Progress Report for IGEM 22-001

The Cyberdome — An Investment in Idaho's Cybersecurity Future

1st July 2021 – 30th June 2022

Year One Full-year Progress Report

BOISE STATE UNIVERSITY

IGEM 22-001

The Cyberdome — An Investment in Idaho's Cybersecurity Future

1st July 2021 – 30th June 2022, Year One Full-year Progress Report

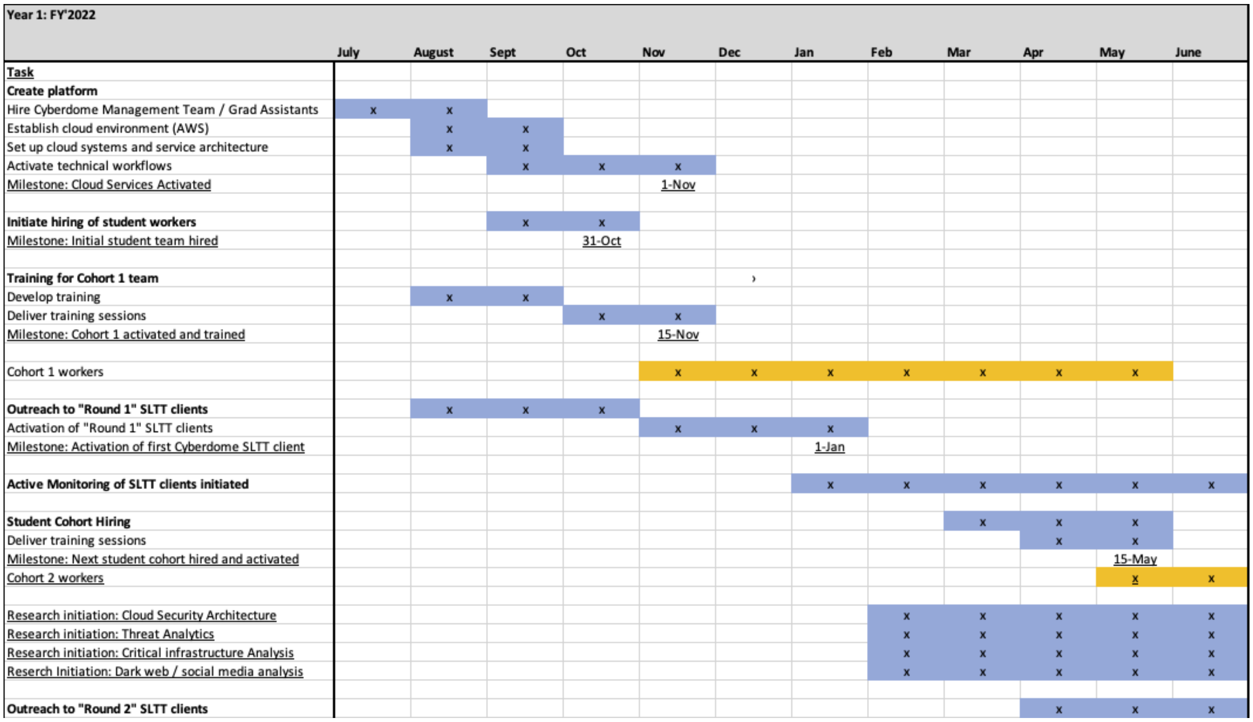
Table of Contents

IGEM 22-01: The Cyberdome –
An Investment in Idaho's Cybersecurity Future
1st July 2021 – 30th June 2022, Year One Full-year Progress Report

Project Summary

The Idaho Global Entrepreneurial Mission (IGEM) and State Board of Education Higher Education Research Council (HERC) have provided the first year of funding to the Institute for Pervasive Cybersecurity (IPC) at Boise State University to build and establish the **Cyberdome** – a Security as a Service (SECaaS) oriented platform meant to leverage force-multiplying efforts of our students to secure critical cyber/physical assets of rural and remote clients.

The IPC is pleased to inform HERC that the project continues on track and within budget against the timeline below. **Figure 1** below shows the relevant view of the timeline provided during award discussions. This has been used to track our progress towards success.



Year 1: FY'2022	July	August	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June
Task												
Create platform												
Hire Cyberdome Management Team / Grad Assistants	x	x										
Establish cloud environment (AWS)		x	x									
Set up cloud systems and service architecture		x	x									
Activate technical workflows			x	x	x							
Milestone: Cloud Services Activated					1-Nov							
Initiate hiring of student workers			x	x								
Milestone: Initial student team hired				31-Oct								
Training for Cohort 1 team						›						
Develop training		x	x									
Deliver training sessions				x	x							
Milestone: Cohort 1 activated and trained					15-Nov							
Cohort 1 workers					x	x	x	x	x	x	x	
Outreach to "Round 1" SLTT clients		x	x	x								
Activation of "Round 1" SLTT clients					x	x	x					
Milestone: Activation of first Cyberdome SLTT client							1-Jan					
Active Monitoring of SLTT clients initiated							x	x	x	x	x	x
Student Cohort Hiring									x	x	x	
Deliver training sessions										x	x	
Milestone: Next student cohort hired and activated											15-May	
Cohort 2 workers											x	x
Research initiation: Cloud Security Architecture								x	x	x	x	x
Research initiation: Threat Analytics								x	x	x	x	x
Research initiation: Critical infrastructure Analysis								x	x	x	x	x
Reserch Initiation: Dark web / social media analysis								x	x	x	x	x
Outreach to "Round 2" SLTT clients										x	x	x

Figure 1. July to June view of Cyberdome timeline

This progress report summarizes the activities during the project's first twelve (12) months. Please note: Objective #1 from our proposal continued to be the primary focus this first full-year period. The other objectives will be balanced in future reporting periods now that the platform is built, operational, and has the expected number of clients per our goals.

Project Accomplishments

The Cyberdome proposal identified three primary objectives:

1. ***Create competency-based learning platforms for Idaho cybersecurity learners***
2. ***Reduce critical cybersecurity risks for State, Local, Tribal, and Territorial (SLTT) clients***
3. ***Produce innovative research, tools, and techniques to transfer to commercial efforts***

Progress to date toward implementing these strategies is detailed in the following subsections.

Objective One: Create competency-based learning platforms for Idaho cybersecurity learners

Following receipt of funding in July 2021, the IPC successfully hired its two full-time staff members in August and September, respectively. Each team member comes with over a decade of technology industry experience, enabling each to provide direct mentorship to our undergraduate students & graduate assistants assigned to building the platform. Further, three (3) graduate assistants were enabled in the August and September timeframe. The delayed hiring/enablement of these staff members and graduate assistants did not impact the overall activation timeline.

Undergraduate student hiring has been ongoing against the general timeline provided above as well. A more concise hiring timeline across all roles is provided below in **Figure 2**.

