OWASP
Open Web Application Security Project

Threat Intelligence

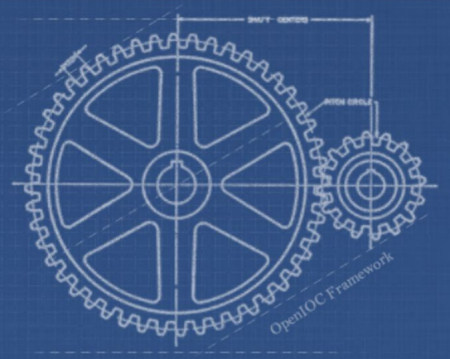
Sherif Mansour

Threat Intelligence is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it...

OpenIOC

An **Open Framework** for **Sharing Threat Intelligence**

Sophisticated Threats Require Sophisticated Indicators



Overview

In the current threat environment, rapid communication of pertinent threat information is the key to quickly detecting, responding and containing targeted attacks. OpenIOC is designed to fill a void that currently exists for organizations that want to share threat information both internally and externally in a machine-digestible format. OpenIOC is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise.

OpenIOC was originally designed to enable MANDIANT's products to codify intelligence in order to rapidly search for potential security breaches. Now, in response to requests from across the user community, MANDIANT has standardized and open sourced the OpenIOC schema and is releasing tools and utilities to allow communication of threat information at machine speed.

Why OpenIOC?

Sophisticated Indicators

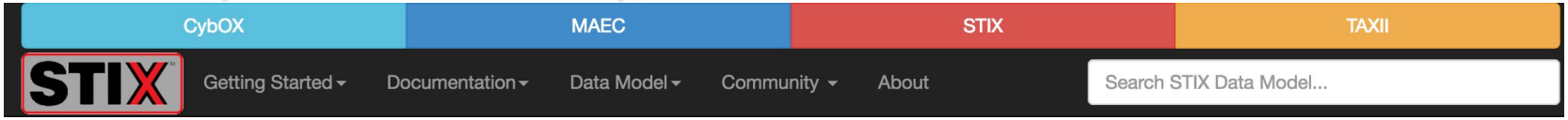
Traditional methods of identifying security breaches no longer work. Simple signatures are too easy for an intruder to circumvent. Organizations need to be able to communicate how to find attackers on their networks and hosts using a machine digestible format that removes human delay from intelligence sharing.

Advanced Threat Detection

By using the OpenIOC framework, you will have the most advanced threat detection capability available. By joining the OpenIOC community, your organization can benefit from the network effect of threat intelligence from organizations within your industry, as well as global Fortune 1000 companies.

Extendable & Customizable

By allowing for extensions and customization, OpenIOC offers your organization the option of using MANDIANT's field tested Indicators of Compromise, as well as creating your own custom sets of indicators, and any combination thereof that you need to complete your mission.



STIX transitioned to OASIS - an open standards organization. **Read the FAQ to learn more.**

Structured Threat Information eXpression (STIX™)

A structured language for cyber threat intelligence.

Download Current Release

Other Downloads

See Examples & Idioms »

New! Help build STIX 2.0!

Community

Join the OASIS TC to help build this growing, open-source industry effort. See who's already using STIX.

Documentation

Dig a little deeper and learn about suggested practices, and other documentation. Or, Follow our blog to get latest STIX news straight from the source.

Tooling

Bindings & APIs

python

Java

Tools and Utilities

GitHub

Have questions, comments, or feedback?

Reach out to us at stix@mitre.org!

facebook for developers | Producten | Documenten | Tools & Support | Nieuws | Video's | Zoeken | Aanmelden

ThreatExchange

Learn about threats. Share threat information back. Everyone becomes more secure.

Apply for the Beta

Scale your intelligence

Threats like malware and phishing will often attack many targets. Safeguard yourself using shared intelligence from other particpants.

Overview

Threatbutt About Careers Contact

Threatbutt

Defense in derpth™

Maximum protection from threatening threaty threats like

cyber hacking

Winner of the RSA Conference "best vendor" award!

What Can Threat Intel Tell Me?

1. Information about "bad actors”

- **Public Threat Feeds**
- **Private Threat Feeds**

2. Alerting if your org is listed as a bad actor

3. TTP Tactics, Techniques, Procedures

Information about "bad actors”

- Origins – IPs/ASN/Domains
- Compromised Organizations / accounts
- Malware signatures etc..

Alerting if your org is listed as a bad actor

If you find this, you are having a bad day!

TTP Tactics, Techniques, Procedures

- Learning from other's grief!
- Allows you to check if your org is prepared for defending, detecting such campaigns

What can go wrong?

- Poor data quality
- False positives
- Unable to leverage data – difficult to integrate