JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

AOS-25-0679
September 2025

STIX Modeler Tool

User Guide

Version 1.0

Prepared for: Department of Homeland Security (DHS)
Cybersecurity and Infrastructure Security Agency (CISA)

Prepared by: The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099

Hannah Ripley
Luanne Chamberlain

Task No.: CYS98
Contract No.: N0024-22-D-6404

CONTENTS

FIGURES

TABLES

1. INTRODUCTION

1.1 Purpose and Audience

The Structured Threat Information Expression (STIX) Modeler is a React-based [1] user interface tool for creating, modifying, and visualizing STIX 2.1 [2] bundles. Appendix A provides a guide to downloading and installing the tool and extensions.

This report provides an overview of the STIX Modeler User Interface (UI) components and common use cases for modeling activities. The intended audience for this tool is **cybersecurity professionals** and **threat intelligence analysts** who need to understand and analyze structured threat intelligence data. Common uses include:

- Visualizing attack kill chains (using MITRE ATT&CK® [3] (Adversarial Tactics, Techniques, and Common Knowledge) and STIX)
- Analyzing the spread of malware or campaigns over time
- Understanding adversary infrastructure (Internet Protocols (IPs), domains, tools)
- Collaborative threat sharing [e.g., via Information Sharing and Analysis Centers **(**ISACs)]

1.2 Document Organization

This report is organized as follows:

- Section 2 provides some STIX background concepts and definitions.
- Section 3 is the STIX Modeler User Guide.
- Section 4 provides report conclusions.
- Appendix A is a guide to getting started with the STIX Modeler.
- Appendix B provides the detailed definitions of all STIX Objects fields for all objects.
- Appendix C is a list of acronyms and abbreviations.

2. BACKGROUND AND DEFINITIONS

This section describes several concepts that are essential to understanding STIX and the STIX Modeler. STIX 2.1 bundles are containers used to share a set of cyber threat intelligence (CTI) objects in a structured and machine-readable format. Figure 2-1 shows the STIX Modeler landscape.

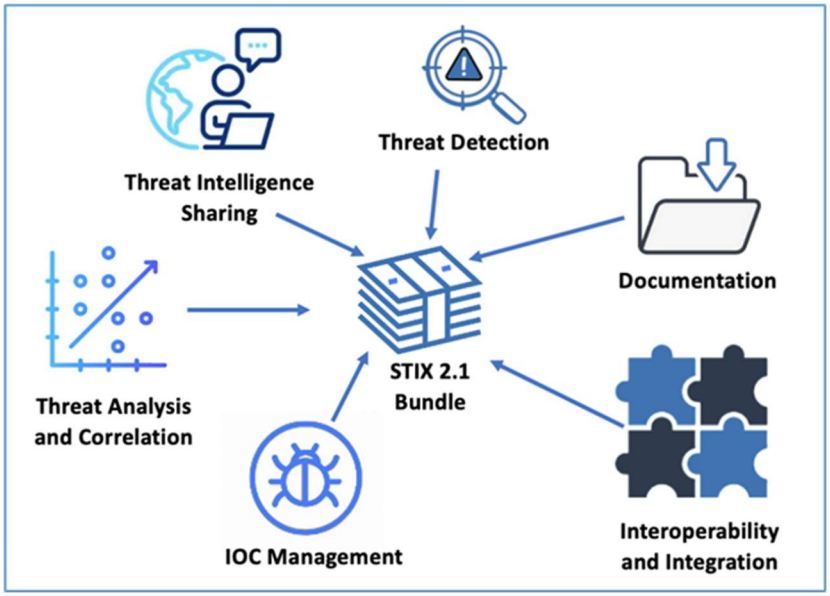


Figure 2-1 STIX Modeler Landscape

The STIX Modeler can be used for:

- **Sharing Threat Intelligence**: between organizations and between vendors and consumers
- **Threat Analysis and Correlation**: context-rich investigation
- **Indicators of Compromise (IOC) Management**: distribution of IOCs
- **Threat Detection**: automated IOC ingestion and detection
- **Documentation**: historical threat intelligence records and after-action reporting
- **Interoperability and Integration**: interoperability between tools or integration into new tools

STIX objects are the building blocks used to describe threat intelligence. STIX objects are written in **JavaScript Object Notation (**JSON). STIX objects belong to four main categories:

1. **STIX Domain Objects (SDOs)** represent intelligence and threat information (e.g., malware, campaigns, threat actors). The format of an SDO is shown in Table 2-1.
2. **STIX Relationship Objects (SROs)** link SDOs to SCOs, SDOs to SDOs, and SCOs to SCOs together, showing the relationship between them. The format of an SRO is shown in Table 2-2.
3. **STIX Cyber Observable Objects (SCOs)** represent observables (e.g., IP addresses, file hashes, domain names). The format of an SCO is shown in Table 2-3.

4. **STIX Meta Objects (SMOs)** provide additional information (e.g., purpose). The format of an SMO is shown in Table 2-4.

Each object also contains a *spec_version* field that refers to the unique identifier for a specific STIX specification or version. Its value, for the STIX Modeler examples in this report, is 2.1, representing STIX version 2.1. STIX objects may have additional, optional fields.

Table 2-1 STIX Domain Object (SDO)

Field	Description
type	The object type (e.g., malware, threat-actor, etc.)
id	Unique ID in the form *type*--<*UUID*>
created	When the object was created
modified	Last time the object was modified

Table 2-2 STIX Relationship Object (SRO)

Field	Description
type	Always "relationship"
id	Unique ID in the form *relationship*--<*UUID*>
created	Timestamp of when the object was created
modified	Timestamp of the last modification
relationship_type	Describes the kind of relationship (e.g., uses, attributed-to, indicates)
source_ref	The ID of the source object (e.g., threat-actor--...)
target_ref	The ID of the target object (e.g., malware--...)

Table 2-3 STIX Cybersecurity Observable Object (SCO)

Field	Description
type	The type of observable (e.g., file, ipv4-addr, domain-name, email-message, url, process)
id	Unique ID in the form *type*--<*UUID*>

Table 2-4 STIX Meta Object (SMO)

Field	Description
type	"marking-definition"
id	STIX ID (e.g., marking-definition--...)
created	Creation timestamp
definition_type	Type of marking: "tlp" or "statement"
definition	The actual marking content (e.g., { "tlp": "amber" })[1]
external_references	Sources or citations

A STIX 2.1 bundle is a container that groups together multiple STIX objects for sharing and exchanging CTI. Like STIX objects, STIX bundles are structured JSON objects. Table 2-5 shows the format of a STIX bundle; Figure 2-2 shows a notional instantiation of the bundle; and Figure 2-3 shows the visual depiction of the bundle.

Table 2-5 STIX Bundle

Field	Description
type	Must be "bundle"
id	A unique ID in the format bundle--UUID
spec_version	Must be "2.1" for STIX 2.1
objects	A list of STIX objects (SDOs, SCOs, SROs, etc.)

[1] "tlp" refers to "Traffic Light Protocol," which "is a system of markings that designates the extent to which recipients may share potentially sensitive information," and is used by the Cybersecurity and Infrastructure Security Agency (CISA)

```
type": "bundle",
"id": "bundle--c9f42f0a-9f1d-4cb9-bd24-cd923d9e16f6",
"spec_version": "2.1",
"objects": [
 {
  "type": "threat-actor",
  "spec_version": "2.1",
  "id": "threat-actor--a1b2c3d4-e5f6-7890-abcd-111111111111",
  "created": "2025-06-04T12:00:00Z",
  "modified": "2025-06-04T12:00:00Z",
  "name": "Silent Jackal",
  "threat_actor_types": ["crime-syndicate"],
  "aliases": ["Shadow Fangs"]
 },
 {
  "type": "malware",
  "spec_version": "2.1",
  "id": "malware--f1e2d3c4-b5a6-7890-cdef-222222222222",
  "created": "2025-06-04T12:01:00Z",
  "modified": "2025-06-04T12:01:00Z",
  "name": "PhantomRAT",
  "malware_types": ["remote-access-trojan"],
  "is_family": true
 },
 {
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--12345678-9abc-def0-1234-333333333333",
  "created": "2025-06-04T12:02:00Z",
  "modified": "2025-06-04T12:02:00Z",
  "name": "C2 Domain Indicator",
  "indicator_types": ["malicious-activity"],
  "pattern": "[domain-name:value = 'malicious.example.com']",
  "pattern_type": "stix"
 },
 {
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--aaaa1111-bbbb-2222-cccc-444444444444",
  "relationship_type": "uses",
  "created": "2025-06-04T12:03:00Z",
  "modified": "2025-06-04T12:03:00Z",
  "source_ref": "threat-actor--a1b2c3d4-e5f6-7890-abcd-111111111111
  "target_ref": "malware--f1e2d3c4-b5a6-7890-cdef-222222222222"
 },
 {
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--eeee5555-ffff-6666-gggg-777777777777",
  "relationship_type": "indicates",
  "created": "2025-06-04T12:04:00Z",
  "modified": "2025-06-04T12:04:00Z",
  "source_ref": "indicator--12345678-9abc-def0-1234-333333333333",
  "target_ref": "malware--f1e2d3c4-b5a6-7890-cdef-222222222222"
 }
]
}
```


Figure 2-2 Example STIX Bundle

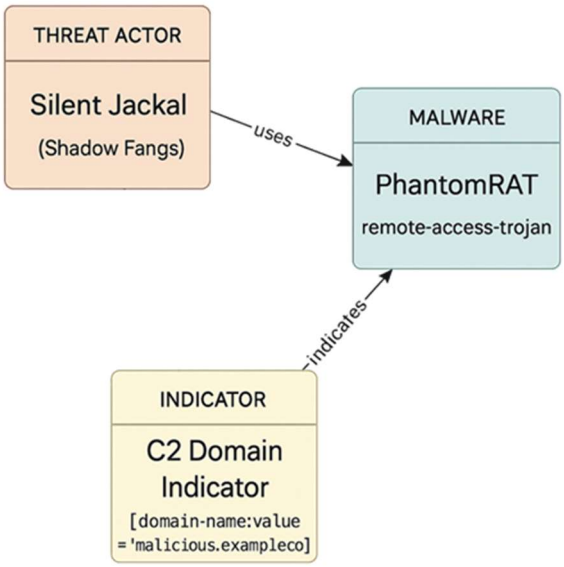


Figure 2-3 Visual Depiction of the Bundle

A STIX schema defines the structure, fields, data types, and constraints used to create and validate STIX objects — including SDOs, SCOs, SROs, Bundles, and SMOs. This ensures that cyber threat

information exchanged using STIX is consistent and understandable by both humans and automated systems. A simple *Indicator* schema is shown in Figure 2-4.

