Cyber Observable eXpression — CybOX™
A Structured Language for Cyber Observables

CybOX provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security that improves the consistency, efficiency, and interoperability of deployed tools and processes, as well as increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics.

Examples of cyber observables include:

- **A Registry Key is created**
- **A File is deleted**
- **A Mutex exists**
- **Specific HTTP Get Request received**
- **A file has a specific MD5 hash**
- **Data is sent to an address on a socket**
- **Network traffic occurs to specific IP addresses**
- **Email from a specific address is observed**
- **Application logs show communication on certain ports**
- **A service's configuration is changed**
- **A remote thread is created**

International in scope and free for public use, CybOX is a structured language 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, indicator sharing, etc. CybOX provides a common structure for representing cyber observables across and among these use cases thereby improving consistency, efficiency, interoperability, and overall situational awareness for the enterprise.

Challenge

The concept of observable events or properties in the operational cyber realm is a central underlying element of many of the different activities involved in cyber security. Until recently, no uniform structured mechanism existed for specifying, capturing, characterizing, or communicating these cyber observables. Each activity area, each use case and often each supporting tool vendor uses its own unique approach that inhibits consistency, efficiency, interoperability and overall situational awareness.

Solution

CybOX is a standardized language for representing cyber observables, whether dynamic events or stateful properties that are observable in the operational cyber domain. CybOX is not targeted at a single cyber security use case but rather is intended to be flexible enough to offer a common solution for all cyber security use cases requiring the ability to deal with cyber observables. It is also intended to be flexible enough to allow both the high-fidelity description of instances of cyber observables that have been measured in an operational context as well as more abstract patterns for potential observables that may be targets for observation and analysis apriori. By specifying a common structured schematic mechanism for these cyber observables, CybOX enables detailed automatable sharing, mapping, detection and analysis heuristics.

CybOX is targeted to support a wide range of relevant cyber security domains including:

- Threat assessment and characterization (detailed attack patterns)
- Malware characterization
- Operational event management
- Logging

CybOX
cybox.mitre.org

CybOX is a U.S. Department of Homeland Security–led effort of the office of Cybersecurity and Communications. MITRE, operating as DHS's FFRDC, manages the CybOX website, community engagement, and discussion lists to enable open and public collaboration with all stakeholders.

- Cyber situational awareness
- Incident response
- Indicator sharing
- Digital forensics
- Etc.

Through utilization of the standardized CybOX Language, relevant observable events or properties can be captured and shared, defined in indicators and rules, or used to adorn the appropriate portions of attack patterns and malware profiles in order to tie the logical pattern constructs to real-world evidence of their occurrence or presence for attack detection and characterization. Incident response and management can then take advantage of all of these capabilities to investigate occurring incidents, improve overall situational awareness and improve future attack detection, prevention and response.

Supported Use Cases

CybOX is intended to be flexible enough to provide a common foundation for a wide diversity of cyber security use cases requiring the ability to deal with cyber observables. For most use cases, the utilization of CybOX should be indirect with primary focus on the use case domain-specific standard or solution which leverages CybOX as an enabler. See table at right for examples of current use cases.

Feedback Requested

CybOX Community members can make contributions to CybOX development and manage issue tracking for the CybOX schemas, utilities, specifications, and supporting information by joining the CybOX Community at https://cybox.mitre.org/community/. Members of the cyber security community are invited to participate in this growing community effort.

Supported Use Case	Relevant Process	Domain Specific Standard
Analyze event data from diverse set of sensors of different types and different vendors	Event Management	CybOX
Detect malicious activity utilizing attack patterns	Attack Detection	Common Attack Pattern Enumeration and Classification (CAPEC™)
Detect malicious activity utilizing malware behavior characterizations	Attack Detection	Malware Attribute Enumeration and Characterization (MAEC™)
Enable automated attack detection signature rule generation	Attack Detection	CybOX, MAEC, CAPEC, STIX
Characterize malicious activity utilizing attack patterns	Incident Response/ Management	CAPEC, STIX
Identify new attack patterns	Threat Characterization	CAPEC
Prioritize existing attack patterns based on tactical reality	Security Testing and Secure Development	CAPEC, STIX
Characterize malware behavior	Malware Analysis	MAEC
Guide malware analysis utilizing attack patterns	Malware Analysis	MAEC, CAPEC
Detect malware effects	Attack Detection and Incident Response/ Management	STIX, MAEC, Open Vulnerability and Assessment Language (OVAL®)
Enable collaborative attack indicator sharing	Information Sharing	STIX, TAXII
Empower and guide incident management utilizing attack patterns and malware characterizations	Incident Response/ Management	STIX, CAPEC, MAEC, CybOX
Enable consistent, useful and automation-capable incident alerts	Incident Response/ Management	STIX, MAEC, CAPEC, CEE
Enable automatic application of mitigations specified in attack patterns	Incident Response/ Management	STIX
Enable incident information sharing	Incident Response/ Management	STIX, Trusted Automated eXchange of Indicator Information (TAXII™)
Support correlation between observed properties and malicious indicators as part of digital forensics	Digital Forensics	STIX, MAEC, CAPEC, ongoing work to refine Digital Forensics XML (DFXML) based on CybOX
Capture digital forensics analysis results	Digital Forensics	Ongoing work to refine DFXML based on CybOX
Capture digital forensics provenance information	Digital Forensics	Ongoing work to refine DFXML based on CybOX
Enable collaborative sharing of digital forensics information	Digital Forensics	Ongoing work to refine DFXML based on CybOX, STIX, TAXII
Enable explicit and implicit sharing controls for cyber observable information	Information Sharing	STIX, CybOX, TAXII
Enable new levels of meta-analysis on operational cyber observables	Cyber Situational Awareness	CybOX, STIX