CEDAR Lab Research Project

THREAT INFORMATION ASSISTANT (TIA)

Basic Information

Project Lead	Alicia Thoney	Team Size	3-5
Group	TIA	Meeting Time	TBD
Start Date	June 2022	End Date	September 2022

Project Description

The Threat Information Assistant (TIA) is a web application that compiles and displays vulnerabilities associated with a specific software or hardware configuration. The user will provide a configuration and TIA will represent the cyber-threat information (CTI) using the Structured Threat Information eXpression (STIX) language.

Context

As our technological dependencies strengthen, it is no secret that cybersecurity threats and attacks are on the rise. According to an article on cybersecurity Ventures, global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025 [1]. "This represents the greatest transfer of economic wealth in history […] and will be more profitable than the global trade of all major illegal drugs combined" [1]. Due to the staggering cost of cybercrime, the ability to defend, monitor, and understand the cybersecurity world is critical. "For cyber analysts, having the right information, in context, when most needed without cognitive overload could lead to effective decision making in cyber operations" [2]. Aggregating mass amounts of data and displaying said data in a digestible fashion will immensely help cyber analysts and infrastructure maintainers make educated decisions about their products. "In recent years, visualization has emerged as a promising technique to better equip analysts to operate effectively in an evolving digital threat landscape" [3].

Contributions

This project adds a new research avenue to the CEDAR lab. While the focus of this topic is not novel, the addition of a full stack application offers students experience in a new field of computer science. Moreover, students adapt in full stack development could contribute to future lab and university project needs.

Project Goals / Objectives

Goals	Ideal Date	Progress
Delegate Tasking, Learn	June 10	In Progress
Create Full Stack Framework	June 17	In Progress
Load CISA Vulnerabilities	June 17	Not Started

Goals	Ideal Date	Progress
Integrate STIX Graphing Library	June 24	Not Started
Graph Config and Vulns	July 1	Not Started
Graph ATPs and Malware	August 1	Not Started
Integrate Data Analysis	August 15	Not Started
Integrate Front-End Framework (React)	August 31	Not Started

Skills Explored / Lessons to Learn

The following skills will be explored during the project, we will learn:

- Front-end development (HTML/CSS, JavaScript, Bootstrap)
- Back-end development (Go)
- Data Management and Analysis

In-Lab Benefits

This project will benefit the following projects in the following ways:

- TIA: The lab will be able to use this resource as a means to maintain and prioritize asset updates. Through some data compilation, we can easily decide what infrastructure is more vulnerable and actively attacked and update accordingly.
- Extension: Once the initial development phase is completed, there will be significant room for improvement and extension.
    - Introducing user accounts
    - Storing previous STIX graphs from configurations
    - Enriching STIX graphs with data like attack patterns/campaigns
    - Increasing data aggregation and analysis

Benefits Beyond the Lab

This project will benefit researchers beyond the lab in the following ways:

- Service for infrastructure security

Resources Required

People	3-5 Undergraduate Researchers, 1 graduate mentor
Skills	Software development, cybersecurity information understanding
Materials	None
Time	3 months
Monetary Support	None
Other	N/A

References

[1] Morgan, S. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved June 7, 2022, from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] C. Inibhunu et al., "Adapting level of detail in user interfaces for Cybersecurity operations," 2016 Resilience Week (RWS), 2016, pp. 13-16, doi: 10.1109/RWEEK.2016.7573300.

[3] *Diane Staheli, Tamara Yu, R. Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna, and Lane Harrison. 2014. Visualization evaluation for cyber security: trends and future directions. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security (VizSec '14). Association for Computing Machinery, New York, NY, USA, 49–56. https://doi-org.libproxy.uwyo.edu/10.1145/2671491.2671492*