Schema

package: "https://openc2_stix_sco"
version: "0-wd01 "
title: "STIX SCO Core jadn"
exports: ["STIX-Cybersecurity-Observables", "SCO", "artifact", "autonomous_system", "directory", "domain_name", "email_addr", "email_message", "file", "ipv4_addr", "ipv6_addr", "mac_addr", "mutex", "network_traffic", "process", "software", "url", "user_account", "windows_registry_key"]
config: {"$MaxBinary": 5555, "$MaxString": 5555, "$MaxElements": 555, "$Sys": "$", "$TypeName": "^[A-Za-z][-:_A-Za-z0-9]{0,63}$", "$FieldName": "^[A-Za-z][-:_A-Za-z0-9]{0,63}$", "$NSID": "^[A-Za-z][A-Za-z0-9]{0,7}$"}

Compound Types

STIX-Cybersecurity-Observables

An Array of Cybersecurity Observables in STIX formatting

STIX-Cybersecurity-Observables (ArrayOf(SCO))

SCO

Availiable Cybersecurity Observables in the STIX language

SCO (Choice)

ID	Name	Type	Description
1	Artifact	artifact	
2	Autonomous-System	autonomous-system	
3	Directory	directory	
4	Domain-Name	domain-name	
5	Email-Addr	email-addr	
6	File	file	
7	IPv4-Addr	ipv4-addr	
8	IPv6-Addr	ipv6-addr	
9	Mac-Addr	mac-addr	
10	Mutex	mutex	
11	Network-Traffic	network-traffic	
12	Process	process	
13	Software	software	
14	URL	url	
15	User-Account	user-account	
16	Windows-Registry-Key	windows-registry-key	
17	X509-Certificate	x509-certificate	

artifact

The Artifact Object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload.

artifact (Record)

id	name	type	#	description
1	type	Artifact$Type	1	The value of this property MUST be `artifact`.
2	id	Artifact$Id	1	
3	mime_type	Artifact$Mime-type	1	The value of this property MUST be a valid MIME type as specified in the IANA Media Types registry.
4	payload_bin	Binary	1	Specifies the binary data contained in the artifact as a base64-encoded string.
5	url	url	1	The value of this property MUST be a valid URL that resolves to the unencoded content.
6	hashes	Artifact$Hashes	1	Specifies a dictionary of hashes for the contents of the url or the payload_bin. This MUST be provided when the url property is present.
7	encryption_algorithm	encryption_algorithm_enum	1	If the artifact is encrypted, specifies the type of encryption algorithm the binary data (either via payload_bin or url) is encoded in.
8	decryption_key	String	1	Specifies the decryption key for the encrypted binary data (either via payload_bin or url).
9	spec_version	spec_version	1	
10	object_marking_refs	object_marking_refs	1	
11	granular_markings	granular_markings	1	
12	defanged	defanged	1	
13	core_extensions	extensions	1	

encryption_algorithm_enum

encryption_algorithm_enum (Enumerated)

ID	Name	Description
1	AES-256-GCM	
2	ChaCha20-Poly1305	
3	mine-type-indicated	

autonomous-system

The AS object represents the properties of an Autonomous Systems (AS).

autonomous-system (Record)

id	name	type	#	description
1	type	Autonomous-system$Type	1	
2	id	Autonomous-system$Id	1	
3	number	Integer{0..*}	1	Specifies the number assigned to the AS. Such assignments are typically performed by a Regional Internet Registries (RIR).
4	name	String	1	Specifies the name of the AS.
5	rir	String	1	Specifies the name of the Regional Internet Registry (RIR) that assigned the number to the AS.
6	spec_version	spec_version	1	

id	name	type	#	description
7	object_marking_refs	object_marking_refs	1	
8	granular_markings	granular_markings	1	
9	defanged	defanged	1	
10	core_extensions	extensions	1	

directory

The Directory Object represents the properties common to a file system directory.

directory (Record)

id	name	type	#	description
1	type	Directory$Type	1	
2	id	Directory$Id	1	
3	path	String	1	Specifies the path, as originally observed, to the directory on the file system.
4	path_enc	Directory$Path-enc	1	Specifies the observed encoding for the path.
5	ctime	timestamp	1	Specifies the date/time the directory was created.
6	mtime	timestamp	1	Specifies the date/time the directory was last written to/modified.
7	atime	timestamp	1	Specifies the date/time the directory was last accessed.
8	contains_refs	Directory$Contains-refs	1	Specifies a list of references to other File and/or Directory Objects contained within the directory.
9	spec_version	spec_version	1	
10	object_marking_refs	object_marking_refs	1	
11	granular_markings	granular_markings	1	
12	defanged	defanged	1	
13	core_extensions	extensions	1	

domain-name

The Domain Name represents the properties of a network domain name.

domain-name (Record)

id	name	type	#	description
1	type	Domain-name$Type	1	
2	id	Domain-name$Id	1	
3	domain_name	String	1	Specifies the value of the domain name.
4	resolves_to_refs	Domain-name$Resolves-to-refs	1	Specifies a list of references to one or more IP addresses or domain names that the domain name resolves to.
5	spec_version	spec_version	1	
6	object_marking_refs	object_marking_refs	1	
7	granular_markings	granular_markings	1	
8	defanged	defanged	1	
9	core_extensions	extensions	1	

email-addr

The Email Address Object represents a single email address.

email-addr (Record)

id	name	type	#	description
1	type	Email-addr$Type	1	
2	id	Email-addr$Id	1	
3	email_address	String	1	Specifies a single email address. This MUST not include the display name.
4	display_name	String	1	Specifies a single email display name, i.e., the name that is displayed to the human user of a mail application.
5	belongs_to_ref	String	1	Specifies the user account that the email address belongs to, as a reference to a User Account Object.
6	spec_version	spec_version	1	
7	object_marking_refs	object_marking_refs	1	
8	granular_markings	granular_markings	1	
9	defanged	defanged	1	
10	core_extensions	extensions	1	

email-message

The Email Message Object represents an instance of an email message.

