Catalogue of Cybersecurity Standards

Zareen Syed, Tim Finin and Ankur Padia

University of Maryland Baltimore County
1000 Hilltop Circle, MD, USA 21250
zsyed@umbc.edu, finin@cs.umbc.edu, pankur1@umbc.edu

Table of Contents

1. High level descriptions and frameworks

1.1 Structured Threat Information eXpression (STIX)

1.2 Open Vulnerability and Assessment Language (OVAL)

1.3 The Vocabulary for Event Recording and Incident Sharing (VERIS)

1.4 The Incident Object Description Format (IODEF)

2. Actionable observables

2.1 Cyber Observables eXpression (CybOX)

2.2 Mandiant's Open Indicators of Compromise (OpenIOC)

2.3 Malware Attribute Enumeration and Characterization (MAEC)

3. Enumerations

3.1 Common Attack Pattern Enumeration and Classification (CAPEC)

3.2 Common Vulnerabilities and Exposures (CVE)

3.3 Common Weakness Enumeration (CWE)

3.4 The Common Configuration Enumeration (CCE)

3.5 Common Platform Enumeration (CPE)

4. Scoring and measurement frameworks

4.1 Common Vulnerability Scoring System (CVSS)

4.2 Common Weakness Scoring System (CWSS)

4.3 The Extensible Configuration Checklist Description Format (XCCDF)

4.4 Common Configuration Scoring Scheme (CCSS)

5. Process frameworks

5.1 The Security Content Automation Protocol (SCAP)

5.2 Cybersecurity Information Exchange, Recommendation ITU-T X.1500 (CYBEX)

6. Transport

6.1 Trusted Automated eXchange of Indicator Information (TAXII)

6.2 The OASIS Customer Information Quality (CIQ)

Catalog of Cybersecurity Standards

1. High level descriptions and frameworks

These standards combine multiple types of information for e.g. including indicators, affected assets, actions that were taken, and other contextual information.

1.1 Structured Threat Information eXpression (STIX)

STIX™ is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. STIX provides a unifying architecture tying together a diverse set of cyber threat information including:

1. Cyber Observables
2. Indicators
3. Incidents
4. Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.)
5. Exploit Targets (e.g., vulnerabilities, weaknesses or configurations)
6. Courses of Action (e.g., incident response or vulnerability/weakness remedies or mitigations)
7. Cyber Attack Campaigns
8. Cyber Threat Actors

Overseeing Organization: STIX is being transitioned from MITRE and DHS to OASIS.

1.2 Open Vulnerability and Assessment Language (OVAL)

OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community. Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

Overseeing Organization: OVAL has been transitioned from MITRE to Center for Internet Security (CIS).

1.3 The Vocabulary for Event Recording and Incident Sharing (VERIS)

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a metrics framework designed to provide a common language for describing security incidents and their effects in a structured manner. The difference between STIX incidents and VERIS is in purpose and use: VERIS is an after-the-fact characterization of cyber incidents intended for post-incident strategic trend analysis and risk management. STIX provides the capability to capture information about security incidents and their effects but does so in the context of a broader threat intelligence framework.

Overseeing Organization: Verizon

1.4 The Incident Object Description Format (IODEF)

The Incident Object Description Format (IODEF) is an Internet Engineering Task Force (IETF) standard developed for exchange of incident information. There is no formal relationship between STIX and IODEF, although it is possible to leverage IODEF within STIX in order to represent incident information. Doing so, however, would lose the richness and architectural alignment provided by the STIX Incident structure.

Overseeing Organization: IETF, Managed Incident Lightweight Exchange (MILE) working group

2. Actionable observables

Standards for cyber observables represent information used to detect attacks or malicious activity (such as system libraries used by a malware). A cyber observable is a measurable event or stateful property in the cyber context. Examples of measurable events include registry key creation, file deletion, and the sending of an HTTP GET request; examples of stateful properties include the MD5 hash of a file, the value of a registry key, and the name of a process.