Job Title	August 2021	September 2021	October 2021	November 2021	December 2021	February 2022	March 2022	May 2022	Grand Total
Analyst	1		4	1	2	8	2	7	25
Cyberdome Mgr		1							1
Engineer	2	2	1			4		2	11
Graduate Asst	3							1	4
Lead Analyst								1	1
Lead Engineer	1								1
Total	**7**	**3**	**5**	**1**	**2**	**12**	**2**	**11**	**43**

Figure 2. Hiring timeline by month over the reporting period

Recruiting, Hiring, and Training Processes

General Recruitment

Via the statewide cybersecurity program, the Cyberdome staff leveraged peer contacts throughout Idaho and worked to build connections to bolster recruitment and hiring efforts for Analysts and Engineers. A goal of the team continues to be enabling students from all eight public higher education institutions across Idaho to participate. As shown in **Figure 1**, the team's grant proposal timeline suggested the Institute would hire a full cohort of 14 interns and have them trained and ready to activate by mid-November. Throughout this period, the Cyberdome team faced several unexpected challenges that impacted the ability to recruit and fill these roles:

- The initial assumption that leadership would be able to find a Manager to lead the platform recruiting and training efforts by July 2021 was not met. Instead, the Cyberdome Manager started in early September 2021, which effectively pushed back the platform's development timeline by a full two months.
- The initial budget proposed each student would be hired at a wage of $12.50 per hour. The Cyberdome leadership team had very little success recruiting at this wage rate due to inflationary market impacts that started in 2021 and have continued since. Feedback from staff and faculty of academic programs indicated that the job market and inflation had rapidly increased the rate interns could command. One Computer Science program staff member commented that their program now pays even their most inexperienced interns $14.00 per hour. This proved to be true as a super-majority of early Cyberdome internship applicants were in their sophomore and junior years with limited knowledge developed through coursework or work experience.
- It took the Cyberdome team time to build connections with staff and faculty outside Boise State University to enable internship marketing and outreach efforts. This effort continues as other institutions face staff/instructor turnover.
- The team discovered a "direct pathway" challenge between four-year institution students vs students choosing a pathway from a community college. "Direct pathway" students have a significant gap in applied areas of technical knowledge. In particular, "direct pathway" students have not been equipped with the skillset of a strong foundation in TCP/IP networking. Such a foundation is critical to success as an early-stage Cybersecurity Engineer or Analyst. A critical lack of appropriate networking curriculum at four-year institutions impacts student success as operational cybersecurity professionals. In April 2022, the Cyberdome's most recent round of Analyst recruiting, only 30% (six out of twenty students) of "direct pathway" students from four-year institutions demonstrated the networking skill sets needed to merit a 2nd interview opportunity. This curriculum gap is one to be addressed via the statewide cybersecurity curriculum development efforts.

As a result of these challenges, the team hired and trained ten student interns before the expected start of Cohort 1 in mid-November. The profile of all interns hired to date is different than initially anticipated. The Cyberdome team anticipated hiring students who were in their final year of their associate's or bachelor's degree and wanted a capstone experience before graduation. Instead, many early hires were juniors and even first-year graduate students searching for internships they could engage with early in their studies. As a result, comprehensive post-internship hiring metrics are not yet available. Two interns in the first cohort were in/near their final semesters and have reported being hired at well above average market salary levels. The first intern was a BS graduate of Boise State's computer science program and was involved in the development of our virtual city portal. The student was hired in the local market as a programmer at a base salary of $105,000. The second intern graduated a semester after completing their Cyberdome internship with a BS in computer science w/cybersecurity emphasis. They were subsequently hired in the local market by an international company into a security engineer role at a base salary of $100,000.

Additionally, starting in February 2022, Cyberdome staff made the decision that they must increase student wages to attract students with a class standing and depth of knowledge commensurate with initial expectations. Analysts now earn $15.25 per hour and Engineer wages start at $16.00 per hour. This change made a meaningful difference as 96% of our current interns are expected to graduate within 12 months and 68% are within 7 months of graduating. This has also impacted our go-forward budgets and the expected number of Cyberdome graduates. At this point, barring any further inflationary pressures, the Cybedome team expects to reduce the number of supported students to 23 from the original 28 supported students in the grant proposal. Doing so will not require a budget impact to the original funding request. While the number of students per cohort will decrease, the anticipated ROI and economic impact is expected to remain the same. This is due to the base / premium salary increases occurring for entry-level cybersecurity roles.

The Cyberdome team has worked quickly to catch up on hiring and currently employs 25 interns including 16 Analysts and 9 Engineers. This includes active interns from six of Idaho's eight public higher education institutions with Boise State University, College of Eastern Idaho, College of Southern Idaho, College of Western Idaho, Idaho State University, and Lewis-Clark State College all represented. A graduate student from the University of Idaho is expected to join the program in August 2022.

Analyst Recruiting

July 2021 - December 2021

The Cyberdome team recruited eight Cybersecurity Analyst workers between August and December. This initial cohort completed initial assessments, and individualized training, and then provided significant feedback as to the quality and relevance of the training for future enhancements. Changes from this feedback were then incorporated into the training to provide a quality experience for subsequent cohorts.

The initial cohort of analyst interns was composed of students from the Boise metropolitan area as well as rural Idaho locations. Students were recruited from the Twin Falls and Lewiston/Clarkston areas, connecting remotely. The final composition of the cohort was five Boise-local students and three remote students. The cohort consisted solely of Boise State students.

January 2022 - June 2022

The second cohort of Cybersecurity Analysts was recruited through two waves of hiring. The first wave consists of ten analysts hired between February and March. The second wave was recruited in May and consists of seven analysts. One analyst from the February to March cohort was removed from the program after three weeks due to not showing up for shifts.

The Cyberdome team increased outreach to statewide public institutions other than the Boise area during this timeframe. Substantial effort was made to identify key faculty and administrators at the other public institutions, and contacts were made. A student-oriented presentation was developed and given to students in classes that were either Cybersecurity specific, or closely related (e.g., Computer Science). This resulted in greater institutional diversity in the second cohort of Analysts. The breakdown of contributions from each institution is given in Chart 1.