email-message (Record)

id	name	type	#	description
1	type	Email-message$Type	1	
2	id	Email-message$Id	1	
3	date	timestamp	1	Specifies the date/time that the email message was sent.
4	content_type	String	1	Specifies the value of the 'Content-Type' header of the email message.
5	from_ref	String	1	Specifies the value of the 'From:' header of the email message.
6	sender_ref	spec_version	1	Specifies the value of the 'From' field of the email message.
7	to_refs	Email-message$To-refs	1	Specifies the mailboxes that are 'To:' recipients of the email message.
8	cc_refs	Email-message$Cc-refs	1	Specifies the mailboxes that are 'CC:' recipients of the email message.
9	bcc_refs	Email-message$Bcc-refs	1	Specifies the mailboxes that are 'BCC:' recipients of the email message.
10	message_id	String	1	Specifies the Message-ID field of the email message.
11	subject	String	1	Specifies the subject of the email message.
12	received_lines	Email-message$Received-lines	1	Specifies one or more Received header fields that may be included in the email headers.
13	additional_header_fields	Email-message$Additional-header-fields	1	Specifies any other header fields found in the email message, as a dictionary.
14	raw_email_ref	String	1	Specifies the raw binary contents of the email message, including both the headers and body, as a reference to an Artifact Object.
15	is_multipart	Boolean	1	Indicates whether the email body contains multiple MIME parts.
16	body_multipart	Email-message$Body-multipart	1	Specifies a list of the MIME parts that make up the email body. This property MAY only be used if is_multipart is true.
17	body	String	1	Specifies a string containing the email body. This field MAY only be used if is_multipart is false.
18	spec_version	spec_version	1	

id	name	type	#	description
19	object_marking_refs	object_marking_refs	1	
20	granular_markings	granular_markings	1	
21	defanged	defanged	1	
22	core_extensions	extensions	1	

file

file (Record)

id	name	type	#	description
1	type	File$Type	1	The value of this property MUST be `file`.
2	id	File$Id	1	
3	extensions	String	1	The File Object defines the following extensions. In addition to these, producers MAY create their own. Extensions: ntfs-ext, raster-image-ext, pdf-ext, archive-ext, windows-pebinary-ext
4	hashes	File$Hashes	1	Specifies a dictionary of hashes for the file.
5	size	File$Size	1	Specifies the size of the file, in bytes, as a non-negative integer.
6	name	String	1	
7	name_enc	File$Name-enc	1	Specifies the observed encoding for the name of the file.
8	magic_number_hex	Hex	1	Specifies the hexadecimal constant ('magic number') associated with a specific file format that corresponds to the file, if applicable.
9	mime_type	String	1	Specifies the MIME type name specified for the file, e.g., 'application/msword'.
10	ctime	timestamp	1	Specifies the date/time the file was created.
11	mtime	timestamp	1	Specifies the date/time the file was last written to/ modified.
12	atime	timestamp	1	Specifies the date/time the file was last accessed.
13	parent_directory	String	1	Specifies the parent directory of the file, as a reference to a Directory Object.
14	contains_refs	File$Contains-refs	1	Specifies a list of references to other Observable Objects contained within the file.
15	content_ref	String	1	Specifies the content of the file, represented as an Artifact Object.
16	spec_version	spec_version	1	
17	object_marking_refs	object_marking_refs	1	
18	granular_markings	granular_markings	1	
19	defanged	defanged	1	
20	core_extensions	extensions	1	

ipv4-addr

The IPv4 Address Object represents one or more IPv4 addresses expressed using CIDR notation.

ipv4-addr (Record)

id	name	type	#	description
1	type	Ipv4-addr$Type	1	
2	id	Ipv4-addr$Id	1	
3	ipv4_addr	Ipv4-addr$Ipv4-addr	1	
4	resolves_to_refs	Ipv4-addr$Resolves-to-refs	1	
5	belongs_to_refs	String	1	
6	spec_version	spec_version	1	

id	name	type	#	description
7	object_marking_refs	object_marking_refs	1	
8	granular_markings	granular_markings	1	
9	defanged	defanged	1	
10	core_extensions	extensions	1	

ipv6-addr

ipv6-addr (Record)

id	name	type	#	description
1	type	Ipv6-addr$Type	1	
2	id	Ipv6-addr$Id	1	
3	ipv6_addr	Ipv6-addr$Ipv6-addr	1	The IPv6 Address Object represents one or more IPv6 addresses expressed using CIDR notation.
4	resolves_to_refs	Ipv6-addr$Resolves-to-refs	1	Specifies a list of references to one or more Layer 2 Media Access Control (MAC) addresses that the IPv6 address resolves to.
5	belongs_to_refs	Ipv6-addr$Belongs-to-refs	1	Specifies a reference to one or more autonomous systems (AS) that the IPv6 address belongs to.
6	spec_version	spec_version	1	
7	object_marking_refs	object_marking_refs	1	
8	granular_markings	granular_markings	1	
9	defanged	defanged	1	
10	core_extensions	extensions	1	

mac-addr

Specifies one or more mac addresses expressed using CIDR notation.

mac-addr (Record)

id	name	type	#	description
1	type	Mac-addr$Type	1	
2	id	Mac-addr$Id	1	
3	mac_address_value	Mac-addr$Mac-address-value	1	Specifies one or more mac addresses expressed using CIDR notation.
4	spec_version	spec_version	1	
5	object_marking_refs	object_marking_refs	1	
6	granular_markings	granular_markings	1	
7	defanged	defanged	1	
8	core_extensions	extensions	1	

mutex

The Mutex Object represents the properties of a mutual exclusion (mutex) object.

mutex (Record)

id	name	type	#	description
1	type	Mutex$Type	1	
2	id	Mutex$Id	1	
3	name	String	1	Specifies the name of the mutex object.
4	spec_version	spec_version	1	
5	object_marking_refs	object_marking_refs	1	
6	granular_markings	granular_markings	1	
7	defanged	defanged	1	

id	name	type	#	description
8	core_extensions	extensions	1	

network-traffic

The Network Traffic Object represents arbitrary network traffic that originates from a source and is addressed to a destination.

network-traffic (Record)

id	name	type	#	description
1	type	Network-traffic$Type	1	
2	id	Network-traffic$Id	1	
3	extensions	network_traffic_extensions_dictionary	1	The Network Traffic Object defines the following extensions. In addition to these, producers MAY create their own. Extensions: http-ext, tcp-ext, icmp-ext, socket-ext
4	start	Network-traffic$Start	1	Specifies the date/time the network traffic was initiated, if known.
5	stop	Network-traffic$Stop	1	Specifies the date/time the network traffic ended, if known.
6	is_active	Boolean	1	Indicates whether the network traffic is still ongoing.
7	src_port	Network-traffic$Src-port	1	Specifies the source port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.
8	dst_port	Network-traffic$Dst-port	1	Specifies the destination port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.
9	protocols	Network-traffic$Protocols	1	Specifies the protocols observed in the network traffic, along with their corresponding state.
10	src_byte_count	Integer{0..*}	1	Specifies the number of bytes, as a positive integer, sent from the source to the destination.
11	dst_byte_count	Integer{0..*}	1	Specifies the number of bytes, as a positive integer, sent from the destination to the source.
12	src_packets	Integer{0..*}	1	Specifies the number of packets, as a positive integer, sent from the source to the destination.
13	dst_packets	Integer{0..*}	1	Specifies the number of packets, as a positive integer, sent from the destination to the source.
14	ipfix	ipfix_choice	1	Specifies any IP Flow Information Export (IPFIX) data for the traffic.
15	src_payload_ref	String	1	Specifies the bytes sent from the source to the destination.
16	dst_payload_ref	String	1	Specifies the bytes sent from the source to the destination.
17	encapsulates_refs	Network-traffic$Encapsulates-refs	1	Specifies the bytes sent from the source to the destination.
18	encapsulated_by_ref	String	1	Links to another network-traffic object which encapsulates this object.
19	spec_version	spec_version	1	
20	object_marking_refs	object_marking_refs	1	
21	granular_markings	granular_markings	1	

