TIA: Threat Information for Your Most Severe Vulnerabilities

Your Best Friend In The Digital Age

Summer 2022

Team Members


William Frost


Jenna Goodrich


Ally Hays


Francis Korsah


Alicia Thoney


Calvin VanWormer


Marc Wodahl

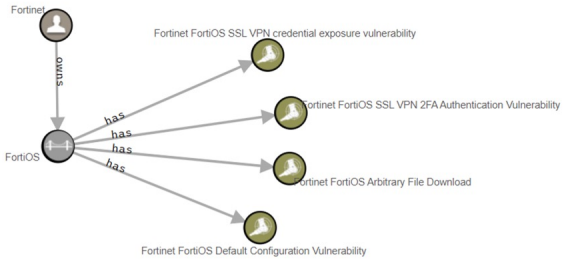

Shawna Wolf

Problem Statement

This research involves the development of a web application that compiles and graphically displays vulnerabilities associated with a specific software or hardware configuration.

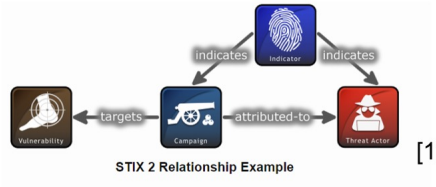
Results

Currently, TIA can generate 359 unique STIX graphs to represent CTI from 134 vendors and 351 products.



Background

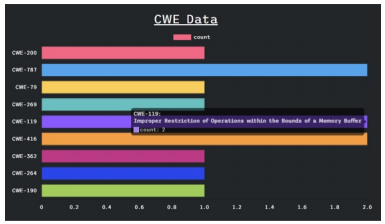
STIX: Structured Threat Information eXpression can be represented visually for an analyst or stored as JSON and machine-readable
CTI: Cyber Threat Information
CWE: Common Weakness Enumeration
Vendor: An organization
Products: Commodities owned by a vendor

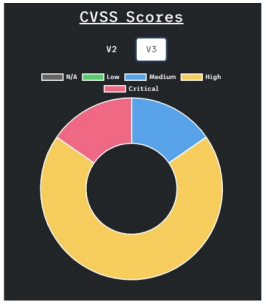


STIX 2 Relationship Example [1]

Methods

After selecting a vendor and product, three forms of CTI are returned: a table representing the known exploited vulnerabilities, CWEs and severity scores charts, and a graph generated with the STIX language.

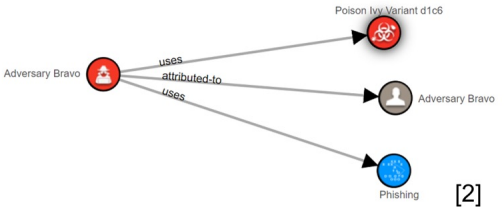




Challenges & Future Work

Future work includes:

- Enrichment of STIX graphs
- Integration of INL IX-Discovery Tools
- Serverless functionality



[2]

Advisor: Dr. Mike Borowczak
Project Lead: Alicia Thoney
Group Members: Allyson Hays, Calvin VanWormer, Francis Korsah, Jenna Goodrich, Marc Wodahl, Shawna Wolf, William Frost

[1] https://oasis-open.github.io/cti-documentation/stix/intro.html
[2] https://oasis-open.github.io/cti-documentation/stix/gettingstarted.html

University of Wyoming
UW College of Engineering and Physical Sciences
UW Cybersecurity Education and Research Center
UW School of Computing
UW College of Engineering and Physical Sciences Electrical Engineering and Computer Science
CEDAR