1.0 Introduction

Sharing in cybersecurity threat intelligence emerged from the recognition of growing threats coming from nation-state, cybercriminal and hacktivist actors, coupled with newly minted public policies aimed at ameliorating the negative effects of data breaches, intellectual property theft and cyber espionage. The public policies promoting involvement in this practice have been crafted to encourage cyber threat intelligence sharing among and between owners and operators of critical infrastructure as well as government guardians of networks and endpoints using well-vetted trust circles (DHS, 2016). As this new ecosystem has developed, a global standards body known as the Organization for the Advancement of Structured Information Systems (OASIS) has sponsored a Technical Committee to develop the language, syntax, and logic for a set of protocols for threat intelligence sharing. These protocols are:

- Structured Threat Information Expression (STIX); and
- Trusted Automated Exchange for Indicator Information (TAXII).

In parallel, several key corporate giants and innovative start-ups have developed tools for enabling the sharing of Indicators of Compromise (IOCs) and other data about intrusions, breaches, data theft, and other types of attacks effecting the confidentiality, integrity and availability of key data resources. Public policy analysts have often pointed out the severe lack of trained analysts for implementing the new processes that are emerging as part of this new ecosystem. In response, various public and private universities and technical schools have begun to develop training programs to fill this critical skills shortage and educational system gap.

This paper seeks to outline an approach to training cyber threat analysts using a technique that builds on the use of a threat intelligence platform (TIP) as a key tool in conveying the tradecraft of cybersecurity threat intelligence. If a TIP is designed to give the threat analyst a high level of configurability it exposes its internal logic to the analyst, thereby empowering the trained analyst to carefully design the threat hunting parameters. This will help to reduce false positives and, at the same time, increase the value of data that are collected for the decision-makers who need to take proactive defensive or remedial action.

The TIP selected for our case study was developed by EclecticIQ, an Amsterdam-based company with offices in London and Northern Virginia in the U.S. This platform was selected from among seven TIP candidates because of its close conformance to the STIX data model and its robust application interfaces that can be easily configured for interoperability with other tools used by network defenders and guardians. The training programs using this TIP have been designed by Cyber Threat Intelligence Network (CTIN), a U.S.-based company with offices in Europe and the U.S. specializing in the design, development and delivery of cybersecurity training programs.
2.0 The need for trained cyber threat intelligence analysts

As more intelligence teams (including those within ISACs and ISAOs) become established, and members begin to realize the benefits of threat intelligence sharing for fortifying their networks and reducing liabilities and risks associated with data breaches, there will be an increased need for individuals that understand how to interpret the IOCs, enrich the data, and know how to characterize the activity of threat actors that may be engaging in attacks on member networks. There are currently, in our view, very few threat analysts that understand how to use TIPs, how to read STIX-related data, how to enrich IOCs, how to analyze the patterns in order to test various hypotheses on threat actor intent and motivation, how to make assertions on possible attribution, and how to represent the findings in a manner that will be helpful for decision-makers. CTIN is actively engaged in training programs through red team/blue team exercises, pop-up event-based security operations center training, symposia and other forums for hands-on training for threat hunters.

Poaching of cybersecurity talent is a growing concern. As noted in Riley,

“In January 2015, MasterCard hit Nike with a $5M cyber talent poaching suit. The suite noted that companies are desperate for information security talent amid highly publicized data breaches at Target Corp. and Home Depot Inc. While the area is fast growing skilled workers are limited and in demand” (2015).

Currently threat analysts are not only being poached, but they are also being recruited from the ranks of network engineers, database managers, ethical hackers, software developers, and other specialty disciplines that have bearing on the information technology and cybersecurity fields. Even for these specialized workers, there is a steep learning curve to develop an understanding of the tools and techniques used to analyze attacks, to establish threat actor tactics, techniques and procedures (TTPs), and to develop application interfaces (APIs) between TIPs and existing in-house tools for monitoring networks and generating security metrics.

There is a role in workforce training for TIP-based instruction for workers seeking skills upgrades, such as the experienced professionals listed above. In addition, there is a also role for TIP-based training for new analysts seeking to develop a career dedicated to threat analysis.

