IDAHO NATIONAL LABORATORY INNOVATION SHEET

Structured Threat Intelligence Graph (STIG)

STIG is a unique means to easily share threat information with owners and operators of the critical infrastructure sectors.

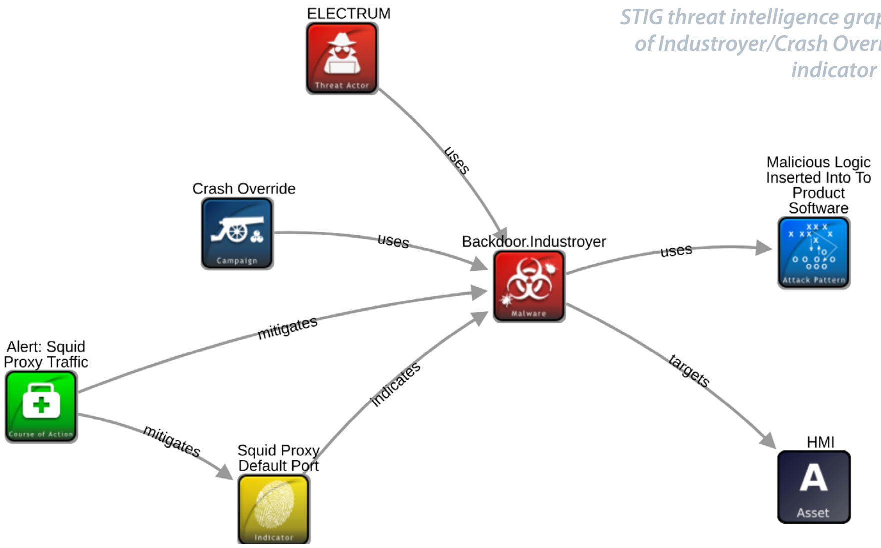
Shared threat information is essential for the protection of critical infrastructure from today's cyber adversary. However, that information is too complex and cumbersome, which hampers its application in the operational environment. Security information and threat intelligence sharing is a long-standing grand challenge. Mechanisms for sharing this information have been inadequate for many reasons, including the inability to encompass all types of information or provide context, not well-suited to indexing and querying, inflexible, not parseable or extensible, and too burdensome. As a result, threat analysts spend too much time normalizing the data before they can perform their analysis. Without a common tool set to analyze, relate and share findings, critical infrastructure owners and operators work separately and suboptimally in the face of detecting, protecting and mitigating cyberattacks.

The Idaho National Laboratory-developed tool, Structured Threat Intelligence Graph (STIG), enables sharing actionable threat information that can be applied in the operational environment. It provides a threat analysis capability with easy-to-use visual programming, facilitating the process of creating, editing, analyzing and querying Structured Threat Intelligence eXpression (STIX) with graph theoretic queries. STIG's ability to visualize relationships between threat characteristics, exploit indicators and courses of action is unparalleled for analyzing threat intelligence.

Beyond Actionable Threat Intelligence

STIX v2 provides a context-rich standard that can be tailored for installation specifics.

