IGEM Grant Report

☑ Progress (due Jan. 1) □ Annual (due Jul. 31) □ Final (due Aug. 31)

IGEM Grant # _ ***IGEM 22-001**_______* Principal Investigator _Edward Vasko_

Submission Date _December 31, 2022_ Primary Institution _Boise State University_

Instructions: Complete each section of this report directly on this template. Completed reports must be 4 pages or less in 12 pt Arial font, excluding the expenditure report. Reports that do not follow these requirements will be returned for revision. Submit reports by the appropriate due date to HERC@osbe.idaho.gov

Section 1: Summary of project accomplishments for the reporting period and plans for the upcoming reporting period.

Objective 1: Workforce development metrics:

For the reporting period[1], the Cyberdome project has funded an equivalent of 16 full student internships. During this period, student workers from four of our public institutions - Boise State University, College of Western Idaho, College of Eastern Idaho, and Lewis Clark State College - worked together to monitor & detect client issues.

Objective 2: Risk reduction for clients:

For the reporting period[2], our technology platform reported a total of 34,711 client alerts to our student workers. From these alerts, the students were able to analyze the reported data and filter this information to 6,010 possible incidents. These incidents were then further examined with our lead mentor team members for possible impact levels to our clients. Of the possible incidents, a total of 78 escalated to our clients. The team then worked with our clients to determine next steps and escalation paths. These alerts, incidents, and escalations would not have been caught without the technology, processes, and student workers in the Cyberdome.

Objective 3: Produce innovative research, tools, & techniques

Our Co-PIs and Graduate Assistants (GAs) are working on four papers for submission before the end of the annual period. The papers range across topics such as: anomaly detection in process execution, malware polymorphism mitigation, cybersecurity predictive models, and election security. We continue to refine one avenue for technology licensing/transfer involving predictive individualized training for cybersecurity workers.

Status of other planned accomplishments from last year's report:

The team continues to expand the Cyberdome client portfolio. Through our partnership with PlexTrac, the Cyberdome Risk Assessment team is working with a pilot client to conduct on-going risk assessments. Further, a separate team of analysts, including a graduate student, are implementing the MISP (www.misp-project.org) threat intelligence platform with the goal of providing analysis/reporting to our clients as well as interested state-level agencies.

[1] Reporting report of July 1, 2022 thru November, 15, 2022

[2] Reporting report of July 1, 2022 thru November, 30, 2022

Building recurring (annual) penetration testing offering for clients with vulnerability scans.
One Cyberdome portfolio service we continue working towards is remote vulnerability scanning for our clients' networks. Our student worker team has successfully operated the service in an initial test environment.

Continue development of the Virtual City/CyberRange as a training platform.
Our refurbished public range computing cluster, "Manticore," has been refreshed via the efforts of our Lead Engineer and two student workers. Manticore has been restored to full service and student workers will be helping to build it into a multi-school lab environment. This range is a cornerstone of the Idaho Cyber Range. Future collaborations with CWI, LC State, and other schools will begin in Q1'23.

Continue activating Cybedome clients.
Increasingly complex clients provide real world experience for our engineers and analysts as they architect and implement sensors, and monitor the events and alerts, respectively. We have seven prospective clients in varying stages of movement forward towards activation.

Training improvements
The team continues to improve training for engineers and analysts based on new methods, approaches, and available content. This includes 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. Analyst specific training will soon include exercises in simulated security events, how to detect and then threat hunt events, and how to manage cases (including client etiquette).

Platform refinement & automation
There are many regular, repetitive tasks involved in the regular upkeep of Cyberdome systems and lab environments, and student workers have been involved with documenting these processes and will start working to automate them in the near future.

Section 2: High-level summary of budget expenditures for the period just completed. If budget is underspent at time of report, explain why and plans for expending funds.
Section 6 presents an expenditure report for the first 4.5 months of this period. To date, we believe spending is on track. The wage category is slightly over budget, but student workers tend to reduce their total working hours during the holiday season and finals week. Fringe is significantly under budget, partially attributed to the fact the wages charged to this grant have primarily come from non-benefited staff who charge a much lower fringe rate than full-time staff and co-PIs. Spend on fringe/benefits should closely resemble wage utilization by the end of the fiscal year in June.

Other Expense (OE) spending is significantly under budget, particularly spending associated with Amazon Web Services. We will likely spend down our OE budget by moving these funds to cover salary expenses. Starting in January, we plan to hire another mentor into a temporary position to assist our full-time staff with Engineering and student worker supervision efforts. Additional hiring includes up to six "tier two" student workers to provide Analyst interns with additional mentorship.

Section 3: Demonstration of economic development/impact, including the following as applicable: patents, copyrights, plant variety protection certificates received or pending; technology licenses signed, start-up businesses created, and industry involvement; private sector engagement; jobs created; external funding; any other pertinent information.

Industry Involvement/Private Sector Engagement
PlexTrac - our new technology partner, PlexTrac (an Idaho-based cybersecurity company), has provided the Cyberdome licensing for our student workers to use in establishing a risk-assessment offering to our clients.

Other early-stage industry involvement includes international companies like Sophos (www.sophos.com; used by University of Idaho), and US-focused companies such as AllPoints Logistics (www.allpointsllc.com); CRI Advantage (www.criadvantage.com; an Idaho-based company), Silent Sector (www.silentsector.com), and Shadowscape (www.shadowscape.io; an Idaho-based cybersecurity company).