Exhibit 2-1: Student Visualization Using the EclecticIQ Platform

To illustrate this point, the Figure 2-1 is a student-developed visualization from a student project where new student analysts were asked to upload indicators of compromise from a report on the Duke’s APT (Lehtio, 2015) into the EclecticIQ platform. Graduate-level intelligence program students were given access to the EclecticIQ platform as part of a semester-long training in cyber threat analysis. Their hands-on experience with a TIP helped them move from a theoretical understanding of the concepts to a practical understanding of the process of threat hunting and, importantly, the documentation of the artifacts found from threat hunting.
An additional advantage of using the EclecticIQ platform was that they gained a greater understanding of why data enrichment services are so critical to the process and how to configure a TIP to integrated multiple data enrichment sources.

3.0 The purpose and design of a Threat Intelligence Platform (TIP)

One of the first studies to effectively characterize the emerging ecosystem for TIPs was a Gartner Report published in December, 2014 (Lawson & McMillan). The authors laid out how TIPs function to aggregate threat intelligence “feeds” from multiple open source and proprietary sources while serving as a platform for enriching IOCs with supplemental data and information. They then showed how TIPs can use native visualization tools to aid the threat analyst in characterizing the actions of the threat actors, as conveyed through the interpretation of enriched IOCs. Also, importantly, they distinguished between human readable threat intelligence and machine readable threat intelligence (MRTI), a distinction that is important when using a TIP for training purposes. But before looking at the functionality of a TIP, let’s review the legal authorities that have given rise to the practice of threat intelligence sharing in the U.S. and Europe.

3.1 The Emergence of sharing organisations, ISACs and ISAOs, in the U.S.

In the U.S., sixteen Information Sharing and Analysis Centers (ISACs) have been formed under the auspices of Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience. PPD-21 outlines the responsibilities of the U.S. Department of Homeland Security and other sector specific agencies (SSAs) in critical infrastructure/key resource (CI/KR) protection. PPD-21 forms the legal framework for the private/public partnership (PPP) to protect critical infrastructure facilities as shown on Exhibit 3-1.

Exhibit 3-1 – Critical Infrastructure Categories and Federal Sector Specific Agency Liaisons

<table>
<thead>
<tr>
<th>SSAs and CI Sectors</th>
<th>Sector Specific Agency (SSA)</th>
<th>Critical Infrastructure Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPD-21, Critical Infrastructure &amp; Resilience, February 12, 2013 &amp; Appendix B of the National Infrastructure Protection Plan</td>
<td>Dept. of Agriculture, Food &amp; Drug Administration (FDA)</td>
<td>Food &amp; Agriculture</td>
</tr>
<tr>
<td></td>
<td>Department of Defense (DOD)</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td></td>
<td>Department of Energy (DOE)</td>
<td>Energy</td>
</tr>
<tr>
<td></td>
<td>Department of Health &amp; Human Services (HHS)</td>
<td>Healthcare &amp; Public Health</td>
</tr>
<tr>
<td></td>
<td>Department of the Treasury</td>
<td>Banking &amp; Financial Services</td>
</tr>
<tr>
<td></td>
<td>Environmental Protection Agency (EPA)</td>
<td>Water &amp; Wastewater Services</td>
</tr>
<tr>
<td></td>
<td>Department of Homeland Security (DHS)</td>
<td>Chemical</td>
</tr>
<tr>
<td></td>
<td>DHS &amp; General Services Administration (GSA)</td>
<td>Commercial Facilities</td>
</tr>
<tr>
<td></td>
<td>DHS &amp; Department of Transportation</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dams</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nuclear Reactors, Materials &amp; Waste</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Government Facilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transportation Systems</td>
</tr>
</tbody>
</table>
The 2011 “Science of Security Joint Statement of Understanding” between federal agencies of the U.S., Canada and the U.K. list seven core themes that serve as the foundational basis for the cybersecurity discipline. A well-designed and highly configurable TIP provides a technology platform whereby each of these seven core themes can be made explicit. Threats can be given context related to the sector targeting, TTPs of the threat actors, attack methodologies, and threat actor attribution.