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
 "title": "Simple STIX Indicator Schema",
 "type": "object",
 "properties": {
  "type": {
   "type": "string",
   "const": "indicator"
  },
  "id": {
   "type": "string",
   "pattern": "^indicator--[0-9a-fA-F-]{36}$"
  },
  "spec_version": {
   "type": "string",
   "enum": ["2.1"]
  },
  "created": {
   "type": "string",
   "format": "date-time"
  },
  "modified": {
   "type": "string",
   "format": "date-time"
  },
  "name": {
   "type": "string"
  },
  "pattern": {
   "type": "string"
  },
  "pattern_type": {
   "type": "string",
   "enum": ["stix"]
  },
  "valid_from": {
   "type": "string",
   "format": "date-time"
  }
 },
 "required": ["type", "id", "spec_version", "created",
              "modified", "pattern", "pattern_type", "valid_from"],
 "additionalProperties": true
}
```

Figure 2-4 Example STIX Schema

A STIX 2.1 extension **(**Figure 2-5**)** allows the user to customize or extend the standard STIX object types (Figure 2-6) without violating the STIX 2.1 specification.

```
extension
{
 "type": "extension-definition",
 "id": "extension-definition--abc123...",
 "name": "Malware Severity Extension",
 "description": "Adds a severity rating to malware objects",
 "created": "2024-06-01T00:00:00Z",
 "modified": "2024-06-01T00:00:00Z",
 "created_by_ref": "identity--1234...",
 "schema": "https://example.com/stix-extensions/malware-severity-extension.schema.json",
 "extension_types": ["property-extension"],
 "object_marking_refs": ["marking-definition--tlp-white"]
}
```

Figure 2-5 Example STIX Extension

Figure 2-6 Example STIX Object with an Extension

A STIX Modeler node is a graphical vertex representation of a STIX object, either an SDO or an SCO. Figure 2-3 has three nodes: representing a Threat Actor SDO ("Silent Jackal"), a Malware SDO ("PhantomRAT"), and an Indicator SDO ("C2 Domain Indicator").

A STIX Modeler edge is a graphical representation of a relationship between two STIX objects, either an SRO or an embedded (i.e. specified by an object property) relationship. Figure 2-3 has two edges: representing two SROs named "uses" and "indicates."

Nodes and edges, as defined in this document, are STIX Modeler structures but are not official STIX 2.1 specification-defined structures.

3. USER GUIDE

3.1 Overview

The STIX Modeler enables several capabilities:

- Creating SDOs and SCOs
- Modifying existing SDOs and SCOs
- Creating SROs
- Creating new STIX bundles
- Modifying STIX bundles
- Visualizing STIX bundles
- Creating extended (defined by a STIX extension schema) SDOs and SCOs
- Validating STIX bundles

3.2 STIX Modeler Canvas

All elements of the STIX Modeler are contained within the **canvas**. Figure 3-1 shows the default view for the STIX Modeler. The red notations on the canvas identify the elements and buttons; more detail is provided in the sections that follow.

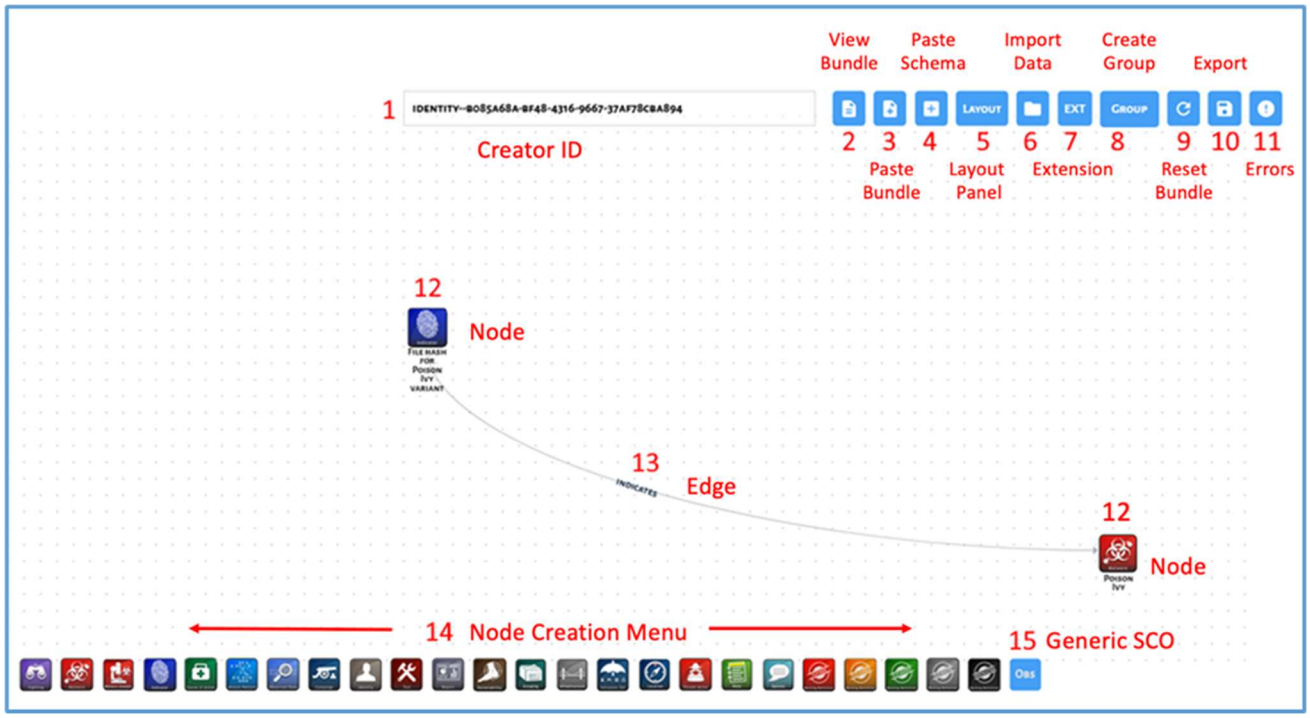


Figure 3-1 The STIX Modeler Canvas

The canvas is comprised of the following elements:

1. The **Creator ID field** specifies the *created_by_ref* value for nodes created using the STIX Modeler UI.
2. The **View Bundle button** opens the View Bundle panel.
3. The **Paste Bundle button** opens the Paste Bundle panel.
4. The **Paste Schema button** opens the Paste Schema panel.
5. The **Layout button** opens the Auto Layout panel.
6. The **Import Data button** opens the File Import panel.
7. The **Extension button** opens the Extension Selection panel.
8. The **Group button** enables the Grouping Mode.
9. The **Reset button** deletes all nodes and relationships from the STIX Modeler UI.
10. The **Export button** exports the bundle as a JSON file.
11. The **View Errors button** opens the Errors panel.
12. A **node** represents an SDO or SCO.
13. An **edge** represents a relationship, either:
    - An SRO, where the *source_ref* value is the source node ID and the *target_ref* value is the target node ID
    - A reference property of the source node (typically ending in *_ref*), with a value of or including the target node ID
14. The **Node Creation menu** contains SDO icons, which may be dragged onto the UI to create a new node of the specified type.
15. The **Observable Icon** represents a generic SCO and may be dragged onto an existing node to create a new SCO (of a relevant type, if one exists).

3.3 Nodes

3.3.1 Creating a Node

Dragging an icon from the **Node Creation menu** onto the UI creates a new node of the specified type (Figure 3-2).

Figure 3-2 Dragging a New Node Onto the Canvas

3.3.2 Editing a Node

Clicking on a node in the STIX UI opens the **Details panel**. The Details panel allows node properties to be updated. Required fields that have not been filled in yet are bordered by a red box. The Delete button deletes the node (Figure 3-3). Table 3-1 describes the fields common to all objects. Appendix B describes other fields that are specific to each object type.

Figure 3-3 Editing a Node's Properties

Table 3-1 Fields Common to All Objects

Field	Description	Auto Filled	Default	Editable
type	The type of this object	Y		N
spec_version	The version of the STIX specification used to represent this object	Y	2.1	N
created_by_ref	The ID of the identity object that describes who created this object	Y		Y
labels	The set of terms used to describe this object	N		Y
