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

<table>
<thead>
<tr>
<th>Common Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>TODO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course of Action Specific Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>name, description, start_on, content, action-steps</td>
</tr>
<tr>
<td>Property Name</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>type (required)</td>
</tr>
<tr>
<td>labels (optional)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>name (required)</td>
</tr>
<tr>
<td>description (optional)</td>
</tr>
<tr>
<td>start_on (optional)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>content (optional)</td>
</tr>
<tr>
<td>action-steps (optional)</td>
</tr>
</tbody>
</table>
## Action Step Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name (required)</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>description (optional)</td>
<td>string</td>
<td>An optional description for this action step.</td>
</tr>
<tr>
<td>type (optional)</td>
<td>course-of-action-type-ov</td>
<td>textual, openc2, powershell, sh Extension examples: cisco:asa, symantec:sep</td>
</tr>
<tr>
<td>value (optional)</td>
<td>string</td>
<td>The action step content in the case where the type requires a single string value. This property <strong>SHOULD NOT</strong> be used if object is used</td>
</tr>
<tr>
<td>object (optional)</td>
<td>object</td>
<td>The action step content in the case where the type requires an object construct instead of a single string value. This property <strong>SHOULD NOT</strong> be used if value is used</td>
</tr>
<tr>
<td>next-steps (optional)</td>
<td>list of type string</td>
<td>The set of named next action step(s) to execute after completion of this action step.</td>
</tr>
</tbody>
</table>

## 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.

<table>
<thead>
<tr>
<th>Embedded Relationships</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>created_by_ref</td>
<td>identifier (of type identity)</td>
</tr>
<tr>
<td>object_marking_refs</td>
<td>identifier (of type marking-definition)</td>
</tr>
</tbody>
</table>
## Common Relationships

<table>
<thead>
<tr>
<th>Source</th>
<th>Relationship Type</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Relationship Type</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

## 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.*

```json
{
    "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-a1c-6a4751cae5ff" },
{ "type": "indicator", "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f", "created_by_ref": "identity--f431f809-377b-45e0-a1c-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-a1c-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" } } } ] }
**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.

```json
{
  "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-6a4751ca5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751ca5ff",
      "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-6a4751ca5ff",
      "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": {
            "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-6a4751caefff"    },    {      "type": "indicator",      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751caefff",      "created": "2016-04-06T20:03:48.000Z",      "modified": "2016-04-06T20:03:48.000Z",      "labels": [        "Malicious Filehash"      ]    }]}

"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"  }]}
[{
  "name": "Bad File1",
  "description": "This indicator should be detected and deleted if present",
  "pattern": "[file:hashes.'SHA-256' = 'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3f8eaf70922761e18c859ee52a9c' OR file:hashes.'MD5' = 'ceda3f77fc6ca6ec00f57d76c9a6879f']",
  "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-6a4751ca50ff",
  "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": "bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3f8eaf70922761e18c859ee52a9c",
            "md5": "ceda3f77fc6ca6ec00f57d76c9a6879f"
          }
        }
      }
    },
    {
      "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.

```json
{
  "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",
      "value": "0谈及""}
```
"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
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.

<table>
<thead>
<tr>
<th>Vocabulary Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oasis:openc2:v&lt;X&gt;</td>
<td>OASIS OpenC2 standard JSON version identified by the X</td>
</tr>
<tr>
<td>textual</td>
<td>Unstructured textual description of a course of action that does not conform to any standard language</td>
</tr>
<tr>
<td>cisco:ios:v&lt;X&gt;</td>
<td>Cisco IOS v&lt;X&gt; where is a number for the version of IOS commands used</td>
</tr>
<tr>
<td>powershell</td>
<td>Powershell commands</td>
</tr>
<tr>
<td>sh</td>
<td>Shell commands</td>
</tr>
</tbody>
</table>