These seven core themes are:

- Common language
- Core principles
- Attack analysis
- Measurable security
- Risk
- Agility
- Human factors

Riley (2015) has systematically addressed each of these factors in his 2015 paper promoting a framework for an Science of Security; the reader is referred to the original source for an in-depth discussion of this convergence. The important point here is that this framework is fundamental to the design of a training program that has adequate depth and breadth to address the various functions of TIPs as they are currently being used in operational threat intelligence. CTIN uses this framework for delivery of its own curriculum for academic, and corporate operational customers. The EclecticIQ platform provides a tool that links the theoretical concepts to the operational workflows that are characteristic of a threat hunting cell as described by Zimmermann (2014).

In the U.S. Information Sharing and Analysis Organizations (ISAOs) have their origins in E.O. 13636, Improving Critical Infrastructure Cybersecurity issued in February, 2013, issued in close coordination with PPD-21. ISAOs are often organized along topical (e.g., Maritime & Ports ISAO) or geographic lines (e.g., Cyber Maryland). Both ISACs & ISAOs can benefit from a common TIP used by and among their members for sharing atomic-level data on threats to CI/KR. Atomic-level IOCs and enrichments are used to correlate with other data sources to triangulate the origin of an IOC. Atomic-level indicators can be contrasted with context-based information that for providing a narrative about an on-going campaign or a set of vulnerabilities and weaknesses that have been targeted. Both types of sharing are important for ISACs & ISAOs.

### 3.2 The Drivers for Threat Intelligence Sharing in the E.U.

In Europe as well, threat intelligence sharing has received renewed interest, funding and political attention after the events in the last two years. In addition to the new data privacy regulations coming into force in 2018 (e.g., General Data Protection Regulation [GDPR]), other initiatives spearheaded by the European central banking authorities and by national cybersecurity centers (NCSCs) (e.g. the UK, the Netherlands), all set new and higher requirements for protection of personal data, as well as for protecting critical national infrastructure in the EU. In fact, the European Central Bank (ECB) has just issued a new mandate that all European Banks, including those that fall within the Brexit Framework,
must perform regular “thematic reviews” and report all “significant cyber incidents” effective in the summer of 2017.¹

Other pan-European cooperation bodies, like EUROPOL, have also defined frameworks for sharing cyber intelligence information, for example the OSINT Dashboard (EC3) and The Common Taxonomy for the National Network of CSIRTs. In this context, the incentives for both public sector and for profit private organisations to collaborate in matters of information security and to share intelligence about existing and developing threats have been raised to a level that should ensure the need for trained cyber intelligence and cyber defence analysts only continues to grow. CTIN and EclecticIQ are collaborating to embark on multiple programs for workforce training. This includes, but is not limited to, veteran skills upgrades, support to corporate training programs, and ISAC/ISAO staff and member training. EclecticIQ is also supporting the practical laboratory exercises of graduate students in the Cyber Threat Analysis course at the Ridge College of Intelligence Studies at Mercyhurst University.

3.3 STIX: A Common Language for Threat Intelligence Sharing

In order to effectively share threat intelligence a common ontology characterizing each of the data elements to be shared must be agreed upon by all parties. An understanding of this should be foundational in any cyber threat analyst training program. The Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Systems (OASIS) released a Committee Specification for STIX 2.0 in July 2017 that provides such an ontology.² STIX is built on multiple predecessor ontologies that have emerged over the past few decades from specific communities of interest such as risk management professionals, threat analysts, malware analysts, incident response professionals, remedial action engineers, data architects, digital forensics specialists and others.

