UNFETTER

The Unfetter Project utilizes several data types to support several workflows for cyber security professionals. Some of those data types are from the Structured Threat Information eXpression (STIX™) structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner.

VERSION 1 / NOVEMBER 2018

Assessments

A survey of the Indicators (analytics) and Sensors (monitoring software) that your organization implements and to what level. Unfetter uses the survey to help users understand gaps, their relative importance, and which should be addressed.

Unique to Unfetter
(not in STIX)

Attack Patterns

A type of TTP* that describes behaviors and actions adversaries may take in your network. Attack Patterns are used to help categorize an attack, generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed. Examples of an attack pattern could be 'spear phishing', 'lateral movement', or 'exploit vulnerability'.

*TTP: Tactics, Techniques, and Procedures

Campaigns

A group of adversarial behaviors that describe a set of malicious activities or attacks occurring over a period of time against a specific set of targets. Campaigns usually have well defined objectives and may be part of an Intrusion Set.

Courses of Action

An action taken to prevent an attack or respond to an attack in progress. Critical Controls or Mitigations are examples of Courses of Action. They could be technical, automated response, or analytical, but can also represent higher level actions like employee training or penetration testing. Related to this, a Course of Action could be to apply Security Patches to prevent Vulnerability Exploitation.

Indicators

Patterns that can be used to detect suspicious or malicious cyber activity.

Identities

Represent individuals, organizations or groups as well as categories of individuals, organizations or groups.

Malware

A type of TTP*, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.

*TTP: Tactics, Techniques, and Procedures (cite as in Attack Pattern)

Sightings

An instance in which a particular Campaign, Intrusion Set, or Incident was observed. May also denote the potential observation of an element of Cyber Threat Intelligence (CTI) (e.g., Indicator, Malware).

Tools

Legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can inform understanding how campaigns are executed. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, system administrators, network administrators, or even normal users. This object type MUST NOT be used to characterize malware or tools used as part of a course of action in response to an attack.

Threat Actors

Individuals, groups, or organizations believed to be operating with malicious intent. Threat Actors can be characterized by: motives, capabilities, intentions/goals, sophistication level, past activities, access to resources, and their role in an organization.

Intrusion Sets

A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns, organization, and other activities that are tied together by shared attributes indicating a common known or unknown Threat Actor. Threat Actors can move from supporting one Intrusion Set to another or may support multiple Intrusion Sets at the same time.

Reports

A survey of the Courses of Actions that your organization implements and to what level (High, Medium, or Low). Unfetter will use the survey to help you understand your gaps, how important they are, and which should be addressed. You may create multiple reports to see how new or different Courses of Actions implemented may change your security posture.

Sensors

The basic monitoring elements that collect information about your network and can be used to inform assessments of your network's security. The number of sensors necessary for your environment depends on how closely you want to monitor your network.

Unique to Unfetter
(not in STIX)

FUTURE

Relationships

Used to link two STIX Data Objects (SDOs) and describe how they relate to each other. Relationships enable STIX to clearly express cyber threat intelligence (CTI). Although major components are valuable when assessed independently, STIX is most effective when components inform contextual understanding for threat analysis. An indicator for an IP Address without context is much less informative than relating the IP Address to a relevant TTP, relating the TTP to a Threat Actor or Actors known to use it, the Incidents where it was observed, and to Courses of Action that can mitigate its impact.

Observed Data

Collected information observed on a system or network (e.g., an IP address). While Indicators of Compromise (IOC) represent assumptions behind attacks, raw information informs this conclusion. In many cases, it may be beneficial for organizations to share this data with each other. Similar to indicators, sightings can contain references to observed Indicators on other organizations' networks and could inform searches for malware. This may inform further, more detailed conclusions.

Vulnerabilities

An error or mistake in software that can be leveraged by a hacker to gain access to a system or network.

Incidents

Discrete instances of Indicators impacting an organization, along with information discovered during an incident response investigation. This information can consist of data such as time-related information, parties involved, assets affected, impact assessment, related Indicators, related Observables, leveraged TTP, attributed Threat Actors, intended effects, nature of compromise, requested Courses of Action, Courses of Action taken, confidence in characterization, handling guidance, source of Incident information, log of actions taken, etc.