id	name	type	#	description
22	defanged	defanged	1	
23	core_extensions	extensions	1	

ipfix_choice

Specifies any IP Flow Information Export (IPFIX) data for the traffic.

ipfix_choice (Choice)

ID	Name	Type	Description
1	ipfix_string	String	
2	ipfix_integer	Integer{0..*}	

process

The Process Object represents common properties of an instance of a computer program as executed on an operating system.

process (Record)

id	name	type	#	description
1	type	Process$Type	1	
2	id	Process$Id	1	
3	extensions	process_extensions_dictionary	1	
4	is_hidden	Boolean	1	
5	pid	Integer{0..*}	1	Specifies the Process ID, or PID, of the process.
6	created_time	timestamp	1	Specifies the date/time at which the process was created.
7	cwd	String	1	Specifies the current working directory of the process.
8	command_line	String	1	Specifies the full command line used in executing the process, including the process name (which may be specified individually via the binary_ref.name property) and any arguments.
9	environment_variables	Process$Environment-variables	1	Specifies the list of environment variables associated with the process as a dictionary.
10	opened_connection_refs	String	1	Specifies the list of network connections opened by the process, as a reference to one or more Network Traffic Objects.
11	creator_user_ref	Process$Creator-user-ref	1	Specifies the user that created the process, as a reference to a User Account Object.
12	image_ref	String	1	Specifies the executable binary that was executed as the process image, as a reference to a File Object.
13	parent_ref	String	1	Specifies the other process that spawned (i.e. is the parent of) this one, as represented by a Process Object.
14	child_refs	Process$Child-refs	1	Specifies the other processes that were spawned by (i.e. children of) this process, as a reference to one or more other Process Objects.
15	spec_version	spec_version	1	
16	object_marking_refs	object_marking_refs	1	

id	name	type	#	description
17	granular_markings	granular_markings	1	
18	defanged	defanged	1	
19	core_extensions	extensions	1	

software

The Software Object represents high-level properties associated with software, including software products.

software (Record)

id	name	type	#	description
1	type	Software$Type	1	
2	id	String	1	%^software--
3	name	Software$Name	1	Specifies the name of the software.
4	cpe	Software$Cpe	1	Specifies the Common Platform Enumeration (CPE) entry for the software, if available. The value for this property MUST be a CPE v2.3 entry from the official NVD CPE Dictionary.
5	swid	Software$Swid	1	Specifies the Software Identification (SWID) Tags entry for the software, if available.
6	languages	Software$Languages	1	Specifies the languages supported by the software. The value of each list member MUST be an ISO 639-2 language code.
7	vendor	Software$Vendor	1	Specifies the name of the vendor of the software.
8	version	Software$Version	1	Specifies the version of the software.
9	spec_version	spec_version	1	
10	object_marking_refs	object_marking_refs	1	
11	granular_markings	granular_markings	1	
12	defanged	defanged	1	
13	core_extensions	extensions	1	

user-account

The Software Object represents high-level properties associated with software, including software products.

user-account (Record)

id	name	type	#	description
1	type	User-account$Type	1	The value of this property MUST be `user-account`.
2	id	User-account$Id	1	
3	user_account_extensions	user_account_extensions_dictionary	1	The User Account Object defines the following extensions. In addition to these, producers MAY create their own. Extensions: unix-account-ext.
4	user_id	String	1	Specifies the identifier of the account.
5	credential	String	1	Specifies a cleartext credential. This is only intended to be used in capturing metadata from malware analysis (e.g., a hard-coded domain administrator password that the malware attempts to use for lateral movement) and SHOULD NOT be used for sharing of PII.

id	name	type	#	description
6	account_login	String	1	Specifies the account login string, used in cases where the user_id property specifies something other than what a user would type when they login.
7	account_type	String	1	Specifies the type of the account. This is an open vocabulary and values SHOULD come from the account-type-ov vocabulary.
8	display_name	String	1	Specifies the display name of the account, to be shown in user interfaces, if applicable.
9	is_service_account	Boolean	1	Indicates that the account is associated with a network service or system process (daemon), not a specific individual.
10	is_privileged	Boolean	1	Specifies that the account has elevated privileges (i.e., in the case of root on Unix or the Windows Administrator account).
11	can_escalate_privs	Boolean	1	Specifies that the account has the ability to escalate privileges (i.e., in the case of sudo on Unix or a Windows Domain Admin account).
12	is_disabled	Boolean	1	Specifies if the account is disabled.
13	account_created	timestamp	1	Specifies when the account was created.
14	account_expires	timestamp	1	Specifies the expiration date of the account.
15	credential_last_changed	timestamp	1	Specifies when the account credential was last changed.
16	account_first_login	timestamp	1	Specifies when the account was first accessed.
17	account_last_login	timestamp	1	Specifies when the account was last accessed.
18	spec_version	spec_version	1	
19	object_marking_refs	object_marking_refs	1	
20	granular_markings	granular_markings	1	
21	defanged	defanged	1	
22	core_extensions	extensions	1	

url

The URL Object represents the properties of a uniform resource locator (URL).

url (Record)

id	name	type	#	description
1	type	Url$Type	1	The value of this property MUST be `url`.
2	id	Url$Id	1	
3	url_value	Url$Url-value	1	Specifies the value of the URL.
4	spec_version	spec_version	1	
5	object_marking_refs	object_marking_refs	1	
6	granular_markings	granular_markings	1	
7	defanged	defanged	1	
8	core_extensions	extensions	1	

windows-registry-key

The Registry Key Object represents the properties of a Windows registry key.