STIX is a conceptual data model that extends and builds on these ontologies and makes explicit various elements that can affect the technology stack during an attack scenario. STIX has also been informed by the Resource Descriptive Framework (RDF) and the Ontology for a Web Language (OWL) of the World Wide Web Consortium (W3C). STIX plays a key role in analyst and incident responder decisions regarding the following:

- Collection of internal and external “feeds” including open source and proprietary feeds;
- Fusion of disparate data sources into a single data set used to evaluate correlations;
- Query of aggregate data sets to test analyst hypotheses regarding potential correlations;
- Enrichment of raw data with secondary and tertiary correlations that reveal more about the threat actors’ motivations and intent;
- Storage of raw and processed data for easy access, comparison, and correlation;
- Processing of data for analytical and reporting services; and
- Analysis of data for furthering the testing of hypotheses regarding potential threat actor activity.

² The OASIS CTI TC STIX 2.0 Specification went through three rounds of public review before passage as a Committee Specification.
In essence, the TIP takes in raw data which is processed and mapped to the STIX data model. Then it is used by the analyst for testing of hypotheses regarding the Who, What, When, Why and How questions about threat activity. The more integrated the TIP is with other sharing members and/or with an entities’ own internal tools for network and endpoint monitoring, the more effective the threat analyst can be when using the TIP. If, for example, an ISAO selected the EclecticIQ Platform as its TIP, all of the threat hunters and analysts would ingest their threat data into that platform. This would allow for the build-out of a very specialized database upon which to perform further correlation, analytics and testing.

Students of cyber threat analysis must understand these basics in order to be discriminating in allowing feeds from previous non-JSON sources into their TIP and in order to deploy conversion programs for non-compliant data sources. The EclecticIQ platform provides the cyber threat analyst with a configuration menu that allows for very easy programming of these application interfaces.

Work is ongoing within the CTI TC to further develop and extend the STIX data model to include other data objects important to key communities of interest, to further define additional Cyber Observable objects, and to further define the STIX Patterning language. As the protocol suite matures threat analysts will have an even more robust ontology for characterizing suspicious activity on their endpoints and networks. Also, students of cyber threat analysis must grasp the significance of the new STIX 2.0 Patterning language (as given in Part 5 of the Committee Specification) and understand its implications for making the data model truly responsive to the dynamic threat environment. It is this Patterning Language that jettisons STIX 2.0 above all of the other predecessor ontologies making it more effective for today’s complex threat environment.

Students of cyber threat analysis can get involved in helping to further refine the STIX 2.x data model by becoming a member of OASIS and joining the CTI TC and its various subcommittees. Also, vendors of TIP and supplementary products will need to update their tools to reflect this evolving ecosystem just as EclecticIQ is going.3

The following subsection outlines the design implications when incorporating the STIX 2.0 data model into a TIP for a threat sharing program under an ISAC or an ISAO or for use by a managed security services provider (MSSP).

3.4 Design Implications for Using TIPs

As the STIX ontology and data model matures, the TIPs will be revised by the various vendors, including EclecticIQ, to reflect data elements that can be captured and characterized according to the STIX data model and shared under the sharing definitions of ISACs and ISAOs. How the cyber threat analyst uses the platform is contingent on many variables that stem from the sharing standards established by the ISAC/ISAO, the data processing needs of the community of interest, and the processing and visualization power of the TIP. Also, importantly, the database handling and mapping capabilities along with the seamlessness of the APIs will, in large part, dictate how accessible historical data are and how rapidly the analyst can respond to threats in real-time. EclecticIQs rich visualization engine provides a mechanism for cyber threat analysts to use when communicating linkages between indicators of

3 At present the candidate objects for STIX Version 2.1 include: Confidence, Course of Action (To be integrated with the OASIS OpenC2 protocol suite), Event, Incident, Infrastructure, Internationalization, Location, Opinion, Intel Note, and Malware (Expanded from Ver. 2.0).
compromise that indicate a related malicious infrastructure. This is an especially valuable feature for reporting to non-technical decision-makers.

