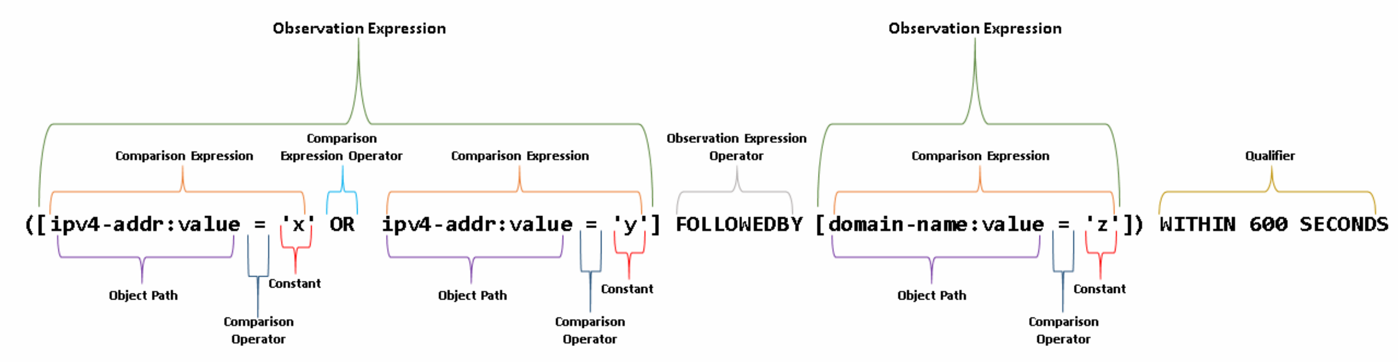
STIX Patterning Quick Reference (v1.2)



Definitions

- **SCO:** STIX Cyber Observables - the data model for describing STIX 2 *observations*.
  - Think of *SCO* as defining the scaffolding upon which STIX Patterning is hung.
- **observations:** Represent data about systems or networks observed at a point in time - for example, metadata about a file on disk or network traffic between hosts.
- **pattern expression:** a *STIX pattern* instance.
- **object path:** Specifies which properties of a *SCO* object to evaluate as part of a *comparison expression*.
- **constant:** a specific value, such as an integer, float, string, etc.
- **comparison operators:** For evaluating an *object path* against one or more constants.
- **comparison expressions:** An *object path* and a constant joined by a *comparison operator*.
- **qualifiers:** Provide a restriction on the *observations* that are considered valid for matching the preceding *observation expression*.
- **observation operators:** Used to combine two *observation expressions* operating on two different *observed data* instances into a single pattern.
- **observation expression:** One or more *comparison expressions* joined by *boolean operators*, delimited by square brackets. *Observation expressions* may be constrained by appending one or more *qualifiers*.
  - Complex *observation expressions* may be constructed recursively by joining multiple *observation expressions* with an *observation operator*.

Comparison Operators

NOTE: in the table below, *a* is **always** an object path and *b* is **always** a constant which is a valid representation of the SCO type corresponding to the object path.

Comparison Operators	Description	Example(s)
a = *b*	*a* equal to *b*	file:name = 'foo.dll'
a != *b*	*a* not equal to *b*	file:size != 4112
a > *b*	*a* greater than *b*	file:size > 256
a < *b*	*a* less than *b*	file:size < 1024
a >= *b*	*a* greater than or equal to *b*	file:size <= 25145
a <= *b*	*a* less than or equal to *b*	file:size >= 33312
a IN (*x*,*y*,...)	*a* equal to one or more of the constants in the specified set.	process:name IN ('proccy', 'proximus', 'badproc')
a LIKE *b*	*a* evaluates to *b* according to SQL *LIKE* syntax: % - any zero or more characters _ - any single character	directory:path LIKE 'C:\\Windows\\%\\foo'
a MATCHES *b*	*a* evaluates to *b* according to PCRE syntax	directory:path MATCHES '^C:\\Windows\\w+$'