windows-registry-key (Record)

id	name	type	#	description
1	type	Windows-registry-key$Type	1	The value of this property MUST be `windows-registry-key`.
2	id	Windows-registry-key$Id	1	
3	key	Windows-registry-key$Key	1	Specifies the full registry key including the hive.
4	registry_values	Windows-registry-key$Registry-values	1	Specifies the values found under the registry key.
5	modified_time	timestamp	1	Specifies the last date/time that the registry key was modified.
6	creator_user_ref	String	1	Specifies a reference to a user account, represented as a User Account Object, that created the registry key.
7	number_of_subkeys	Integer{0..*}	1	Specifies the number of subkeys contained under the registry key.
8	spec_version	spec_version	1	
9	object_marking_refs	object_marking_refs	1	
10	granular_markings	granular_markings	1	
11	defanged	defanged	1	
12	core_extensions	extensions	1	

x509-certificate

The X509 Certificate Object represents the properties of an X.509 certificate.

x509-certificate (Record)

id	name	type	#	description
1	type	X509-certificate$Type	1	The value of this property MUST be `x509-certificate`.
2	id	X509-certificate$Id	1	
3	is_self_signed	Boolean	1	Specifies whether the certificate is self-signed, i.e., whether it is signed by the same entity whose identity it certifies.
4	hashes	X509-certificate$Hashes	1	Specifies any hashes that were calculated for the entire contents of the certificate.
5	version	String	1	Specifies the version of the encoded certificate.
6	serial_number	String	1	Specifies the unique identifier for the certificate, as issued by a specific Certificate Authority.
7	signature_algorithm	String	1	Specifies the name of the algorithm used to sign the certificate.
8	issuer	String	1	Specifies the name of the Certificate Authority that issued the certificate.
9	validity_not_before	timestamp	1	Specifies the date on which the certificate validity period begins.
10	validity_not_after	timestamp	1	Specifies the date on which the certificate validity period ends.
11	subject	spec_version	1	Specifies the name of the entity associated with the public key stored in the subject public key field of the certificate.

id	name	type	#	description
12	subject_public_key_algorithm	String	1	Specifies the name of the algorithm with which to encrypt data being sent to the subject.
13	subject_public_key_modulus	String	1	Specifies the modulus portion of the subject's public RSA key.
14	subject_public_key_extensions	Integer{0..*}	1	Specifies the exponent portion of the subject's public RSA key, as an integer.
15	x509_v3_extensions	X509-certificate$X509-v3-extensions	1	Specifies any standard X.509 v3 extensions that may be used in the certificate.
16	spec_version	spec_version	1	
17	object_marking_refs	object_marking_refs	1	
18	granular_markings	granular_markings	1	
19	defanged	defanged	1	
20	core_extensions	extensions	1	

mime-part-type

Specifies a component of a multi-part email body.

mime-part-type (Record)

id	name	type	#	description
1	body	String	1	Specifies the contents of the MIME part if the content_type is not provided OR starts with text/
2	body_raw_ref	String	1	Specifies the contents of non-textual MIME parts, that is those whose content_type does not start with text/, as a reference to an Artifact Object or File Object.
3	content_type	String	1	Specifies the value of the 'Content-Type' header field of the MIME part.
4	content_disposition	String	1	Specifies the value of the 'Content-Disposition' header field of the MIME part.

email-additional-header-fields

Specifies any other header fields (except for date, received_lines, content_type, from_ref, sender_ref, to_refs, cc_refs, bcc_refs, and subject) found in the email message, as a dictionary.

email-additional-header-fields (ArrayOf(email_additional_header_field))

email_additional_header_field

Specifies any other header fields (except for date, received_lines, content_type, from_ref, sender_ref, to_refs, cc_refs, bcc_refs, and subject) found in the email message, as a dictionary.

email_additional_header_field (MapOf(email_additional_header_fieldname, email_additional_header_value)[0..*])

email_additional_header_value

email_additional_header_value (Choice)

ID	Name	Type	Description
1	String_Value	Email-additional-header-value$String-value	
2	String_Array	Email-additional-header-value$String-array	

windows_registry_value_type

windows_registry_value_type (Record)

id	name	type	#	description
1	name	String	1	Specifies the name of the registry value. For specifying the default value in a registry key, an empty string MUST be used.
2	data	String	1	Specifies the data contained in the registry value.
3	registry_data_type	win_registry_data_type	1	Specifies the registry (REG_*) data type used in the registry value.

win_registry_data_type

Specifies the registry (REG_*) data type used in the registry value.

win_registry_data_type (Enumerated)

ID	Name	Description
1	REG_NONE	
2	REG_SZ	
3	REG_EXPAND_SZ	
4	REG_BINARY	
5	REG_DWORD	
6	REG_DWORD_BIG_ENDIAN	
7	REG_DWORD_LITTLE_ENDIAN	
8	REG_LINK	
9	REG_MULTI_SZ	
10	REG_RESOURCE_LIST	
11	REG_FULL_RESOURCE_DESCRIPTION	
12	REG_RESOURCE_REQUIREMENTS_LIST	
13	REG_QWORD	
14	REG_INVALID_TYPE	

x509_certificate_extensions_type

x509_certificate_extensions_type (Record)

id	name	type	#	description
1	basic_constraints	String	1	Specifies a multi-valued extension which indicates whether a certificate is a CA certificate.
2	name_constraints	String	1	Specifies a namespace within which all subject names in subsequent certificates in a certification path MUST be located.
3	policy_constraints	String	1	Specifies any constraints on path validation for certificates issued to CAs.
4	key_usage	String	1	Specifies a multi-valued extension consisting of a list of names of the permitted key usages.
5	extend_key_usage	String	1	Specifies a list of usages indicating purposes for which the certificate public key can be used for.
6	subject_key_identifier	String	1	

id	name	type	#	description
				Specifies the identifier that provides a means of identifying certificates that contain a particular public key.
7	authority_key_identifier	String	1	Specifies the identifier that provides a means of identifying the public key corresponding to the private key used to sign a certificate.
8	subject_alternative_name	String	1	Specifies the additional identities to be bound to the subject of the certificate.
9	issuer_alternative_name	String	1	Specifies the additional identities to be bound to the issuer of the certificate.
10	subject_directory_attributes	String	1	Specifies the identification attributes (e.g., nationality) of the subject.
11	crt_distribution_points	String	1	Specifies how CRL information is obtained.
12	inhibit_any_policy	String	1	Specifies the number of additional certificates that may appear in the path before anyPolicy is no longer permitted.
13	private_key_usage_period_not_before	timestamp	1	Specifies the date on which the validity period begins for the private key, if it is different from the validity period of the certificate.
14	private_key_usage_period_not_after	timestamp	1	Specifies the date on which the validity period ends for the private key, if it is different from the validity period of the certificate.
15	certificate_policies	String	1	Specifies a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.
16	policy_mappings	String	1	Specifies one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy

file_extensions_dictionary

file_extensions_dictionary (Record)

id	name	type	#	description
1	ntfs_ext	ntfs_ext	1	The NTFS file extension specifies a default extension for capturing properties specific to the storage of the file on the NTFS file system.

