Indicators of Compromise Explained

Blue Team Level 1 Certification (Standard) > TI3) Operational Threat Intelligence > Indicators of… IN PROGRESS

Indicators of compromise are a core part of threat intelligence, and allow us to share information on threats in several different formats. This information is used to power intrusion detection and prevention systems, endpoint detection and response systems, firewalls, and other automated defenses. Human analysts can also use these to perform threat exposure checks against their environments to identify the early, or late, signs of a cyberattack.

EXAMPLES OF IOCS

Below is a list of typical indicators of compromise that are shared publicly and between organizations.

- **Email Addresses –** These are mailboxes that have been acting maliciously, such as sending emails containing malicious URLs, malicious attachments, or attempting to socially-engineer email recipients into taking actions they wouldn't usually take such as giving out information.
- **IP Addresses –** These IPs have acted maliciously, such as performing unauthorized port or vulnerability scans, hosting malicious content or websites, or have been linked to malicious actor infrastructure such as command-and-control (C2) servers. WHOIS lookups can also be conducted to gain more information, such as who owns the IP, where it's geographically based, hostname, and occasionally contact details.
- **Domain Names/URLs –** Sites that have been acting maliciously, such as hosting malware, phishing sites, or other malicious content.
- **File Hashes/File Names –** We can easily share intelligence about malware or other malicious files, often by referring to them by their unique hash values (typically MD5, sha256, or sha1). These can be used by security teams to blacklist the specific file hashes so that they are detected and deleted by security solutions such as endpoint detection and response (EDR).

IOC FORMATS

STIX and TAXII are a common method of sharing threat intelligence, such as indicators of compromise. These values alone don't mean a lot, but with STIX we can share information in a structured format, providing a lot more than just lists of IOCs.

STIX:

Structured Threat Information eXpression, or STIX, was developed by MITRE and the OASIS Cyber Threat Intelligence Technical Committee as a standardized language for sharing threat information. For some organizations and information sharing committees this has been the standard and is widely used. Whilst STIX is designed to be used in conjunction with TAXII, it can be shared without it. STIX is designed to share not just IOCs, but also threat:

- Motivations
- Abilities
- Capabilities
- Response

You can read more about STIX at this link – https://oasis-open.github.io/cti-documentation/stix/intro.html

MITRE have also provided some examples of indicators in STIX format, so you can get a feel of what STIX looks like here – https://stix.mitre.org/language/version1.0.1/samples.html

TAXII:

Trusted Automated eXchange of Intelligence Information, or TAXII, defines how cyber threat information can be shared by using services and message exchanges. Designed to handle STIX information, this platform is run on a server and allows the sharing of information between specified groups or provide a public "threat stream" that individuals can sign up to and receive intelligence.

You can read more about STIX and TAXAII at this link – https://medium.com/sekoia-io-blog/stix-and-taxii-c1f596866384

Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic