STIX 2.0 Specification - Pre-Draft

Vocabularies - Version 0.2

Document Table of Contents

Document Development Status

TODO - This section should be removed from the document prior to completion. It is included here to help visually track where things are at in the process.

Each physical documents contains a table that defines 4 levels of development for each TLO and CTI concept. The first level is called Concept. Content coming in to one of the documents starts as a Concept. Once the community starts to work on it it will move to Development. During this phase, the group will flesh out the design and come up with normative text. As the group comes to general consensus the TLO will move to a Review phase. During this phase the community can comment and offer suggestions on the normative text and design. After a period of time of no comments or feedback, the TLO will move to its final stage of Draft.

Object / Concept	Status	MVP
`asset-kind-cv`	Concept	Undecided
`campaign-status-cv`	Concept	Undecided
`coa-kind-cv`	Concept	Undecided
`coa-stage-cv`	Concept	Undecided
`high-medium-low-cv`	Concept	Undecided
`intended-effect-cv`	Concept	Undecided
`malicious-infrastructure-label-cv`	Concept	Undecided
`malicious-tool-label-cv`	Concept	Undecided
`malware-label-cv`	Concept	Undecided
`planning-and-operations-cv`	Concept	Undecided
`report-label-cv`	Concept	Undecided
`threat-actor-kind-cv`	Concept	Undecided
`threat-actor-motivation-cv`	Concept	Undecided

`threat-actor-sophistication-cv`	Concept	Undecided

1. Controlled Vocabularies

1.1. Asset Kind

Type Name: `asset-kind-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`access-reader`	A device that protects an access point, using credentials. Both the access point and the credentials themselves can be virtual (password) or physical (access card).
`administrator`	
`atm`	An automatic teller machine.
`auditor`	
`auth-token`	A token used during authentication of an object, such as a user or system.
`backup`	A copy of data on a different storage device to be available in the case of destruction of the original data.
`broadband`	
`call-center`	A group of individuals that handles telephone inquiries for an organization
`camera`	A device for taking a photograph or video
`cashier`	A cashier is a person who handles the cash register at various locations such as the point of sale in a retail store.
`customer`	An individual or organization that purchases a product or service.

`database`	Software for efficiently storing large amounts of data.
`dcs`	A distributed control system (DCS) is a control system for a process or plant, where elements are distributed throughout the system.
`desktop`	A personal computer that generally isn't portable.
`developer`	An individual that develops hardware, software, etc.
`dhcp`	Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
`directory`	A file system artifact for storing a collection of other file system artifacts, including other directories
`disk-drive`	A device used to store data on a disk medium
`disk-media`	
`dns`	Domain name system (DNS) is a collection of names of a computer hardware and/or software artifacts on a computer network
`documents`	
`end-user`	
`executive`	
`file`	A file system artifact for storing data in a particular format
`finance`	
`firewall`	A network security system that limits access to trusted traffic
`flash-drive`	A solid state data storage device that does not contain any moving parts.
`former-employee`	An individual who was previously employee by an organization
`gas-terminal`	An internet enabled gasoline dispensing device.
`guard`	An individual who secures a particular device or location

`helpdesk`	A resource for users of a product to troubleshoot problems
`hsm`	A hardware security model (HSM) is a device that securely stores a digital cryptographic key.
`human-resources`	A department in an organization that performs personnel management.
`ids`	An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station
`kiosk`	
`lan`	A local area network (LAN)
`laptop`	A portable personal computer.
`log`	A digital recording of the activity of a device or process
`mail`	
`mainframe`	
`maintenance`	
`manager`	
`media`	An object used to store and deliver data
`mobile-phone`	A portable telephone that communicates over a cellular network
`network`	A collection of devices that are connected either physically or virtually
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`partner`	
`payment-card`	
`payment-switch`	

`pbx`	A private branch exchange (PBX) is a telephone switching system local to an organization
`ped-pad`	
`peripheral`	A device, which usually not logically or physically part of the main device, but connected physically or virtually.
`person`	
`plc`	A programmable logic controller (PLC) is a digital device used to control an electromechanical device.
`pos-controller`	
`pos-terminal`	
`print`	
`private-wan`	
`proxy`	
`public-wan`	
`remote-access`	
`router-or-switch`	
`rtu`	Remote Terminal Unit (RTU)
`san`	
`scada`	
`server`	
`smart-card`	
`tablet`	A portable personal computer without a hardware keyboard
`tapes`	A data media that uses spools of magnetic tape
`telephone`	
`unknown`	An unknown asset

`user-device`	
`voip-adapter`	
`voip-phone`	A telephone that communicates over voice internet protocol (VoIP)
`web-application`	A software application running on a server, which is accessed over the internet using a browser.
`wlan`	Wireless local area network (WLAN)

1.2. Campaign Status

Type Name: `campaign-status-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`ongoing`	This campaign is currently taking place.
`historic`	This campaign occurred in the past and is currently not taking place.
`future`	This campaign is expected to take place in the future.

