STIX 2.1 Major Changes and Additions

STIX 2.1 differs from STIX 2.0 in the following ways:

1. New objects: Grouping, Infrastructure, Language-Content (internationalization), Location, Malware-Analysis, Note, Opinion
2. Objects that have undergone significant change: Course of Actions, Malware, all SCOs
3. New concepts: Confidence and Internationalization
4. STIX Cyber-observable Objects can now be directly related using STIX Relationship Objects
5. Renamed conflicting properties on Directory Object, File Object, Process Object, and Windows Registry Key Object.
6. Added relationship from Indicator to Observed Data called "based-on".
7. Added description property to Sighting
8. Made some SCO relationships external on Domain-Name, IPv4-Addr, and IPv6-Addr.

STIX 2.0 vs STIX 2.1 Object Comparison

The following tables compares the objects and extensions defined in the STIX 2.0 specifications to the ones in the STIX 2.1 specification.

STIX Domain Objects	Type Name	STIX 2.0	STIX 2.1	STIX 2.1 Change Details: • added optional property **`confidence`** • added optional property **`lang`**
Attack Pattern	attack-pattern	●	●	• added optional property **`aliases`**
Campaign	campaign	●	●	
Course of Action	course-of-action	●	●	• added optional property **`action_type`** • added optional property **`os_execution_envs`** • added optional property **`action_bin`**

				• added optional property **action_reference** • removed property **action**
Grouping	grouping		●	
Identity	identity	●	●	• added optional property **roles**
Indicator	indicator	●	●	• added require property **indicator_types** • added required property **pattern_type** • added optional property **pattern_version** • added relationship from Indicator to Observed Data called "based-on".
Infrastructure	infrastructure		●	
Intrusion Set	intrusion-set	●	●	
Location	location		●	
Malware	malware	●	●	• change property **name** from required to optional • added required property **malware_types** • added required property **is_family** • added optional property **aliases** • added optional property **first_seen** • added optional property **last_seen** • added optional property **os_execution_envs** • added optional property **architecture_execution_envs** • added optional property **implementation_languages** • added optional property **capabilities**

				• added optional property **`sample_refs`**
Malware Analysis	malware-analysis		●	
Note	note		●	
Observed Data	observed-data	●	●	• deprecated property **`objects`** (*changed to optional*)
Opinion	opinion		●	
Report	report	●	●	• added required property **`report_types`**
Threat Actor	threat-actor	●	●	• added required property **`threat_actor_types`** • added optional property **`first_seen`** • added optional property **`last_seen`**
Tool	tool	●	●	• added required property **`tool_types`** • added optional property **`aliases`**
Vulnerability	vulnerability	●	●	
STIX Relationship Objects				**STIX 2.1 Change Details:** • added optional property **`confidence`** • added optional property **`lang`**
Relationship	relationship	●	●	
Sighting	sighting	●	●	• added optional property **`description`**
STIX Cyber Observable				**STIX 2.1 Change Details:** • top-level objects like STIX Domain objects and can now be directly related using STIX Relationship Objects; **remove 'x-fireeye-com-' prefix**

				• added optional property **`defanged`**
Artifact	artifact	●	●	• added optional property **`encryption_algorithm`** • added optional property **`decryption_key`**
AS	autonomous-system	●	●	
Directory	directory	●	●	• renamed conflicting property **`created`** with **`ctime`** • renamed conflicting property **`modified`** with **`mtime`** • renamed conflicting property **`accessed`** with **`atime`**
Domain Name	domain-name	●	●	• deprecated property **`resolved_to_refs`**
Email Address	email-addr	●	●	
Email Message	email-address	●	●	
File	file	●	●	• renamed conflicting property **`created`** with **`ctime`** • renamed conflicting property **`modified`** with **`mtime`** • renamed conflicting property **`accessed`** with **`atime`** • removed property **`is_encrypted`** • removed property **`encryption_algorithm`** • removed property **`decryption_key`**
Archive File Extension	archive-ext	●	●	• removed property **`version`**
NTFS File Extension	ntfs-ext	●	●	
PDF File Extension	pdf-ext	●	●	
Raster Image File Extension	raster-image-ext	●	●	• removed property **`image_compression_algorithm`**

Windows PE Binary File Extension	windows-pebinary-ext	●	●	
IPv4 Address	ipv4-addr	●	●	• deprecated property **resolved_to_refs** • deprecated property **belongs_to_refs**
IPv6 Address	ipv6-addr	●	●	• deprecated property **resolved_to_refs** • deprecated property **belongs_to_refs**
MAC Address	mac-addr	●	●	
Mutex Object	mutex	●	●	
Network Traffic	network-traffic	●	●	
HTTP Request Extension	http-request-ext	●	●	
ICMP Extension	icmp-ext	●	●	
Network Socket Extension	socket-ext	●	●	• removed property **protocol_family**
TCP Extension	tcp-ext	●	●	
Process Object	process	●	●	• renamed conflicting property **created** with **created_time** • removed property **arguments** • removed property **name** • renamed property **binary_ref** with **image**-ref
Windows Process Extension	windows-process-ext	●	●	• added optional property **integrity_level**
Windows Service Extension	windows-service-ext	●	●	
Software Object	software	●	●	
URL	url	●	●	

User Account	user-account	●	●	• added optional property **credential** • renamed property **password_last_changed** with **credential_last_changed**
Unix Account Extension	unix-account-ext	●	●	
Windows Registry Key	windows-registry-key	●	●	• renamed property **modified** with **modified_time**
X.509 Certification	x509-certificate	●	●	
STIX Meta Objects				**STIX 2.1 Change Details:**
Language Content (internationalization)	language-content		●	
Marking Definition	marking-definition	●	●	
Bundle	bundle	●	●	