Progress Report for IGEM 22-001

The Cyberdome — An Investment in Idaho's Cybersecurity Future

1st July 2021 – 31th December 2021

Mid-year Progress Report

BOISE STATE UNIVERSITY

IGEM 22-001

The Cyberdome — An Investment in Idaho's Cybersecurity Future

1st July 2021 – 31th December 2021, Mid-year Progress Report

Table of Contents

IGEM 22-01: The Cyberdome – An Investment in Idaho's Cybersecurity Future

1st July 2021 – 31th December 2021, Mid-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 in order 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 is currently 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**
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
Outreach to "Round 1" SLTT clients		x	x	x		
Activation of "Round 1" SLTT clients					x	x

Figure 1. July to December view of Cyberdome timeline

This progress report summarizes the activities during the first six (6) months of the project. Please note: Objective #1 from our proposal was the primary focus this period. The other goals will have stronger focus in future reporting periods now that the platform is built.

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, 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 – Eric Stevens (Cyberdome Lead), and Marlin Roberts (Cyberdome Manager) 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 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.

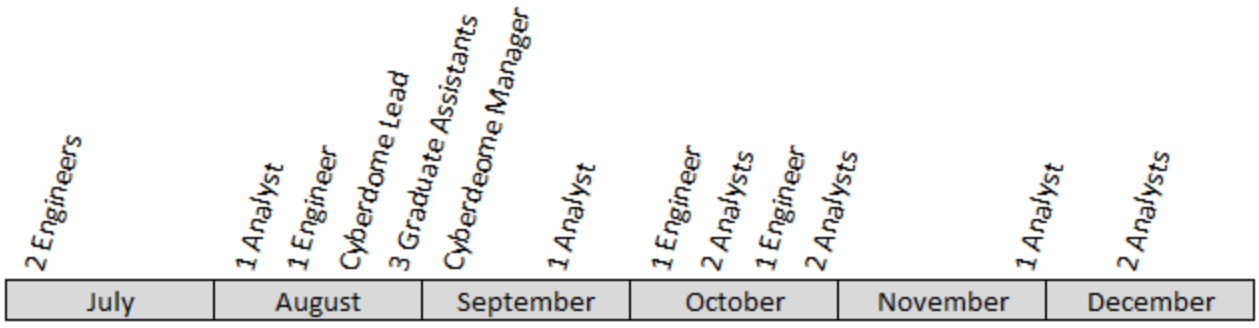

Figure 2. Hiring timeline by month over reporting period.

Details on the activities and accomplishments of the funded graduate assistants and undergraduate workers are provided in the next sections.

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 development of the final software environment, which consisted of pfSense (www.pfsense.org), Security Onion (www.securityonionsolutions.com), and different Linux virtual machines.

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 in order to provide access to the cloud resources in a secure manner. 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 in order to maintain this data for research purposes.

Cyberdome Engineer Contributions

The Cyberdome hired four student workers into the role of Cyber Security Engineer, with skill sets in computer science and engineering. These workers were generally tasked with 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, 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.

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.

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 in order 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 the 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 was created. The portal is capable of summarizing security operations and control 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 task management system and collaborative workspace for knowledge capture and dissemination was established. Industry standard tools like Jira and Confluence were selected as they met the necessary requirements, while at the same time providing workforce development by training our students to use tools they would likely see in their careers. The tools are being 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 provide a complete security solution. 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, end-point detection and response, network and host intrusion detection, vulnerability scanning, threat hunting, and case management.

Throughout this current cohort, the engineers have gained valuable knowledge that is directly applicable to working in a cyber security field. These skills include secure networking, open source software configuration, hardware configuration, cloud computing, documentation rigor, and project management. The first cohort of engineering students are still in flight within the Cyberdome platform so future employment opportunities will be tracked in the next period.

Knowledge and Skill Assessment / Training Enhancement Program

A key goal of the Cyberdome is workforce development. This is accomplished by hiring, training and developing student workers in the roles of Cybersecurity Analyst and Cybersecurity Engineer. To this end, the IPC 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 curriculum, the assessment tool will continue to be updated. Further, this tool is being examined for possible technology transference.

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 (Canvas). This allows the IPC to provide training remotely, track student progress and selectively expose training modules based on 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

The Cyberdome is utilizing an open-source platform, Security Onion. Training on the individual components of the platform was obtained from several sources. In addition to this, the Cyberdome is pursuing a relationship with commercial security platform providers in order to provide even more platform exposure to the analysts and engineering teams.

Recruitment and Training

In support of Objective #1, hiring to fill Analyst roles is ongoing. The Cyberdome team recruited eight Cybersecurity Analyst workers between October and November. This initial cohort completed initial assessments, 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 in order 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 through our established VPN. The final composition of the cohort was five Boise-local students and three remote students. The infrastructure is in place to have all of the students work either in the IPC, or remotely once the Cyberdome is activated.

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 is expected to renew in 2022 and these activities will be used to recruit other communities into the Cyberdome.

The first client connections will occur in the next report period. The next reporting period report will outline the efforts to enable clients and present other research objectives.