ntfs_ext

The NTFS file extension specifies a default extension for capturing properties specific to the storage of the file on the NTFS file system.

ntfs_ext (Record)

id	name	type	#	description
1	sid	String	1	Specifies the security ID (SID) value assigned to the file.
2	alternate_data_streams	Ntfs-ext$Alternate-data-streams	1	Specifies a list of NTFS alternate data streams that exist for the file.

ntfs_atlternate_data_stream

ntfs_atlternate_data_stream (Record)

id	name	type	#	description
1	name	String	1	Specifies the name of the alternate data stream.
2	hashes	Ntfs-atlternate-data-stream$Hashes	1	Specifies a dictionary of hashes for the data contained in the alternate data stream.
3	size	Ntfs-atlternate-data-stream$Size	1	Specifies the size of the alternate data stream, in bytes, as a non-negative integer.

hashes

The Hashes type represents one or more cryptographic hashes, as a special set of key/value pairs

hashes (Record)

id	name	type	#	description
1	MD5	Hashes$Md5	1	Specifies the MD5 message digest algorithm.
2	SHA-1	Hashes$Sha-1	1	Specifies the MD5 message digest algorithm.
3	SHA-256	Hashes$Sha-256	1	Specifies the MD5 message digest algorithm.
4	SHA-512	Hashes$Sha-512	1	Specifies the MD5 message digest algorithm.
5	SHA3-256	Hashes$Sha3-256	1	Specifies the MD5 message digest algorithm.
6	SHA3-512	Hashes$Sha3-512	1	Specifies the MD5 message digest algorithm.
7	SSDEEP	Hashes$Ssdeep	1	Specifies the MD5 message digest algorithm.
8	TLSH	Hashes$Tlsh	1	Specifies the MD5 message digest algorithm.

network_traffic_extensions_dictionary

The User Account Object defines the following extensions. In addition to these, producers MAY create their own.

network_traffic_extensions_dictionary (Record)

id	name	type	#	description
1	http_request_ext	http_request_ext	1	The HTTP request extension specifies a default extension for capturing network traffic properties specific to HTTP requests.
2	icmp_ext	icmp_ext	1	The ICMP extension specifies a default extension for capturing network traffic properties specific to ICMP.
3	socket_ext	socket_ext	1	The Network Socket extension specifies a default extension for capturing network traffic properties associated with network sockets.
4	tcp_ext	tcp_ext	1	The TCP extension specifies a default extension for capturing network traffic properties specific to TCP.

http_request_ext

The HTTP request extension specifies a default extension for capturing network traffic properties specific to HTTP requests.

http_request_ext (Record)

id	name	type	#	description
1	request_method	String	1	Specifies the HTTP method portion of the HTTP request line, as a lowercase string.
2	request_value	String	1	Specifies the value (typically a resource path) portion of the HTTP request line.
3	request_version	String	1	Specifies the HTTP method portion of the HTTP request line, as a lowercase string.
4	request_header	Http-request-ext$Request-header	1	Specifies the value (typically a resource path) portion of the HTTP request line.
5	message_body_length	String	1	Specifies the HTTP method portion of the HTTP request line, as a lowercase string.
6	message_body_data_ref	String	1	Specifies the value (typically a resource path) portion of the HTTP request line.

icmp_ext

The ICMP extension specifies a default extension for capturing network traffic properties specific to ICMP.

icmp_ext (Record)

id	name	type	#	description
1	icmp_type_hex	Hex	1	Specifies the ICMP type byte.
2	icmp_code_hex	Hex	1	Specifies the ICMP code byte.

socket_ext

The Network Socket extension specifies a default extension for capturing network traffic properties associated with network sockets.

socket_ext (Record)

id	name	type	#	description
1	address_family	address_family	1	Specifies the address family (AF_*) that the socket is configured for.
2	is_blocking	Boolean	1	Specifies whether the socket is in blocking mode.
3	is_listening	String	1	Specifies whether the socket is in listening mode.
4	options	Socket-ext$Options	1	Specifies any options (SO_*) that may be used by the socket, as a dictionary.
5	socket_type	socket_type	1	Specifies the type of the socket.
6	socket_descriptor	Socket-ext$Socket-descriptor	1	Specifies the socket file descriptor value associated with the socket, as a non-negative integer.
7	socket_handle	Integer{0..*}	1	Specifies the handle or inode value associated with the socket.

tcp_ext

The TCP extension specifies a default extension for capturing network traffic properties specific to TCP.

tcp_ext (Record)

id	name	type	#	description
1	src_flags_hex	Hex	1	Specifies the source TCP flags, as the union of all TCP flags observed between the start of the traffic (as defined by the start property) and the end of the traffic (as defined by the end property).
2	dst_flags_hex	Hex	1	Specifies the destination TCP flags, as the union of all TCP flags observed between the start of the traffic (as defined by the start property) and the end of the traffic (as defined by the end property).

address_family

Specifies the current status of the service. windows-service-status-enum

address_family (Enumerated)

ID	Name	Description
1	AF_UNSPEC	
2	AF_INET	
3	AF_IPX	

ID	Name	Description
4	AF_APPLETALK	
5	AF_NETBIOS	
6	AF_INET6	
7	AF_IRDA	
8	AF_BTH	

socket_option

Specifies any options (SO_*) that may be used by the socket, as a dictionary.

socket_option (Record)

id	name	type	#	description
1	socket_option	Socket-option$Socket-option	1	
2	option_value	Integer{0..*}	1	

socket_type

Specifies the type of the socket.

socket_type (Enumerated)

ID	Name	Description
1	SOCK_STREAM	
2	SOCK_DGRAM	
3	SOCK_RAW	
4	SOCK_RDM	
5	SOCK_SEQPACKET	

user_account_extensions_dictionary

The User Account Object defines the following extensions. In addition to these, producers MAY create their own.

user_account_extensions_dictionary (Record)

id	name	type	#	description
1	unix_account_ext	unix_account_ext	1	The User Account Object defines the following extensions. In addition to these, producers MAY create their own.

unix_account_ext

unix_account_ext (Record)

id	name	type	#	description
1	gid	Number{0..*}	1	Specifies the primary group ID of the account.