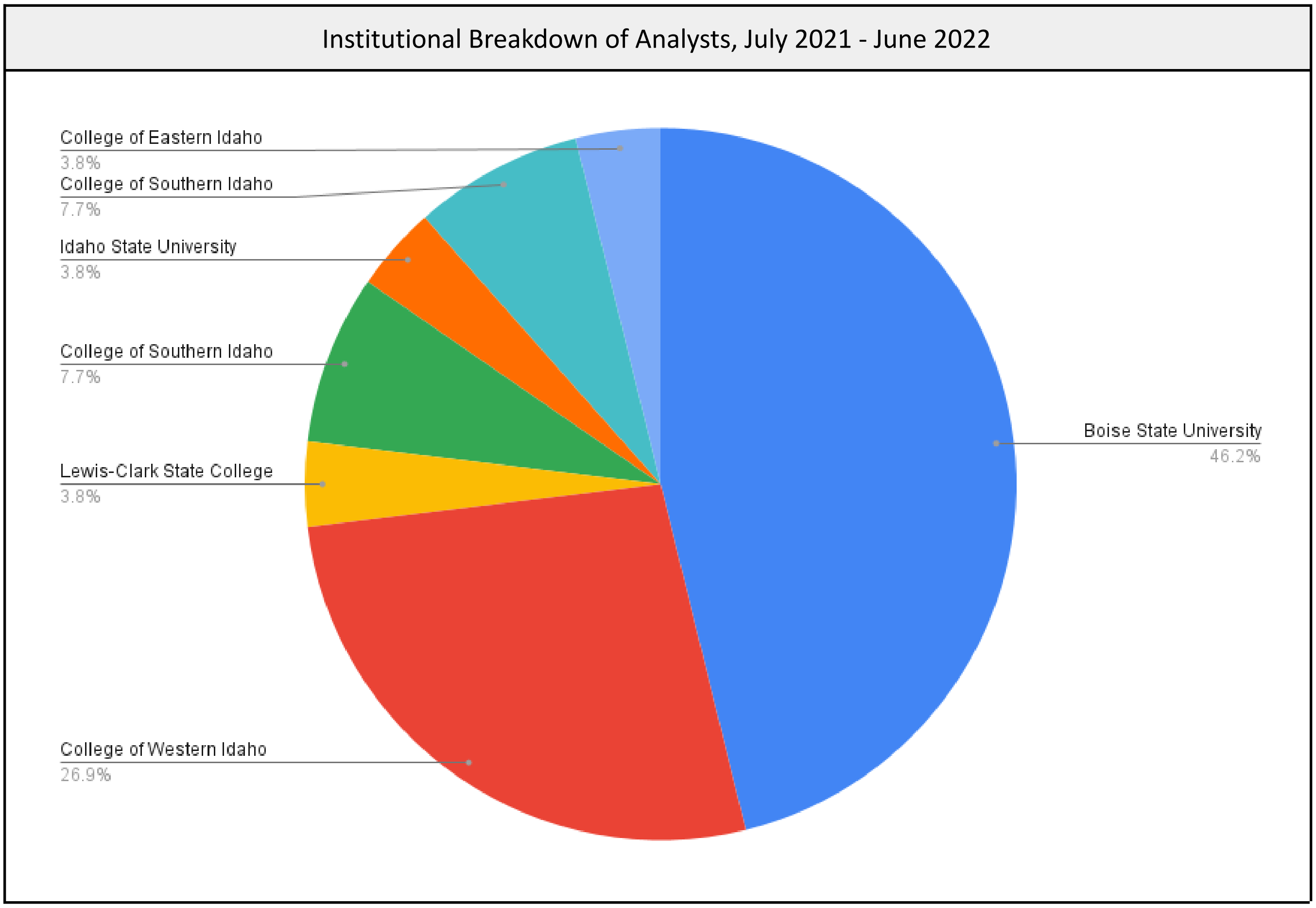
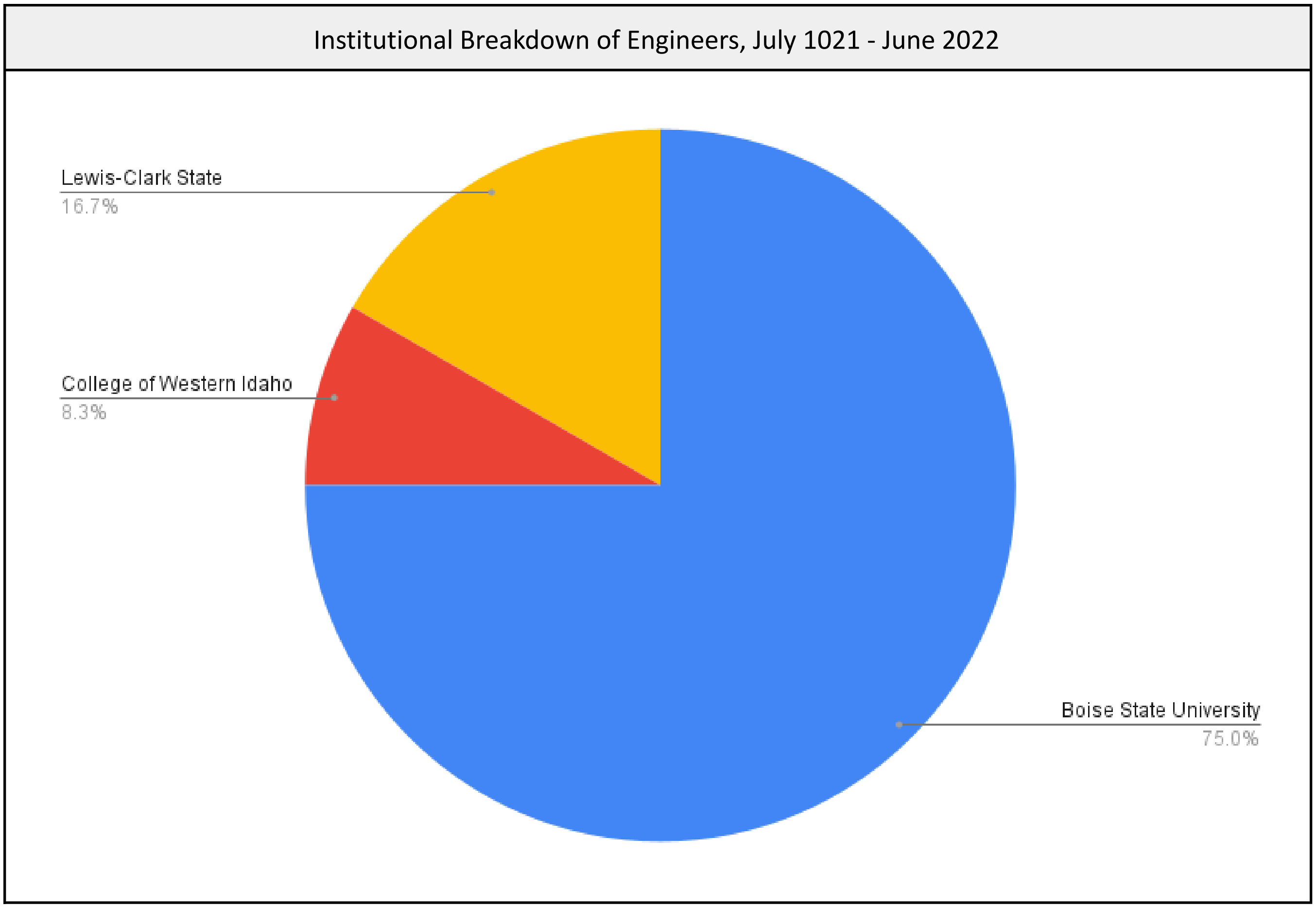