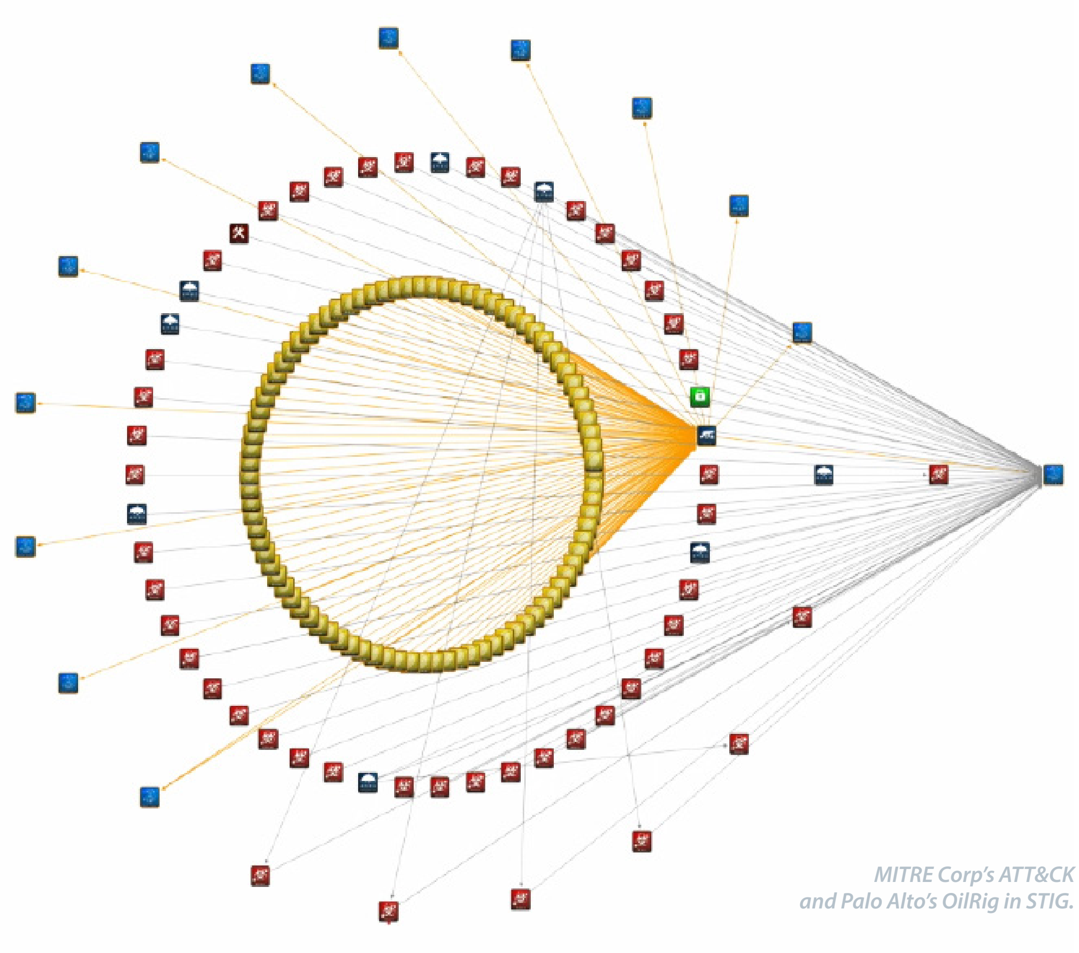
Southern California Edison, a primary member of the California Energy Systems for the 21st Century (CES-21) Program, championed the research at INL leading to the development of STIG. Seeing the potential for wider application of structured threat sharing, the California Public Utilities Commission (CPUC) is reviewing a request to open source STIG. This technology applies graph theory to provide a threat analysis capability with uniquely easy-to-use visual programming. Contributing to a CES-21 objective, STIG simplifies the development of machine readable and actionable industrial control system indicators of compromise and remediation actions.



STIG threat intelligence graphical representation of Industroyer/Crash Override malware with an indicator and course of action.

This rich context provides actionable threat information to be shared across energy sector stakeholders. Beyond actionable, validated STIX-compliant JavaScript Object Notation (JSON) code can be applied to the operational environment. The need for an analysis tool to share security threat information and intelligence has escalated and existing tools have proven to be inadequate. STIG has a graph database back end to allow highlighting of related threat data objects to focus on the most critical areas concerning the analyst in visual display, rather than reading thousands of lines of code to identify these relationships. STIG's graph data model offers scalability, visual discovery of relationships without complex queries (see OilRig figure), easy collaboration between analysts, and the ability to populate the database dynamically – meeting the dynamic nature of today's cyberthreat.

STIG provides a threat analysis tool based on the graph nature of the international standard STIX v2. This context-rich standard provides usable information focused on the relationships between the data objects. The STIG tool creates STIX-validated JSON code or imports partial STIX objects into the graph view for further relationship development.



MITRE Corp's ATT&CK and Palo Alto's OilRig in STIG.

For more information

Robert M. Caliva
Program Manager
208-526-8238
Idaho National
Engineering Laboratory

Jed Haile
Senior Cybersecurity
Researcher & STIG Developer
208-526-4616

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

www.inl.gov

A U.S. Department of Energy
National Laboratory