Objective three: Produce innovative research, tools, 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 utilized research time to examine and craft accepted papers for conferences. These are all peer-reviewed conference papers or posters. The provided Cyberdome grant time has been acknowledged in each paper and is expected to be leveraged in production efforts in future reporting periods:

- 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.
- Serra, E., Squicciarini, A., Ayyapureddi, S., and Ratul, Q., 2021. A Few Shot Transfer Learning Approach Identifying Private Images With Fast User Personalization. Accepted as a full paper to IEEE BigData 2021.
- Carpenter, J., Layne, J., Serra, E., and Cuzzoccrea, A., 2021. Detecting Botnet Nodes via Structural Node Representation Learning. Accepted as a full paper to IEEE BigData 2021.
- Quebrado, M.[*], Serra, E., and Cuzzoccrea, A., 2021. Android Malware Identification and Polymorphic Evolution Via Graph Representation Learning. Accepted as a full paper to IEEE BigData 2021.
- 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. Accepted as a full paper to IEEE BigData 2021.

Co-PI Dr. Francesca Spezzano utilized research time to examine and craft accepted papers for conferences. These are all peer-reviewed conference papers or posters. The provided Cyberdome grant time has been acknowledged in each paper and is expected to be leveraged in production efforts in future reporting periods:

- Shrestha A., Spezzano F., Characterizing and Predicting Fake News Spreaders in Social Networks. Accepted for publication in the International Journal of Data Science and Analytics - Springer.

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. The tools and programs could potentially be offered as a course by an institution such as Boise State. By leveraging the online learning platforms available at Boise State, the IPC has created a program that can be offered as a fully remote program.

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

The Cyberdome team is well on its way to further sustained growth in all objective areas. Some examples of efforts being undertaken in the next reporting period include:

1. 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, automation, and ensure continuous improvement of the Cyberdomes security posture.

2. Continue developing the Cyberdome Client Web Portal to include automated authorization emails, integrated interconnection between clients and Cyberdome analysts, improve multi-tenancy support, and security harden the interface.

3. 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 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.

4. The activation of the Cyberdome's first client is scheduled for mid-January 2022. Deployment of our first sensor to this client will occur and monitoring will begin in mid-January. This will provide real world experience for our analysts as they monitor the events and alerts, but will also begin building the data store of real world events that can then be used to further academic research. It will also provide workforce development of our engineers as they respond to the daily requirements of keeping a functioning Security Operations Center (SOC) online.

5. 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.

6. Develop more formal training for analysts. This should include exercises in simulated security events, how to detect and then threat hunt events, and how to manage cases including client etiquette

Faculty and Student Participation

In total, there are 14 Cyberdome Student Workers (both graduate and undergraduate), and three (3) graduate assistants, supported by this grant. The Cyberdome Student Workers report to the Cyberdome Manager and the graduate assistants report to their faculty advisors and co-PIs, Dr. Edoardo Serra and Dr. Francesca Spezzano.

Name	Cyberdome Staff	Cyberdome Student Workers	Graduate Assistants
PI Edward Vasko	1	0	0
Cyberdome Manager Marlin Roberts	1	14	0
co-PI Edoardo Serra	0	0	2
co-PI Francesca Spezzano	0	0	1
co-PI Jidong Xiao	0	0	0
co-PI Sin Ming Loo	0	0	0
co-PI Amit Jain	0	0	0
Total	2	14	3

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 project. Software costs such as ticketing, and Amazon Web Services (AWS) have been minimal to date, but it is expected that these costs will grow to projected levels as clients are onboarded. All other costs to date have gone towards the wages and benefits of employees connected to this grant. Five faculty, three graduate assistants, three professional staff (two FTEs + PI Vasko's partial efforts), and fourteen student employees were directly supported via the grant during this period. Faculty involvements during this period were limited to those previously mentioned in the Objective 3.

Expenditures for July 1, 2021 to November 27, 2021[1]				
Category	**Annual Budget**	**Actual Spend**	**Budget Remaining**	**% Remaining**
Staff and Faculty Wages	$210,904	$49,609	$161,295	76%
Fringe and Benefits	$77,100	$17,181	$59,919	78%
Graduate Assistant Wages	$78,000	$19,924	$58,076	75%
Grad Assistant Scholarships	$30,360	$14,457	$15,903	52%
Grad Assistant Fringe	$14,912	$3,242	$11,670	78%
Student Wages	$185,257	$8,798	$176,459	95%
Student Fringe	$12,968	$395	$12,573	97%
Equipment & Support[2]	$90,500	$4,409	$86,091	95%
Total	**$700,000**	**$118,015**	**$581,985**	**83%**

[1] Please note: The financial reporting period for actual spend is through the end of the November period because the December financial month has not closed, and will not be closed by the required reporting date of January 1. An eleven (11) month review will be provided in the annual report as well 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.

[2] The Equipment & Support category is a combination of the grant line items "Servers & Support," "Cloud," "Storage," and "Ticketing" If there is a need for a breakdown of these items, the team can provide it. As indicated, the spend to date is relatively small across all categories and is expected to significantly increase in the second reporting period.