2.1 Cyber Observables eXpression (CybOX)

The Cyber Observable eXpression is a standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain. A wide variety of high-level cyber security use cases rely on such information including: event management/logging, malware characterization, intrusion detection, incident response/management, attack pattern characterization, etc. CybOX provides a common mechanism (structure and content) for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability and overall situational awareness. STIX leverages

CybOX for this purpose, such as in indicator patterns, infrastructure descriptions, and course of action parameters.

Overseeing Organization: Cybox is being transitioned from MITRE to OASIS.

2.2 Mandiant’s Open Indicators of Compromise (OpenIOC)

The STIX Indicator's test mechanism field is an extensible alternative to providing an indicator signature in something other than CybOX. Mandiant’s Open Indicators of Compromise, Open Vulnerability and Assessment Language (OVAL), SNORT rules, and YARA rules are supported as default extensions to that test mechanism field.

Overseeing Organization: MANDIANT

2.3 Malware Attribute Enumeration and Characterization (MAEC)

MAEC is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns. By eliminating the ambiguity and inaccuracy that currently exists in malware descriptions and by reducing reliance on signatures, MAEC aims to improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware; reduce potential duplication of malware analysis efforts by researchers; and allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances. STIX leverages MAEC via the TTP construct for this purpose, and additionally both STIX and MAEC use CybOX.

Overseeing Organization: MITRE, DHS

3. Enumerations

Enumerations define global identifiers to reference shared data objects for e.g. Common Vulnerabilities and Exposures (CVE).

3.1 Common Attack Pattern Enumeration and Classification (CAPEC)

CAPEC is a publicly available, community developed list of common attack patterns along with a comprehensive schema and classification taxonomy. Attack patterns are descriptions of common methods for exploiting software systems. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. STIX can utilize Common Attack Pattern Enumeration and Classification (CAPEC) for structured characterization of tactics, techniques, and procedures (TTP) attack patterns through use of the CAPEC schema extension.

Overseeing Organization: MITRE, DHS

3.2 Common Vulnerabilities and Exposures (CVE)

CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE’s common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Overseeing Organization: MITRE, DHS

3.3 Common Weakness Enumeration (CWE)

CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Overseeing Organization: MITRE, DHS

3.4 The Common Configuration Enumeration (CCE)

The Common Configuration Enumeration, or CCE, assigns unique entries (also called CCEs) to configuration guidance statements and configuration controls to improve workflow by facilitating fast and accurate correlation of configuration issues present in disparate domains. In this way, it is similar to other comparable data standards such as the Common Vulnerability and Exposure (CVE) List, which assigns identifiers to publicly known system vulnerabilities.

Overseeing Organization: Transitioned from MITRE to NIST

3.5 Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE does not identify unique instantiations of products on systems, such as the installation of XYZ Visualizer Enterprise Suite 4.2.3 with serial number Q472B987P113. Rather, CPE identifies abstract classes of products, such as XYZ Visualizer Enterprise Suite 4.2.3, XYZ Visualizer Enterprise Suite (all versions), or XYZ Visualizer (all variations).

Overseeing Organization: Transitioned from MITRE to NIST

4. Scoring and measurement frameworks

These standards define quantitative description of threats.

4.1 Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. It attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized. The scores are based on a series of measurements (called metrics) based on expert assessment. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Overseeing Organization: It is under the custodianship of the Forum of Incident Response and Security Teams (FIRST).

4.2 Common Weakness Scoring System (CWSS)

The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry. CWSS standardizes the approach for characterizing weaknesses. Users of CWSS can invoke attack surface and environmental metrics to apply contextual information that more accurately reflects the risk to the software capability, given the unique business context it will function within and the unique business capability it is meant to provide. This allows stakeholders to make more informed decisions when trying to mitigate risks posed by weaknesses. CWSS is distinct from - but not a competitor to - the Common Vulnerability Scoring System (CVSS). These efforts have different roles, and they can be leveraged together.