created	The time at which this object was created	Y		Y
modified	The time at which this object was last modified	Y		Y
revoked	Whether this object has been revoked	Y	False	Y

Field	Description	Auto Filled	Default	Editable
confidence	The confidence the creator has in the correctness of their data	N	0	Y
external_refs	A list of external references which refers to non-STIX information	N		Y

3.3.3 Creating an SCO Node

New SCOs can be created by dragging the **Observable Icon** onto an existing node. In Figure 3-4, the Observable Icon is being dragged to overlay the Poison Ivy Malware node on the canvas.

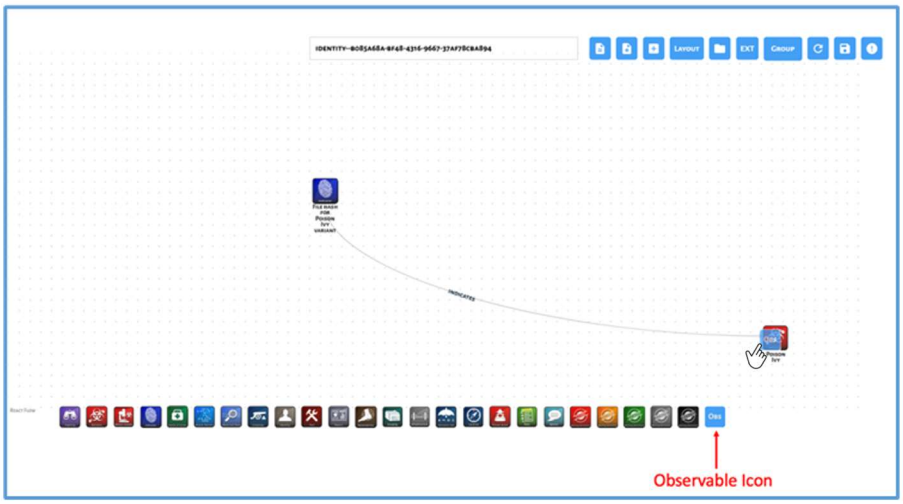


Figure 3-4 Creating an SCO Node

When the observable is dropped, the relevant SCOs for the target node are enumerated in the Possible Relationships panel (Figure 3-5).

Selection of an SCO in the Relationship Selection panel creates both of the following:

- A new SCO, of the specified type
- A new relationship between the SCO and the target node

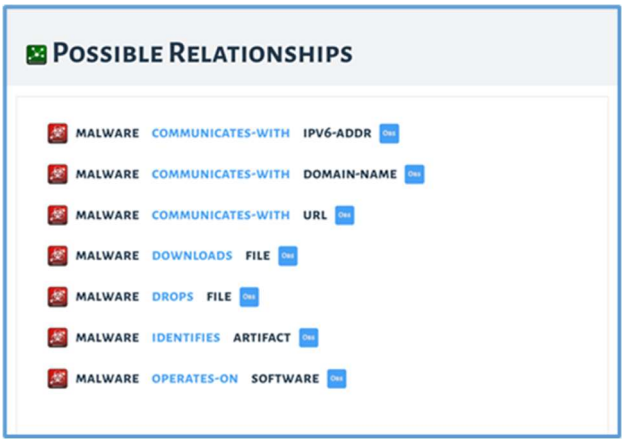


Figure 3-5 Possible Relationships Between Malware SDO and All SCOs

3.3.4 Grouping Nodes

Grouping Mode can be used to create a new Group via node selection. Nodes can be clicked to be selected in Grouping Mode. The steps for group node selection are shown in Table 3-2. Figure 3-6 shows a new grouping.

Table 3-2 Grouping Nodes

	When the **Group** button is selected, the user enters a new mode where any number of nodes can be selected. When selected, a node is bordered by a blue box. Clicking a selected node will deselect it.
	After selecting all the nodes in the group, the **Create Group button** creates a new Group node, where the *object_refs* property contains the selected node IDs.
	The selection of nodes for a group can be canceled by choosing the **Cancel button,** which exits Grouping Mode without the creation of a new group.

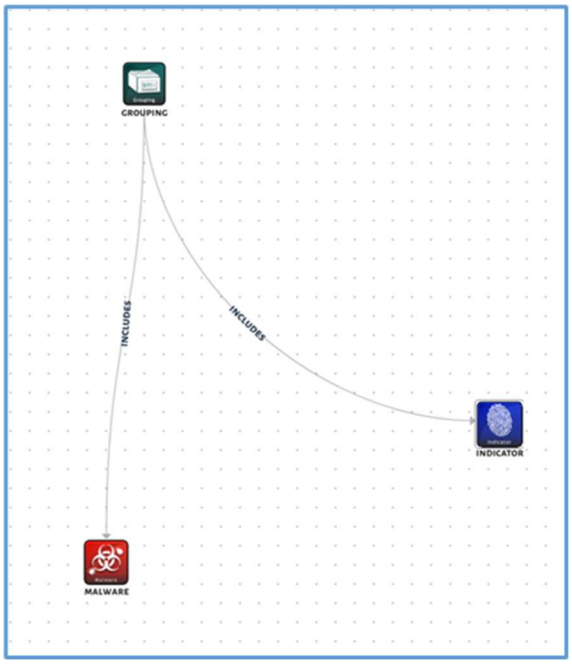


Figure 3-6 Creating a New Grouping

3.4 Relationships

3.4.1 Creating a Relationship

A new relationship can be created by clicking the edge of a node and dragging the relationship to the edge of a second node. In Figure 3-7, the cross-hair on the malware node shows that the source of the relationship has been selected. Figure 3-8 shows dragging the relationship to its target, the indicator node.

Figure 3-9 shows the panel that is displayed when the user drops the relationship line onto the target. The **Relationship Selection panel** lists possible relationship types between two nodes. Clicking a relationship in the Relationship Selection panel creates a new relationship of the specified type. The **Create New Relationship button** opens the New Relationship panel.

Figure 3-10 shows the established relationship.

Figure 3-7 Starting the Creation of a Relationship

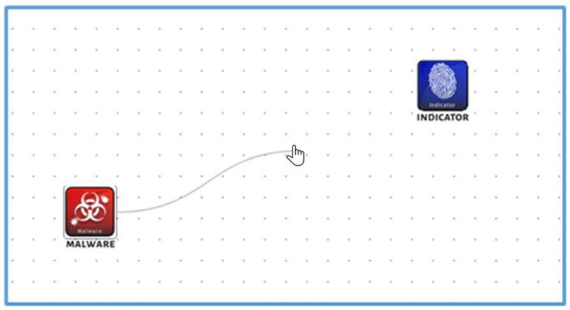


Figure 3-8 Dragging Relationship Connector to Target Node

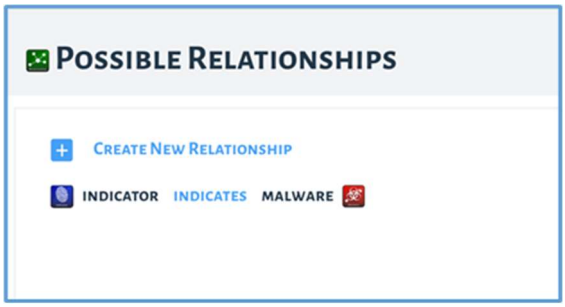


Figure 3-9 Possible Relationship Panel

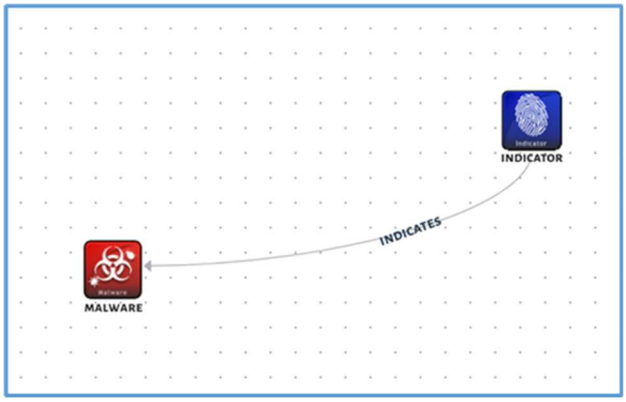


Figure 3-10 The Established Relationship

3.4.2 Defining a New Relationship Type

The **New Relationship panel,** shown in Figure 3-11**,** allows a new relationship type to be defined between two nodes. From the Possible Relationships panel (shown in Figure 3-9), the user can select New Relationship option at the top.

Clicking the Submit button creates an instance of the new relationship type between the specified nodes. The new relationship type is also added to the Possible Relationships list. The *x-exclusive* property should be *True* to indicate a 1:1 relationship. The default is *False*.

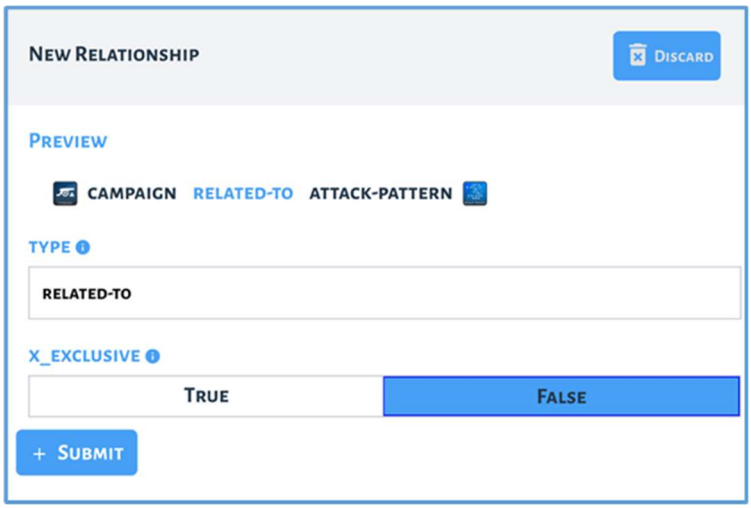


Figure 3-11 The New Relationship Panel

3.4.3 Editing a Relationship

Clicking on an existing relationship edge opens the Edit Relationship panel (Figure 3-12). The **Edit Relationship panel** allows a relationship to be modified or deleted. Clicking the Delete button deletes the relationship.

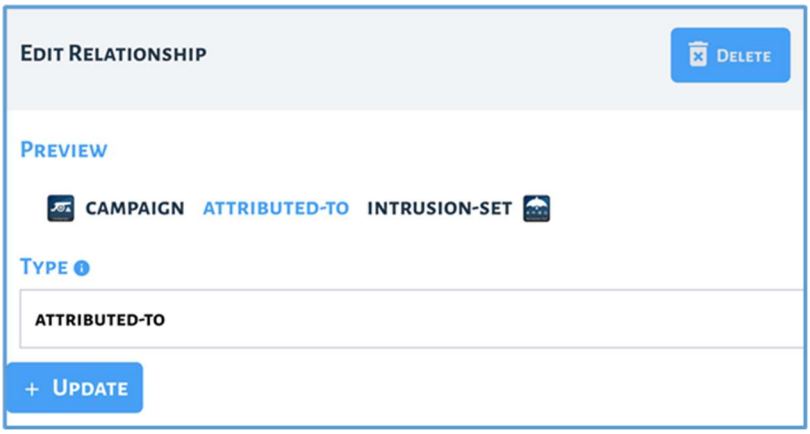


Figure 3-12 Editing a Relationship

3.4.4 Configuring Layout

Figure 3-13 shows an imported bundle. The nodes can be manually moved around to make the visualization easier to understand. The STIX Modeler also offers a tool for automatically rearranging it.

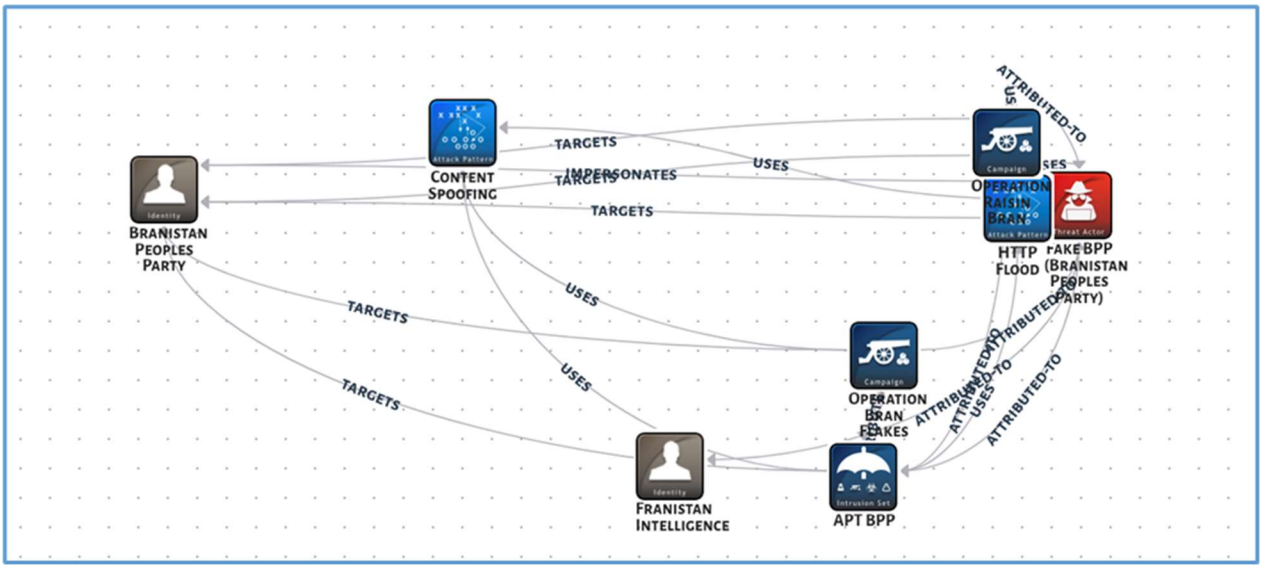


Figure 3-13 An Imported Bundle

The **Layout panel** enables positional arrangement of nodes in the STIX Modeler UI (Figure 3-14).

Nodes may be arranged in the following Layout Modes:

- Hierarchy, according to incoming and outgoing relationships
- Grid, according to node type

Nodes can be oriented in the following orientations:

- Row, where elements are grouped horizontally
- Column, where elements are grouped vertically (Figure 3-15)

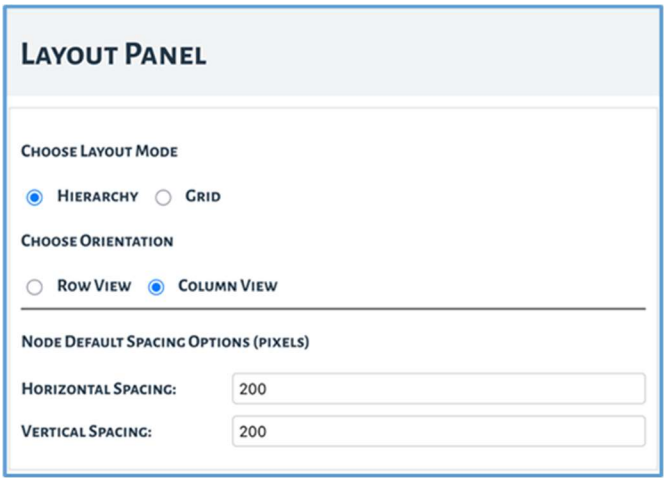


Figure 3-14 The Layout Panel

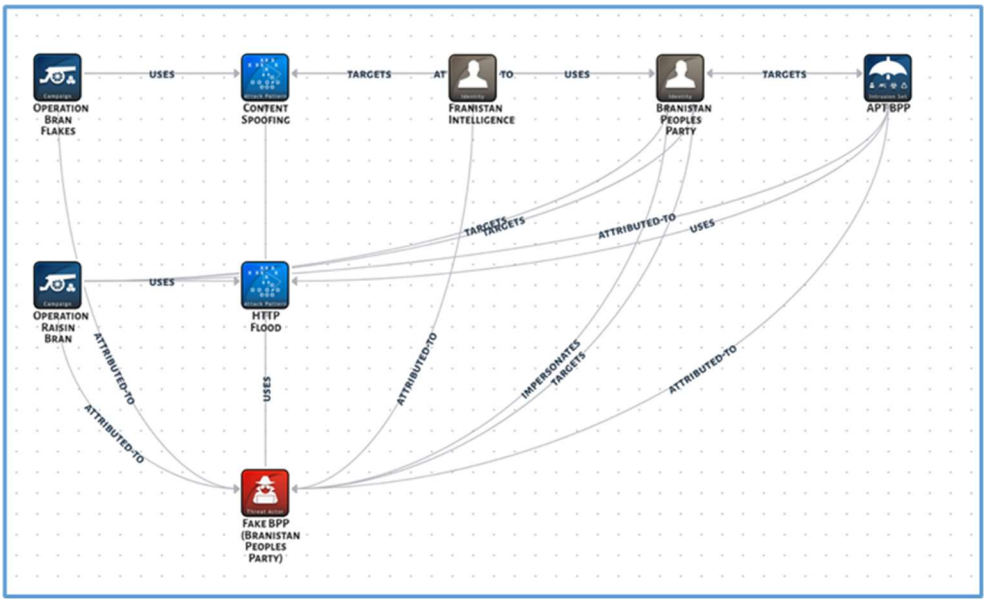


Figure 3-15 Hierarchical, Column View

3.5 STIX Bundles

3.5.1 Importing a Bundle Panel

The **Paste Bundle panel** allows the contents of a STIX bundle JSON file to be directly pasted and loaded into the STIX Modeler UI. Clicking the Load button causes the STIX bundle to be imported and visualized in the STIX Modeler UI. Figure 3-16 shows the bundle from Figure 2-2 pasted into the pop-up window. Figure 3-17 shows the visual depiction after pasting the bundle.