Chart 1. Analysts Hiring by Institution over Reporting Period

Engineer Recruiting

Engineer recruiting efforts included posting on institutional job sites, as well as identifying analyst candidates that had skills appropriate for the engineering position. Also, both roles were presented to students as part of the classroom recruitment efforts. Students considered for the engineering position typically had stronger applied technology experience (e.g. prior networking or integration experience). During the initial startup of the Cyberdome, most engineering tasks required an on-site presence. Owing to this, between July 2021 and December 2021 the initial round of recruited engineers was from Boise State University. After the initial on-site tasks were completed, the recruiting expanded to include remote candidates. The final institutional breakdown of engineers is given in Chart 2.



Institutional Breakdown of Engineers, July 1021 - June 2022

Chart 2. Engineer Hiring by Institution over Reporting Period

Key Technical Partnerships & Economic Development

Upon initial funding, the Cyberdome team intended to utilize SecurityOnion as our core production monitoring platform. This aligned with both our simulation environment and the statewide cybersecurity efforts to build out the Idaho Cyber Range. SecurityOnion training had been provided during the first year funding cycle of the statewide initiative and aligning to this platform was intended to strengthen the objectives and goals of both the statewide effort and the Cyberdome. Unfortunately, it was discovered that the SecurityOnion platform is not fully "multi-tenant" (e.g., able to securely separate multiple clients' logs and monitoring information) and would therefore not meet the goals of the second Cyberdome objective to "Reduce critical cybersecurity risks for SLTT clients." While this finding may have presented a terminal problem to this program, instead, a search was undertaken to find a commercial partner that could meet the stated objectives of the Cyberdome.

The Cyberdome team was able to connect, and subsequently partner, with Stellar Cyber, a recognized leader in the Open eXtended Detection and Response (OpenXDR) community. The Stellar Cyber executive team entered into a memo of understanding (MOU) with Boise State to provide gratis licensing, support, and training to Cyberdome interns. As well, they enabled outreach to an extensive partner community that is actively looking to hire Cyberdome interns. The Cyberdome graduate students, along with the Lead Engineer, undertook the effort of switching the core platform to Stellar Cyber, thereby providing multi-tenancy for SLTT clients, before our critical launch date.

In addition to Stellar Cyber, two other technology partners have stepped forward to provide gratis licensing to their commercial products. One company, PlexTrac, is headquartered in Boise and has recently raised over $80M to support its growth and go-to-market strategies. Through an MOU, PlexTrac has enabled the Cyberdome to leverage its reporting platform to enhance our client experiences and metric presentation. Our graduate assistants and undergraduate interns are in the process of integrating the PlexTrac platform with Stellar Cyber and expect to have this completed within the 2nd year reporting period. Further, PlexTrac and the IPC have internship and hiring pathways enabled for a wider audience of students.

The third technology partner is HYCU. The partnership MOU enables the Cyberdome to utilize HYCU's R-Score ransomware scoring platform. This platform enables our interns to work directly with our SLTT clients on determining key governance and risk metrics for future tracking and reporting purposes.

Where appropriate, these technology partners have enabled training for our interns, along with platform certification opportunities as part of their respective MOUs.

Beyond these initial technology partners, PI Vasko is in discussions with key national cybersecurity partners to enable further technology integrations for our SLTT clients, as well as applied learning opportunities for our interns. Further, PI Vasko is engaging with national Managed Security Service Providers (MSSPs) to communicate Idaho's cybersecurity workforce development efforts via the Cyberdome. These efforts have resulted in local & national media outlets covering the story of the Cyberdome and its objectives. A summary list of coverage is provided below:

- KIVI News 6 (Local): https://www.youtube.com/watch?v=Eo8_jwQIl6k
- KTVB (Local): https://www.ktvb.com/article/news/local/boise-state-cyberdome-program-bolsters-rural-cybersecurity/277-ee67d2f3-7b85-4572-907b-e9a309b65720
- Geekwire (National): https://www.geekwire.com/2022/boise-state-universitys-new-cybersecurity-program-helps-train-workers-and-protect-rural-communities/
- EdScoop (National): https://edscoop.com/boise-state-welcome-to-the-cyberdome/

Cyberdome Knowledge and Skill Assessment / Training Enhancement Program

The key objective of workforce development is accomplished by hiring, training and developing student workers in the roles of Cybersecurity Analyst and Cybersecurity Engineer. To this end, the Cyberdome team leveraged the educational background and experience of a graduate assistant as well as the industry experience of the Cyberdome Manager to create a comprehensive training program built around available cybersecurity resources.

To ensure that the training program fully aligned with industry expectations, an analysis was conducted of the cybersecurity industry roles specified at the National Initiative of Cybersecurity Careers and Studies (NICCS). These roles are defined in the NICE framework developed by NIST. In particular, the roles of Cyber Defense Analyst and Cyber Defense Infrastructure Support Specialist were identified as being highly aligned with the goals of the Cyberdome project. Since the roles defined in the NICE framework are competency-based, the objective of making a competency-based learning platform is strongly realized through this.

Once industry roles were identified, the knowledge, skills, and abilities (KSAs) defined for each role were utilized to create a KSA assessment tool for both pre and post-evaluation of the participants. This assessment tool uses both self and peer evaluation methods to determine a baseline skill set as well as determine what progress a participant has made towards being a workforce-ready graduate.

Leveraging statewide cybersecurity collaboration efforts and this assessment tool, prospective students from around Idaho can now provide a list of courses taken at any public institution and the Cyberdome management team can produce a knowledge and skill gap assessment for each worker. Utilizing this output, proscriptive training support is enabled for workers before they engage in production monitoring activities. As our college and university partners further build and enhance their respective cybersecurity curricula, the assessment tool will continue to be updated. Further, this tool is being examined for possible technology transference. In future funding years, the Cyberdome team intends to provide a report to each participating institution on knowledge and skill gaps identified so potential curriculum enhancements can be made.

Initial assessments were conducted on the first cohort of workers. These initial assessments provided a baseline from which further training was developed to close the gap between actual and desired competencies. Training content was organized into a comprehensive course shell housed in Boise State's learning management system. This allows the IPC to provide training remotely, track student progress and selectively expose training modules based on the determined knowledge and skills of a participant.