Overseeing Organization: MITRE, DHS

4.3 The Extensible Configuration Checklist Description Format (XCCDF)

XCCDF was created to document technical and non-technical security checklists using a standardized format. The general objective is to allow security analysts and IT experts to create effective, interoperable automated checklists, and to support the use of these checklists with a wide variety of tools. A checklist is an organized collection of rules about a particular kind of system or platform. Automation is necessary for consistent and rapid verification of system security because of the sheer number of things to check and the number of hosts within an organization that need to be assessed (often many thousands). XCCDF enables easier, more uniform creation of security checklists, which in turn helps to improve system security by more consistent and accurate application of sound security practices. Adoption of XCCDF lets security professionals, security tool vendors, and system auditors exchange information more quickly and precisely, and also permits greater automation of security testing and configuration assessment. XCCDF development is being pursued by NIST, the NSA, The MITRE Corporation, and the US Department of Homeland Security. XCCDF is intended to serve as a replacement for the security hardening and analysis documentation written in prose. XCCDF is used by the Security Content Automation Protocol.

Overseeing Organization: NIST

4.4 Common Configuration Scoring Scheme (CCSS)

CCSS addresses software security configuration issue vulnerabilities. CCSS is largely based on CVSS and CMSS, and it is intended to complement them.

Overseeing Organization: NIST

5. Process frameworks

These are frameworks for exchanging security information, they leverage formats and protocols defined by other standards.

5.1 The Security Content Automation Protocol (SCAP)

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP. SCAP combines a number of open standards that are used to enumerate software flaws and configuration issues related to security. They measure systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact. It is a method for using those open standards for automated vulnerability management, measurement, and policy compliance evaluation. SCAP defines how the following standards (referred to as SCAP 'Components') are combined:

1. Common Vulnerabilities and Exposures (CVE)
2. Common Configuration Enumeration (CCE)
3. Common Platform Enumeration (CPE)
4. Common Weakness Enumeration (CWE)
5. Common Vulnerability Scoring System (CVSS)
6. Extensible Configuration Checklist Description Format (XCCDF)
7. Open Vulnerability and Assessment Language (OVAL)

Overseeing Organization: NIST

5.2 Cybersecurity Information Exchange, Recommendation ITU-T X.1500 (CYBEX)

Recommendation ITU-T X.1500 describes techniques for the exchange of security information. It includes guidance in on several key functions related to information exchange: structuring security information, identifying security information and entities; establishment of trust between entities; requesting and responding with security information; and assuring the integrity of the security information exchange.

Overseeing Organization: ITU-T

6. Transport

6.1 Trusted Automated eXchange of Indicator Information (TAXII)

TAXII (Trusted Automated eXchange of Indicator Information) is the main transport mechanism for cyber threat information represented in STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner. Like STIX, TAXII is led by DHS and the STIX and TAXII communities work closely together (and in fact consist of many of the same people) to ensure that they continue to provide a full stack for sharing threat intelligence.

Overseeing Organization: OASIS

6.2 The OASIS Customer Information Quality (CIQ)

The OASIS Customer Information Quality (CIQ) is a language for representing information about individuals and organizations. The STIX Identity structure uses an extension mechanism to represent identify information used to characterize malicious actors, victims and intelligence sources. The STIX-provided extension leverages CIQ. CIQ Specifications enables organisations to have a unified and consistent representation and standardization of their party data (e.g. employee, members, suppliers, partners, customers, etc) and use it to support various application requirements in the organisation that deal with party data (e.g. Master Data Management (MDM), Customer/Party Data Integration, Party identification/recognition/identity management, HR, billing, sales, marketing, data quality and integrity, e-commerce/e-business, party data exchange, postal services, customer/party views, etc). By representing and managing party data consistently using CIQ specifications as the base scheme for an organisation, and extending it to support specific business requirements, unique identitification, integration, standardisation, matching, synchonization and management of quality party information/data is possible.

Overseeing Organization: OASIS