process_extensions_dictionary

process_extensions_dictionary (Record)

id	name	type	#	description
1	windows_proccess_extension	windows_proccess_extension	1	The Windows Process extension specifies a default extension for capturing properties specific to Windows processes.

id	name	type	#	description
2	windows_service_ext	windows_service_ext	1	The Windows Service extension specifies a default extension for capturing properties specific to Windows services.

windows_proccess_extension

The Windows Process extension specifies a default extension for capturing properties specific to Windows processes.

windows_proccess_extension (Record)

id	name	type	#	description
1	aslr_enabled	Boolean	1	Specifies whether Address Space Layout Randomization (ASLR) is enabled for the process.
2	dep_enabled	Boolean	1	Specifies whether Data Execution Prevention (DEP) is enabled for the process.
3	priority	String	1	Specifies the current priority class of the process in Windows.
4	owner_sid	String	1	Specifies the Security ID (SID) value of the owner of the process.
5	window_title	String	1	Specifies the title of the main window of the process.
6	startup_info	startup_info_dictionary	1	Specifies the STARTUP_INFO struct used by the process, as a dictionary.
7	integrity_level	windows_integrity_level_enum	1	Specifies the Windows integrity level, or trustworthiness, of the process.

startup_info_dictionary

startup_info_dictionary (Array)

ID	Type	#	Description
1	String	1	
2	String	1	
3	String	1	
4	String	1	
5	String	1	
6	String	1	
7	String	1	
8	String	1	
9	Null	1	
10	Null	1	
11	Integer{0..*}	1	
12	Integer{0..*}	1	
13	Integer{0..*}	1	
14	Integer{0..*}	1	
15	Integer{0..*}	1	
16	Integer{0..*}	1	
17	Integer{0..*}	1	
18	Startup-info-dictionary$Cbreserved2	1	

windows_integrity_level_enum

windows_integrity_level_enum (Enumerated)

ID	Name	Description
1	low	
2	medium	

ID	Name	Description
3	high	
4	system	

service_status

Specifies the current status of the service. windows-service-status-enum

service_status (Enumerated)

ID	Name	Description
1	SERVICE_CONTINUE_PENDING	
2	SERVICE_PAUSE_PENDING	
3	SERVICE_PAUSED	
4	SERVICE_RUNNING	
5	SERVICE_START_PENDING	
6	SERVICE_STOP_PENDING	
7	SERVICE_STOPPED	

service_type

Specifies the type of the service. windows-service-enum

service_type (Enumerated)

ID	Name	Description
1	SERVICE_KERNEL_DRIVER	
2	SERVICE_FILE_SYSTEM_DRIVER	
3	SERVICE_WIN32_OWN_PROCESS	
4	SERVICE_WIN32_SHARE_PROCESS	

windows_service_ext

The Windows Service extension specifies a default extension for capturing properties specific to Windows services.

windows_service_ext (Record)

id	name	type	#	description
1	service_name	String	1	Specifies the name of the service.
2	descriptions	Windows-service-ext$Descriptions	1	Specifies the descriptions defined for the service.
3	display_name	String	1	Specifies the displayed name of the service in Windows GUI controls.
4	group_name	String	1	Specifies the name of the load ordering group of which the service is a member.
5	start_type	start_type	1	Specifies the start options defined for the service. windows-service-start-enum
6	service_dll_refs	Windows-service-ext$Service-dll-refs	1	Specifies the DLLs loaded by the service, as a reference to one or more File Objects.
7	service_type	service_type	1	Specifies the type of the service. windows-service-enum
8	service_status	service_status	1	Specifies the current status of the service. windows-service-status-enum

start_type

Specifies the start options defined for the service. windows-service-start-enum

start_type (Enumerated)

ID	Name	Description
1	SERVICE_AUTO_START	
2	SERVICE_BOOT_START	
3	SERVICE_DEMAND_START	
4	SERVICE_DISABLED	
5	SERVICE_SYSTEM_ALERT	

spec_version

The version of the STIX specification used to represent the content in this cyber-observable.

spec_version (Enumerated)

ID	Name	Description
1	2.0	
2	2.1	

object_marking_refs

The list of marking-definition objects to be applied to this object.

object_marking_refs (ArrayOf(identifier){1..*})

granular_marking

granular_marking (Record)

id	name	type	#	description
1	selectors	identifier	1	A list of selectors for content contained within the STIX object in which this property appears.
2	lang	String	1	Identifies the language of the text identified by this marking.
3	pattern	identifier	1	The marking_ref property specifies the ID of the marking-definition object that describes the marking.

granular_markings

The set of granular markings that apply to this object.

granular_markings (ArrayOf(granular_marking){1..*})

extensions

Specifies any extensions of the object, as a dictionary.

extensions (Record{1..*})

id	name	type	#	description
1	extension	Extensions$Extension	1	
2	extension_definition	extension	1	

properties

Rules for custom properties

properties (Array)

ID	Type	#	Description
1	Binary	1	
2	Hex	1	The hex data type encodes an array of octets (8-bit bytes) as hexadecimal. The string MUST consist of an even number of hexadecimal characters, which are the digits '0' through '9' and the letters 'a' through 'f'. In order to allow pattern matching on custom objects, all properties that use the hex type, the property name MUST end with '_hex'.
3	Properties$Array	1	
4	String	1	
5	Integer{0..*}	1	
6	Boolean	1	
7	Number{0..*}	1	
8	extensions	1	

extension

extension (Record{1..*})

id	name	type	#	description
1	extension_type	extension_type_enum	1	The type of extension.
2	properties	properties	1	

extension_type_enum

extension_type_enum (Enumerated)

ID	Name	Description
1	new-sdo	
2	new-sco	
3	new-sro	
4	property-extension	
5	toplevel-property-extension	

Artifact$Hashes

Specifies a dictionary of hashes for the contents of the url or the payload_bin. This MUST be provided when the url property is present.

Artifact$Hashes (ArrayOf(hashes))

Directory$Contains-refs

Specifies a list of references to other File and/or Directory Objects contained within the directory.

Directory$Contains-refs (ArrayOf(String){1..*})

Domain-name$Resolves-to-refs

Specifies a list of references to one or more IP addresses or domain names that the domain name resolves to.

Domain-name$Resolves-to-refs (ArrayOf(String))

Email-message$To-refs

Specifies the mailboxes that are 'To:' recipients of the email message.

Email-message$To-refs (ArrayOf(String){1..*})

Email-message$Cc-refs

Specifies the mailboxes that are 'CC:' recipients of the email message.

