Version	1 donorici	00/4	Manual Que.	Stion
		CAN_Ubuntu_18	-04 STIG		2.9.4	DISA+NIWC	1.2	yes	
Host File O Select OU(s) O Entire Domain		Canonical Ubunt			2.3.3	DISA+NIWC	1.2	yes	
Create or Select	a Windows host file	Canonical_Ubuntu_20-04_LTS_STIG			1.7.4	DISA+NIWC	1.2	yes	
Windows Hosts	3	Canonical_Ubunt			001.009	DISA	1.2	no	
Country of Mandeum hand file		MOZ_Firefox_Lin			6.3.3	DISA+NIWC	1.2	yes	
Create a new Windows host file		Oracle_Linux_7_			2.12.4	DISA+NIWC	1.2	yes	
Create a Windows Host File		Oracle_Linux_8_	SIIG		1.6.4	DISA+NIWC DISA+NIWC	1.2	yes	
Observe an anisting Mindaux basets file		RHEL 7 STIG			3.12.5	DISA+NIWC	1.2	yes yes	
Choose an existing Windows hosts file		RHEL 8 STIG			1.10.5	DISA+NIWC	1.3	yes	
C:\Program Files\SCAP Compliance Browse		SLES 12 STIG			2.10.4	DISA+NIWC	1.2	yes	
Edit Windows host file		SLES 15 STIG			1.4.4	DISA+NIWC	1.2	yes	
Edit Windows ho	ost file	🖂 🗌 MacOS							
Edit Windows Host File		macOS_11.0			6.1		1.3	no	
		macOS_12.0			3.1		1.3	no	
3. Select remote UNIX Hosts and Credentials		macOS_13.0			1.1		1.3	no	
UNIX Hosts 1 of 2 Enabled		□ Solaris □ Solaris_10_SPARC_STIG □ Solaris 10_X86_STIG			2.4.3	DISA+NIWC	1.2		
Edit/Select UNIX Hosts					2.4.3	DISA+NIWC	1.2	yes yes	
		Solaris_11_SPARC_STIG			2.4.4	DISA+NIWC	1.2	yes	
		Solaris 11 X86			2.4.4	DISA+NIWC	1.2	yes	
<ol><li>Select Content</li></ol>		Windows						-	
SCAP 3 of 40 Enabled Show Scan Output 5. Start Scan			Reader_DC_Continuous_Track_STI	G	2.2.3	DISA+NIWC	1.3	yes	
		Google_Chrome	Current_Windows		2.8.3	DISA+NIWC	1.2	yes	
		IE_11_STIG			2.5.4	DISA+NIWC	1.2	yes	
		TIS 10.0 Sonior STIG			295	NINA/C	13	VAC	>
	Start Scan	Computer Status	Stream Status	Current Stream					
	6	1							
View Results		Log							
Total Sessions	24								
lew Sessions	- Chaine		CAP 1.2 content streams from: C:\F AL content files from C:\Program Fi						
vew Sessions	15		L content files from C:\Program Fil						
	View Results	17:54:51: Content verifical		one of a compliance on					
		17:55:01: Validating 'U_C/ 17:55:01: XML schema va	tion of C:\Users\ocds\Desktop\U_C AN_Ubuntu_22-04_LTS_V1R9_STK Ilidation successful for:U_CAN_Ubu stalled: Canonical_Ubuntu_22-04_L	G_SCAP_1-2_Benchmark intu_22-04_LTS_V1R9_S1	xml'		k (1)\U_CA	N_Ubuntu_22-	04_LTS
		17:55:03: Checking for ne 17:55:03: Checking 0 SC	w/modified content, please wait						

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



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

> Application Servers (x3 Database Servers (x3) Network Cabling (Fiber & Ethernet)



project & company websites.

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

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

# **Contact Information**

Team Lead | Project Manager | Scrum Master Lead Instructor | Technical Writer Senior Systems Engineer | Webmaster Information Systems Engineer | AI Developer Research Technologist | Infrastructure Architect IT Capstone Professor | Mentor | Project Advisor

Home. (n.d.). Scrum.org. https://www.scrum.org/ https://www.agilealliance.org/agile101/ https://blogs.nvidia.com/blog/chat-with-rtx-available-now/ (n.d.). https://stigviewer.com/stig/microsoft\_windows\_10/2023-09-29/ https://gohugo.io/

https://doi.org/10.6028/nist.sp.800-53r5 ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001



consulting, and training tailored to individual customer requirements and circumstances

Scott Gilstrap: rgilstra@students.kennesaw.edu | https://www.linkedin.com/in/randolph-scott-gilstrap-00144b21/

roducts and services to protect

ousinesses and individuals from

igital threat

- Stephanie Acquire: saguirr5@students.kennesaw.edu | https://www.linkedin.com/in/stephanie-a-b7336b262/
- Chris Dunbar: cdunbar@students.kennesaw.edu | https://www.linkedin.com/in/chdunbar/

consulting business while fulfilling

the requirements of the IT 7993

- Ryan LeBlanc: rleblanc@students.kennesaw.edu | https://www.linkedin.com/in/ryan-leblanc1/
- Justin Place: jplace2@students.kennesaw.edu | https://www.linkedin.com/in/j-98b303142/
- Dr. Jing Xie: <u>yxie2@kennesaw.edu</u> | <u>https://www.linkedin.com/in/ying-xie-96231367/</u>

### References

- Agile Alliance. (2024, April 12). What is Agile? | Agile 101 | Agile Alliance. Agile Alliance |
- Clayton, J. (2024, March 5). Chat with RTX now free to download. NVIDIA Blog.
- Microsoft Windows 10 security technical implementation guide. STIG Viewer | Unified Compliance Framework®.
- Hogan, B. P. (2020). Build websites with Hugo fast web development with Markdown. The Pragmatic Bookshelf. Hugo. (n.d.). The World's Fastest Framework for Building Websites. Retrieved April 11, 2024, from
- Otto, M., & Thornton, J. (n.d.). Bootstrap. Bootstrap. Retrieved April 11, 2024, from https://getbootstrap.com/ Force, J. T. (2020). Security and privacy controls for information systems and organizations.
- National Institute of Standards and Technology. (2018). Framework for improving Critical Infrastructure Cybersecurity. In NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Institute of Standards and Technology. (2012). Guide for conducting risk assessments. In NIST Special Publication 800-30 (p. 95 pages). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf