




Taegan Williams

 taeganw@gmail.com
 taeganw
 taeganw.github.io

OBJECTIVE:

Motivated cybersecurity expert seeking a career in development and research that offers personal growth through challenges in a collaborative learning environment.

EDUCATION:

University of Idaho, Moscow

July 2017 – December 2022

- Master of Cybersecurity
- Bachelor of Computer Science
- Minor in Mathematics and Business
- Entrepreneurship, Cybersecurity, and Critical Infrastructure and Resilience Graduate Certificate

SANS Technology Institute

September 2019 – August 2020

- Undergraduate Certificate in Applied Cybersecurity
- GIAC Foundational Cybersecurity Technologies (2021)
- GIAC Security Essentials Certification (2020)
- GIAC Certified Incident Handler (2020)
- GIAC Certified Forensic Analyst (2020)

ACHIEVEMENTS:

- US DOE Secretary's Honor Award for identifying cybersecurity risk and mitigations in U.S. Infrastructure 2024
- Recognition of Accomplishment from IN-40 director for improving mitigations against U.S. Infrastructure 2024
- Initiated Research towards the automation and support of *Cyber Threat Intelligence Hypothesis Generation* 2024
- Presented "Improving Communication with a Tiered Risk Mitigation Framework" at Idaho Falls B-Sides 2022

CLASSES:

Computer Science:

Python for Machine Learning, Compiler Design, Analysis of Algorithms, Software Engineering, Theory of Computation, Probability and Statistics

Cybersecurity:

Cyber Informed Engineering, Advanced Forensics & Malware Analysis, Applied Security Concepts, Computer and Network Forensics, Advanced Network Security, Cryptography, Information Assurance, Critical Infrastructure Security and Resilience Fundamentals

PROFICIENCIES:

Programming Languages:

Lua, Spicy, C, C++, C#, Python, SQL, HTML5, CSS, PHP

Specializations and Services:

Electric Power, Reverse Engineering, Splunk, Git, MySQL, Cisco, Ansible, Terraform, Vagrant, Docker, AWS, MITRE Stix, Zeek, Malcom

Cybersecurity:

ICS, Protocol Analysis, Linux & Windows Security, Defensible Network Architecture, Vulnerability Assessment, Incident Handling and Response, Computer and Network Exploits, Hacker Tools, Imaging and Forensics

PREVIOUS EMPLOYMENT:



Idaho National Laboratory, Idaho Falls

Critical Infrastructure Cyber Protection & Defense Analyst

July 2021 to June 2025

40 hrs. / week

- Researched and identified vulnerabilities in industrial control system equipment and protocols to develop mitigations and protections for open-source tools used by threat hunters and analyst.

University of Idaho, Idaho Falls

Graduate Research Assistant

August 2021 to December 2022

40 hrs. / week

- I administered the purchase and configuration of on-site cloud infrastructure for a cybersecurity lab with complete visibility into exercises via open-source and educationally available software.

My Site Marketing, Coeur d'Alene


Project Manager

July 2020 to May 2022

20 hrs. / week

- Responsible for day-to-day management and development of web design, front-end/back changes, graphic design, site launches, and search engine optimization.



 taeganw@gmail.com

 **LinkedIn:** taeganw

 **taeganw.github.io**



Taegan Williams



taeganw@gmail.com



taeganw



taeganw.github.io

PAPERS:

Masters - Networked Cybersecurity Exercises: Resilient ICS Gamification using Containerization (2021-2022)

<https://doi.org/10.53735/cisse.v10i1.167>

The United States needs more resources for students to learn cybersecurity principles around industrial control systems. Through the gamification of operations networks, the PicoCTF 2019 framework and Docker, students can traverse the Purdue Enterprise Architecture and complete challenges to take control of physical processes.

CISSE - RADICL CTF - Platform for Industrial Control System Education (2022)

<https://doi.org/10.53735/cisse.v10i1.159>

Post-secondary institutions can use gamification to increase student interest. RADICL CTF provides post-secondary institutions with new opportunities for low-cost, guided industrial control system education exercises to help students master adversarial thinking. RADICL CTF is a platform for students to design, implement and evaluate exercises that test their understanding of core concepts, answering the need for more interactive education methods.

RACER: Resilient Ansible Cyber Education Range (2021)

<https://github.com/taeganw/RACER>

A resilient cyber range for students to practice creating a dynamic defense-in-depth network leverages multiple systems and software to create a realistic learning environment. RACER provides total visibility through services for inventory management, state monitoring, event monitoring, and incident management outside of the environment's scope to ensure the lab's productivity and its exercises. This ansible script sets up open-source software such as Nagios, Trac, Wazuh, Suricata, and RT-IR.

PROJECTS:

Cyber Threat Intelligence Hypothesis Generation (2024)

Through research on strategies for rapid response and limited time on target threat hunting, this project aimed to improve traditional strategies by identifying the relationship between incident context, collected CTI, and existing frameworks to inform novel hypothesis generation strategies for threat hunters.

RADICL Cyber Range (2022)

The Idaho Falls RADICL Lab aims to provide a resilient cyber range for students to practice defense in depth networks. I configured the cloud infrastructure to facilitate students' interaction for red, blue exercises. I designed and implemented a network security plan for layer 2 and layer 3 segmentation. This project taught me key switching and routing protocols, chassis and power management, service monitoring, and interaction with Cisco products.

Capstone Project - Satellite Attitude Determination, Communication, and Control with AI (2020-2021)

http://mindworks.shoutwiki.com/wiki/Satellite_Atitude_Determination,_Communication,_and_Control_with_AI

Commercial CubeSats miniature satellites are expensive, but individual components are less so. This project will reduce costs by integrating commercially available orientation control and communication systems. I developed the ground server to receive Short Burst Data (SBD) and RUDICS communication from our cube satellite.

Collegiate Cyber Defense Club Guidebook (2021)

Wrote and compiled a reference guide with step-by-step security solutions for Windows, Ubuntu, and Centos operating systems. This guide also includes setup and security for business services such as database, SSH, Active Directory, email, website, and firewall). Used to help support our team within the Collegiate Cyber Defense Competition.

Personal Rack Server (2021-current)

I evaluate security and automation solutions on a rack-mounted server that runs a type one hypervisor. I have connected a Ubiquiti Dream Machine Pro router and set up services such as L2TP VPN with RADIUS, Ant Radio, Nagios, Kasm Workspaces, Pfsense, and Security Onion.



taeganw@gmail.com



LinkedIn: taeganw



taeganw.github.io