Some communities are using legacy ontologies for TIP design and will continue along such a path. But, because of the global participation of the CTI TC members it is likely that legacy data models will be retired as more and more tools are designed to reflect the STIX 2.0 data model. Some criteria for TIP design and development are as follows:

- Ease of process for on-boarding new users;
- Data useable to threat analysts, risk and fraud analysts, malware analysts, network engineers and guardians, data scientists, decision makers, incident responders;
- Automated & manual ingestion of structures, semi-structured, and unstructured data;
- Automated & manual exporting of select data subsets in a variety of formats;
- APIs for security incident and event management (SIEM) consoles & other 3rd-Party tools (firewalls, routers and IDS/IPS network devices);
- Redaction capability to enforce privacy laws, regulations and restrictions;
- Crowdsourcing from multiple distributed threat analysts that each independently sight threat indicators and share with a designation of malicious;
- Visual analysis of IOCs and enriched data (internal or used through an API); and
- Seamless integration with incident response tools.

Apart from the idealized version, there are specific design criteria that drive vendor build cycles based on customer needs. It is a matter of priority, scheduling, staffing, and the sales cycle. Importantly for our exposition here, it is also a matter of having trained cyber threat analysts that understand the underlying threat context and how to use the STIX 2.x model to capture ongoing threat activity for their organisation. Students trained as part of CTIN’s programs, using the EclecticIQ platform, have an advantage in the job marketplace because they have been exposed to the seven core principles from Riley’s work and the hands-on practice that the EclecticIQ platform provides.

Some TIP vendors have made a design decision to incorporate extensive internal queries into the back-office processing engine of the TIP, not exposed to the analyst. Others have exposed the query functionality enabling the analyst full rein in designing his/her inquiry path.

Eclectic IQ has made the design decision to expose the query functionality to the analyst, to allow for fine-tuning of query statements that closely match the data and the research objectives of the analyst. This gives the analyst more control over data that are extracted from open source and proprietary feeds. It also allows for the reduction of false positives, which is a problem that is plaguing many ISACs and ISAOs due to the immaturity of the users and the feeds.

An idealized version of a fully developed STIX-based TIP is given as Exhibit 3-2.
A platform like EclecticIQs provides outputs that can very easily be used for sophisticated statistical analysis tools such as those using the Multi-Attribute Utility Theory (MAUT) approach as shown in Exhibit 3-2.4

There is also wide variability with respect to the use of internal tools for visualization and graphic representation of the threat data. Some TIPs do not provide a visualization engine; they only provide for APIs to other tools such as Key Lines5 or Tableau6. Others have been built to include very robust, dynamic and editable visualization tools. The EclecticIQ platform includes a visualization tool that can show correlations between malicious infrastructures, threat actor tools and TTPs, targeted vulnerabilities in a victim’s infrastructure and other useful variables.

4 An explanation of how MAUT is used can be found here: https://www.ctg.albany.edu/publications/guides/and_justice_for_all?chapter=9&PrintVersion=2
5 A tool developed by Cambridge Intelligence. A summary of the tool can be found here: https://cambridgeistelligence.com/keylines/
6 A premium subscription visualization engine. Information on the tool can be found here: https://www.tableau.com/
### 4.0 Applied learning

Whether for workforce training or for academic education of information technology students, applied and hands-on lab work is critical to enforcing learning objectives and providing students with practical knowledge upon which to build. This section describes our proposal for using the EclecticIQ TIP for both training frameworks.

### 4.1 Capabilities of the EclecticIQ TIP to Be Used for Training Purposes

We have argued that training for threat analysts requires that the analyst be given theoretical frameworks guiding hypothesis formulation and testing and knowledge of the tradecraft for effective integration into ongoing threat intel teams. We have also argued that a robust and highly configurable TIP is most useful for ensuring that the analyst understand the basic workflows and all of the various features needed for ingesting feeds, enriching data, performing analysis, and presenting findings.

And, in Section 3.4 we enumerate a series of evaluation criteria that a decision-maker could apply when making a procurement decision for an MSSP, an ISAO sharing platform, or an enterprise-level internal threat hunting team. Exhibit 4-1 summarizes some of the features of the EclecticIQ TIP in accordance with these criteria that illustrate why it is the perfect candidate for training in any of these applications.