Training content covers a variety of areas related to the determined roles:

- General Cybersecurity concepts
- Networking concepts and practical networking tools
- Common attack types and attributes
- Cybersecurity defense principles
- Platform-specific programs and tools

For previously discussed reasons, the Cyberdome team shifted to utilizing a commercial product via our partner, Stellar Cyber. The use of Security Onion is ongoing within our training/simulation platform (e.g., Boise State's connection to the Idaho Cyber Range). Training on the individual components of the platform was obtained from several sources and enables our students to engage in multiple open-source/commercial platforms as a result of their engagement in the Cyberdome.

Graduate Assistant Contributions

The three graduate assistants assigned to the IPC have experience and backgrounds in computer science and education, as well as practical experience using Amazon Web Services (AWS). These backgrounds aligned well with the immediate needs of the IPC in the development of training and deploying the cyber security platform to the cloud.

The graduate assistants assisted in establishing the AWS environment, which included setting up identity and access management, security settings, and all related virtual machines for operating the Cyberdome. They also gained critical experience in creating Amazon Machine Images (AMIs) from base operating system images to facilitate the development of the final software environment, which consisted of pfSense, Security Onion, Stellar Cyber, and different Linux virtual machines.

At the beginning of 2022, the Cyberdome switched its primary security software from Security Onion to Stellar Cyber. Using Stellar Cyber's software upgraded the Cyberdome with multi-tenant access through a single web interface, integrated threat hunting tools, response features (e.g., upgraded our SIEM to have Security Orchestration & Automated Response [SOAR] capabilities), and easily configurable forward deployment sensor hardware and software (e.g., what used to take up to two-days to configure now takes less than an hour). By contrast, Security Onion required a separate interface per tenant (and would have increased costs as a result), demanded more costly equipment to achieve the same functionality, and lacked other key functionality like SOAR. Additionally, the graduate assistants were able to demonstrate API access to stored data using Stellar Cyber's published API set. The Stellar Cyber REST API makes academic data analysis much more streamlined than using Security Onion.

Extensive work was performed on analyzing and securing cloud access mechanisms and establishing role-based access control models. A sophisticated virtual private network (VPN) was deployed to provide secure access to the cloud resources. This was accomplished with open source software (OpenVPN) and includes encrypted access to resources, restricted port access, and multi-factor authentication (MFA) for additional security. The VPN allows both Cyberdome engineers and analysts to access the full cyber security platform from any location, enabling remote work across the state. A VPN is also used to provide secure site-to-site connectivity to client on-premise monitoring hardware.

The graduate assistants researched and documented the underlying data stores in the security platform. These data stores contain the collected data from Cyberdome clients and include event logs and signature analysis of packet data. The graduate assistants are now actively designing a data warehouse that will be deployed to maintain this data for research purposes in future funding reports.

Cyberdome Engineer Contributions

The Cyberdome started with four (4) student workers in the role of Cyber Security Engineer. Starting in February 2022 the number of engineers increased to nine (9). Engineer skill sets included computer science, networking, computer, and electrical engineering. The engineers were tasked with the development of supporting systems, deployment of test systems, and creating virtual test environments.

The engineers' first key task was the creation of an extensive virtual simulation environment that enables analyst skill development. The training environment is composed of common technical services that might be found in a typical city. This Virtual City is now being utilized as a training testbed and contains elements found in storefronts, utilities, and SLTT environments. This test facility provides a complete, isolated sandbox for security exercises and research. The engineers gained valuable skills in networking such as establishing a provider network, local area networking, bridging, switching, routing, and setting up VPNs. Additionally, they developed skills in virtualization technologies such as securely configuring virtual clusters, and automating the creation and destruction of virtual machines. All of these skills are directly applicable to their chosen cyber engineer careers and also enabled a deeper understanding of core cybersecurity principles.

Between July and December 2021, a group of engineers and senior computer science students built a tool for configuring appliances in the Virtual City, called the Virtual City Web Controller. This tool allows for the automated creation of accounts for student access to the Virtual City. The tool is capable of starting virtual machine instances within the Virtual City using predetermined scenarios. This allows for the rapid configuration of the Virtual City for use in expanded training and collaboration. This tool provides the basis for being able to quickly and efficiently instantiate virtual scenarios such as a compromised office, or create multiple environments on the same provider network.

Before switching to Stellar Cyber's commercial sensor, the engineering team researched and developed a configuration for the on-premise technologies (a "sensor") to be deployed at client sites. The sensor acts as the central hub that collects data from client systems and networks, and sends logs and parsed signatures to the security platform in the cloud. A version of the sensor was developed and deployed inside the Virtual City as a prototype before attempting to build a production version on a stand-alone server. The sensor is a complex combination of virtualized systems housed in one physical device. These include a VPN for security, port rerouting for external access, multiple virtual machines for sensing, processing, and shipping of data, and finally vulnerability scanning tools for investigating alerts. Several prototypes of the sensor were developed before a suitable model was created. Ultimately one was deployed to monitor the Virtual City itself. This deployment has the added benefit of creating test data for Cyberdome analysts for use in training. This sensor serves as a prototype for all subsequent sensors built for actual Cyberdome clients.

Several engineers developed a penetration testing plan for use against both Cyberdome assets and possible client environments. The key goal of this is to ensure assets are monitored, tested, and secure. This plan used industry-standard tools and was tested against the Virtual City and the model client sensor to validate the plan's usefulness while also hardening Cyberdome assets. This plan served as a training vehicle for current students and will be used to train future cohorts as they execute and update the current plan. This has the added benefit of also continuously improving the Cyberdome's security posture. Penetration testing techniques are a fundamental part of a cyber professional's tool kit, and this experience is directly applicable to the future careers of engineers and analysts. Additionally, this work provides the basis for developing a similar strategy for testing Cyberdome clients, as well as improving our risk assessment procedures.

Engineers configured a suite of assets with open source vulnerability scanning tools. These systems can be used to scan in-house assets as well for conducting risk assessments with actual clients. It also provided the students with hands-on training on how to set up a penetration testing and vulnerability scanning platform. Kali Linux was used as the base operating system as this is a common platform used in the security industry.

The requirements and foundational code base for a Cyberdome Client Web Portal were created. The portal is capable of summarizing security operations and controlling events and alerts, while also providing clients a portal for managing their team's access. This project will provide further training for a new cohort of engineers as they develop the project, and may also lead to technology transfer opportunities.

A self-contained, mobile network lab was developed and demonstrated for outward recruiting and education. The lab consisted of a managed switch, WiFi Router, and fifteen Raspberry Pi[1] computers. The hands-on workshop showcased ad-blocking, Internet detection, and basic penetration testing techniques. Through the workshop, basic networking concepts (which would be implemented in a home or small workplace environment) were explained and demonstrated to non-technical audiences. The mobile lab is completely self-contained so that when penetration testing is performed no access to the outside world was possible. The mobile network lab was first used at the multi-day Hackfort event in Boise in March, 2022 and resulted in community outreach to approximately 40 attendees. The pictures below provide perspective of the structure and outreach conducted at Hackfort.

