Structured Threat Observable Toolset (STOTS)

Provides an effective defense for the nation's critical infrastructure systems through situational awareness, and details of the activity in a system. STOTS provides a platform agnostic, open, and scalable toolset to help gain the insight and knowledge necessary to stay ahead of the dangers targeting our critical infrastructure.

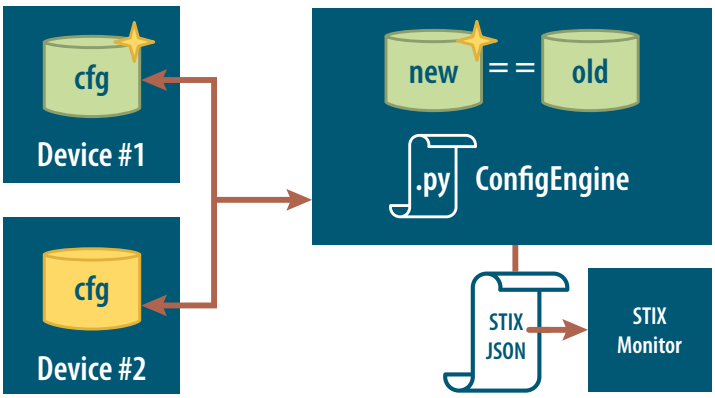
Timely detection and situational awareness are essential for the protection of critical infrastructure from today's cyber adversary. However, doing so often relies on closed, proprietary systems running continually on remote network nodes. STOTS changes this by introducing a framework, which provides an open standard using Structured Threat Information eXpression (STIX v2) as well as the ability to provide just-in-time collection and analysis for remote systems.

STOTS was originally developed by INL as part of the larger California Energy Systems for the 21st Century (CES-21) Program for SCE with further development championed by Pacific Gas & Electric (PG&E)

Developed by Idaho National Laboratory, STOTS provides a platform-agnostic, customizable and scalable toolset that can provide the user with increased awareness and ability to detect malicious activity occurring within networks, hosts or embedded systems. Using STIX allows the flexibility to share detected artifacts with others, utilize a standard format across all STOTS components and provide results that can be easily read and understood by both computers and operators.

On-Demand Standardized Artifacts

STIX provides a context-rich standard that can be tailored for specific roles and uses. This rich context allows for malicious artifacts to be shared across energy sector stakeholders in order to enhance each other's stance with respect to cyber security.



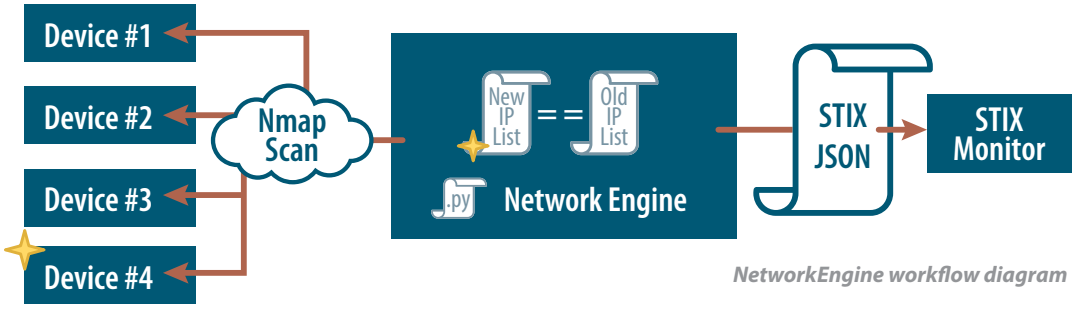
ConfigEngine workflow diagram

STOTS provides a collection of detection and monitoring tools based on the international standard STIX. This context-rich standard provides usable information which can be shared with others and fed to a unified STIX monitor for immediate logging and remediation. STOTS provides customizable on-demand monitoring capabilities to both information technology and operational technology environments.

STOTS currently provides the following features through various engines detailed below:

- **ConfigEngine**
  - Detects internal device configuration file changes made to hardware
- **NetworkEngine**
  - Identifies the addition of unknown/unplanned devices attaching to a network
  - Alerts when a device is suddenly removed from a network or loses connectivity
- **ProcessEngine**
  - Checks for the presence of known malicious processes running on a remote system
  - Notifies when a system critical process is no longer running on remote equipment

Idaho National Laboratory



NetworkEngine workflow diagram

STOTS

Structured Threat Observable Tool Set

- **PacketEngine**
  - Provides deep packet inspection of all traffic traversing a network
- **SyslogEngine**
  - Generates critical event entries from standard locally collected Syslogs
- **FileEngine**
  - Identifies additions, deletions, and other changes to remote files within a monitored directory
- **CommandLineEngine**
  - Identifies undesired or malicious shell commands being executed on a remote system

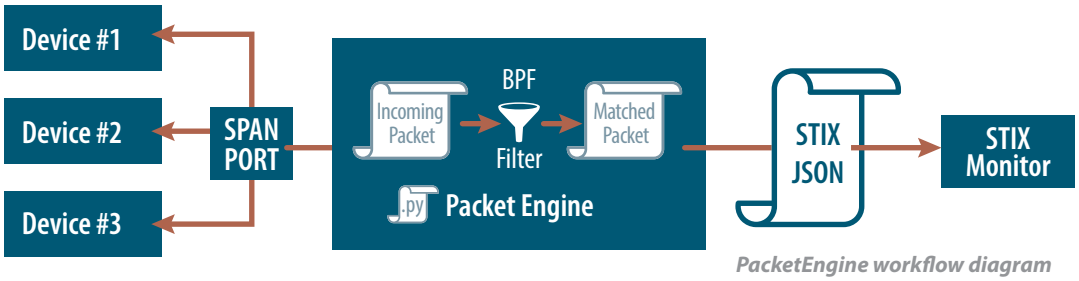
Existing cyber security technologies either utilize propriety formats to detect artifacts or choose to abstract attack behavior details from the user. Existing tools rely heavily on agent-based software that must be actively running on each system that requires monitoring.

STOTS provides the advantage of utilizing a standard STIX format for each detected artifact as well as being designed for just-in-time on-demand polling of only the needed STOTS components – eliminating the need for continuous monitoring and analysis of remote devices.

STOTS configured with a STIX based artifact monitor is capable of on-demand remediation providing a flexible, robust, open, expandable, customizable, and capable alternative to existing proprietary security solutions.

STOTS was originally developed by INL for SCE as part of the larger California Energy Systems for the 21st Century (CES-21) with further development championed by Pacific Gas & Electric (PG&E).

This technology applies the open and flexible STIX standard, enabling monitoring of malicious activity and discovering current applicability to cyber alerts. STOTS provides the needed alternative to current complex, proprietary system monitoring solutions.



PacketEngine workflow diagram

For more information

Robert M. Caliva
208-526-8238
robert.caliva@inl.gov

Bryce McClurg
208-526-4990
bryce.mcclurg@inl.gov

Rita Foster
208-526-3179
rita.foster@inl.gov

www.inl.gov

github.com/idaholab/stots

A U.S. Department of Energy National Laboratory

19-50503-R7