#### Exhibit 4-1 – The EclecticIQ Threat Intelligence Platform: Summary of Features

<table>
<thead>
<tr>
<th>#</th>
<th>Customer question</th>
<th>Platform Capability</th>
</tr>
</thead>
</table>
| 1  | Summary of the Onboarding Process         | 1. Workshop to discuss the data sources, data types, transport mechanisms, users and use-cases, also integration with other systems and plan deployment (week1)  
2. Deployment (weeks 2-3)  
3. UAT (week 4)  
4. GoLive into Production (weeks 5-6) |
| 2  | Manual and/or automated ingestion of feeds | 1. Automatic ingestion of feeds (e.g. STIX/TAXII)  
2. Manual Upload of files (e.g. PDF)  
3. Manual TI creation via the Entity Editor feature (STIX) |
| 3  | Exporting of feeds (formats, capability)   | 1. Outgoing feeds, configurable timing, various formats. |
| 4  | Integration with SIEMs                    | HPE ArcSight, Splunk, IBM QRadar, etc. |
| 5  | Intelligence Reporting Functionality      | Report and metrics |
| 6  | Third party integrations                  | 1. In addition to the SIEM integrations, enrichment possibilities abound (e.g. VirusTotal, GeoIP, Passive DNS, etc)  
2. End Point protection solutions |
| 7  | Visual analysis integration               | Graph feature native to the system |
| 8  | Integration with Incident Response        | Ability to ingest / create / distribute Incident Report entities inside the platform (STIX incidents). |
The EclecticIQ TIP has pre-defined APIs for a number of state-of-the-art vendor products designed to support the cybersecurity supply chain.

4.2 Example Workflows for TIPs

To effectively apply a TIP-based learning curriculum lessons for students of cyber threat analysis should be drawn directly from the workflows of operational units such as MSSPs and internal threat huntingcells. Specific use cases can give students a sense of how TIPs function within an enterprise when different geographically dispersed teams collaborate on cyber threat intelligence sharing. Also, use cases built on ISACs and ISAOs as trust communities can be used for training purposes.

Also, it is sometimes easier to help mid-career professionals understand the usefulness of TIPs by building on use cases they are familiar with such as a formal Incident Response workflow. In this case a network engineer may have a set of tools he/she uses that can be supplemented by seeking additional threat data from a sharing community during an incident. Exhibit 4-2 illustrates such a use case as it would be used on the EclecticIQ platform.

Exhibit 4-2 – Incident Responder Uses EclecticIQ TIP as Basis for Researching IOCs

Another possible use case for training students on how to perform cyber threat analysis by using a TIP is that of a sharing community. This scenario is quite common in Europe and the U.S. ISACs and ISAOs cannot find qualified personnel to perform these functions. Our joint training programs are aimed at filling this workforce gap by offering our joint programs for veteran training, in-house information technology staff upgrade training, ISAC and ISAO member training and other training scenarios.
Note that the cyber threat analyst has the option of either ingesting indicators of compromise manually or configuring his instance of the platform for automatic ingestion. Many corporate customers have used the automatic ingestion feature by configuring a bi-directional flow between a security event and incident monitoring (SEIM) devise and the EclecticIQ TIP. This approach is the full realization of the STIX 2.0 data model for enabling wire speed machine readable threat intelligence. Advanced persistent threats and other complex attack vectors are common in the modern world; why not use tools and training that prepares the workforce to counter these threats?

This workflow is illustrated by Exhibit 4-3.

Exhibit 4-3 – Member of ISAC or ISAO Shares IOCs to the Trust Community

5.0 Conclusions

In this paper we have shown how the capabilities of the TIP are important in the design, development and deployment of threat intelligence training programs. Depending upon the learning objectives of the specific training program there are many features of TIPs that can be used to focus the curriculum. This can include, but not is limited to:

- Cyber threat analysis;
- Programming for inbound and outbound feeds (e.g., XML, JSON, ANTLR, Python, etc.);
- Query Programming (e.g., SQL, Elastic Search with Kibana);
- Predictive analysis;
- Visualization techniques;
- Analysis of competing hypotheses;
- Report writing.

The STIX 2.0 data model will drive innovation in the TIP market and vendors that do not adapt their products quickly will not be able to keep up with market innovations from data feed producers, third-
party enrichment services, analytic and visualization vendors and the needs of consumers. Students of cyber threat analysis that are seeking to hone their current skills or re-tool for this emerging ecosystem will have greatly increased opportunities by using a robust TIP as part of their skills enhancement program.