A task management system and collaborative workspace for knowledge capture and dissemination was also established. Commercial tools like Jira and Confluence were selected as these tools met the requirements while at the same time providing workforce development by training interns in the use of

[1] Raspberry Pi is a trademark of Raspberry Pi Ltd

platforms they would likely see in their careers. The tools are used to help the Cyberdome track work being done while at the same time maintaining a history that can be used to develop future training.

The combination of the AWS cloud-based security control center and the customer-deployed sensor provides the core of our Cyberdome platform. The solution is not only scalable but becomes more cost-efficient at scale as some resources can be shared across clients. The solution is deployable anywhere there is an Internet connection and two available network ports. The solution provides appliances for packet capture and analysis, log management, endpoint detection and response, network and host intrusion detection, vulnerability scanning, threat hunting, and case management.

Throughout this current cohort, the engineers gained valuable knowledge that is directly applicable to working in the cybersecurity field. These skills include secure networking, open-source software configuration, hardware configuration, cloud computing, documentation rigor, and project management. Several of the first cohort engineering students have completed their internships, while the second cohort is just getting started.

Cybersecurity Analyst Contributions

Pre-Cyberdome Activation (July - December 2021)

The first round of analysts was recruited in late 2021, before the initial activation of the Cyberdome. These analysts were instrumental in developing the training and documentation for subsequent cohorts.

Training developed in the online learning management system Canvas was vetted by these analysts and improvements were made. The initial training heavily emphasized basic network and security concepts. Additional training content from TryHackMe was tested and incorporated into the curriculum. Based on feedback from these analysts, additional training was added around the initial security platform Security Onion. This was subsequently replaced with training content from Stellar Cyber.

Documentation of Cyberdome procedures was developed and vetted by the initial group of analysts. The day-to-day operating procedures were initially created around the Security Onion platform and were changed to Stellar Cyber shortly before the activation of the first Cyberdome Client. Documentation is housed in a cloud-based document management system, allowing access for local and remote users.

Analysts were evaluated for their strengths and weaknesses, and a lead student analyst was identified. The lead analyst acts as a primary source of information for the other analysts and provides feedback to the other analysts on incident activity.

Activation of Cyberdome Clients (January - June 2022)

The current service level agreement with Cyberdome clients specifies monitoring coverage from 8 am to 6 pm, 7 days a week.

Upon activation of the first Cyberdome client in mid-January, 2022, analysts moved to a new schedule designed to cover the service level agreement. Shifts were initially set to 4 hours in length and could be performed in the Cyberdome office facilities, or remotely via VPN access. A minimum of two analysts were required to cover each shift. This allowed for redundancy in case an analyst could not cover an assigned shift. As recruiting expanded to other clients, it was determined that 4-hour shifts were not flexible enough for some students who had classes in 4-hour blocks. Schedules starting with the second cohort had shift lengths of 2 hours on weekdays and 5 hours on weekends.

Analyst SOC duties involve triaging alerts and incidents generated by the Stellar Cyber platform. Triaging consists of an initial assessment of the severity of the incident, followed by researching the incident using available resources, and concluding with either resolution or escalation. An escalation chain to the lead student analyst and then the Cyberdome Manager was implemented. Incidents that merited communication with a Cyberdome client were documented and forwarded to the client for further investigation and resolution.

Skill Development

In feedback from various industry partners, it became clear that additional "essential" skill development (aka, "soft skills") would be welcome. A primary skill was identified as being able to present a complicated subject clearly and concisely. To this end, analysts were required to research a cyber security topic or vulnerability and present their findings to other analysts and Cyberdome management.

Continuity of Operations

Several steps were taken to provide continuity of operations across cohorts. These steps involved the cadence of recruitment and personnel additions.

To avoid the disruption that may occur if a cohort ends at the same time a new cohort begins, an overlapping recruitment process was adopted. A typical cohort of students lasts six months. However, a new cohort of approximately seven analysts begins every three months, creating an overlap of cohorts. This ensures that the Cyberdome is staffed with experienced analysts at all times. This also allows for the mentoring of new analysts by more experienced analysts on each shift.

The initial hierarchy of analysts had one student chosen as the lead analyst for that particular cohort. Lead analysts vary in skills from cohort to cohort; to have a strong lead analyst available to all cohorts, a position for a full-time lead analyst was created. Recruitment for this position ended with the successful hiring of an experienced lead analyst in May 2022.

Maturity of Cyberdome Processes

Cyberdome processes are still at an early stage of development. Critical processes, such as those involving incident triage and management are relatively mature and suitable. Ancillary processes, such as analyst feedback and performance monitoring are still in development and will continue through future cohorts. Maturity of processes is an on-going effort and future cohort participants are engaged to build these feedback and performance processes.

Maturity of Analyst Recruitment and Hiring Process

The recruitment and hiring process has greatly improved over the course of three analyst cohorts. Contacts at the various institutions have been made that allow Cyberdome personnel to present directly to students. These presentations have been enormously successful, resulting in more than sufficient analyst candidates.

Objective Two: Reduce critical cybersecurity risks for State, Local, Tribal, and Territorial (SLTT) clients

The IPC, as part of its community outreach efforts, conducts risk assessments for SLTT clientele around the state. Funding for these assessments is outside the scope of the Cyberdome effort. The assessments are mentioned here, however, to show the interwoven service portfolio for rural SLTT clients the IPC provides and represents the ongoing efforts to recruit client communities to the Cyberdome. Funding for future risk assessments was renewed for 2022 and these activities will be used to recruit other communities into the Cyberdome.

The activation of the Cyberdome's first client occurred in mid-January 2022. This provided a real-world experience for our analysts as they monitor the events and alerts. It also initiated building the data store of real-world events that can then be used to further academic research. At the end of the first year reporting period, the IPC and Cyberdome staff are pleased to report that a total of four (4) clients are activated, with another five (5) clients "in-flight" towards activation over the coming months. This puts the Cyberdome at a total number of nine (9) clients, almost double the number in the original grant request. The budget savings to accomplish this came about as a result of platform savings by moving to Stellar Cyber, along with savings from delayed cohort hiring. Further, this doubling of clients and careful first year budget planning does not require any additional funding in future years.

The Cyberdome provides each client access to a Web Dashboard for their particular network through https://cyberdome.us. From there the client can see the number of ongoing alerts, with severity, in real-time. Additionally, clients are informed through email concerning particular incidents which cannot be determined as either benign or false positives. More robust client reporting is still in flight so each client can easily see the number of incidents occurring and being resolved in a format understandable by a non-technical audience. A list of clients, along with their asset and activation dates are provided in Table 1 below.