Email-message$Cc-refs (ArrayOf(String){1..*})

Email-message$Bcc-refs

Specifies the mailboxes that are 'BCC:' recipients of the email message.

Email-message$Bcc-refs (ArrayOf(String){1..*})

Email-message$Received-lines

Specifies one or more Received header fields that may be included in the email headers.

Email-message$Received-lines (ArrayOf(String))

Email-message$Additional-header-fields

Specifies any other header fields found in the email message, as a dictionary.

Email-message$Additional-header-fields (ArrayOf(email-additional-header-fields))

Email-message$Body-multipart

Specifies a list of the MIME parts that make up the email body. This property MAY only be used if is_multipart is true.

Email-message$Body-multipart (ArrayOf(mime-part-type))

File$Hashes

Specifies a dictionary of hashes for the file.

File$Hashes (ArrayOf(hashes))

File$Contains-refs

Specifies a list of references to other Observable Objects contained within the file.

File$Contains-refs (ArrayOf(String){1..*})

Ipv4-addr$Resolves-to-refs

Ipv4-addr$Resolves-to-refs (ArrayOf(String))

Ipv6-addr$Resolves-to-refs

Specifies a list of references to one or more Layer 2 Media Access Control (MAC) addresses that the IPv6 address resolves to.

Ipv6-addr$Resolves-to-refs (ArrayOf(String))

Ipv6-addr$Belongs-to-refs

Specifies a reference to one or more autonomous systems (AS) that the IPv6 address belongs to.

Ipv6-addr$Belongs-to-refs (ArrayOf(String))

Network-traffic$Protocols

Specifies the protocols observed in the network traffic, along with their corresponding state.

Network-traffic$Protocols (ArrayOf(String){1..*})

Network-traffic$Encapsulates-refs

Specifies the bytes sent from the source to the destination.

Network-traffic$Encapsulates-refs (ArrayOf(String){1..*})

Process$Environment-variables

Specifies the list of environment variables associated with the process as a dictionary.

Process$Environment-variables (ArrayOf(String))

Process$Creator-user-ref

Specifies the user that created the process, as a reference to a User Account Object.

Process$Creator-user-ref (ArrayOf(String){1..*})

Process$Child-refs

Specifies the other processes that were spawned by (i.e. children of) this process, as a reference to one or more other Process Objects.

Process$Child-refs (ArrayOf(String){1..*})

Software$Languages

Specifies the languages supported by the software. The value of each list member MUST be an ISO 639-2 language code.

Software$Languages (ArrayOf(String))

Windows-registry-key$Registry-values

Specifies the values found under the registry key.

Windows-registry-key$Registry-values (ArrayOf(windows_registry_value_type))

X509-certificate$Hashes

Specifies any hashes that were calculated for the entire contents of the certificate.

X509-certificate$Hashes (ArrayOf(hashes))

X509-certificate$X509-v3-extensions

Specifies any standard X.509 v3 extensions that may be used in the certificate.

X509-certificate$X509-v3-extensions (ArrayOf(x509_v3_extensions_type))

Email-additional-header-value$String-array

Email-additional-header-value$String-array (ArrayOf(String){2..*})

Ntfs-ext$Alternate-data-streams

Specifies a list of NTFS alternate data streams that exist for the file.

Ntfs-ext$Alternate-data-streams (ArrayOf(ntfs_atlternate_data_stream))

Ntfs-atlternate-data-stream$Hashes

Specifies a dictionary of hashes for the data contained in the alternate data stream.

Ntfs-atlternate-data-stream$Hashes (ArrayOf(hashes))

Http-request-ext$Request-header

Specifies the value (typically a resource path) portion of the HTTP request line.

Http-request-ext$Request-header (ArrayOf(String))

Socket-ext$Options

Specifies any options (SO_*) that may be used by the socket, as a dictionary.

Socket-ext$Options (ArrayOf(socket_option))

Windows-service-ext$Descriptions

Specifies the descriptions defined for the service.

Windows-service-ext$Descriptions (ArrayOf(String){1..*})

Windows-service-ext$Service-dll-refs

Specifies the DLLs loaded by the service, as a reference to one or more File Objects.

Windows-service-ext$Service-dll-refs (ArrayOf(String))

Properties$Array

Properties$Array (ArrayOf(String){1..*})

Primitive Types

Name	Definition	Description
email_additional_header_fieldname	String(pattern="^((?!((^|,)(date|received_lines|content_type|from_ref|sender_ref|to_refs|cc_refs|bcc_refs|subject))+$).)*$")	Specifies any other header fields (except for date, received_lines, content_type, from_ref, sender_ref, to_refs, cc_refs, bcc_refs, and subject) found in the email message, as a dictionary.
Null	String(pattern="^NULL$")	This Is Wrong
defanged	Boolean	Defines whether or not the data contained within the object has been defanged.
identifier	String(pattern="^[a-z][a-z0-9-]+[a-z0-9]--[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[1-5][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$")	Represents identifiers across the CTI specifications. The format consists of the name of the top-level object being identified, followed by two dashes (--), followed by a UUIDv4.
Hex	String(pattern="^([a-fA-F0-9]{2})+$")	
timestamp	String(pattern="^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$")	
Artifact$Type	String(pattern="^artifact$")	The value of this property MUST be `artifact`.
Artifact$Id	String(pattern="^artifact--")	
Artifact$Mime-type	String(pattern="^(application|audio|font|image|message|model|multipart|text|video)/[a-zA-Z0-9.+_-]+")	The value of this property MUST be a valid MIME type as specified in the IANA Media Types registry.
Autonomous-system$Type	String(pattern="^autonomous-system$")	
Autonomous-system$Id	String(pattern="^autonomous-system--")	
Directory$Type	String(pattern="^directory$")	
Directory$Id	String(pattern="^directory--")	
Directory$Path-enc	String(pattern="^[a-zA-Z0-9/\\.+_:-]{2,250}$")	Specifies the observed

