**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 _June 30, 2024_____ 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 funded an equivalent of 22 six-month long student internships. During this period, student workers from 7 of our public institutions, including Boise State University, College of Western Idaho, College of Eastern Idaho, Lewis Clark State College, North Idaho College, Idaho State University, 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 75,704 client alerts to our student workers covering 33,812 assets total monitored assets in our client community. From these alerts, the students were able to analyze the reported data and filter this information to 8,219 cases 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 834 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 and published a total of five papers. Published papers range across topics such as: protecting data integrity for outsourced databases, email encryption methods, and nation-initiated cyber-attacks. Further work is being done on identifying anomalous events within complex enterprise networks that host a variety of event sources.

Other accomplishments during this period

*Building recurring (annual) penetration testing offering for clients with vulnerability scans.*

We established 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 are now executing scans.

*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. The Canvas course material 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 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. Costs associated with Other Expenses (software, AWS, and student certification expenses) continue to increase over time. AWS expenses have risen throughout the period as a result of the increased number of Cyberdome clients exceeding the five Cyberdome clients projected in the original grant application. In 2H FY'24 we examined storage cost models to align our client demand with short-term and long-term budget needs. We expect to consume the entire FY'24 budget.

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

**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 beginning of the grant period in July 2023, twelve departing interns responded to surveys indicating that they had accepted a full-time job offer and reported their salaries. The median wages for these students were $70,000. The median wage for those with a bachelor's or master's degree was $70,000 while those with an associate's degree earned $46,800.

Grants Received

Four Federal grants leverage the Cyberdome data/platform. 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. Finally, Boise State is the recipient of a $3.2M NSF Scholarship for Service (SFS) grant and a recurring DoD Cybersecurity Scholarship Program (CySP) scholarship. The Cyberdome was a key differentiator for our grant applications.

Technology Transfer/Licensing Opportunity:

We examined the possibility of licensing integration work performed by a Cyberdome worker and found this to not be a viable solution.

**Section 4:** Number of faculty and student participants as a result of funding, and brief description of student efforts.

Student Participation

Funding has sponsored 22 student internships; Section 1 outlines various accomplishments of the student team. Three Graduate Assistants (GAs) are also supported by this project.

Faculty / GA Participation

There are a total of three GAs and four Co-PIs working on the specific research areas of this grant. Specific Co-PI/GA accomplishments include

- Utilizing our VirtualCity environment to tackle the challenge of identifying anomalous events within complex enterprise networks that host a variety of event sources. This team recently submitted a paper detailing a new system that excels in automatically detecting anomalies from multiple event sources, outperforming existing methodologies (named Captor). Further, this research extends to the automated interpretation of these anomalous events through the utilization of artificial intelligence.
- Further research on forecasting targeted attacks from adversarial nations based on news and conflict data. A particular emphasis on targeting specific organizations or

types is now underway. This approach involves integrating detailed textual descriptions of organizations with news data to enhance the precision of predicting targets beyond mere country-level analysis.

Paper Submitted / Published

A total of five papers were submitted and published in this period. 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.

Published papers / submitted, 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.
- " Unveiling the Efficacy of BERT's Attention in Memory Obfuscated Malware Detection," to the *19th International Conference on Information Security Practice and Experience (ISPEC 2024),* which will take place in October 2024.
- 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.
- Detecting Anomalies in Voter Registration Data", Nahid Anwar and Amit Jain. Published and presented at 8th Annual Summer Conference on Election Science, Reform, and Administration on 16-17th May at University of Southern California

Other accomplishments during this period:

Two GAs successfully defended their PhD thesis and/or presented papers at international conferences. 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.

**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 have been 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 70 students across the state, and platform support for up to 70 rural communities. Further collaboration occurs with Idaho Office of Emergency Management (IOEM) for funding related to cybersecurity support for rural & underserved communities.

**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**

| | Revised Budget | Projected Spend | Projected Funds Remaining |
|---|---|---|---|
| Salaries | $476,008.85 | $476,008.85 | 0% |
| Benefits | $86,603.56 | $86,603.56 | 0% |
| Other Expenses | $130,387.59 | $130,387.59 | 0% |
| Capital Equipment | $7,000.00 | $7,000.00 | 0% |
| **Totals** | $700,000.00 | $700,000.00 | 0% |

*Projected spend includes anticipated expenses incurred through 6/30/2024; $624,398 of this budget has been spent as of 6/3/2024.