1.3. COA Kind

Type Name: `coa-kind-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`diplomatic-actions`	Engaging in communications and relationship building with threat actors to influence positive changes in behavior.
`eradication`	Identifying, locating, and eliminating malware from the network.
`hardening`	Securing a system by reducing its attack surface by removing unnecessary software, usernames or logins, and services.
`internal-blocking`	Host-based blocking of traffic from an internal compromised source.
`logical-access-restrictions`	Activities associated with restricting logical access to computing resources.
`monitoring`	Setting up network or host-based sensors to detect the presence of a threat.
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`patching`	A specific form of hardening, patching involves applying a code fix directly to the software with the vulnerability.
`perimeter-blocking`	Perimeter-based blocking of traffic from a compromised source.
`physical-access-restrictions`	Activities associated with restricting physical access to computing resources.
`policy-actions`	Modifications to policy that reduce the attack surface or infection vectors of malware.
`public-disclosure`	Informing the public of the existence and characteristics of the threat or threat actor to influence positive change in adversary behavior.
`rebuilding`	Re-installing a computing resource from a known safe source in order to ensure that the malware is no longer present on the previously compromised resource.

`redirection`	Re-routing of suspicious or known malicious traffic away from the intended target to an area where the threat can be more safely observed and analyzed.
`redirection-honey-pot`	Setting up a decoy parallel network that is intended to attract adversaries to the honey pot and away from the real network assets.
`training`	Training users and administrators how to identify and mitigate threats.

1.4. COA Stage

Type Name: `coa-stage-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`remedy`	This COA is applicable to the "Remedy" stage of the threat management lifecycle, meaning it may be applied proactively to prevent future threats.
`response`	This COA is applicable to the "Response" stage of the threat management lifecycle, meaning it may be applied as a reaction to an ongoing threat.
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.5. High/Medium/Low

Type Name: `high-medium-low-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`high`	
`medium`	
`low`	
`none`	
`unknown`	
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.6. Intended Effect

Type Name: `intended-effect-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`account-takeover`	The intended effect of the incident was for the attacker to obtain control over an account (financial, etc)
`advantage`	The intended effect of the incident was for the attacker to obtain some advantage over the target
`advantage-economic`	The intended effect of the incident was for the attacker to obtain some economic advantage over the target
`advantage-military`	The intended effect of the incident was for the attacker to obtain some military advantage over the target
`advantage-political`	The intended effect of the incident was for

	the attacker to obtain some political advantage over the target
`brand-damage`	The intended effect of the incident was for the attacker to cause some brand damage on the target
`competitive-advantage`	The intended effect of the incident was for the attacker to obtain some non-specific competitive advantage over the target
`degradation-of-service`	The intended effect of the incident was reducing the level of services provided by the target
`denial-and-deception`	
`destruction`	The intended effect of the incident was to cause the destruction of a software or hardware system.
`disruption`	
`embarrassment`	The intended effect of the incident was to expose a socially unacceptable action by the target
`exposure`	
`extortion`	The intended effect of the incident was force the payment of some sort to prevent the attacker from taking some action.
`fraud`	
`harassment`	The intended effect of the incident was to pressure or intimidate the target
`ics-control`	
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

theft	The intended effect of the incident was to perpetrate a non-specific theft
theft-credentials	The intended effect of the incident was to perpetrate a theft of credentials
theft-identity	The intended effect of the incident was to perpetrate a theft of the target's identity
theft-intellectual-property	The intended effect of the incident was to perpetrate a theft of intellectual property
theft-proprietary-information	The intended effect of the incident was to perpetrate a theft of proprietary information
traffic-diversion	
v	

1.7. Malicious Infrastructure Label

Type Name: malicious-infrastructure-label-cv	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
anonymization	
anonymization-proxy	
anonymization-tor-network	
anonymization-vpn	
communications	
communications-blogs	
communications-forums	

