STIX + OpenC2

Automated Courses of Action

OpenC2 Provides

- OpenC2 enables the machine to machine exchange of commands to achieve investigative, remediation and/or mitigation effects.
- OpenC2 enables real-time automated and active cyber defense through the use of standardized commands
- OpenC2 provides the action to be taken, not the "why" it should be taken or the authentication to take the action.
    - The why is one of the areas where STIX can help
    - STIX can also give the "what" to look for along with all other aspects that come from additional context.

OpenC2 Terminology

- **Actuator:** The device or sensor that executes a native OpenC2 command
- **OpenC2 Proxy:** Provide a mapping of OpenC2 commands to and from devices that do not natively support OpenC2.
- **Orchestrator:** Is a mission manager that will issue the OpenC2 commands to the appropriate actuators, and in the synchronous case, ensure the commands are executed in the correct order

Effects Based Actions

- **Investigate:** Gather information and report on the threat or weakness

- **Remediate:** Prevent, eliminate, and remove the threat or weakness

- **Mitigate:** Contain the threat or weakness through compensating controls

Additional Actions

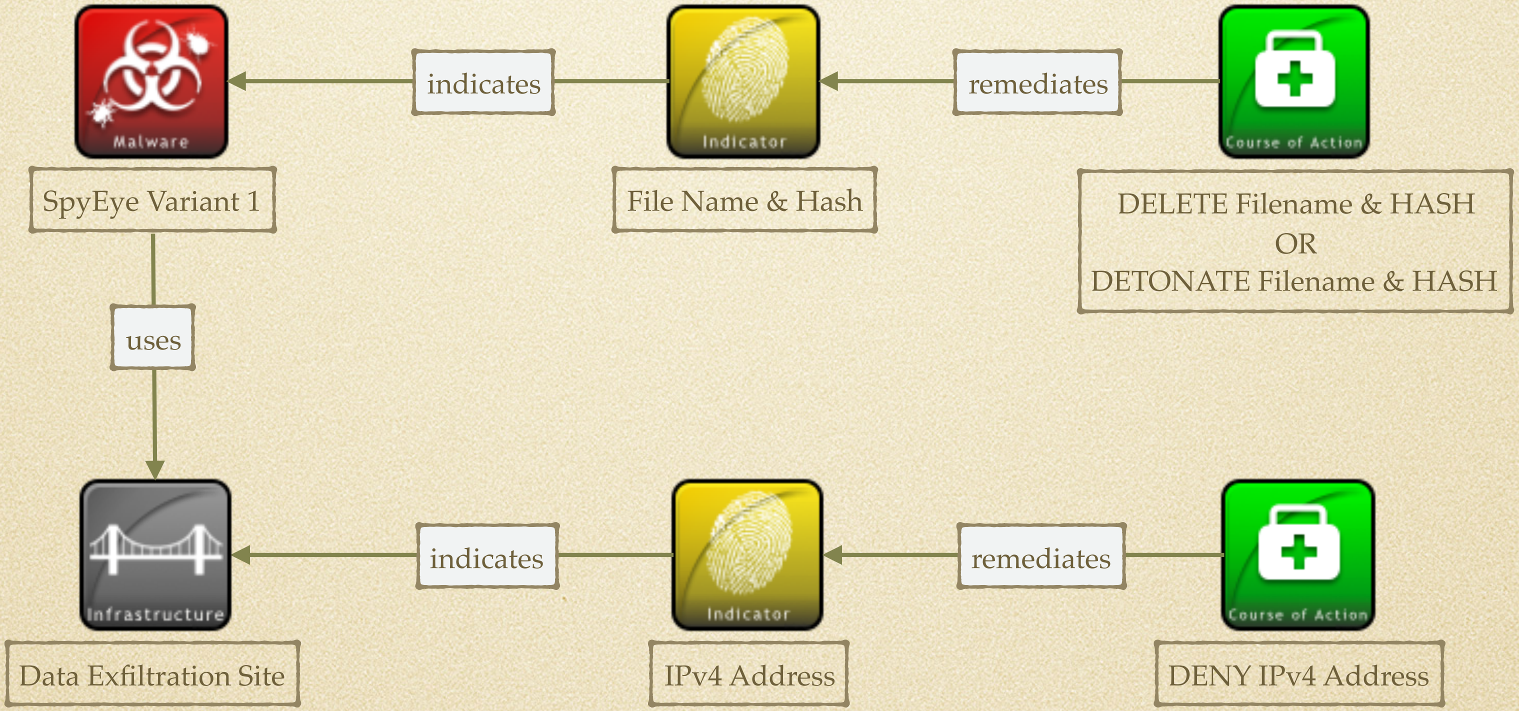
- Gather and Convey Information
  - Scan, Locate, Query, Report, Get, Notify
- Control Permissions
  - Deny, Contain, Allow
- Control Activities
  - Start, Stop, Restart, Pause, Resume, Cancel, Set, Update, Move, Redirect, Delete, Snapshot, Detonate, Restore, Save, Modify, Throttle, Delay, Substitute, Copy, Sync

STIX with OpenC2

- An analyst identifies a new piece of malware and its corresponding data exfiltration sites.
  - As a member of the SOC she knows and understands the cyber defenses in their organization and all of their enclaves / business units.
- The analyst creates the following STIX SDOs and SROs
  - 1x Malware, 1x Infrastructure, 2x Indicators
  - 2x Courses of Action
  - 5x Relationships
- The Course of Actions contain OpenC2 commands to DENY access at the Firewall and Proxy.

Big Picture

STIX Data



SpyEye Variant 1

indicates

File Name & Hash

remediates

DELETE Filename & HASH
OR
DETONATE Filename & HASH

uses

Data Exfiltration Site

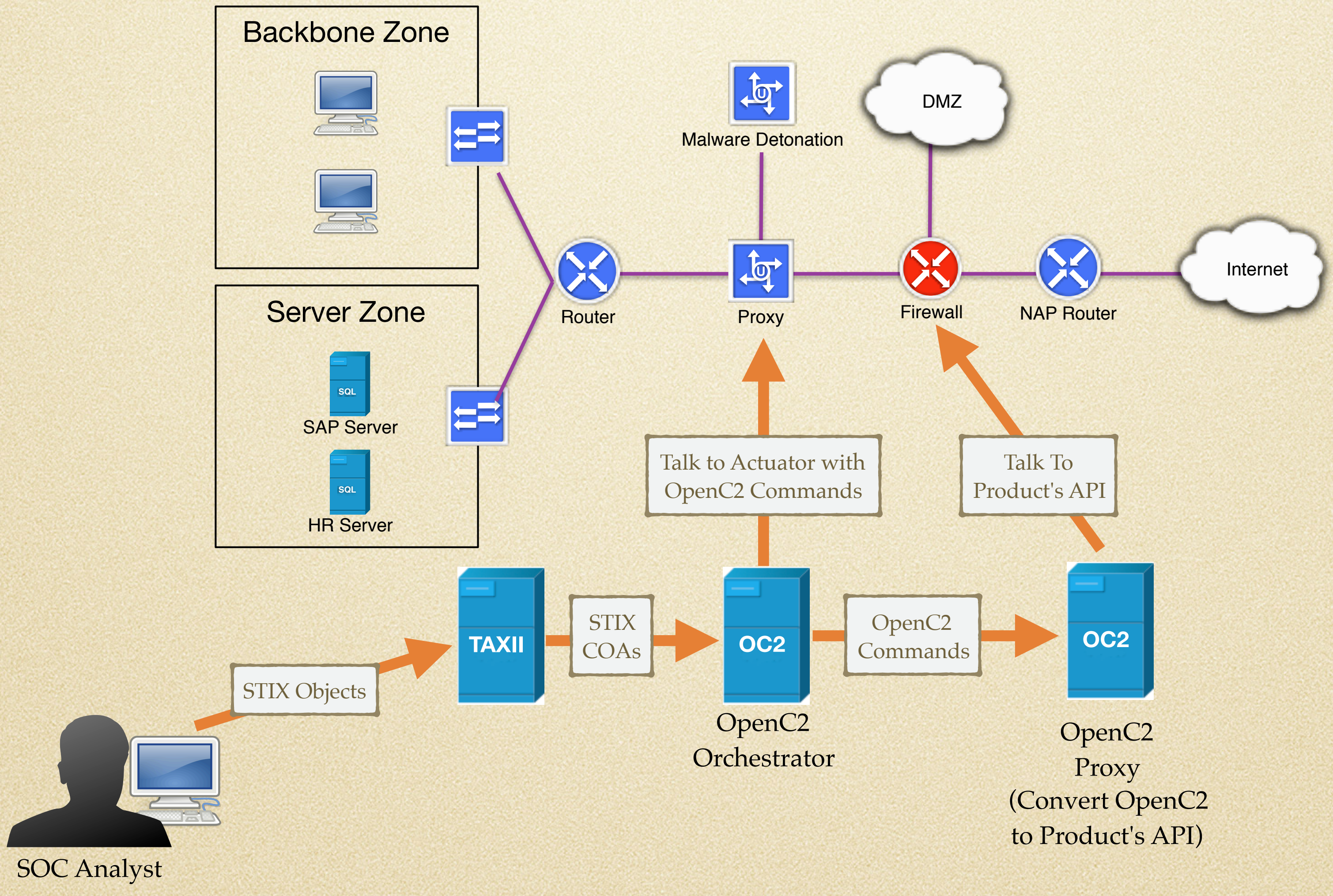
indicates

IPv4 Address

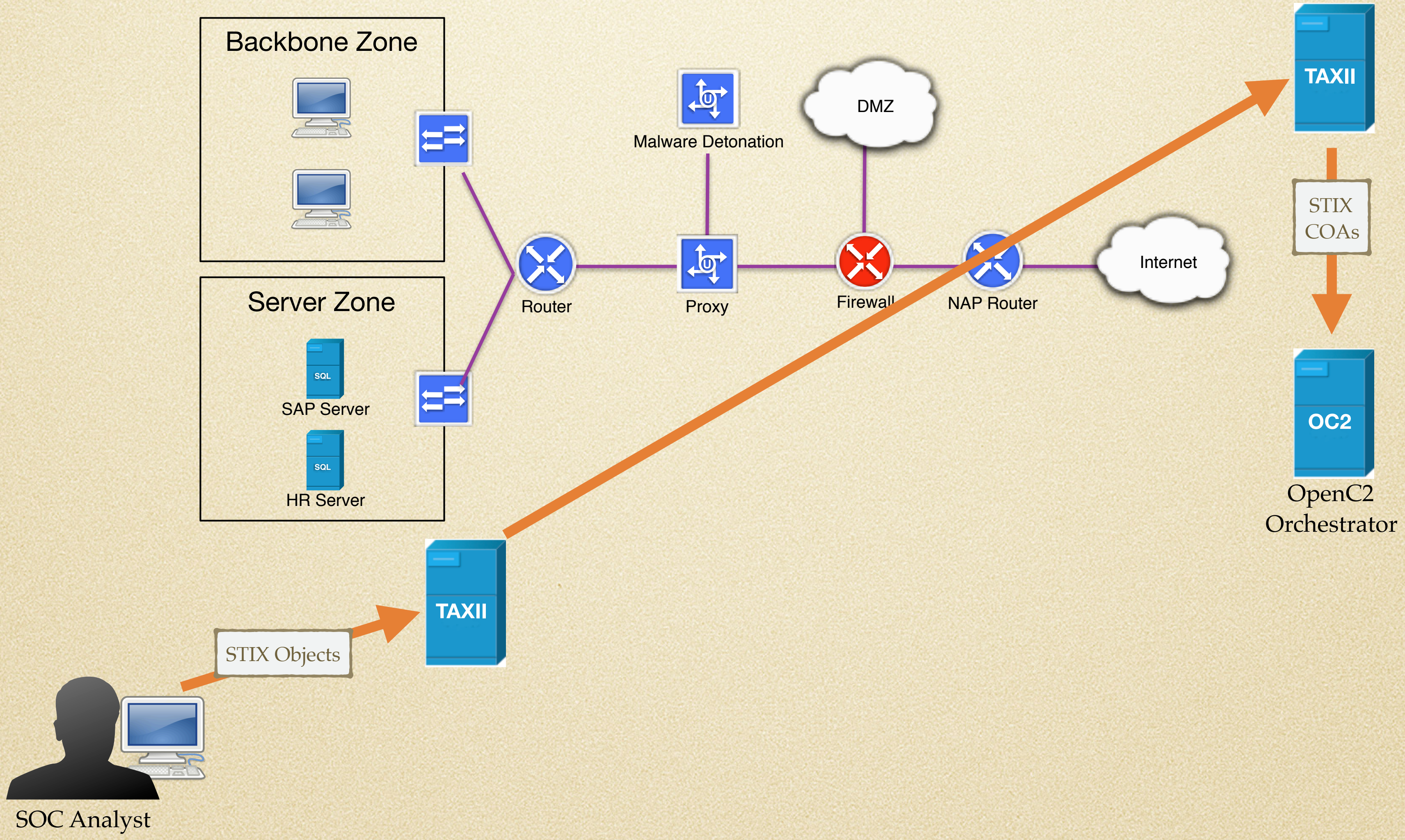
remediates

DENY IPv4 Address

Logical Flow



Logical Flow External Sharing



Indicator 1

```
{
  "type": "indicator",
  "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "created": "2016-04-06T20:03:48Z",
  "modified": "2016-04-06T20:03:48Z",
  "labels": ["malicious-activity"],
  "version": 1,
  "name": "Poison Ivy Malware",
  "description": "This file is part of Poison Ivy",
  "pattern": "[ file.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3' ]",
  "valid_from": "2016-01-01T00:00:00Z"
}
```

Indicator 2

```
{
  "type": "indicator",
  "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3e",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "created": "2016-04-06T20:03:48Z",
  "modified": "2016-04-06T20:03:48Z",
  "labels": ["malicious-activity"],
  "version": 1,
  "name": "Poison Ivy Malware",
  "description": "This file is part of Poison Ivy",
  "pattern": "[ ipv4-addr:value = '198.51.100.0/24' ]",
  "valid_from": "2016-01-01T00:00:00Z"
}
```

OpenC2 Examples

- These examples are based on the current OpenC2 designs that are based on the old CybOX 2.x model.
- We would need to get these updated to support STIX Cyber Observables 2.x
- We should also look to use the STIX Patterning grammar in some places here instead of the object model
- We would add 4 properties to the STIX COA

Course of Action Delete

```
{
  "type": "course-of-action",
  "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3e",
  ...,
  "action": "delete",
  "target": {
    "type": "stix:File",
    "specifiers": {
      "FileName": "malware.exe",
      "Hash": "...",
    }
  "actuator": {
    "type": "endpoint-server"
}
```

Course of Action Deny

```
{
  "type": "course-of-action",
  ...,
  "action": "deny",
  "target": {
    "type": "cybox:Network_Connection",
    "specifiers": {
      "Layer4Protocol": "UDP",
      "DestinationSocketAddress": {
        "IP_Address": {"Address_Value": "1.2.3.4"},
        "Port": {"Port_Value": 443}
    } },
  "actuator": {
    "type": "network-firewall", "specifiers": {"port": "2"}
  },
  "modifiers": {
    "response": "ack", "where": "perimeter"
  },
}
```

Possibilites - Option 1

- We create a Security Playbook SDO
  - This would track all of the human and automated processes and events used during an event /incident
  - This would reference specific COAs (OpenC2) that must/could/should/might be used
- STIX Course of Action SDO becomes a wrapper that can support human courses of action and OpenC2 atomic automated courses of action.