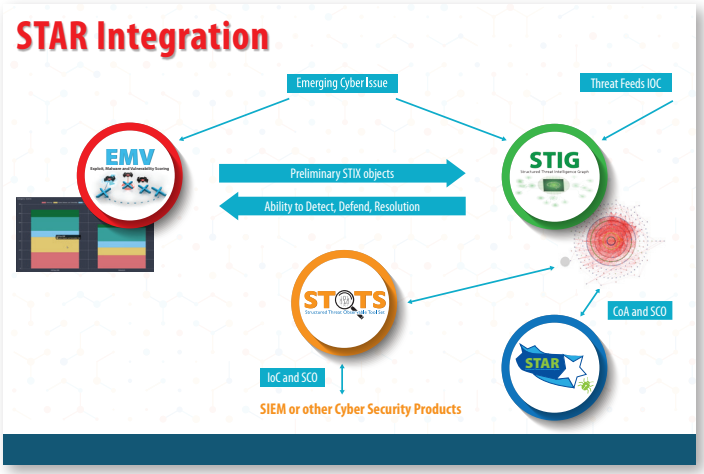
Structured Threat Automated Response (STAR)

Provides a flexible framework to automatically execute courses of action in response to received cyber observable data objects. Based on the Structured Threat Information eXpression (STIX) v2.1, STAR enables the execution of tailored responses to cyber issues in an operational environment.

STAR provides a framework by which STIX formatted Courses of Actions can be loaded into a Python based web server for later execution. The execution of which is determined by the content of the associated STIX formatted Observable Data that is later uploaded to the same web server. This provides a simple and effective means for rapidly importing STIX courses of action and executing responses once a corresponding cyber observable is received. Integrating STAR with STOTS (Structured Threat Observable Toolset) for the just-in-time indication of cyber observables and the advanced graph analysis capability of Structured Threat Intelligence Graph (STIG) application provides a robust and flexible automated response environment. The cyber issue analysis and risk management application Exploit, Malware and Vulnerability Scoring (EMV) enables the tracking and prioritization of cyber issues with the creation of STIX objects for refining in STIG, indication in STOTS and response in STAR. STAR provides the final critical step of executing response enabling a method for managing ongoing/potential cyber incidents in a machine to machine automated threat response capability.

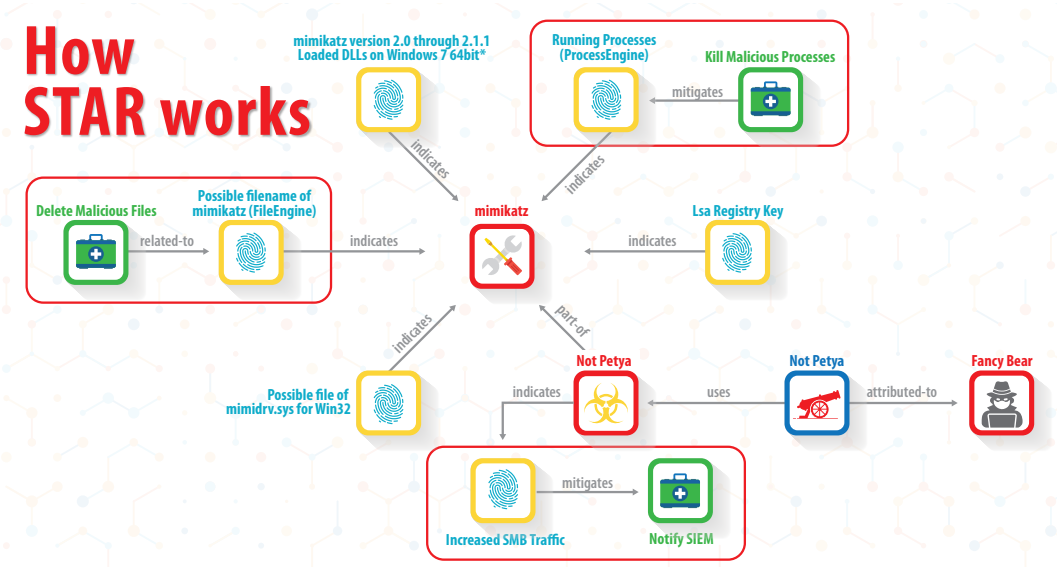
EMV Scoring and STIG provides the analytical capability to prioritize cyber issues and create sharable, actionable and implementable structured threat using advance graph analytics enabling a visual representation for ease of communication across stakeholders in charged to defend our nation's critical infrastructure. EMV creates skeleton STIX objects that can be tailored and programmed in STIG acting as a visual programing tool producing STIX validated objects and relationship. STOTS is the utility tools set that provides an interface to other cyber security products, create tailored indication of potential or active cyber issues to gain the cyber artifact or observable enabling response. STAR provides the capability to act on the indicators and related cyber observables though courses of action created in STIG. These modular tools can function independently without integration for a surgical and tailored indication and response or be interfaced through the STIX standard for inherent advanced analytical capabilities in cyber security products.



STAR is part of larger applications and tool sets for machine to machine automated response

STAR was developed by INL as part of the Validation and Measuring Automated Response (VMAR) project which was funded by the Department of Energy Cybersecurity of Energy Systems and Emergency Response (DOE-CESER) and is a collaborative effort with San Diego Gas & Electric (SDG&E).

Idaho National Laboratory



Examples of Indicator/Course of Action Pairs used by STAR

Being able to automatically respond to any threat that appears on an Operational Technology or Information Technology network has long been desired as a way to protect critical systems and networks which STAR enables. STAR provides a modular and flexible framework for executing STIX based courses of action in direct response to the receipt of a STIX based observable data event.

Currently STAR has the ability to execute courses of actions which contain fully developed Python code. When a Python based course of action is triggered it is executed to completion in a separate process which allows STAR to continue accepting and processing other incoming observable data. Python provides the flexibility to develop any number of remediation techniques. These can include firewall rule modification, port blocking, device configuration changes, security team notification, and/or advanced system logging and other potential indications based on the STOTS modules.

STAR's development is currently in a proof of concept phase (TLR 3). Functionality is currently limited, yet STAR was been designed in such a manner as to be able to easily add or enhance its existing capabilities. STAR's proof of concept will enable more automated response functionality. Open sourcing STAR will enable future enhancements which may include integration with existing commercial SEIM software as well as development of a GUI (Graphical User Interface) to load STIX objects and monitor actions taken.

Impact

Various tools and techniques exist for a system to respond in the event of an intrusion or attack. The advantage that STAR has over its competition is that it is cross platform, modular, flexible, and light weight. If a particular response is not sufficient for the intrusion detected a new more robust response can be quickly written and implemented with minimal effort.

STAR provides a framework to automatically execute STIX based courses of action in response to received STIX based observable data objects.

For more information

Robert M. Caliva
Program Manager
208-526-8238

Bryan Beckman
Senior Infrastructure Security Software Developer with Brigham Young University
Intern Aaron Cowley
208-526-1111

Rita Foster
Infrastructure Strategist & Technical Lead
208-526-3179

www.inl.gov

github.com/idaholab/star

A U.S. Department of Energy National Laboratory

20-50510_R2