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 19, 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 17 students who began their internships in May and completed their internship experience on December 9, 2023. An additional two students were hired in July 2023 and will complete their internships in January 2024. 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 18,800 client alerts to our student workers covering 13,448 total monitored client assets. From these alerts, the students analyzed the reported data and filtered this information to 4,700 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 503 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 four papers, with three papers being selected for publication. Published papers range across topics such as: protecting data integrity for outsourced databases, email encryption methods, and nation-initiated cyber-attacks. Also, we are pursuing licensing discussions on integration work done by our students for possible technology transfer.

Status of other planned accomplishments from last year's report:
Building recurring (annual) penetration testing offering for clients with vulnerability scans. We continue working to establish a centrally-maintained and monitored vulnerability scanning tool. The technical challenges relating to the deployment of a vulnerability scanner that can effectively and expeditiously scan our clients' networks have largely been overcome, and we have successfully conducted several scanning tests with a client.

Our next step will be to work with our pilot client on reporting. We will use this process to establish baseline practices such as helping clients interpret the report and establish action items from it. Many of our clients have not had reporting materials like this before, and these reports can appear overwhelming at first glance. We expect this to be implemented in 2H FY'24.

Continue development of the Virtual City/CyberRange as a training platform.
The largest non-direct action/learning lab activity that was engaged in this year by Cyberdome interns was the development of a lab environment that simulates a "standard-issue corporate network" that we refer to as the "Virtual City." The lab environment currently holds virtual images of desktops, server and attacker environments, and can simulate a wide range of attack and defense scenarios. This project, developed in conjunction with NSA CAE funding received by Boise State’s Computer Science department, established a base framework for this virtual environment that we can duplicate and use for a variety of different types of activities.

We further built upon the Virtual City by creating a "SIEMulation Lab,” used to test a variety of security monitoring tools[1]. As part of their day-to-day efforts, interns use our SIEM, Stellar Cyber, to detect and categorize events of concern. However, our interns rarely get to see activity that they already know to be malicious. The SIEMulation Lab, enables attacks on a monitored network. Teams review the associated alerts these tools generate, and use that information to establish baselines for what different types of security concerns look like in the real world. This enriches our documentation, and allows our interns to clearly see alerts that are generated by the types of malicious activity they are looking for during their daily monitoring of our customers' networks.

Continue activating Cybedome clients.
Increasingly complex clients provide real world experience for our engineers and analysts as they architect and implement solutions. We have 11 clients and approximately 20 prospective clients in varying stages of movement forward towards activation, far exceeding our original grant goal of five clients.

Training improvements
The team continues to improve onboarding materials and training procedures for new students. For example, our initial Canvas course has been completely re-worked with direct student involvement. Further, a job-shadowing program has been implemented through which students are teamed together to exchange critical knowledge.

Other improvements include enabling workflows for self-sufficiency in the worker decision cycle. One key aspect of this effort is the formalization of “Tier Two Interns” that provide guidance and quality assurance on responses intended for clients.

Platform refinement & automation
Cyberdome engineers implemented a tool that integrates our ticketing platform into our

[1] *Also known as Security Information and Event Management (SIEM) tools.

primary monitoring tool. Workers are now able to log new issues with minimized effort; clients can see the status of and recommendations for important logged issues, and regular status reports and recommendations can easily be created from the issues documented inside our ticketing platform. This ongoing effort has been maintained through multiple revisions of the core environment, and is developed in such a way to continue to be usable even if our security tools change or expand.

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.

To date, our spend rate has been normal relative to our expectations and the first two years of this award. All salary spent on the grant has come from full-time staff, graduate assistants, and interns while Co-PI's are expected to include their effort in the Spring or early summer semester.

Costs associated with Other Expenses (software, AWS, and student certification expenses) continue to increase over time. In particular, AWS expenses have risen from just under $1,200/month in January 2023 to a projection of nearly $4,000/month in December 2023. This increase is due to exceeding the five Cyberdome clients projected in the original grant application. We now serve 11 clients and the increased storage and compute requirements have caused the budget increase. In 2H FY'24 we will exam storage cost models in order to align our client demand with short-term and long-term budget needs. At the moment, we project these costs to continue increasing month over month through the end of FY'24. We expect to consume the entire FY'24 budget.

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 mission. We are actively filtering partners based on showing a willingness to fit rural client risks and offer licensing for low-/no-cost.

Economic Development via Jobs Created:

Since the start of this reporting period, 24 interns have responded to surveys requesting anticipated wages. These surveys are completed during the final two weeks of the internship experience, while in the middle of job searches. At the time of the completion of these surveys, only three students had accepted full-time positions. Their reported wages were for $65,000, $85,000, and $98,000 per year (an average of $82,666/year). Additionally, the Cyberdome staff connected with a recent graduate that reported a new job offer of $78,000. All four interns were bachelor's degree seeking students.

Technology Transfer/Licensing Opportunity:

We are examining a possible licensing for integration work performed by a Cyberdome worker. This project improves worker efficiency by integrating workflow and messaging between operational platforms and is not currently offered in the marketplace.

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

Graduate students: Funding supports a total of three GAs and five Co-PIs working on research topics. Specific Co-PI/GA accomplishments include four papers being submitted with three selected for publication. Two GAs successfully defended their PhD thesis and/or presented papers at international conferences. The papers range across multiple topics (list provided below). Published papers include:

- Jyh-haw Yeh, Md Mashrur Arifin*, Ning Shen*, Ujwal Karki*, Yi Xie* and Archana Nanjundarao*. "Integrity Coded Databases - Protecting Data Integrity for Outsourced Databases," Computers and Security (Elsevier), Available Online October 2023, https://doi.org/10.1016/j.cose.2023.103569

- Jyh-haw Yeh, Srisarguru Sridhar* and K. Dakota White^. "Developing Accessible Email Encryption Using a Certificateless One-Way Key Agreement Scheme," 2023 4th Information Communication Technologies Conference, May 2023.

- Lakha, B., Duran, J., Serra, E., & Spezzano, F. (2023, October). Prediction of Future Nation-initiated Cyberattacks from News-based Political Event Graph. In *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 1-8). IEEE.

One additional paper received suggestions and is being re-submitted to other venues:

- "Detecting Anomalies in Voter Registration Data", Nahid Anwar and Amit Jain. Submitted to 2023 IEEE Intelligence and Security Informatics. Will resubmit to another venue.

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 submitted in support of Governor Little's Cybersecurity Task Force objectives, of which PI Vasko was a member. On-going funding requests include four full-time mentors, internships for 70 students, and platform support for up to 50 additional rural communities. This effort is on-going with the new January'24 legislative session.

Employer partners
PI Vasko's on-going efforts from employer partners for this program include leveraging the identified "Activation Gap" thesis in our original proposal. Under that thesis, the Cyberdome eliminates up to 3 months from an employee's activation period. If an employer provides the Cyberdome the resulting savings of between $10,000 - $15,000, the employer potentially receives a tax-donation AND an employee that activates in their environment faster than ever before. This messaging is on-going.

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.

Budget report for this period

	Original Budget	Projected* Mid-year Spend	Percent of Budget Spent
Salaries	$472,052.00	$217,012.40	46.0%
Benefits	$109,716.00	$33,471.26	30.5%
Other Expenses	$118,232.00	$39,368.14	33.3%
Totals	**$700,000.00**	**$289,851.80**	**41.4%**

*July 1st – December 8th, 2023