Cyberdome Clients			
Name	**Assets**	**Residents**	**Activation Date**
Jefferson County	200	26,000	03/22
City of Sun Valley	200	2,500	01/22
Cambridge School District	100	400	03/22
Midvale School District	200	300	03/22

Table 1. Year-one Cyberdome Client Information

The next reporting period report will outline the efforts to enable clients and present other research objectives.

Objective three: Produce innovative research, tools, and techniques to transfer to commercial efforts

Early-stage development of research, tools, and techniques have come as a result of platform and staffing activation. The Cyberdome team has leveraged available opportunities to conduct research, or develop the following specific items:

Co-PI Dr. Edoardo Serra and his students have been focusing their Cyberdome research effort on the design of Machine Learning systems to detect and explain cyber malicious threats. Part of the research focuses on the use of graph formalism to process security log data (currently, IoT device communications and application API calls) through the use of advanced graph representation techniques. In this context, they have already produced the following publications (all peer-reviewed conference papers that acknowledge the Cyberdome grant):

- Carpenter, J., Layne, J., Serra, E., and Cuzzoccrea, A., 2021. Detecting Botnet Nodes via Structural Node Representation Learning. IEEE BigData 2021: 5357-5364.
- Quebrado, M., Serra, E., and Cuzzoccrea, A., 2021. Android Malware Identification and Polymorphic Evolution Via Graph Representation Learning. IEEE BigData 2021: 5441-5449.

Another part of his research focuses on the explainability of attack classification models to facilitate threat investigation. In particular, the research focus was on automatically associating to subgraphs of the API call graph to a specific attack technique reported in the Att&ck[2] Knowledge base. Always in the context of explainability, Dr. Serra evaluated standard explanation techniques, called attribution techniques, to explain classification models to detect specific threats in network traffic and power systems. The result of the analysis is that current attribution techniques literature produces inconsistent explanations in the domain of cyber security, and further research effort is required. The following are the related papers already published (all peer-reviewed conference papers or posters that acknowledge the Cyberdome grant):

- Fairbanks, J., Orbe, A., Patterson, C., Serra, E., and Scheepers, M., 2022. Identifying ATT&CK Tactics in Android Malware Control Flow Graph Through Graph Representation Learning and Interpretability. The Thirty-Sixth AAAI Conference on Artificial Intelligence - Student Abstract and Poster Program, 2022.
- Fairbanks, J., Orbe, A., Patterson, C., Serra, E., and Scheepers, M., 2021. Identifying ATT&CK Tactics in Android Malware Control Flow Graph Through Graph Representation Learning and Interpretability. IEEE BigData 2021: 5602-5608.
- Ratul, Q., Serra, E., and Cuzzoccrea, A.., 2021. Evaluating Attribution Methods in Machine Learning Interpretability. IEEE BigData 2021: 5239-5245.

Thanks to such preliminary results, Dr. Serra, in collaboration with PI Vasko, submitted a proposal to the National Centers of Academic Excellence in Cyberdefense (NCAE-C) entitled "Meta Data Traffic Anomaly Detection via Interpretable Temporal Structural Provenance Graph Representation Learning."

The current research of Dr. Serra and his students is on the extended provenance graphs[3] to integrate different security logs and efficient explainable graph representation techniques to better process and interpret the generated provenance graphs. Research papers on such fields are currently in preparation.

Co-PI Dr. Francesca Spezzano and her students have been working on the definition of new organizational security risk measurements with indirect factors through the analysis of information contained in social media and news. In particular, a piece of such research focuses on the idea of monitoring the behavior of the organization's employees over social media. The risk of an organization can be related indirectly to how hazardous the behavior the organization employs over social media. This can be especially true in the case of exposure to social engineering attacks. In particular, Dr. Spezzano focuses on the assumption that the larger the number of employees in an organization that ingenuously spread fake news, the higher the risk that such employees can be deceived by social engineering attacks and expose the organization to risk. In this specific field, Dr. Spezzano published the following peer-reviewed journal paper acknowledging such a grant:

[2] https://attack.mitre.org/

[3] Han, X., Pasquier, T., & Seltzer, M. (2018). Provenance-based intrusion detection: opportunities and challenges. In *10th USENIX Workshop on the Theory and Practice of Provenance (TaPP 2018)*.

- Shrestha A., Spezzano F., Characterizing and Predicting Fake News Spreaders in Social Networks. International Journal of Data Science and Analytics 13(4): 385-398 (2022).

In the same direction of security risk measurements with indirect factors led by Dr. Spezzano, Dr. Serra also contributed by measuring how employees of an organization care about privacy. The assumption, in this case, is that the more the employees disclose private information on social media, the higher the likelihood that such information will be used by malicious individuals to damage the organization. In particular, the research focuses on detecting shared images on social media that disclose private information. Of specific interest in the detection of images that disclose documents. For this specific context, the following peer-reviewed conference acknowledging such a grant was published:

- Serra, E., Squicciarini, A., Ayyapureddi, S., and Ratul, Q., 2021. A Few Shot Transfer Learning Approach Identifying Private Images With Fast User Personalization. IEEE BigData 2021: 1204-1213.

All these factors, even indirectly, can estimate real risk for the organization that cannot be detected otherwise. Thanks to the research and collaboration facilitated by the Cyberdome grant, Dr. Spezzano, in collaboration with Dr. Serra, Dr. Jain, and PI Vasko, submitted an educational proposal to "National Centers of Academic Excellence in Cyberdefense" entitled "Integrated Faculty Workshop on Artificial Intelligence for Cybersecurity.''

Dr. Spezzano currently is working on searching other undirected factors that can estimate cyber risk from social media. In addition, Dr. Spezzano, in collaboration with Dr. Serra, are working together to predict the kinds of targeted organizations and attacks directly from news events. This work is currently done by creating machine learning models that correlate historical news events with known disclosed cyber incidents. With such a model, given the most recent news event, we will estimate the likelihood that a particular kind of organization can be targeted by a specific kind of attack and for which motivation. The prediction of such information is very important in the prioritization of cyber operations. A research paper is in preparation.

Co-PI Dr. Jidong Xiao utilized research time to work with his Ph.D. student Shariful Alam on developing a framework, based on the Intel virtualization technology, for protecting sensitive and private data against cold boot attacks. A full paper is written. It was first submitted to the 2022 International Conference on Dependable Systems and Networks (DSN). The paper was not accepted for publication and the team received critical feedback from the reviewers and is working on revising the paper and are planning to soon submit the revised paper to the 2022 Annual Computer Security Applications Conference (ACSAC).