Set Operators	Description	Example(s)
a ISSUBSET *b*	*a* is of type ipv4-addr or ipv6-addr. *b* is an IP address (single or CIDR). Evaluates to true if *a* is equal to or logically contained within *b*.	ipv4-addr:value ISSUBSET '198.51.100.0/24'
a ISSUPERSET *b*	*a* is of type ipv4-addr or ipv6-addr. *b* is an IP address (single or CIDR). Evaluates to true if *a* is equal to *b* **or** if *b* is logically contained within *a*.	ipv4-addr:value ISSUPERSET '198.51.100.0/24'

This quick reference card is intended as an aid to people working with the STIX Patterning Language. It is neither comprehensive nor guaranteed to be error-free. For an authoritative and comprehensive reference, consult the OASIS CTI TC specification:

https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html

Observation / Comparison Expression Operators

Observation / Comparison Operators	Description
a AND *b* [*a*] AND [*b*]	This operator may be used either in the context of a comparison expression or an observation expression. In either case, **both** *a* and *b* must evaluate to true.
a OR *b* [*a*] OR [*b*]	This operator may be used either in the context of a comparison expression or an observation expression. In either case, **at least one** of *a* and *b* must evaluate to true.
[*a*] FOLLOWEDBY [*b*]	This operator may **only** be used in the context of a observation expression. **Both** observation expressions *a* and *b* evaluate to true on **different** observations **and** the timestamp on *b* is ≥ on *a*.

Object Path Syntax

Type	Syntax	Example(s)
Basic	<object-type>:<property_name>	file:size
List	<object-type>:<property_name>[list_index].<property_name>	file:extensions.windows-pebinary.sections[*].entropy > 7.0
Dictionary	<object-type>:<property_name>.<key_name>	file:hashes.ssdeep
Reference	<object-type>:<property_name>.<dereferenced_object_property>	directory:contains_refs[*].name = 'foobar.dll'

Observation Expression Qualifiers

NOTE: Qualifiers may be chained, e.g., *a* REPEATS *x* TIMES WITHIN *y* SECONDS.

Observation Expression Qualifiers	Description
a REPEATS *x* TIMES	Evaluates to true when *a* matches **exactly** *x* times, with each observation expression matching on a **different** observation.
a WITHIN *x* SECONDS	Evaluates to true when **all** of the observations matched by observation expression *a* occur within the specified time window.

Constants

Patterning Constant	SOCS Data Type(s)	Example(s)
`boolean`	`boolean`	`true` or `false`
`binary`	`binary`, `hex`, `string`	`b'ABI='`
`hex`	`binary`, `hex`, `string`	`h'0012'`
`integer`	`integer`, `float`	`-3`
`float`	`integer`, `float`	`-3.1415926`
`string`	`string`, `binary`, `hex`	`'foo and\\/or bar'`
`timestamp`	`timestamp`	`t'2014-01-13T07:03:17Z'`

Examples

Description	Example
matching on a file hash	[file:hashes.'SHA-256' = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']
matching on an IP address	[ipv4-addr:value = '8.8.8.8']
matching on a domain name	[domain-name:value = 'example.com']
matching on an email address	[email-addr:value = 'jane.smith@example.com']
matching on a phishing email	[email-message:body_multipart.[*].body_raw_ref.hashes.'SHA-256' = '9c9815c6a10d7ad3898cfd0b4750f2cdb252959b44cf5f9728c7cbff8f7df481' AND email-message:from_ref MATCHES '.+\\@example\\.com$']
matching on network traffic	[network-traffic:dst_ref.type = 'ipv4-addr' AND network-traffic:dst_ref.value = '203.0.113.33/32']
matching on a file hash followed by a Windows™ Autostart Registry Key being set followed by C2 beaconing	[file:hashes.'SHA-256' = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f'] FOLLOWEDBY [windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\EvilExe'] FOLLOWEDBY ([network-traffic:dst_ref.type = 'domain-name' AND network-traffic:dst_ref.value = 'example.com'] REPEATS 5 TIMES WITHIN 1800 SECONDS)