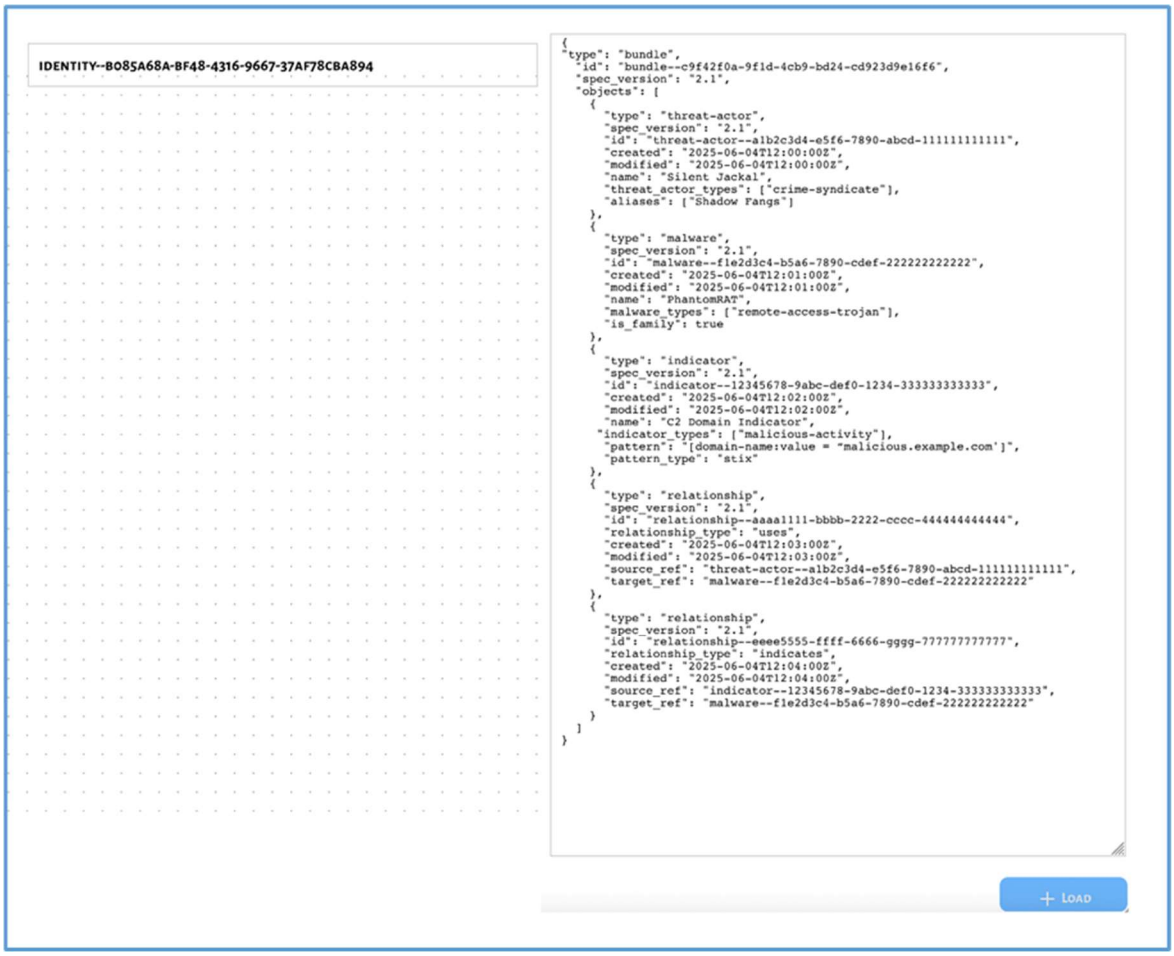


Figure 3-16 The Paste Bundle Panel

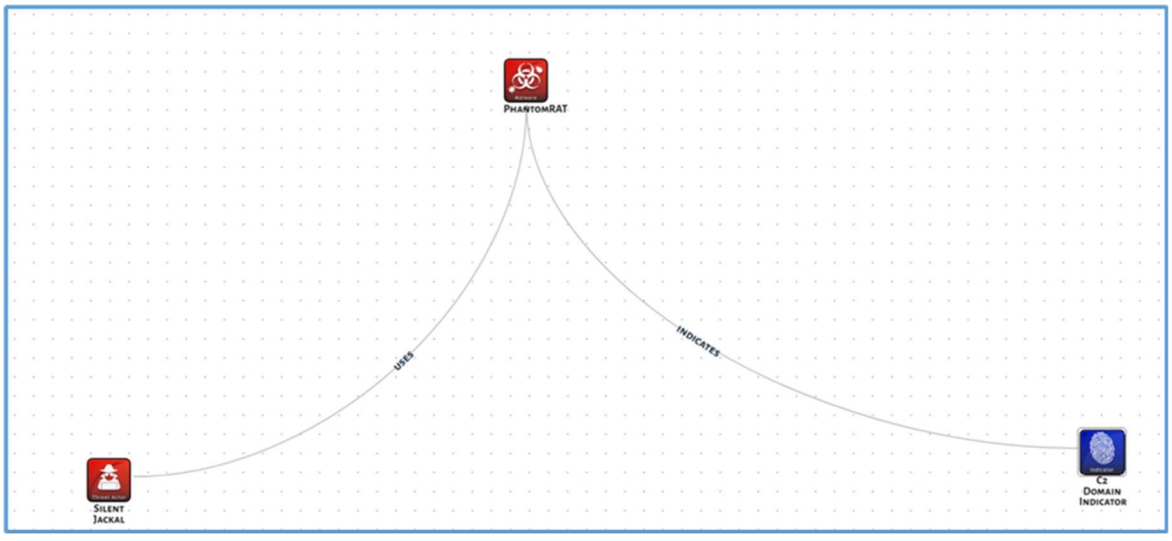
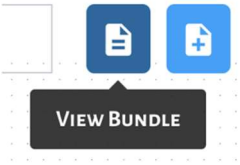


Figure 3-17 Visual Depiction After Pasting the Bundle

3.5.2 Viewing a STIX Bundle



The **View Bundle panel** (Figure 3-18) displays the STIX bundle JSON contents.

Clicking the Copy button copies the contents of the STIX bundle JSON representation to the system clipboard.

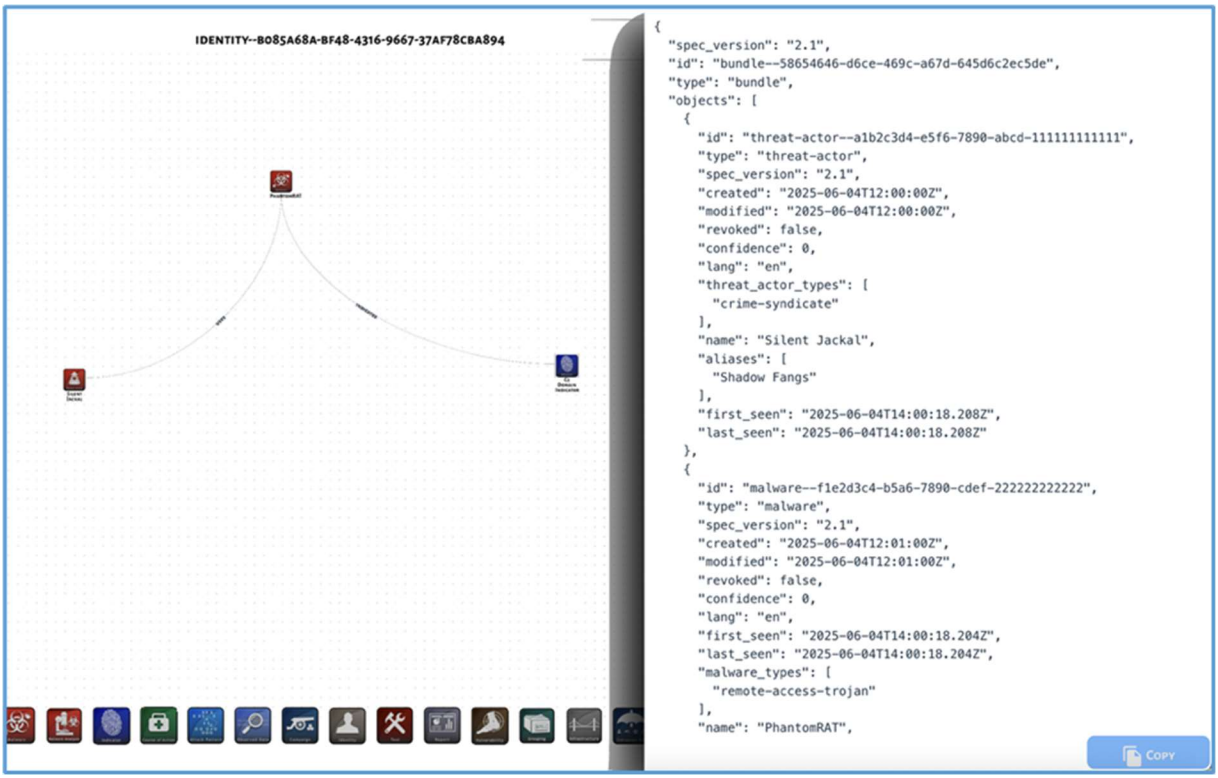


Figure 3-18 The View Bundle Panel

When the View Bundle panel is opened, the bundle is validated. If any STIX object is missing required fields, a pop-up message will be displayed in the top-left corner of the UI and a badge will appear on the Errors button, as shown in Figure 3-19.

Figure 3-19 Invalid STIX Bundle Error Message and Badge Notification

3.5.3 Viewing Bundle Errors

The **Errors panel** enumerates nodes with missing or invalid properties, as shown in Figure 3-20. Clicking on a node listed in the Errors panel opens its associated Details panel.

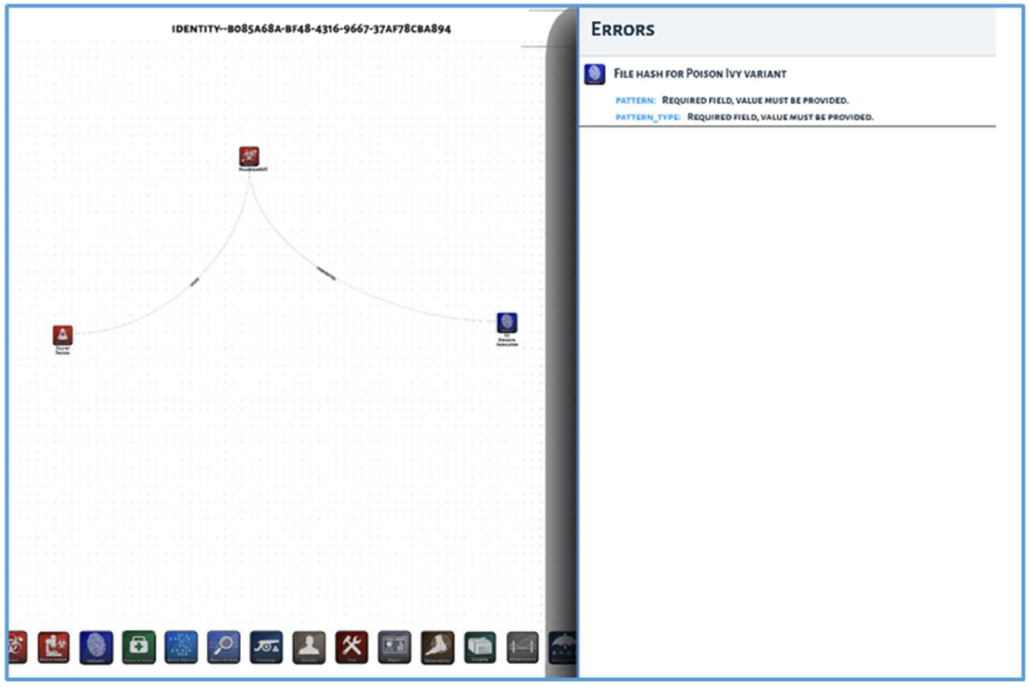
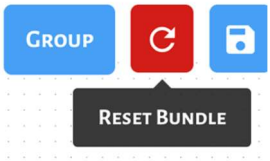


Figure 3-20 The Errors Panel

3.5.4 Exporting a Bundle

The **Export button** locally downloads the STIX bundle as a JSON file. By default, the file is called *bundle.json*.

3.5.5 Resetting a Bundle



The **Reset button** deletes all SDOs, SCOs, and SROs from the STIX bundle, and deletes all nodes and relationships from the STIX Modeler UI.

Resetting the bundle does not remove STIX extensions from the STIX Modeler UI. These must be removed manually via the Extension Editor panel (see section 3.6.2).

3.6 STIX Extensions

3.6.1 Importing an Extension Schema via Paste

The **Paste Schema panel** allows the contents of a STIX extension (either *new-sdo* or *property-extension*) schema JSON file to be directly pasted and loaded into the STIX Modeler UI.

The **Paste Schema panel** allows the contents of a STIX extension (either *new-sdo* or *property-extension*) schema JSON file to be directly pasted and loaded into the STIX Modeler UI, as shown in Figure 3-21.

Clicking the Load button causes the STIX extension schema to be imported to the STIX Modeler UI.

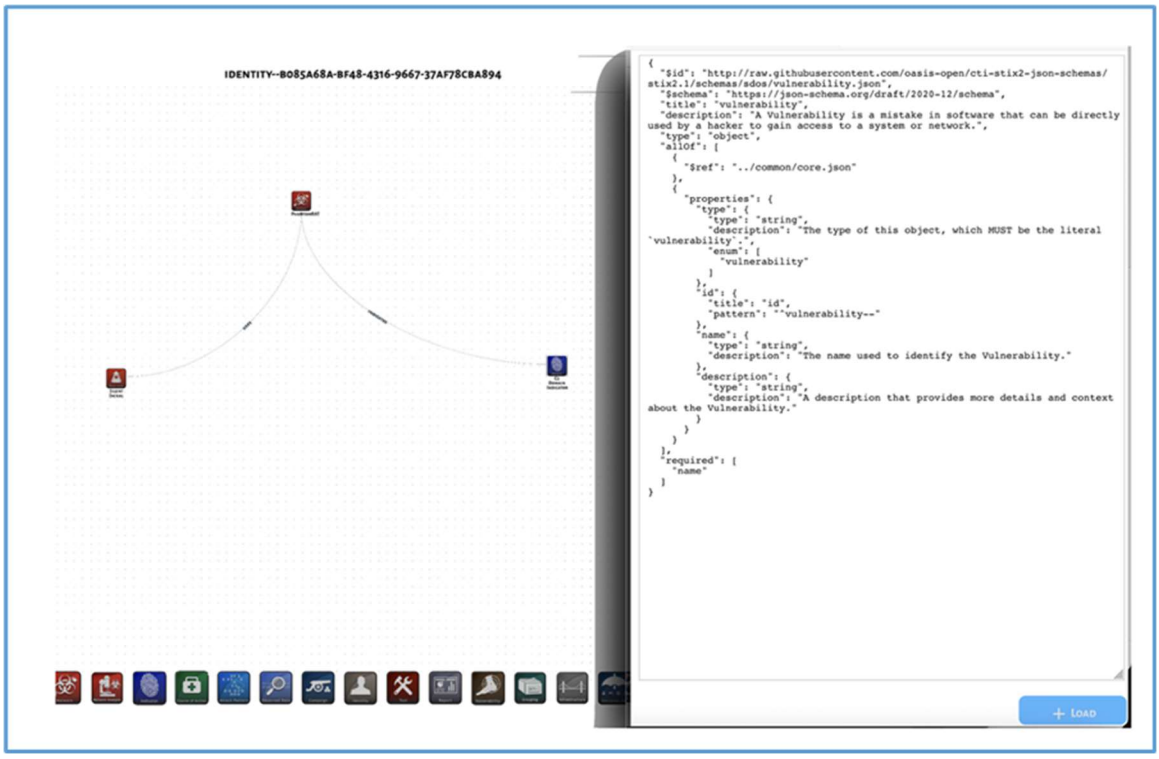


Figure 3-21 The Paste Schema Panel

Upon successfully loading a STIX *new-sdo* extension schema, a new icon (by default, the Custom SDO icon) will be added to the Node Creation menu, as shown in Figure 3-22.

Figure 3-22 New SDO Icon in Node Creation Menu

3.6.2 Editing a STIX Extension

The **Extension Selection panel** lists all imported STIX extensions, as shown in Figure 3-23.

Figure 3-23 The Extension Selection Panel

Clicking on a STIX extension definition in the Extension Selection panel opens the Extension Editor panel, as shown in Figure 3-24.

The **Extension Editor panel** allows the fields of a STIX extension definition to be updated.

The **Update Icon button** allows a new icon image to be selected via a File Selector dialog box. On selection, all nodes of the extension type, as well as the associated Node Selection icon, are updated to display the new image.

The **Delete button** deletes the STIX extension definition, all SDOs and SCOs defined by the extension, and any properties added by the extension.

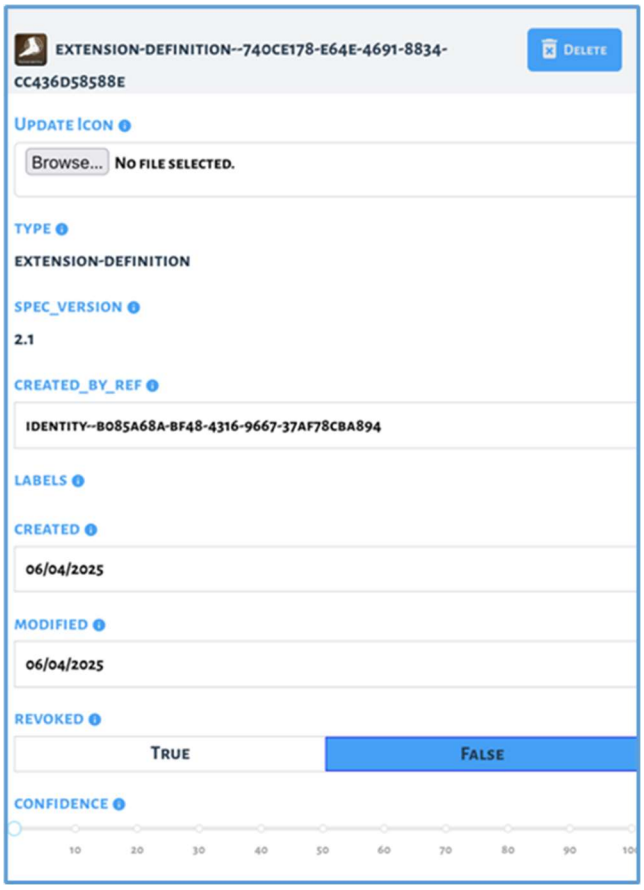


Figure 3-24 The Extension Editor Panel

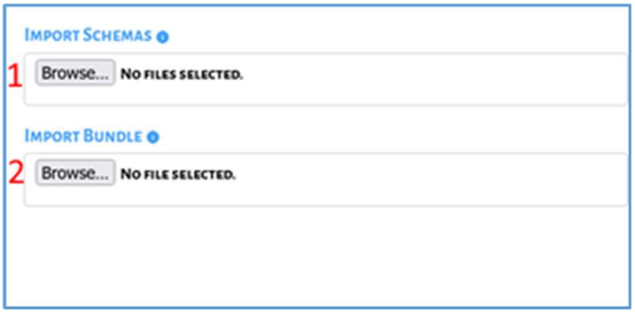


Figure 3-25 The File Import Panel

3.7 Importing a Schema or Bundle From a File

The **File Import panel** enables the selection of local STIX bundle and STIX extension schema JSON files, as shown in Figure 3-25.

The **Import Schemas button** allows one or more local STIX extensions schema JSON files to be selected via a File Selector dialog box, and then imported into the STIX Modeler UI.

The **Import Bundle button** allows one local STIX bundle JSON file to be selected via a File Selector dialog box, and then imported into the STIX Modeler UI.

4. CONCLUSIONS

The STIX Modeler provides a tool for created structured and flexible representations of diverse forms of threat intelligence in STIX 2.1 format. By capturing technical indicators, adversary tactics, attack patterns, infrastructure details, and other contextual information, the modeler enables analysts to organize intelligence in a way that is both machine-readable and operationally useful.

The process begins with extracting key insights from threat intelligence reports, modeling them in structured objects, and building relationships that capture the full context of an adversary's activity. These structured representations can then be combined into STIX bundles and shared with partners to promote interoperability and collective defense.

As threats grow more complex, the ability to represent and exchange threat intelligence in standardized formats is increasingly essential. Leveraging STIX 2.1, integrating with TAXII for automated exchange, and using tools such as the STIX Modeler empower organizations to improve detection, response, and collaboration across the cybersecurity community. This guide serves as a foundation for advancing structured intelligence practices and strengthening defenses against evolving threats.

5. REFERENCES

[1] Meta Platforms, Inc., React.dev, web development page. Available at https://react.dev/. Accessed August 14, 2025.

[2] OASIS, "STIX™ Version 2.1, Committee Specification Draft 01 / Public Review Draft 01," 26 July 2019. Available at https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html. Accessed 14 August 2025.

[3] The MITRE Corporation, MITRE ATT&CK® [Adversarial Tactics, Techniques, and Common Knowledge], ATT&CK Matrix. Available at https://attack.mitre.org/. Accessed 14 August 2025.

[4] Cybersecurity and Infrastructure Security Agency (CISA), "Traffic Light Protocol User Guide 2.0," 2022. Available at https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf. Accessed 12 August 2025.

[5] B. Schneier, "Who Are the Shadow Brokers?" The Atlantic, 23 May 2017. Available at https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778. Accessed 14 August 2025.

[6] The Johns Hopkins University Applied Physics Laboratory (JHU/APL), "ASPR Cyber Capabilities Evaluation and Strategic Support (ACCESS): Cybersecurity Incident Severity Level Scoring Methodology," AOS-24-0366, June 2024.

[7] U.S. Department of Justice Archives, "Justice Department Sues to Block UnitedHealth Group's Acquisition of Change Healthcare," 24 February 2022. Available at https://www.justice.gov/archives/opa/pr/justice-department-sues-block-unitedhealth-group-s-acquisition-change-healthcare. Accessed 14 August 2025.

[8] American Hospital Association, letter to the Chairman and Ranking Member of the U.S. House Committee on Ways and Means, 19 March 2024. Available at https://www.aha.org/system/files/media/file/2024/03/Congress-Urged-to-Help-Hospitals-Impacted-by-Change-Healthcare-Cyberattack-letter-20240320.pdf. Accessed 14 August 2025.

[9] HHS Announces Next Steps in Ongoing Wfork to Enhance Cybersecurity for Health Care and Public Health Sectors | SDAHO

[10] S. Alder, "Healthcare Data Breach Statistics," The HIPAA Journal, 15 July 2025. Available at https://www.hipaajournal.com/healthcare-data-breach-statistics. Accessed August 14 2025.

APPENDIX A. GETTING STARTED WITH THE STIX MODELER

This appendix provides a step-by-step walkthrough for setting up the STIX Modeler and using it with Indicators of Behavior (IOB) extensions.

The IOB project was selected as the example because it relies heavily on custom STIX extensions. Unlike core STIX objects (such as Indicators or Observed Data), IOB introduces new object types to represent adversary behaviors, detections, detectors, and playbooks. This makes IOB an ideal learning case: by working through it, one will not only set up the Modeler but also gain hands-on experience with importing and using extensions — a process that applies to many other extension-based projects.

By the end of this guide, you will have the tool running locally and be able to load and visualize these IOB extensions to capture adversary workflows.

A.1 Basic Installation

Before beginning, follow these steps:

- **Install STIX Modeler:** Follow the installation instructions available at the GitHub repository.
- **Prepare Prerequisites:**
  (1) Install **Node.js** (version 23.7)
  (2) Install **Node Package Manager (npm)** (version 10.9.2) for local deployment.
- **Load the Tool:** Run the application and access the graphical user interface through your browser (e.g., http://localhost:5173/)

A.2 Importing Extensions

The IOB framework demonstrates how STIX extensions can be used to extend the language beyond its core specification. Because IOB depends entirely on extensions to model behaviors and their relationships, it provides a clear and practical example of the import process.

To load the IOB extensions into the STIX Modeler:

- **Download Extension Files:** Obtain the necessary extensions from the Open Cybersecurity Alliance (OCA) GitHub repository. Required extensions include the following:
  - x-oca-behavior
  - x-oca-detection
  - x-oca-detector
  - x-oca-playbook
  - x-oca-coa-playbook-ext

- **Import Extensions:** Use the **Import Schema** feature in STIX Modeler to add these extensions.
- **Select the EXT button:** Select one or more extensions, as shown in Figure A-1.
- **Customize Icons:** Assign custom PNG icons to differentiate imported objects for better visualization. To assign a custom icon, select the extension from the screen shown in Figure A-1, then choose an icon file (such as a PNG image) in the screen shown in Figure A-2

Figure A-1 STIX SDO Extensions

Figure A-2 Assigning Custom Icons for Extension

If you can successfully import the IOB extensions, you can apply the same process to any other STIX extension-based project. IOB is simply the teaching example here, but the workflow you just practiced is the general recipe for extending the Modeler with new schemas.

APPENDIX B. STIX OBJECT FIELDS

B.1 Required Fields for All Objects

This section describes the fields for each type of object; bolded field names are required. Appendix B.1 shows the fields that are required for all objects. A STIX open vocabulary[2] describes STIX objects using a predefined, non-exhaustive list of common and industry-accepted terminology.

Field	Description	Auto Filled	Default	Editable
type	The type of this object	Y		N
spec_version	The version of the STIX specification used to represent this object	Y	2.1	N
created_by_ref	The ID of the source object that describes who created this object	Y		Y
labels	Specifies a set of terms used to describe this object	N		Y
created	Date created	Y		Y
modified	Date last modified	Y		Y
revoked	Whether this object has been revoked	Y	False	Y
confidence	The confidence the creator has in the correctness of their data	N	0	Y
external_refs	A list of external references which refers to non-STIX information	N		Y

B.2 Attack Pattern

Attack Patterns are a type of TTP (i.e., Tactics, Techniques, and Procedures) that describe ways that adversaries attempt to compromise targets.

Field	Description	Field Type
All fields from B.1		
aliases	Alternative names used to identify this Attack Pattern	Text entry
name	The name used to identify the Attack Pattern	Text entry
description	A description that provides more details and context about the Attack Pattern, potentially including its purpose and its key characteristics	Text entry
kill_chain_phases	The list of kill chain phases for which this Attack Pattern instance is used	Choose from list

[2] https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html

B.3 Campaign

A Campaign is a grouping of adversary behavior that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the Campaign	Text entry
description	A description that provides more details and context about the Campaign, potentially including its purpose and its key characteristics	Text Entry
aliases	Alternative names used to identify this Campaign	Text entry
first_seen	The time that this Campaign instance was first seen	Date entry
last_seen	The time that this Campaign instance was last seen	Date entry
objective	The Campaign's primary goal, objective, desired outcome, or intended effect	Text entry

B.4 Course of Action

A Course of Action (COA) is an action taken either to prevent an attack or to respond to an attack that is in progress.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the Course of Action	Text entry
description	A description that provides more details and context about this object, potentially including its purpose and its key characteristic	Text Entry

B.5 Grouping

A Grouping object explicitly asserts that the referenced STIX objects have a shared content.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the Grouping	Text entry

description	A description that provides more details and context about the Grouping, potentially including the purpose and key characteristics	Text entry
context	A short description of the particular context shared by the content referenced by the Grouping	Text entry

B.6 Identity

Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, or groups.

Field	Description	Field Type
All fields from B.1		
roles	The list of roles that this Identity performs (e.g., CEO, Domain Administrators, Doctors, Hospital, or Retailer) No open Vocabulary is yet defined for this property.	Text entry
name	The name of this Identity	Text entry
description	A description that provides more details and context about the Identity	Text entry
identity_class	The type of entity that this Identity describes, e.g., an individual or organization Open Vocab - identity-class-ov	Choose from list
sectors	The list of sectors that this Identity belongs to Open Vocab - industry-sector-ov	Choose from list
contact_info	The contact information (e-mail, phone number, etc.) for this Identity	Text entry

B.7 Indicator

Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.

Field	Description	Field Type
All fields from B.1		
indicator_type	This field specifies the type of indicator. Open Vocab - indicator-type-ov	Choose from list
name	The name used to identify the identity	Text entry
description	A description that provides the recipient with context about this Indicator, potentially including its purpose and its key characteristics	Text entry
pattern	The detection pattern for this indicator	Text entry
pattern_type	The type of pattern used in this indicator	Choose from list

pattern_version	The version of the pattern that is used	Text entry
valid_from	The time from which this indicator should be considered valuable intelligence	Date entry
valid_until	The time at which this indicator should no longer be considered valuable intelligence	Date entry
kill_chain_phases	The phases of the kill chain that this indicator detects	Choose from list

B.8 Infrastructure

Infrastructure objects describe systems, software services, and associated physical or virtual resources.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the Infrastructure	Text entry
description	A description that provides more details and context about this Infrastructure, potentially including its purpose and its key characteristics	Text entry
infrastructure_types	This field specifies the type of infrastructure. Open Vocab - infrastructure-type-ov	Choose from list
aliases	Alternative names used to identify this Infrastructure	Text entry
kill_chain_phases	The list of kill chain phases for which this infrastructure is used	Choose from list
first_seen	The time that this infrastructure was first seen performing malicious activities	Date entry
last_seen	The time that this infrastructure was last seen performing malicious activities	Date entry

B.9 Intrusion Set

An Intrusion Set is a grouped set of adversary behavior and resources with common properties that is believed to be orchestrated by a single organization.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the Intrusion Set	Text entry
description	Provides more context and details about the Intrusion Set object	Text entry
aliases	Alternative names used to identify this Intrusion Set	Text entry
first_seen	The time that this Intrusion Set was first seen	Date entry
last_seen	The time that this Intrusion Set was last seen	Date entry

goals	The high-level goals of this Intrusion Set	Text entry
resource_level	This defines the organizational level at which this Intrusion Set typically works. Open Vocab - attack-resource-level-ov	Choose from list
primary_motivation	The primary reason, motivation, or purpose behind this Intrusion Set Open Vocab - attack-motivation-ov	Choose from list
secondary_motivations	The secondary reasons, motivations, or purposes behind this Intrusion Set Open Vocab - attack-motivation-ov	Choose from list

B.10 Location

LOCATION

A Location represents a geographic location. The location may be described as any, some, or all of the following: region (e.g., North America), civic address (e.g., New York, U.S.), latitude, and longitude.

Field	Description	Field Type
All fields from B.1		
name	The name used to identify the Location	Text entry
description	A textual description of the Location	Text entry
latitude	The latitude of the location in decimal degrees	Text entry
longitude	The longitude of the location in decimal degrees	Text entry
precision	Defines the precision of the coordinates specified by the latitude and longitude properties, measured in meters	Text Entry
region	The region that this Location describes	Text Entry
country	The country that this Location describes	Text Entry
administrative_area	The state, province, or other sub-national administrative area that this Location describes	Text Entry
city	The city that this Location describes	Text Entry
street_address	The street address that this Location describes	Text Entry
postal_code	The postal code for this Location	Text Entry

B.11 Malware

Malware is a type of TTP that is also known as malicious code and malicious software and refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim.

Field	Description	Field Type
All fields from B.1		
aliases	Alternative names used to identify this malware or malware family	Text entry
first_seen	The time that the malware instance or family was first seen	Date entry
last_seen	The time that the malware instance or family was last seen	Date entry
architecture_execution_envs	The processor architectures (e.g., x86 ARM etc.) that the malware instance or family is executable on Open - processor-architecture-os	Choose from list
implementation_languages	The programming language(s) used to implement the malware instance or family Open Vocab - implementation-language-ov	Choose from list
capabilities	Specifies any capabilities identified for the malware instance or family Open Vocab - malware-capabilities-ov	Choose from list
malware_types	The type of malware being described Open Vocab - malware-type-ov	Choose from list
name	The name used to identify the malware	Text entry
description	Provides more context and details about the malware object	Text entry
kill_chain_phases	The list of kill chain phases for which this malware instance can be used	Choose from list

B.12 Malware Analysis

Malware Analysis captures the metadata and results of a particular analysis performed (static or dynamic) on the malware instance or family.

Field	Description	Field Type
All fields from B.1		
product	The name of the analysis engine or product that was used for this analysis	Text entry
version	The version of the analysis product that was used to perform this analysis	Text entry
configuration_version	The version of the analysis product configuration that was used to perform this analysis	Text entry
modules	The particular analysis product modules that were used to perform the analysis	Text entry
analysis_engine_version	The version of the analysis engine or product that was used to perform this analysis	Text entry
analysis_definition_version	The version of the analysis definitions used by the analysis tool	Text entry
submitted	The date and time that this malware was first submitted for scanning or analysis	Date entry
analysis_started	The date and time that the malware analysis was initiated	Date entry
analysis_ended	The date and time that the malware analysis ended	Date entry
result_name	The classification result or name assigned to the malware instance by the scanner tool	Text entry
result	The classification result, as determined by the scanner or tool analysis process	Text entry

B.13 Note

A Note is a comment or note containing informative text to help explain the context of one or more STIX Objects (SDOs or SROs) or to provide additional analysis that is not contained in the original object.

Field	Description	Field Type
All fields from B.1		
abstract	A brief summary of the note	Text entry
content	The content of the note	Text entry
authors	The name of the author(s) of this note (e.g., the analyst(s) that created it)	Text entry

B.14 Observed Data

Observed data conveys information that was observed on systems and networks, such as log data or network traffic, using the Cyber Observable specification.		
Field	**Description**	**Field Type**
All fields from B.1		
first_observed	The beginning of the time window during which the data was observed	Date entry
last_observed	The end of the time window during which the data was observed	Date entry
number_observed	The number of times the data was observed This MUST be an integer between 1 and 999,999,999 inclusive.	Slider

B.15 Opinion

An Opinion is an assessment of the correctness of the information in a STIX Object produced by a different entity and captures the level of agreement or disagreement using a fixed scale.		
Field	**Description**	**Field Type**
All fields from B.1		
explanation	An explanation of why the producer has this Opinion	Text entry
authors	The name of the author(s) of this opinion (e.g., the analyst(s) that created it)	Text entry
opinion	The opinion that the producer has about all of the STIX Object(s) listed in the *object_refs* property	Text entry

B.16 Report

Reports are collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.		
Field	**Description**	**Field Type**
All fields from B.1		
report_types	This field specifies the primary subject of this report. The suggested values for this field are in: Open Vocab report-type-ov	Choose from list
name	The name used to identify the report	Text entry
description	A description that provides more details and context about this report	Text entry
published	The date that this report object was officially published by the creator of this report	Date entry

B.17 Sighting

A Sighting denotes the belief that something in CTI (an indicator, malware, tool, threat actor, etc.) was seen.		
Field	**Description**	**Field Type**
All fields from B.1		
description	A description that provides more details and context about the sighting	Text entry
first_seen	The beginning of the time window during which the SDO referenced by the *sighting_of_ref* property was sighted	Date entry
last_seen	The end of the time window during which the SDO referenced by the *sighting_of_ref* property was sighted	Date entry
count	This is an integer between 0 and 999,999,999 inclusive and represents the number of times the object was sighted	Slider

B.18 Threat Actor

Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent.		
Field	**Description**	**Field Type**
All fields from B.1		
threat_actor_types	This field specifies the type of threat actor. Open Vocab - threat-actor-type-ov	Choose from list
name	A name used to identify this threat actor or threat actor group	Text entry
description	A description that provides more details and context about the threat actor	Text entry
aliases	A list of other names that this threat actor is believed to use	Text entry
roles	This is a list of roles the threat actor plays. Open Vocab - threat-actor-role-ov	Choose from list
goals	The high-level goals of this threat actor— what are they trying to accomplish	Text entry
first_seen	The time that this threat actor was first seen	Date entry
last_seen	The time that this threat actor was last seen	Date entry
sophistication	The skill, specific knowledge, special training, or expertise a threat actor must have to perform the attack Open Vocab - threat-actor-sophistication-ov	Choose from list
resource_level	This defines the organizational level at which this threat actor typically works. Open Vocab - attack-resource-level-ov	Choose from list
primary_motivation	The primary reason, motivation, or purpose behind this threat actor Open Vocab - attack-motivation-ov	Choose from list
secondary_motivations	The secondary reasons, motivations, or purposes behind this threat actor Open Vocab - attack-motivation-ov	Choose from list
personal_motivations	The personal reasons, motivations, or purposes of the threat actor regardless of organizational goals. Open Vocab - attack-motivation-ov	Choose from list

B.19 Tool

Tools are legitimate software that can be used by threat actors to perform attacks.		
Field	**Description**	**Field Type**
All fields from B.1		
aliases	Alternative names used to identify this tool	Text entry
tool_types	The kind(s) of tool(s) being described Open Vocab - tool-type-ov	Text entry
name	The name used to identify the tool	Text entry
description	Provides more context and details about the tool object	Text entry
tool_version	The version identifier associated with the tool	Text entry
kill_chain_phases	The list of kill chain phases for which this tool instance can be used	Choose from list

B.20 Vulnerability

A Vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network.		
Field	**Description**	**Field Type**
All fields from B.1		
name	The name used to identify the vulnerability	Text entry
description	A description that provides more details and context about the vulnerability	Text entry

APPENDIX C. ABBREVIATIONS AND ACRONYMS

ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge
C2	Command and Control
CEO	Chief Executive Officer
CISA	Cybersecurity and Infrastructure Security Agency
COA	Course of Action
CTI	Cyber Threat Intelligence
DHS	Department of Homeland Security
IOB	Indicator of Behavior
IOC	Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centers
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
JSON	JavaScript Object Notation
NPM	Node Package Manager
OCA	Open Cybersecurity Alliance
PNG	Portable Network Graphic
SCO	STIX Cybersecurity Observable Object
SDO	STIX Domain Object
SMO	STIX Meta Object
SRO	STIX Relationship Object
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Intelligence Information
TLP	Traffic Light Protocol
TTP	Tactics, Techniques, and Procedures

UI	User Interface
UUID	Universally Unique Identifier