`communications-internet-relay-chat`	
`communications-micro-blogs`	
`communications–mobile-communications`	
`communications-social-networks`	
`communications–user-generated-content-websites`	
`domain-registration`	
`domain-registration–dynamic-dns-services`	
`domain-registration –legitimate-domain-registration-services`	
`domain-registration–malicious-domain-registrars`	
`domain-registration–top-level-domain-registrars`	
`electronic-payment-methods`	
`hosting`	
`hosting-bulletproof-or-rogue-hosting`	
`hosting-cloud-hosting`	
`hosting-compromised-server`	
`hosting-fast-flux-botnet-hosting`	
`hosting-legitimate-hosting`	
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.8. Malicious Tool Label

Type Name: `malicious-tool-label-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`application-scanner`	
`malware`	Software designed to be used to attack or gain access to a computer system
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`password-cracking`	The process of using a software application to recover a plain text password from its encrypted representation
`penetration-testing`	The process of investigating a computer system to find security weaknesses.
`port-scanner`	A software application that reports on the status of the ports available on a host computer
`traffic-scanner`	A software application that monitors data transferred on a network
`vulnerability-scanner`	A type of software application used to discover vulnerabilities on a host, a network, or in a software product.

1.9. Malware Label

Type Name: `malware-label-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`automated-transfer-scripts`	
`adware`	Any software that is funded by advertising. Adware may also gather sensitive user information from a system.
`dialer`	A program to automatically dial a telephone
`bot`	A program that resides on an infected system, communicating with and forming part of a botnet. The bot may be implanted by a worm or Trojan, which opens a backdoor. The bot then monitors the backdoor for further instructions.
`bot-credential-theft`	A bot for the specific purpose to steal credentials
`bot-ddos`	A bot for the specific purpose to cause a denial of service attack.
`bot-loader`	
`bot-spam`	A bot for the specific purpose to send out spam email
`ddos`	
`ddos-participatory`	
`ddos-script`	
`ddos-stress-test-tools`	
`exploit-kits`	A software toolkit to target common vulnerabilities
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`pos-atm-malware`	Malware that exclusively targets point of sale (POS) systems or automatic teller machines (ATMs)
`ransomware`	A type of malware that encrypts files on a victim's system, demanding payment of ransom in return for the access codes required to unlock files.

remote-access-trojan	A remote access Trojan program or RAT, is a Trojan horse capable of controlling a machine through commands issue by a remote attacker.
rogue-antivirus	A fake security product that demands money to clean phony infections.
rootkit	A method of hiding files or processes from normal methods of monitoring, and is often used by malware to conceal its presence and activities. Rootkits can operate at a number of levels, from the application level - simply replacing or adjusting the settings of system software to prevent the display of certain information - through hooking certain functions or inserting modules or drivers into the operating system kernel, to the deeper level of firmware or virtualization rook kits, which are activated before the operating system and thus even harder to detect while the system is running.

1.10. Planning and Operation

Type Name: planning-and-operations-cv	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
data-exploitation	
Data-exploitation-analytic-support	
Data-exploitation-translation-support	
Financial-resources	
Financial-resources-academic	

`Financial-resources-commercial`	
`Financial-resources-government`	
`Financial-resources-hacktivist-or-grassroot`	
`Financial-resources-non-attributable-finance`	
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.
`planning`	
`planning-osint-gathering`	Open-Source Intelligence (OSINT)
`planning-operational-cover-plan`	
`planning-pre-operational-surveillance-and-reconnaissance`	
`planning-target-selection`	
`skill-development-recruitment`	
`skill-development-recruitment-contracting-and- hiring`	
`skill-development-recruitment-docex-training`	Document Exploitation (DOCEX)
`skill-development-recruitment-internal-training`	
`skill-development-recruitment-military-programs`	
`skill-development-recruitment-security-or-hacker-conferences`	

skill-development-recruitment-underground-forums	
skill-development-recruitment-university-programs	

1.11. Report Label

Type Name: report-label-cv	**Status:** Concept **MVP**: Undecided

Report intent is a controlled vocabulary enumeration descended from string. It is used in the intents field of report.

Vocabulary Value	Description
collective-threat-intelligence	Report is intended to describe a broad characterization of a threat across multiple facets.
threat-report	Report is intended to describe a broad characterization of a threat across multiple facets expressed as a cohesive report.
indicators	Report is intended to describe mainly indicators.
indicators-phishing	Report is intended to describe mainly phishing indicators.
indicators-watchlist	Report is intended to describe mainly network watchlist indicators.
indicators-malware-artifacts	Report is intended to describe mainly malware artifact indicators.
indicators-network-activity	Report is intended to describe mainly network activity indicators.