Co-PI Amit Jain worked with his Ph.D. student on researching machine learning tools to help with election cybersecurity. Part of his time was funded by this grant and a part was funded by another grant. A survey paper is expected to be produced in the next six months.

Assessment and Training Tools

The comprehensive KSA assessment tool as well as competency-based training program can be leveraged by commercial security service providers as a career development tool. PI Vasko is examining likely technology & process transfer opportunities with commercial partners. If a viable route to market is determined, the tools and programs may be transferred to a commercial partner.

As the project is still in an early stage and the platform is nearly activated, other research, tools, and techniques are not expected until later in the project.

Future Plans / Funding Strategy

The Cyberdome team is well on its way to further sustained growth in all objective areas. This section outlines both plans and funding strategies for the Cyberdome efforts.

Future Plans

Some examples of efforts being undertaken in the next reporting period include:

1. Expand the Cyberdome client portfolio to better assist SLTT clients with important cybersecurity functions such as risk assessments, threat intelligence, and community member outreach (e.g. notifications & messaging to residents).

2. Continue to refine processes and operating procedures for current technology platforms while also ensuring our service architecture is open for new technology partners and service enablement for continuing to enhance client deliverables.

3. The penetration testing plan will be used as a basis for building an automated weekly vulnerability scan that will be deployed on Cyberdome assets as well as be made available to Cyberdome clients. A much smaller automated vulnerability scan is planned for use during risk assessments. This will provide further workforce development of cybersecurity systems thinking, vulnerability scanning, and automation, and ensure continuous improvement of the Cyberdome's security posture.

4. Integrate the new technology partners (PlexTrac and HYCU) into the Cyberdome service architecture. This will allow computer science/programming engineering interns to integrate security technologies and present portfolio elements on their resumes after graduating.

5. Continue development of the Virtual City as a training platform. Increase the assets in the virtual city to include more complex storefronts, doctors' offices, workspaces, include simulated transactions, etc. This increases our ability to test from both an offensive and defensive position. It also forms the basis for creating vulnerable systems for use in range exercises with other schools.

6. Pursue commercialization opportunities for the candidate assessment and skill gap training platform.

7. Continually improve training for engineers and analysts based on new methods and approaches. This should include training on how to restore systems when they go down, how to build new system components from scratch, how to monitor the full security grid, and how to scan assets for vulnerabilities.

8. Continue to enhance training for both analysts and engineers. The current plan includes exercises in simulated security events, how to detect and then threat hunt events, and how to manage cases including client etiquette.

Future Funding Efforts

Current plans for future funding models include funding and employer sources. Details of each are provided below.

Federal, State, and private funding sources

The IPC applied for and received an Idaho Workforce Development Council (WDC) Industry Sector Grant equal to $800K over 3 years (approximately $266,000/year). This grant focused on enabling Cyberdome interns through paid efforts similar to those approved by HERC (e.g., 6-month paid internships) and, effectively, doubled the total number of student workers in the Cyberdome. The grant period spans FY'23 through FY'25 with a possible extension into FY'26.

Further funding requests are being put forward in support of Governor Little's Cybersecurity Task Force objectives, of which PI Vasko was a member. This request includes state appropriations equal to four (4) full-time support members, paid internships for up to 55 students across the state, and platform support for up to 18 rural communities.

Employer partners

PI Vasko is actively pursuing sustainable funding from employer partners for this program. An anticipated sustainable funding model will come through the enhanced return on investment employers can achieve by funding an intern stipend for each early-stage cybersecurity career professional. Leveraging the identified "Activation Gap" thesis in our original HERC proposal, employers are spending 6-9 months activating new employees on methods and techniques. Under the thesis that the Cyberdome eliminates up to 3 months of that activation period, then an employer can achieve "twice the training for half the cost." Here is a simple model to validate the opportunity:

- "Fully-loaded" annual salary of Security Analyst: $60,000 base + 35% fringe = $81,000 (Monthly cost: $6,750)
- Three (3) months of salary to provide technical training: $20,250
- Estimated technical training costs: $5,000
- Total hard costs to "activate" a security analyst: $25,250

If an employer provides the Cyberdome half of this expected cost ($12,625) as a gift, the employer potentially receives a tax-deduction AND an employee ready to activate in their environment faster than expected. The reduction in downtime and training costs that are passed on to the Cyberdome enables a doubling of the training time (6 months), enables a better-qualified employee, and helps to reduce the risk to our rural and remote communities around the state.

Patents and Copyrights

There were no patents or copyrights to report at this time.

Startups and Technology Licenses

There were no startups or technology licenses to report at this time.

Expenditure Report

The table below summarizes expenditures associated with the grant project. The project start date was delayed by 2 months in the summer of 2021 as we worked to recruit and onboard a Manager and Lead Engineer to support the project and future interns. This delay in hiring pushed back initial project timelines including the hiring of undergraduate workers and onboarding of new clients. Faculty and staff have worked to quickly catch up and achieve grant goals.

To date, a total of four (4) clients have been onboarded, with several others in the pipeline. In May, a revised annual budget was presented and accepted. This allowed the team to make additional hardware, ticketing, and AWS instance purchases without increasing the total costs associated with the grant. This enabled the team to provide necessary upgrades to our existing clients' hardware, exceed our grant's initial goal of serving five SLTT clients, and increase the quality and volume of data available to our graduate assistant researchers and Co-PI's.

In our first year, the Cyberdome supported 43 total students, faculty, and staff (see **Figure 2**). Our first cohort of 8 students finished their internship experience in the Cyberdome. The second cohort is mid-way through and meeting expectations. There are currently 16 students who will complete their work experience by the end of the summer and an additional 9 are scheduled to graduate from the Cyberdome program in mid-November. Three Graduate Assistants were hired in August 2021 to assist with the development of the Cyberdome platform and conduct research while our five co-PI's continue to serve as advisors to GAs and execute their research.

Additionally, we have purchased a subscription to a cybersecurity training platform, which will help us to further upgrade our interns' offensive and defensive security skill set.

Projected Expenditures for July 1, 2021 to June 30, 2022[4]				
Category	Annual Budget	Revised Budget	Projected Spend	Remaining Amount
Wages	$474,161	$437,522	$437,522	$0
Fringe + GA Scholarship	$135,339	$124,182	$124,182	$0
Equipment and Other Expenses	$90,500	$138,300	$138,388	$(88)[5]
Total	**$700,000**	**$700,00**	**$700,088**	**$(88)**

[4] Please note: The financial reporting period for actual spend is through the middle of the May period because the June financial month has not closed, and will not be closed by the required reporting date of June 30. This annual report reflects a best projection because of this limitation. A recommendation to HERC is to require the mid-year and annual reports on the 1st of the 8th month (February) and 14th month (August), respectively, so accurate period actuals can be presented.

[5] University funds will be used to cover this deficit.