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 _July 31, 2023_____ 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, the Cyberdome project has funded an equivalent of 32 full student internships. During this period, student workers from 5 of our public institutions, including Boise State University, College of Western Idaho, College of Eastern Idaho, Lewis Clark State College, and University of Idaho worked together to monitor & detect client issues.

Objective 2: Risk reduction for clients:

For the reporting period, our technology platform reported a total of 78,809 client alerts to our student workers covering 4,783 total monitored assets in our client community. From these alerts, the students were able to analyze the reported data and filter this information to 6,449 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 431 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) submitted a total of five papers, with one paper being selected for publication. The papers range across topics such as: anomaly detection in process execution, malware polymorphism mitigation, cybersecurity predictive models, useful certificateless email encryption, and election security. After examination of the changes in cybersecurity workforce development frameworks, coupled with industry advancements, we made the decision to stop any further refinement of the one technology licensing/transfer involving predictive individualized training for cybersecurity workers.

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

Building recurring (annual) penetration testing offering for clients with vulnerability scans. After a successful test, our student team established test endpoints with two of our longest standing clients and are almost ready to begin initial tests on the actual scanning and

reporting process. While establishing the network pieces - which has been the most complex part – this student team has also been working on establishing reporting automation processes, which are already complete enough to test. If our initial tests prove to be both successful and the product useful to our clients, we expect to deploy the process to all our clients the second half of 2023.

Continue development of the Virtual City/CyberRange as a training platform.
In recent weeks our “Manticore” public range environment underwent significant retooling in order to create isolate computing sets for our Idaho sister schools & programs to utilize as part of the Idaho Cyber Range (project name: Chimera). This involved significant development effort for all the individual components necessary to implement significant networking and system isolation. All pieces have been initially tested & verified to work.

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 nine active clients and nine prospective clients in varying stages of movement forward towards activation, far exceeding our original grant goal of five clients. Two of these prospective partners include the Idaho Secretary of State and Idaho Rural Education Association.

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 now includes 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. One such example is that automated reports being are pulled from Stellar via API and refinement of client deliverables is on-going.

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.
The table in Section 6 presents an expenditure report for the full-year of this period. An equivalent of thirty-two students, three graduate assistants, five faculty, and 2.5 full-time staff were directly supported by the grant in FY23. As in prior years, in FY23 we experienced a surplus in our Other Expenses (OE) due to much lower than anticipated Amazon Web Services (AWS) expenses. Our original grant proposal submitted in 2021 included an estimated $62,700 towards subscription and storage costs while actual expenses were just under $14,000. These surplus funds were used to pay for expenses including five months of effort from a full-time Engineering mentor and training materials to help interns work towards industry certifications.

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

A wide range of industry partners continue to express interest in supporting the Cyberdome's dual missions. Partners engaged in this period include: PlexTrac (www.plextrac.com), Sophos (www.sophos.com), AllPoints Logistics (www.allpointsllc.com); Secure-IoT (www.secureiot.com), Hyprfyre (www.hyprfire.com) CRI Advantage (www.criadvantage.com), Silent Sector (www.silentsector.com), and Shadowscape (www.shadowscape.io).

Economic Development via Jobs Created:

Since the beginning of the reporting period, 31 student workers responded to surveys indicating their expected wage over the next year. Out of those 31 respondents seven indicated that they already had accepted a job offer and reported an average salary of $51,666 per year. Those who had studied for either a bachelor's or master's degree reported a significantly higher salary of $75,000 compared to those with an associate's degree that report an expected annual salary of $42,000.

Additional funding received through leveraging the Cyberdome:

In the mid-year report, we identified 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

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:

After a detailed examination of the available solution landscape for individualized skill translation, combined with the recent update to the NICE workforce framework, it was decided to place any efforts for technology transfer on hold.

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 32 full student internships. Section 1 outlines various accomplishments of the team.

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 submission of a total of five papers, with one paper being selected for publication. The papers range across topics

such as: anomaly detection in process execution, malware polymorphism mitigation, cybersecurity predictive models, useful certificateless email encryption, and election security. Paper development continues leveraging research on 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.
Published papers, including:

- "Developing Accessible Email Encryption Using a Certificateless One-Way Key Agreement Scheme," 2023 4th Information Communication Technologies Conference, May 2023.

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 are executing on an outreach campaign to the Managed Security Service Providers (MSSPs) market across the nation, discussing the aforementioned sustainability model. PI Vasko is also speaking at regional and national conferences on the results of the Cyberdome enabling experiential learning for cybersecurity employers.

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

	Original Budget	**Revised Budget**	**FY23 Spend***
Salaries	$482,648.00	$526,244.00	$526,244.00
Benefits	$107,974.00	$100,100.00	$100,100.00
Capital Expense	$4,900.00	$7,000.00	$7,000.00
Other Expense**	$115,478.00	$77,656.00	$77,656.00
Annual Totals	$711,000.00	$711,000.00	$711,000.00

*Salaries and Benefits are projected numbers, but overspend is expected in both categories and will be handled via other funding sources with no impact to the HERC grant funds.

**The full-year budget takes into account a HERC approved carry-forward of $11,000 from 2022.