Name	Definition	Description
		encoding for the path.
Domain-name$Type	String(pattern="^domain-name$")	
Domain-name$Id	String(pattern="^domain-name--")	
Email-addr$Type	String(pattern="^email-addr$")	
Email-addr$Id	String(pattern="^email-addr--")	
Email-message$Type	String(pattern="^email-message$")	
Email-message$Id	String(pattern="^email-message--")	
File$Type	String(pattern="^file$")	The value of this property MUST be `file`.
File$Id	String(pattern="^file--")	
File$Size	Integer{0..*}	Specifies the size of the file, in bytes, as a non-negative integer.
File$Name-enc	String(pattern="^[a-zA-Z0-9/\\.+_:-]{2,250}$")	Specifies the observed encoding for the name of the file.
Ipv4-addr$Type	String(pattern="^ipv4-addr$")	
Ipv4-addr$Id	String(pattern="^ipv4-addr--")	
Ipv4-addr$Ipv4-addr	String{1..*}(pattern="^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])(\\/(3[0-2]|[1-2][0-9]|[0-9]))?$")	
Ipv6-addr$Type	String(pattern="^ipv6-addr$")	
Ipv6-addr$Id	String(pattern="^ipv6-addr--")	
Ipv6-addr$Ipv6-addr	String{1..*}(pattern="^s*((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]d|1dd|[1-9]?d)(.(25[0-5]|2[0-4]d|1dd|[1-9]?d)){3}))|:)))(%.+)?s*(\\/(12[0-8]|1[0-1][0-9]|[1-9][0-9]|[0-9]))?$")	The IPv6 Address Object represents one or more IPv6 addresses expressed using CIDR notation.
Mac-addr$Type	String(pattern="^mac-addr$")	
Mac-addr$Id	String(pattern="^mac-addr--")	
Mac-addr$Mac-address-value	String(pattern="^([0-9a-f]{2}[:]){5}([0-9a-f]{2})$")	Specifies one or more mac addresses expressed using CIDR notation.
Mutex$Type	String(pattern="^mutex$")	
Mutex$Id	String(pattern="^mutex--")	

Name	Definition	Description
Network-traffic$Type	String(pattern="^network-traffic$")	
Network-traffic$Id	String(pattern="^network-traffic--")	
Network-traffic$Start	String(pattern="^[0-9]{4}-[0-9]{2}-[0-9]{2} T[0-9]{2}:[0-9]{2}:[0-9]{2}Z")	Specifies the date/time the network traffic was initiated, if known.
Network-traffic$Stop	String(pattern="^[0-9]{4}-[0-9]{2}-[0-9]{2} T[0-9]{2}:[0-9]{2}:[0-9]{2}Z")	Specifies the date/time the network traffic ended, if known.
Network-traffic$Src-port	Integer{0..65535}	Specifies the source port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.
Network-traffic$Dst-port	Integer{0..65535}	Specifies the destination port used in the network traffic, as an integer. The port value MUST be in the range of 0 - 65535.
Process$Type	String(pattern="^process$")	
Process$Id	String(pattern="^process--")	
Software$Type	String(pattern="^software$")	
Software$Name	String{1..*}	Specifies the name of the software.
Software$Cpe	String(pattern="cpe:2\\.3:[aho*\\-](:(((\\?*|*?)([a-zA-Z0-9\\-\\._]|(\\\\[*\\?!\"#$$%&'\\(\\)\\+,/:;<=>@\\[\\]\\^`\\{\\\|}~]))+(\\?*\|\\*?))\|[\\*\\-])){5}(:(([a-zA-Z]{2,3}(-([a-zA-Z]{2}\|[0-9]{3}))?)\|[\\*\\-]))(:(((\\?*\|\\*?)([a-zA-Z0-9\\-\\._]\|(\\\\[\\\\\\*\\?!\"#$$%&'\\(\\)\\+,/:;<=>@\\[\\]\\^`\\{\\\|}~]))+(\\?*|*?))|[*\\-])){4}")	Specifies the Common Platform Enumeration (CPE) entry for the software, if available. The value for this property MUST be a CPE v2.3 entry from the official NVD CPE Dictionary.
Software$Swid	String	Specifies the Software Identification (SWID) Tags entry for the software, if available.
Software$Vendor	String	Specifies the name of the vendor of the software.
Software$Version	String	Specifies the version of the software.
User-account$Type	String(pattern="^user-account$")	The value of this property MUST

Name	Definition	Description
		be `user-account`.
User-account$Id	String(pattern="^user-account--")	
Url$Type	String(pattern="^url$")	The value of this property MUST be `url`.
Url$Id	String(pattern="^url")	
Url$Url-value	String(pattern="^(([^:/?#]+):)?(//([^/?#]*))?([^?#]*)(\?([^#]*))?(#(.*))?")	Specifies the value of the URL.
Windows-registry-key$Type	String(pattern="^windows-registry-key$")	The value of this property MUST be `windows-registry-key`.
Windows-registry-key$Id	String(pattern="^windows-registry-key--")	
Windows-registry-key$Key	String(pattern="^((?!((^|,)(HKLM|HKCC|HKCR|HKCU|HKU|hklm|hkcc|hkcr|hkcu|hku))+$).)*$")	Specifies the full registry key including the hive.
X509-certificate$Type	String(pattern="^x509-certificate$")	The value of this property MUST be `x509-certificate`.
X509-certificate$Id	String(pattern="^x509-certificate--")	
Email-additional-header-value$String-value	String(pattern="[a-zA-Z0-9_-]{0,250}^$")	
Ntfs-atlternate-data-stream$Size	Integer{0..*}	Specifies the size of the alternate data stream, in bytes, as a non-negative integer.
Hashes$Md5	String(pattern="^[a-fA-F0-9]{32}$")	Specifies the MD5 message digest algorithm.
Hashes$Sha-1	String(pattern="^[a-fA-F0-9]{40}$")	Specifies the MD5 message digest algorithm.
Hashes$Sha-256	String(pattern="^[a-fA-F0-9]{64}$")	Specifies the MD5 message digest algorithm.
Hashes$Sha-512	String(pattern="^[a-fA-F0-9]{128}$")	Specifies the MD5 message digest algorithm.
Hashes$Sha3-256	String(pattern="^[a-fA-F0-9]{64}$")	Specifies the MD5 message digest algorithm.
Hashes$Sha3-512	String(pattern="^[a-fA-F0-9]{128}$")	Specifies the MD5 message digest algorithm.
Hashes$Ssdeep	String(pattern="^[a-zA-Z0-9/+:.]{1,128}$")	Specifies the MD5 message digest algorithm.
Hashes$Tlsh	String(pattern="^[a-zA-Z0-9]{70}$")	Specifies the MD5 message digest algorithm.
Socket-ext$Socket-descriptor	Integer{0..*}	Specifies the socket file descriptor value associated with the socket, as a non-negative integer.

Name	Definition	Description
Socket-option$Socket-option	String(pattern="^(SO|ICMP|ICMP6|IP|IPV6|MCAST|TCP|IRLMP)(_[A-Z]+)+$")	
Startup-info-dictionary$Cbreserved2	Integer{0..*}	
Extensions$Extension	String(pattern="^([a-z][a-z0-9]*)+(-[a-z0-9]+)*\\-ext$")	