STIX Course of Action Object

Type Name: `course-of-action`

A Course of Action (CoA) is a recommendation from a producer of intelligence to a consumer on actions that **MAY** be taken in response to that intelligence. A CoA characterizes measures that might be taken in regard to a threat. These measures may be preventative to deter exploitation or corrective to counter its potential impact. A consumer of CoA's **MAY** choose to ignore this recommendation. The CoA may describe automatable actions (applying patches, reconfiguring firewalls), manual processes, or a combination of the two. For example, a CoA that describes how to mitigate a vulnerability could describe how to apply the patch that fixes that vulnerability.

More specifically, the Course of Action SDO contains a title, textual description of the recommended process, labels to characterize the measure and a list of action steps. The action-steps property enables documentation of multiple action steps with temporal sequencing, but no conditional logic. Each Course of Action SDO may be related to other SDOs as necessary, such as to the Vulnerability SDO or TTPs (Tool, Malware, Attack Pattern) that it provides recommended actions on.

Normative description

The **`action-steps`** property contains an ordered list of individual atomic action steps that can be carried out. The start_on property indicates the first action step to be executed and **SHALL** be specified. Further ordering of the action steps is determined by the property *next* of each action step. Before an action step is taken, all of the following conditions must be satisfied:

- The action step **MUST** have been successfully completed before moving on to the *next action* step
- If an action step is not referenced as *next* in any action step, then it **SHALL** be started when resources are available or when the consumer of the CoA decides to start it.

If ordering is not specified via the *start_on* or *next* properties, it is up to the consumer of the CoA to order the action steps.

If for some reason the CoA cannot be represented using action-steps, it could be expressed textually using the **content** property. The CoA **SHALL** contain either the content or action-steps property not both.

Properties

Common Properties
`TODO`
Course of Action Specific Properties
`name`, **`description`**, **`start_on`**, **`content`**, **`action-steps`**

Property Name	Type	Description
`type` (required)	`string`	The value of this property **MUST** be `course-of-action`
`labels` (optional)	`list` of type `open-vocab`	Labels will be used to categorize different types of COAs, for example (preventative) prevention, (corrective) correction etc. An action could have multiple labels since it could be used for multiple purposes. This is an open vocabulary and values **SHOULD** come from the `coa-label-ov` vocabulary.
`name` (required)	`string`	A name used to identify the Course of Action
`description` (optional)	`string`	A description that provides more details and context about the Course of Action, potentially including its purpose and its key characteristics.
`start_on` (optional)	`string`	This optional property represents the named action step contained within action-steps list to begin processing on. If this property is not specified and the action-steps list is defined then the first action-steps listed **SHOULD** be used.
`content` (optional)	`string`	An optional property that may represent a single course of action as a simple string. This property **SHOULD NOT** be specified if the action-steps property is used.
`action-steps` (optional)	`list` of type `action-step`	This optional property represents the action-steps that define what this course of action is recommending. This property **SHOULD NOT** be specified if content is specified.

Action Step Properties

Property Name	Type	Description
`name` (required)	`string`	A name for this action step that uniquely identifies it in the context of this course of action object. This is not a globally unique name.
`description` (optional)	`string`	An optional description for this action step.
`type` (optional)	`course-of-action-type-ov`	textual, openc2, powershell, sh Extension examples: cisco:asa, symantec:sep
`value` (optional)	`string`	The action step content in the case where the type requires a single string value. This property **SHOULD NOT** be used if object is used
`object` (optional)	`object`	The action step content in the case where the type requires an object construct instead of a single string value. This property **SHOULD NOT** be used if value is used.
`next-steps` (optional)	`list` of type `string`	The set of named next action step(s) to execute after completion of this action step.

Relationships

These are the relationships explicitly defined between the Course of Action object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from the Course of Action object by way of the Relationship object. The reverse relationships (relationships "to" the Course of Action object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.
Relationships are not restricted to those listed below. Relationships can be created between any objects using the `related-to` relationship type or, as with open vocabularies, user-defined names.

Embedded Relationships	
`created_by_ref`	`identifier` (of type `identity`)
`object_marking_refs`	`identifier` (of type `marking-definition`)

Common Relationships			
`duplicate-of`, `derived-from`, `related-to`			
Source	Relationship Type	Target	Description
`course-of-action`	`mitigates`	`indicator`, `malware`, `sighting`, `vulnerability`	This Relationship describes that the Course of Action can mitigate the related Indicator, Sighting, Malware or Vulnerability. For example, a `mitigates` Relationship from a Course of Action object to a Malware object indicates that the course of action mitigates the impact of that malware.
`course-of-action`	`investigates`	`indicator`	
`course-of-action`	`remediates`	`malware`, `vulnerability`	
`course-of-action`	`uses`	`course-of-action`	
Reverse Relationships			
—	—	—	—

Examples

IPv4 CIDR Block Example

An IPv4 CIDR with associated COA with an explicit copy of the indicator value to block in the same bundle.
The OpenC2 object does not specify destination IP, source and dest ports or application and its assumed that means to OpenC2 those values are 'any'. The where and direction are also guesses at the correct OpenC2 syntax.