Employers will do well by supporting their employees that seek these skills upgrades. Workforce development is a key concern of companies and public sector organizations. The EclecticIQ TIP working with the advanced training curriculum of CTIN can be used to focus training to achieve this goal. The our joint offering provides an elegant solution for such an objective.

6.0 References


APPENDIX 1 – STIX 2.0 Features

Within the STIX 2.0 data model there are a number of enumeration and classification systems that may be used for external reference for specific subsets of the cybersecurity ecosystem, as illustrated on Exhibit A1-1. Several of these subsystems are incorporated by reference into the STIX 2.0 ontology or can easily be incorporated through the use of open vocabularies, built into the STIX nomenclature.

Exhibit A1-1 – Enumeration and Classification Systems

<table>
<thead>
<tr>
<th>Community of Interest</th>
<th>Acronym</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware research and analysis</td>
<td>MAEC</td>
<td>Malware Attribute Enumeration and Classification</td>
</tr>
<tr>
<td>Incident responders &amp; threat analysts</td>
<td>CAPEC</td>
<td>Common Attack Pattern Enumeration and Classification</td>
</tr>
<tr>
<td>Threat analysts &amp; network engineers</td>
<td>CWSS</td>
<td>Common Weakness Scoring System</td>
</tr>
<tr>
<td>Risk analysts</td>
<td>CWRAF</td>
<td>Common Weakness Risk Analysis Framework</td>
</tr>
<tr>
<td>Network engineers</td>
<td>CWE</td>
<td>Common Weakness Enumeration</td>
</tr>
<tr>
<td>Network engineers &amp; threat analysts</td>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
</tr>
</tbody>
</table>

Exhibit A1-2 provides a summary of the architecture for STIX 2.0 which includes a listing of the eighteen Cyber Observable objects. Note that the nodes are the SDOs and the edges (lines with properties) are the SROs.

Exhibit A1-2 – STIX 2.0 Architecture
Therefore, if a TIP maps well to the STIX 2.0 data model it will also give the cyber threat analyst access to these and other enumeration and classification systems significantly extending the usability of the TIP for multiple communities of interest. STIX can be described as the overarching model that gives each community of interest a common framework for expressing and extending each of these ontologies in a manner that best suits their specific threat intelligence sharing objectives.

The STIX 2.0 Specification is divided into the following five parts:

- STIX Version 2.0 Part 2: STIX Objects
- STIX Version 2.0 Part 3: Cyber Observable Core Concepts
- STIX Version 2.0 Part 4: Cyber Observable Objects
- STIX Version 2.0 Part 5: STIX Patterning

The core concepts include the basic design principles and outline the fact that STIX is a graph-based data model with nodes (STIX Data Objects [SDOs]) and edges (STIX Relationship Objects [SROs]). The Mandatory to Implement (MTI) language for vendors seeking to claim STIX compliance and product interoperability is JavaScript Object Notation (JSON). Data markings for sharing restrictions are provided at the overall “object” level (e.g., Threat Actor Object), and also at more granular levels based on the properties of specific objects in the data model (e.g., “aliases” a Threat Actor may use).

As noted above, STIX 2.0 is highly extensible to the various enumeration and classification systems. As part of the 2.0 revision, STIX has completely subsumed the Cyber Observable Exchange enumeration system formerly known as CybOX.

The STIX data objects included in the recent Version 2.0 release and displayed in Exhibit A1-2 are as follows:

- Attack Pattern
- Campaign
- Course of Action (Stub)\(^7\)
- Identity
- Indicator
- Intrusion Set
- Malware (Stub)\(^8\)
- Observed Data
- Report
- Threat Actor
- Tool
- Vulnerability

The reader will note that parts three and four of the five-part protocol outline the core concepts and the data objects that are now characterized as “Cyber Observables” (i.e., the old CybOX). This includes the following data objects, also displayed in Exhibit 3-3 in the vertical blue box at the right of the figure:

\(^7\) The “Stub” qualifier notes that the Object was included in Version 2.0 with the proviso that it will be further flushed out in subsequent versions.

