Threat Data Intelligence

Introduction

Threat intelligence is the set of activities and resources available to cybersecurity professionals seeking to learn about changes in the threat environment.

Building a threat intelligence program is a crucial part of any organization's approach to cybersecurity.

Threat intelligence information can also be used for predictive analysis to identify likely risks to the organization.

Threat feeds are intended to provide up-to-date detail about threats in a way that your organization can leverage.

Feeds often include technical details about threats, such as IP addresses, hostnames and domains, email addresses, URLs, file hashes, file paths, CVE numbers, and other details about a threat.

Vulnerability databases are also an essential part of an organization's threat intelligence program.

Threat intelligence sources may also provide indicators of compromise (IoCs).

IoCs are the telltale signs that an attack has taken place and may include file signatures, log patterns, and other evidence left behind by attackers.

Open Source Intelligence (OSINT)

Open source threat intelligence is threat intelligence that is acquired from publicly available sources.

Sites that maintains up-to-date lists of open source intelligence sources

- http://www.senki.org/operators-security-toolkit/open-source-threat-intelligence-feeds
- https://cybersecurity.att.com/open-threat-exchange
- http://www.misp-project.org/feeds
- threatfeeds.io

Government Sites that provide open source intelligence

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) site: www.us-cert.gov
- The U.S. Department of Defense Cyber Crime Center site: www.dc3.mil
- The CISA's Automated Indicator Sharing (AIS) program, www.dhs.gov/cisa/automated-indicator-sharing-ais, and their
- Information Sharing and Analysis Organizations program, www.dhs.gov/cisa/information-sharing-and-analysis organizations-isaos

In addition to threat intelligence vendors and resources, threat intelligence communities have been created to share threat information.

Vendor Websites

- http://www.microsoft.com/security/blog/tag/threat-intelligence
- http://tools.cisco.com/security/center/home.x
- http://talosintelligence.com/

Other Public Sources

- http://isc.sans.org/
- http://virusshare.com/
- http://www.spamhaus.org/

Proprietary and Closed-Source Intelligence

Commercial security vendors, government organizations, and other security-centric organizations also create and make use of proprietary, or closed-source intelligence.

They do their own information gathering and research, and they may use custom tools, analysis models, or other proprietary methods to gather, curate, and maintain their threat feeds.

There are a number of reasons that proprietary threat intelligence may be used. like keeping the threat data secret, selling or licensing it, or reduce the chance of the threat actors knowing about the data they are gathering.

Commercial closed-source intelligence is often part of a service offering.

Validating threat data can be difficult in many cases.

The Dark Web

The sudden appearance of credentials on dark web marketplaces likely indicates that a successful attack took place and requires further investigation.

Threat intelligence teams should familiarize themselves with the dark web and include searches of dark web marketplaces for credentials belonging to their organizations or its clients.

The dark web is a network run over standard Internet connections but using multiple layers of encryption to provide anonymous communication.

Hackers often use sites on the dark web to share information and sell credentials and other data stolen during their attacks.

Assessing Threat Intelligence

Regardless of the source of your threat intelligence information, you need to assess it.

Common assessment factors

- Is it timely? A feed that is operating on delay can cause you to miss a threat, or to react after the threat is no longer relevant.
- Is the information accurate? Can you rely on what it says, and how likely is it that the assessment is valid? Does it rely on a single source or multiple sources? How often are those sources correct?
- Is the information relevant? If it describes the wrong platform, software, or reason for the organization to be targeted, the data may be very timely, very accurate, and completely irrelevant to your organization.

Confidence scores allow organizations to filter and use threat intelligence based on how much trust they can give it.

- Low confidence threat information shouldn't be completely ignored, but it also shouldn't be relied on to make important decisions without taking the low confidence score into account.
- Different scores are used by different organizations

Threat Maps

- Threat maps provide a geographic view of threat intelligence.
- Many security vendors offer high-level maps that provide real-time insight into the cybersecurity threat landscape
- Organizations may also use threat mapping information to gain insight into the sources of attacks aimed directly at their networks.

Attackers often relay their attacks through cloud services and other compromised networks, hiding their true geographic location from threat analysis tools.

This information should always be taken with a grain of salt because geographic attribution is unreliable.

Threat Indicator Management and Exchange

Managing threat information at any scale requires standardization and tooling to allow the threat information to be processed and used in automated ways.

Structured Threat Information eXpression (STIX) is an XML language originally sponsored by the U.S. Department of Homeland Security.

STIX 2.0 defines 12 STIX domain objects

Threat Feed Combining

Using a single threat feed can leave you in the dark! Many organizations leverage multiple threat feeds to get the most up-to-date information.

Thread feed combination can also be challenging since they may not use the same format, classification model, or other elements.

Programming Languages like STIX or Open Indicators of Compromise (OpenIOC) can be used to mitigate these issues

STIX

- STIX is an XML-based framework
- Managed by the Organization for the Advancement of Structured Information Standards (OASIS)
- Usually combined with Trusted Automated eXchange of Indicator Information (TAXII) protocol
  - Intended to allow cyber threat information to be communicated at the application layer via HTTPS.
  - Specifically designed to support STIX data exchange.

OpenIOC

- OpenIOC is an XML-based framework
- The OpenIOC schema was developed by Mandiant, and it uses Mandiant's indicators for its base framework.

Conduct Your Own Research

As a security professional you should always stay up-to-date and conduct your own research

Resources

- Vendor security information websites
- Vulnerability and threat feeds from vendors, government agencies, and private organizations
- Academic journals and technical publications, such as Internet Request for Comments (RFC) documents. RFC documents are particularly informative because they contain the detailed technical specifications for Internet protocols.
- Professional conferences and local industry group meetings
- Social media accounts of prominent security professionals