Economic Development via Jobs Created:
Since the beginning of the reporting period, 12 student workers responded to surveys indicating their expected wage over the next year. Out of those 12 respondents six indicated that they already had accepted a job offer and reported an average salary of $52,435 per year. Those who had studied for either a bachelor’s or master's degree reported a significantly higher salary of $62,888 compared to those with an associates degree that report an expected annual salary of $39,370.

Additional funding received through leveraging the Cyberdome:
The Institute for Pervasive Cybersecurity received an Idaho Workforce Development Council (WDC) Industry Sector Grant equal to $800K over 3 years (approximately $266,000/year). The grant period spans FY’23 through FY’25 with a possible extension into FY’26. NOTE: While applied for/awarded in FY’22, receipt of funds did not occur until FY’23.

Two other Federal grants leveraged the Cyberdome data/platforms for delivery/support. The first is a $750,000 2-year grant from the NSA Center for Academic Excellence program. The grant is to develop AI/ML analysis graphs leveraging the Cyberdome datasets and platforms. The second grant is a $280,000 2-year grant for a GenCyber instructor camp that will leverage the Cyberdome platform.

Technology Transfer/Licensing Opportunity:
Co-PI Serra continues to develop/refine a model to automatically identify cybersecurity skills through student provided transcripts. This model has a key goal in mind - to analyze course descriptions to align against specific roles contained in the National Initiative for Cybersecurity Education (NICE) framework. The results of the model allow for an individualized plan to be built for each student worker. Further, the model enables a "gap analysis" for each worker to be completed so that employers can then help the worker complete an individualized learning map to enable faster and more concise success. From this analysis, the platform will also be able to understand where possible KSA+T gaps are in individual courses so that feedback can be provided to individual institutions. Since the roles defined in the NICE framework are competency-based, the objective of this model (and resulting platform) will be to realize an individualized, competency-based learning platform.

Section 4: Number of faculty and student participants as a result of funding, and brief

description of student efforts.
Undergraduate students: For the reporting period, this project has funded an equivalent of 16 full student internships. Section 1 outlines various accomplishments of the team. Even without additional student hiring, we expect to enable 49 full internships in the project's first two years.

There are a total of three GAs and five Co-PIs working on the specific research areas of this grant. Specific Co-PI/GA accomplishments include paper development leveraging research using temporal graph neural network approaches to predict whether government organizations will be affected by a specific type of cyber attack and a survey paper around the detection of fraud in elections.

Prior published papers, including:

- Lakha, B., Mount, S., Serra, E., and Cuzzocrea, A. 2022 Anomaly Detection in Cybersecurity Events a Through Graph Neural Network and Transformer Based Model: A Case Study with BETH Dataset. BigData 2022; and
- Daley, B., Ratul, Q., Serra, E., and Cuzzocrea, A. GAPS: Generality and Precision with Shapley Attribution. Submitted. BigData 2022.

Are being refined to create a new anomaly detection model to consider anomalies in temporal structural patterns in graphs and we are planning to also include a more diversified source of cyber data to improve malicious behavior detection performances and scalability.

Section 5 : Updated details and/or progress on the long-term sustainability plan for the project and description of future plans for project continuation or expansion.

Federal, State, and private funding sources
Funding requests are being put forward in support of Governor Little's Cybersecurity Task Force objectives, of which PI Vasko was a member. The Cyberdome specific request included state appropriations equal to four (4) full-time support mentors, paid internships for up to 55 students across the state, and platform support for up to 18 rural communities. Barring changes from the President's Leadership Council (PLC) or other external factors, this effort is on-going with the new legislative session beginning in January, 2023.

Employer partners
PI Vasko is actively pursuing sustainable funding from employer partners for this program. Leveraging the identified "Activation Gap" thesis in our original proposal, employers are spending 6+ months activating new employees on methods and techniques. Under the thesis that the Cyberdome eliminates up to 3 months of that activation period, if an employer provides the Cyberdome between $10,000 - $15,000 as a gift, the employer potentially receives a tax-donation AND an employee that activates in their environment faster than ever before.

PI Vasko and our communication interns have developed, and are now initiating, a national outreach campaign to mid-sized Managed Security Service Providers (MSSPs) across the nation discussing this specific sustainability model. PI Vasko is also speaking at regional and national conferences on the results of the Cyberdome in shifting competency development back into the "academic sphere."

Section 6: Expenditure Report – Attach an expenditure report as a separate document showing expenses toward the original budget submitted for this project. The expenditure report does not count toward the page limit. A written summary of budget expenditures should be provided in section 2 of this report.

See attached expenditure report below. Explanation for line items that are under budget are provided in Section 2.

Expenditure Report

Expenditures through July 1, 2022 - November 15, 2022				
Category	**Annual Budget**	**Expenditures**	**Remaining**	**% Remaining**
Wages	$482,648.00	$196,031.67	$286,616.33	59.4%
Fringe/Benefits	$139,852.00	$30,250.23	$109,601.77	78.4%
Equipment and Other Expense	$77,500.00	$20,035.93	$57,464.07	74.1%
Total	$700,000.00	$246,317.83	$453,682.17	64.8%