\(^8\) Ibid. Footnote 3.
A Collaboration Between:

- Autonomous System (AS)
- Directory
- Domain Name
- Email Address
- Email Message
- File
- IPV4 Address
- IPV6 Address
- MAC Address
- MUTEX
- Network Traffic
- Process
- Software
- URL
- User Account
- Windows Registry Key
- X509 Certificate

The reader will also note that the final part of the five-part protocol is the new STIX Patterning Language that has been developed by the CTI TC. Patterning was developed as an abstraction layer between the STIX data model and other proprietary frameworks that are in common usage in the cybersecurity industry such as SNORT, Bro, Yara and Suricata. These signature-based ontologies represent tried-and-true methods for network and endpoint defenders in configuring devices on known threats such as malware variants or netflow patterns monitored by intrusion detection systems (IDSs). STIX Patterning provides a common mechanism for integrating threat intelligence and remedial action functions using these signatures.

The key elements of the new STIX Patterning language are:

- Supports STIX patterns for Indicator sharing - Expressed using “Cyber Observable” objects;
- Enhances detection of malicious activity on endpoints & networks;
- Functions as an abstraction layer capable of serializing proprietary correlation rules;
- Is expressed as Unicode – Using ANTLR Grammar;\(^\text{15}\)
- Based on the key building blocks of:
  - Observation Expression
  - Comparison Expression
  - Observation Operator

---

\(^9\) The File Object also includes a number of extensions that further define the properties of the object.

\(^10\) The Network Traffic Object also includes a number of extensions that further define the properties of the object.

\(^11\) https://www.snort.org/

\(^12\) https://www.bro.org/

\(^13\) https://virustotal.github.io/yara/

\(^14\) https://suricata-ids.org/

\(^15\) Another Tool for Language Recognition (ANTLR) was developed by Terrance Parr and is available here: http://www.antlr.org/
Exhibit A1-3 provides an illustration and another example of how the STIX Patterning language works and frames out these key building blocks diagrammatically.

**Exhibit A1-3 – STIX Patterning Language Diagram**

Five select examples of STIX Patterns from the STIX Version 2.0 Specification illustrating the syntax and key building blocks are given below.

**Matching on a Domain Name with IPv4 Resolution**

\[
\text{[domain-name:value} = \text{'www.5z8.info'} \text{AND domain-name:resolves_to_refs['].value} = \text{'198.51.100.1/32']}\]

**Matching on Malware Beaconing to a Domain Name**

\[
\text{[network-traffic:dst_ref.type} = \text{'domain-name'} \text{AND network-traffic:dst_ref.value} = \text{'example.com']} \text{REPEATS 5 TIMES WITHIN 1800 SECONDS}\]

**Matching on an X509 Certificate**

\[

**Matching on an Email Message with specific Sender and Subject**

\[
\text{[email-message:sender_ref.value} = \text{'jdoe@example.com'} \text{AND email-message:subject} = \text{'Conference Info']}\]

**Matching on a File with a set of properties**

\[
\text{[(file:name} = \text{'pdf.exe'} \text{OR file:size} = \text{'371712'}) \text{AND file:created} = \text{'2014-01-13T07:03:17Z']}\]
APPENDIX 2 – STIX 2.0 Versioning

The CTI TC envisions a regular tempo of about six to nine months each for versioning of the STIX 2.x protocol and its supplementary specification for the transport of STIX data objects, TAXII. As the STIX 2.x, JSON-based version matures, more of the original CybOX objects will be updated from their XML-base to the new JSON-base.

Also, importantly, the STIX 2.x Cyber Observable object has been designed to accommodate extensibility into the mobile and cellular market threat arena, the industrial control system (ICS) arena, the internet of things (IoT) arena, and the digital forensics/incident response (DFIR) arena. The STIX 2.0 community is actively seeking additional members to help define the data objects (and their object properties) that will effectively characterize threat activity within these domains.