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.1",
  "objects": [
```

```
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDR C2 Hosting Network"
      ],
      "name": "Bad IP CIDR-198",
      "description": "This indicator should be blocked due to known malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.0/24' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "name": "COA-Block CIDR-198",
      "description": "Block outbound or inbound traffic to & from known bad CIDR",
      "action-steps": [
         {
           "type": "openc2",
           "name" : "1",
           "object": {
              "action": "deny",
              "target" : {
                "network_traffic": {
                  "src_ip": "198.51.100.0/24",
                 },
              }
              "target-options": {
                 "where": "perimeter",
                 "direction": "inbound-interfaces"
              }
           }
        },
        {
           "type": "openc2",
           "name" : "2",
           "object": {
              "action": "deny",
              "target" : {
                "network_traffic": {
                  "dst_ip": "198.51.100.0/24",
                 },
              }
              "target-options" {
                 "where": "perimeter",
                 "direction": "outbound-interfaces"
              }
           }
        }
```

```
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--b61fc7f5-db9d-46e0-9724-46b4e7ca496f",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "relationship_type": "mitigates",
      "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "target_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
    }
  ]
}
```

DNS Lookup Example

A FQDN with associated COA with an explicit copy of the indicator value to redirect a DNS query to a known DNS capture portal in the same bundle.

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Potential Suspicious FQDN"
      ],
      "name": "Bad Domain",
      "description": "This domain should be not be allowed and any connection attempts should
be redirected to a safe portal ",
      "pattern": "[ domain-name:value = 'www.5z8.info' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "name": "COA-Safe Redirect",
      "description": "Capture all DNS queries to this domain and redirect to a known capture
portal.",
      "action-steps": [
         {
           "type": "openc2",
           "name" : "1",
           "object": {
```

```
              "action": "redirect",
              "target" : {
                "network_traffic": {
                  "target_dns": "www.5z8.info",
                  “dst_dns” : “www.safenet.com”
                 },
              }
              "target-options": {
                 "where": "dns-query",
              },
              "actuator": "network",
              "actuator-options": {
                "method": "rpz"
              }
              "command-options": {
                  "start-time": "",
                  "end-time": ""
              }
            }
          }
        ]
    },
    {
      "type": "relationship",
      "id": "relationship--b61fc7f5-db9d-46e0-9724-46b4e7ca496f",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "relationship_type": "mitigates",
      "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "target_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
    }
  ]
}
```

Malware Hash Example

A known Malware Hash with associated COA with an explicit copy of the indicator value to scan endpoints for. The COA will delete files with that hash if any are present and it will send a report about the attempted deletion.

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.1",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious Filehash"
```

```
      ],
      "name": "Bad File1",
      "description": "This indicator should be detected and deleted if present",
      "pattern": "[file:hashes.'SHA-256' =
'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feeaf7092761e18c859ee52a9c' OR file:hashes.'MD5' =
'cead3f77f6cda6ec00f57d76c9a6879f']",
      "valid_from": "2016-01-01T00:00:00Z"
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "name": "COA-Delete-Filehash",
      "description": "Delete files with the attached hash if any are present and report that
deletion was attempted.",
      "action-steps": [
         {
           "type": "openc2",
           "name" : "1",
           "object": {
              "action": "delete",
              "target" : {
                "artifact": {
                  "sha-256":
"bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feeaf7092761e18c859ee52a9c",
                  "md5": "cead3f77f6cda6ec00f57d76c9a6879f"
                },
              }
              "target-options": {
                 "where": "endpoints",
              }
           }
        },
        {
           "type": "textual",
           "name" : "2",
           "value" : "Open/Update IT case with details on where the malicious files were found
and that a delete was attempted.
        }
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--b61fc7f5-db9d-46e0-9724-46b4e7ca496f",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "relationship_type": "remediates",
      "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "target_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
    }
  ]
}
```

Quarantine of Exfiltrating Server

A threat intelligence provider (SuperThreat) has detected that an organization (ACME) has a server that is being used by an adversary to exfiltrate sensitive information. SuperThreat sends an Observed-Data bundled with a CoA describing how to quarantine the affected server. ACME receives the CoA and runs it. The very first action-step is to stop and ask a relevant security team member whether to quarantine the server. This is a manual action that takes in a string as a **question** and an array of strings as **options**. The result must be one of the **options**. If the ACME security team decides to continue then an OpenC2 command is sent to an SDN controller to quarantine the affected server.


```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.1",
  "objects": [
    {
      "type": "identity",
      "name": "SuperThreat",
      "identity_class": "organization",
      "id": "identity--e431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "observed-data",
      "id": "observed-data--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--e431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.17"
        }
      }
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--9e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--e431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
```

```
      "modified": "2016-04-06T20:03:48.000Z",
      "name": "quarantine of exfiltrating server",
      "description": "We saw your server with the attached external ip address being used to
exfiltrate your sensitive data. You should run this CoA to quarantine it then figure out how
to handle it from there.",
      "action-steps": [
        {
          "name" : "quarantine_server",
          "type": "openc2",
          "object": {
            "action": "contain",
            "target" : {
              "type": "ipv4",
              "value": "198.51.100.17",
            },
            "actuator": "sdn_controller"
          }
        },
        {
          "name" : "report_quarantine",
          "type": "textual",
          "value":
            "Create/update IT case with the following information - An exfiltration was
detected from your server with external IP address {198.51.100.17} and the server was
attempted to be quarantined."
          }
        },
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--b61fc7f5-db9d-46e0-9724-46b4e7ca496f",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "relationship_type": "mitigates",
      "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "target_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
    }
  ]
}
```

4.2. Course of Action Type Label (TBD)

Type Name: `course-of-action-type-ov`

This vocabulary is currently used in the following SDO(s):

- Course of Action

Vocabulary Summary	
Course of Action Label is an open vocabulary used to describe the type of Courses of Action. The labels describe the action that is being represented, such as openc2, textual….etc.	
Vocabulary Value	**Description**
oasis:openc2:v<X>	OASIS OpenC2 standard JSON version identified by the X
textual	Unstructured textual description of a course of action that does not conform to any standard language
cisco:ios:v<X>	Cisco IOS v<X> where is a number for the version of IOS commands used
powershell	Powershell commands
sh	Shell commands