`indicators-endpoint-characteristics`	Report is intended to describe mainly endpoint characteristics (hashes, registry values, installed software, known vulnerabilities, etc.) indicators.
`campaign-characterization`	Report is intended to describe mainly a characterization of one or more campaigns.
`threat-actor-characterization`	Report is intended to describe mainly a characterization of one or more threat actors.
`exploit-characterization`	Report is intended to describe mainly a characterization of one or more exploits.
`attack-pattern-characterization`	Report is intended to describe mainly a characterization of one or more attack patterns.
`malware-characterization`	Report is intended to describe mainly a characterization of one or more malware instances.
`ttp-infrastructure`	Report is intended to describe mainly a characterization of attacker infrastructure.
`ttp-tools`	Report is intended to describe mainly a characterization of attacker tools.
`courses-of-action`	Report is intended to describe mainly a set of courses of action.
`incident`	Report is intended to describe mainly information about one or more incidents.
`observations`	Report is intended to describe mainly information about instantial observations (cyber observables).
`observations-email`	Report is intended to describe mainly information about instantial email observations (email cyber observables).

`malware-samples`	Report is intended to describe a set of malware samples.
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.12. Threat Actor Kind

Type Name: `threat-actor-kind-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`cyber-espionage-operations`	
`hacker`	
`hacker-white-hat`	
`hacker-gray-hat`	
`hacker-black-hat`	
`hacktivist`	
`state-actor-agency`	
`ecrime-actor-credential-theft-botnet-operator`	
`ecrime-actor-credential-theft-botnet-service`	
`ecrime-actor-malware-developer`	
`ecrime-actor-`	

`money-laundering-network`	
`ecrime-actor-organized-crime-actor`	
`ecrime-actor-spam-service`	
`ecrime-actor-traffic-service`	
`ecrime-actor-underground-call-service`	
`insider-threat`	
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.13. Threat Actor Motivation

Type Name: `threat-actor-motivation-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`ideological`	The threat actor is motivated by non-specific ideological reasons.
`ideological-anti-corruption`	The threat actor is motivated to attack targets engaging in corruption.
`ideological-anti-establishment`	The threat actor is motivated to attack established authority
`ideological-environmental`	The threat actor is motivated to attack targets engaging in actions detrimental to the

	environment.
`ideological-ethnic-or-nationalist`	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
`ideological-information-freedom`	The threat actor is motivated by the belief in the freedom of information.
`ideological-religious`	The threat actor is motivated to attack targets associated with a religion.
`ideological-security-awareness`	
`ideological-human-rights`	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
`ego`	The threat actor is motivated by enhancing their own self worth.
`financial-or-economic`	The threat actor is motivated by financial gain.
`military`	The threat actor is motivated by the desire to exercise some military advantage.
`opportunistic`	The threat actor is motivated by the relative vulnerability of the target
`political`	The threat actor is motivated by the desire to exercise some political advantage.
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.

1.14. Threat Actor Sophistication

Type Name: `threat-actor-sophistication-cv`	**Status:** Concept **MVP**: Undecided

< enter description >

Vocabulary Value	Description
`innovator`	Demonstrates sophisticated capability. An innovator has the ability to create and script unique programs and codes targeting virtually any form of technology. At this level, this actor has a deep knowledge of networks, operating systems, programming languages, firmware, and infrastructure topologies and will demonstrate operational security when conducting his activities. Innovators are largely responsible for the discovery of 0-day vulnerabilities and the development of new attack techniques.
`expert`	Demonstrates advanced capability. An actor possessing expert capability has the ability to modify existing programs or codes but does not have the capability to script sophisticated programs from scratch. The expert has a working knowledge of networks, operating systems, and possibly even defensive techniques and will typically exhibit some operational security.
`practitioner`	Has a demonstrated, albeit low, capability. A practitioner possesses low sophistication capability. He does not have the ability to identify or exploit known vulnerabilities without the use of automated tools. He is proficient in the basic uses of publicly available hacking tools, but is unable to write or alter such programs on his own.
`novice`	Demonstrates a nascent capability. A novice has basic computer skills and likely requires the assistance of a Practitioner or higher to engage in hacking activity. He uses existing and frequently well known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet and lacks the ability to conduct his own reconnaissance and targeting research.
`aspirant`	Demonstrates no capability.
`other`	Using the value of `other` MAY indicate that an alternative value has been provided using the `vocab-ext` extension point, but no fallback value is being provided.