CYT245 Assignment8 – STIX – 4%

Individual or team work, based on the teamwork policy

You are asked to enter student names below:

1. Ishan Aakash Patel	2.
3.	4.

Team leader is __________Ishan____

Objectives

- Familiarize yourself with STIX language concept and constructs.
- Familiarize yourself with STIX idioms.
- Do practice with the STIX tools – STIX documentation profile.

Tasks

Task 1. Review the sample scenario of communication between companies A and B. See how STIX is used to arrange communication.

Connect to

https://oasis-open.github.io/cti-documentation/stix/intro.html

and then go to

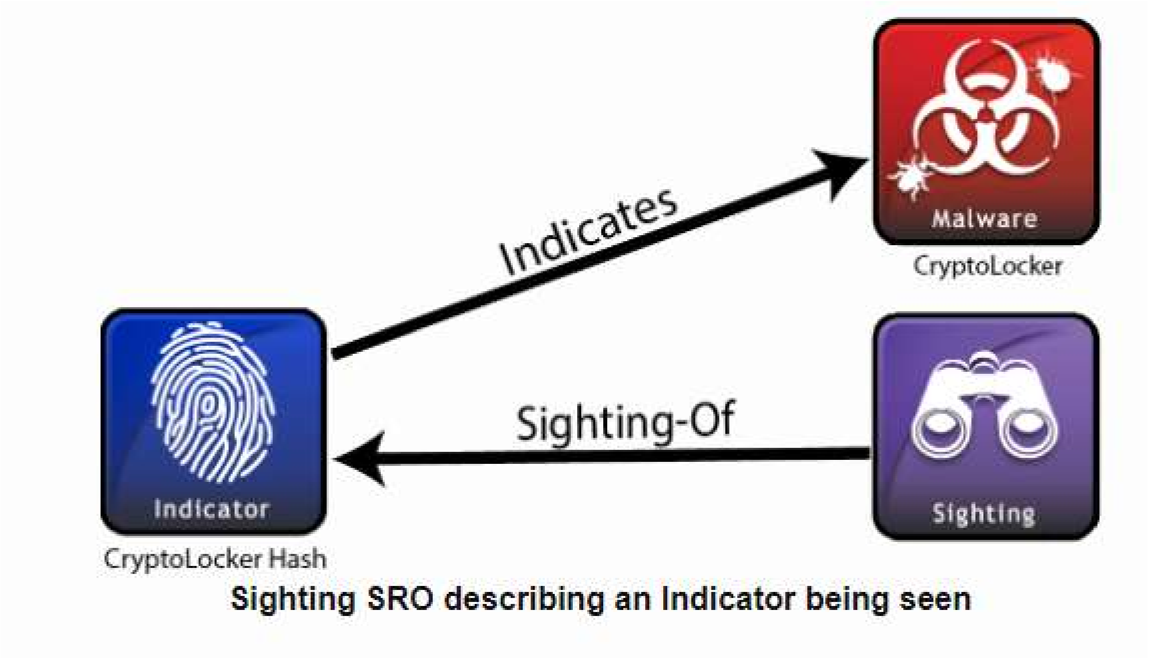
https://oasis-open.github.io/cti-documentation/stix/walkthrough

Review the sample scenario of utilizing STIX.

Answer the following questions:

- In what role is the company A and the company B in this scenario?
- What Indicator the company A decided to share with company B?
- What is the workflow the company A is to implement to share information?
    - Include step-by-step actions
    - For each action indicate what data participate and what tools will be used
- What is the workflow the company B is to implement to share information?
    - Include step-by-step actions
    - For each action indicate what data participate and what tools will be used
- What objects are created in this scenario?
- List the objects and comment the object's content
- Now review the content of STIX Bundle. Comment the nature of this artifact. How it can be used in communication flaw between the companies A and B.

- What is the reason of creating the Sighting object?
    - Comment the picture below



Sighting SRO describing an Indicator being seen

Summary

To summarize, we just looked at how Company A could create some threat intelligence in STIX (an Indicator and the Malware that it indicates) and share it with Company B. Company B was then able to take that intelligence and generate a Sighting SRO to share back to the community.

Task 2. Learn idioms and review the sample of idioms posted on gihub

Connect to

https://stixproject.github.io/about/

then extend Documentation drop-down list and click on Idioms or go directly to

https://stixproject.github.io/documentation/idioms/

Open Command and Control IP List | STIX Project Documentation

Answer the following questions:

- What is a STIX idiom?
- For a given case, what is exact name of the construct?
- For a given case, what exactly are observables and how this information can be used?
- What exactly is known and what is not?
- Review Implementation section. Comment the content of each component (XML, Python Producer, Python Consumer).

Task 3. Work on STIX documentation profiles (similar task is given as the long answer in final exam)

Review attached MS Excel spreadsheet, named “stix1.2_sample_indicator_sharing_profile_r1”, open the tab **Indicator.**

Assume that you need to create the STIX custom document to describe a given IOCs, following the profile requirements.

Abstract Data Model for Indicator construct is available at

IndicatorType | STIX Project Documentation

It is also seen at the spreadsheet.

You also need to review STIX vocabulary at

IndicatorTypeVocab-1.1 | STIX Project Documentation

Review the abstract data model, and then see what is included in the custom profile.

Note: use MS Word document to provide your answer. MS Excel spreadsheet is given as the template only; no need to use it for your answer.

Step 1. Determine data attributes which are required (MUST) to include in the customized document. List them below:

- …

Step 2. Determine data attributes which are desirable (Should) be included in the customized document. List them below:

- ….

Step 3. Create sample of the customized document for a given IOCs

Connect to

https://otx.alienvault.com/pulse/642bda624b63276eba73e5c1?utm_userid=tato1234&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_following

In this alert you see a few IOCs. Your task now is to prepare the content of IOC documentation, following indicator sharing profile. It is expected that you have the sections to address attributes which are marked in the steps 1 and 2, to the best of your ability. Use the terms from STIX vocabulary, such as: Observable, Indicator, TTPs, etc. It is recommended to group the IOCs by Observable Types (e.g. IP Watchlist).

Submission Upload Requirements

Make online submission to BB, only one submission from your team.

If you have more than one document, wrap it up to ZIP, 7ZIP, or RAR folder

Name the file you will uploading as indicated below. The name must include:

- Course ID (CYT715)
- What is this (e.g. lab1, assignment 1, etc)
- Authors by name(s)

Sample: CYT175MLab1_PeterJohnMohammadSue

Note: submissions that do not follow the requirements will not be accepted

Task 1: Scenario Review

Question 1: Roles of Companies A and B

Answer:

- Company A: Acts as the information provider, responsible for generating and sharing threat intelligence.
- Company B: Acts as the information consumer, responsible for receiving, analyzing, and utilizing the threat intelligence shared by Company A .

Question 2: Indicator Shared by Company A

Answer: Company A decided to share an Indicator related to a specific malware identified in their network. This indicator includes details such as the malware's hash values, associated IP addresses, and domains .

Question 3: Workflow for Company A to Share Information

Answer:

Step 1: Identify the threat indicator.

- Data: Details of the threat indicator, such as malware hash values, IP addresses, and domains.
- Tools: STIX editor or similar threat intelligence tool.

Step 2: Create a STIX document with the identified threat indicator.

- Data: Formatted STIX document containing the threat indicator details.
- Tools: STIX editor.

Step 3: Validate the STIX document to ensure it meets the required standards.

- Data: STIX document.
- Tools: STIX validation tool.

Step 4: Share the STIX document with Company B using a secure communication method.

- Data: Validated STIX document.
- Tools: Secure communication platform (e.g., email, STIX/TAXII server) .

Question 4: Workflow for Company B to Share Information

Answer:

Step 1: Receive the STIX document from Company A.

- Data: STIX document containing the threat indicator.

- Tools: Secure communication platform.

Step 2: Parse and analyze the STIX document.

- Data: Indicator details extracted from the STIX document.
- Tools: STIX parser and analysis tools.

Step 3: Generate a Sighting based on the received indicator, indicating that the threat has been observed in Company B's environment.

- Data: Sighting details.
- Tools: STIX editor or similar tool.

Step 4: Share the Sighting with the community or provide feedback to Company A.

- Data: Sighting document.
- Tools: Secure communication platform .

Question 5: Objects Created in the Scenario

Answer:

- Indicator: Contains details about the identified threat, such as malware hash values, IP addresses, and domains.
- Sighting: Indicates that the threat described by the Indicator has been observed in Company B's environment.
- STIX Bundle: A container that holds multiple STIX objects, such as Indicators and Sightings, facilitating efficient sharing of related threat intelligence .

Question 6: STIX Bundle

Answer: The STIX Bundle is a structured container that aggregates multiple STIX objects. It allows for the packaging and sharing of comprehensive threat intelligence in a single document, enabling efficient and cohesive communication between organizations. The Bundle can include various types of STIX objects, such as Indicators, Sightings, and TTPs (Tactics, Techniques, and Procedures) .

Question 7: Reason for Creating the Sighting Object

Answer: The Sighting object is created to report that a specific threat, identified by an Indicator, has been observed. This helps organizations understand the prevalence and impact of the threat, contributing to a collective defense strategy. The Sighting provides valuable feedback to the threat intelligence community, indicating where and when the threat has been detected .

Task 2: STIX Idioms

Question 1: What is a STIX Idiom?

Answer: A STIX idiom is a standardized pattern used to represent common types of threat information within STIX. Idioms ensure consistent and reusable representations, making it easier to share and understand threat data across different organizations .

Question 2: Name of the Construct for a Given Case

Answer: The construct name for the given case is "Command and Control IP List" .

Question 3: Observables and Their Usage

Answer:

- Observables: Specific IP addresses or domains used for command and control activities by malicious actors.
- Usage: These observables can be used to detect and block malicious command and control traffic within a network, enhancing an organization's security posture .

Question 4: Known and Unknown Information

Answer:

- Known: The specific IP addresses or domains involved in command and control activities.
- Unknown: The exact tactics, techniques, and procedures (TTPs) the attackers might use in conjunction with these IP addresses or domains .

Question 5: Implementation Components

Answer:

- XML: Provides a structured format for encoding the threat information, ensuring it can be easily shared and parsed.
- Python Producer: A script or tool that generates the STIX document based on the threat data, automating the creation of STIX-compliant documents.
- Python Consumer: A script or tool that parses and utilizes the STIX document for analysis, enabling the recipient to integrate the threat information into their security systems and processes .

Task 3: STIX Documentation Profiles

Step 1: Data Attributes Which MUST Be Included in the Customized Document

1. @id (xs

This is a unique identifier for the indicator.

2. @timestamp (xs

This records the exact date and time when the indicator was created.

3. Observable (cybox

This attribute captures the observable object related to the indicator, such as a file, IP address, or domain.

4. Indicated_TTP (stixCommon

This attribute links the indicator to related Tactics, Techniques, and Procedures (TTPs) used by threat actors.

Step 2: Data Attributes Which SHOULD Be Included in the Customized Document

1. Title (xs

A descriptive title for the indicator.

2. Type (stixCommon

The category or type of indicator, like IP Watchlist or File Hash Watchlist.

3. Confidence (stixCommon

This field reflects the confidence level in the accuracy of the indicator, such as High, Medium, or Low.

4. These attributes are based on the "Occurrence" column in the provided CSV file, indicating fields marked as "MUST" and "SHOULD." The MUST fields are essential for the customized document, while the SHOULD fields are highly recommended but not mandatory. Fields marked as "MAY" can also be included based on specific use case needs, but they are not listed here as they are optional.

Step 3: Sample Customized Document for Given IOCs

5. Example 1: File Hash Watchlist Indicator

- ID: indicator--001
- Timestamp: 2024-07-26T00:00:00Z
- Title: Malicious File Hashes
- Type: File Hash Watchlist
- Confidence: High

- Observable:
  - Type: File
  - Hashes:
    - MD5: 33b9d824c3bcaa9edde14b2eee238d35
    - MD5: 8aec9363db389e4b18e5e25e17bc7da7
    - SHA1: 7b6ee77b31561d5d1ce924c28f8e6853dcbf59f1
    - SHA1: e243975bde2276b48b74025cf5c27b3b0c8ea198
    - SHA256: 882d95bdbca75ab9d13486e477ab76b3978e14d6fca30c11ec368f7e5fa1d0cb
    - SHA256: d4f545691c8441b5bcb86535b1d0fd16dc06786eb4080087588cd4d0f388d5ca
- Indicated TTP:
  - Type: Malware
  - Name: Unknown Malware

6. Example 2: URL Watchlist Indicator

- ID: indicator--002
- Timestamp: 2024-07-26T00:00:00Z
- Title: Malicious URLs
- Type: URL Watchlist
- Confidence: Medium
- Observable:
  - Type: URL
  - Values:
    - http://www.infoamanewonliag.online/update/download.php?file=installer.exe
    - http://www.infoamanewonliag.online/update/download.php?file=update.exe
    - http://www.infoamanewonliag.online/update/index.php?'+Math.random
    - https://winwin.co.th/intro/installer.exe
    - https://winwin.co.th/intro/update.exe
- Indicated TTP:

    - Type: Attack Pattern
    - Name: Malware Distribution

7. Example 3: Domain Watchlist Indicator

- ID: indicator--003
- Timestamp: 2024-07-26T00:00:00Z
- Title: Malicious Domain
- Type: Domain Watchlist
- Confidence: Medium
- Observable:
    - Type: Domain
    - Value: infoamanewonliag.online
- Indicated TTP:
    - Type: Infrastructure
    - Name: Malicious Domain Infrastructure

8. This sample document includes:

- Required (MUST) fields: @id, @timestamp, Observable, Indicated_TTP.
- Recommended (SHOULD) fields: Title, Type, Confidence.