INDICATORS OF BEHAVIOR

Using Open Standards to represent, detect, and respond to Adversary Behaviors

Charlie Frick, Johns Hopkins Applied Physics Lab, OCA IOB Sub-Project
Vasileios Mavroeidis, University of Oslo, OASIS CACAO Project

Introduction

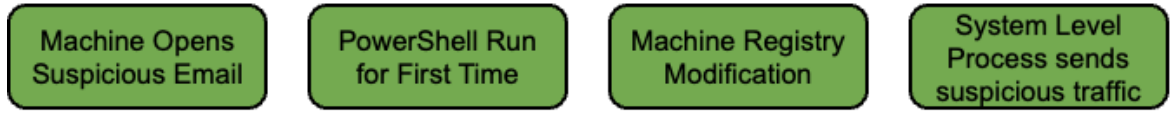
- ATT&CK provides a valuable representation of observed adversary attack patterns within the Structured Threat Information eXchange (STIX) standard format

- OASIS and the Open Cybersecurity Alliance have created reference implementations to help with machine-to-machine sharing, detection, and response to this information
  - Indicators of Behavior (IOB) knowledge bundles in STIX 2.1 to share observed adversary behaviors, connections to ATT&CK, detections, correlation, and response
  - Embedded security playbooks encoded in Collaborative Automated Course of Action Operations (CACAO) standardized format to enable machine speed processing for cybersecurity operations

Indicator of Behavior Concept

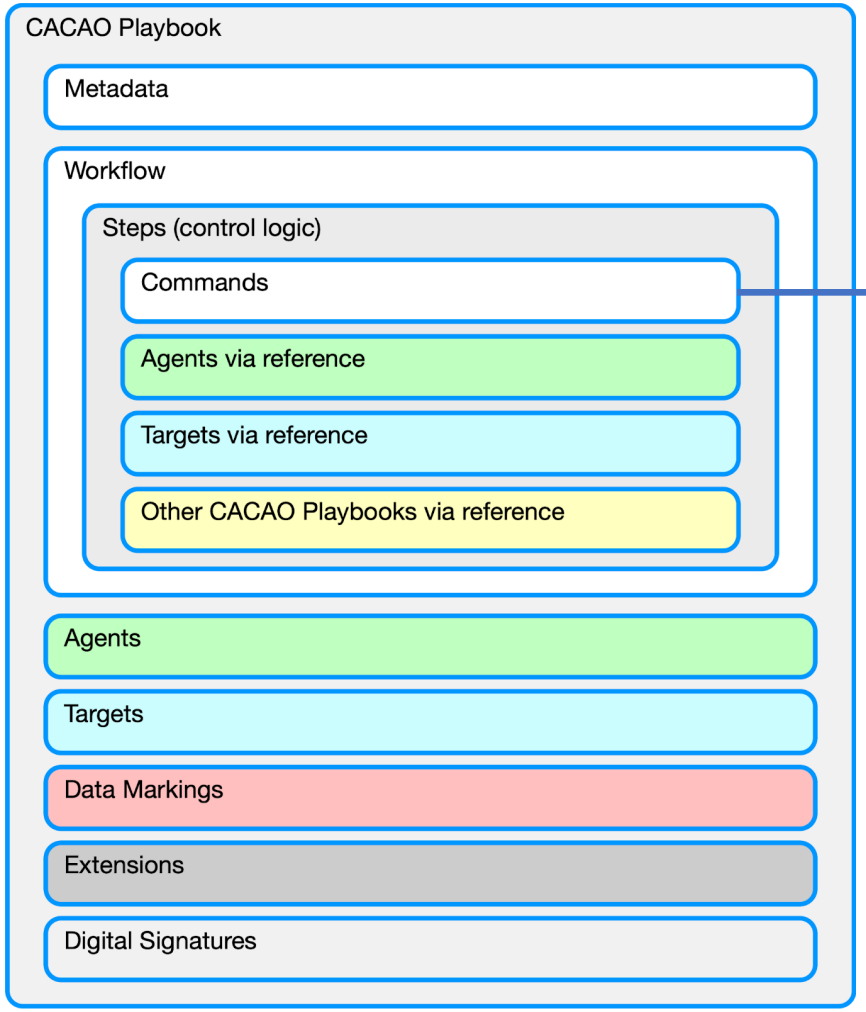
- Network defenders struggle to obtain and use Cyber Threat Intelligence
- STIX provides a standardized format for packaging the data, but the proper context is needed
- Indicator of Behavior (IOB) STIX bundles provide repeatable **sets** of observed adversary behaviors to help defender tools & capabilities
  - Intelligence context provided in machine-readable graph representation
  - Relationships to relevant ATT&CK attack pattern objects
  - Relationships to detection analytics
  - Includes **correlation workflows** to address false-positives
  - Includes response COAs and cybersecurity operations playbooks in standardized formats

Each procedure can be easily detected, but has potential for high false positive rate



The *sequence* of procedures is most likely malicious

CACAO
Cybersecurity Operations Playbooks



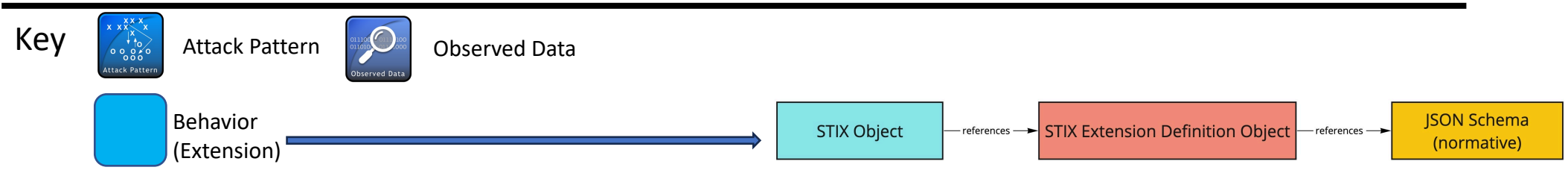
`match-indicator` - This activity matches on an indicator through traffic monitoring, system scans, and log analysis. This activity **MUST** be used with detection playbooks.
`analyze-collected-data` - This activity analyzes historical output from security devices (e.g., logs and network traffic capture). This activity **SHOULD** be used with investigation playbooks.
`identify-indicators` - This activity identifies one or more indicators that can be used to detect a security event. This activity **MUST** be used with investigation playbooks.
`scan-vulnerabilities` - This activity identifies vulnerabilities of a system. This activity **SHOULD** be used with prevention playbooks and **MAY** be used with attack playbooks.
`configure-systems` - This activity confirms secure configuration and if necessary, updates or configures systems or security devices to be resistant to a security event. This activity **MUST** be used with prevention playbooks.
`restrict-access` - This activity blocks applications and network traffic (ports/IP addresses/URLs) to mitigate a security event. This activity **SHOULD** be used with mitigation playbooks.
`disconnect-system` - This activity disconnects a compromised system from the network. This activity **MAY** be used with mitigation playbooks.
`eliminate-risk` - This activity eliminates the risk that a threat will affect a network by restricting capabilities. This activity **MUST** be used with mitigation playbooks.
`revert-system` - This activity reimages a system returning it to a known-good state. This activity **MAY** be used with remediation playbooks.

Example

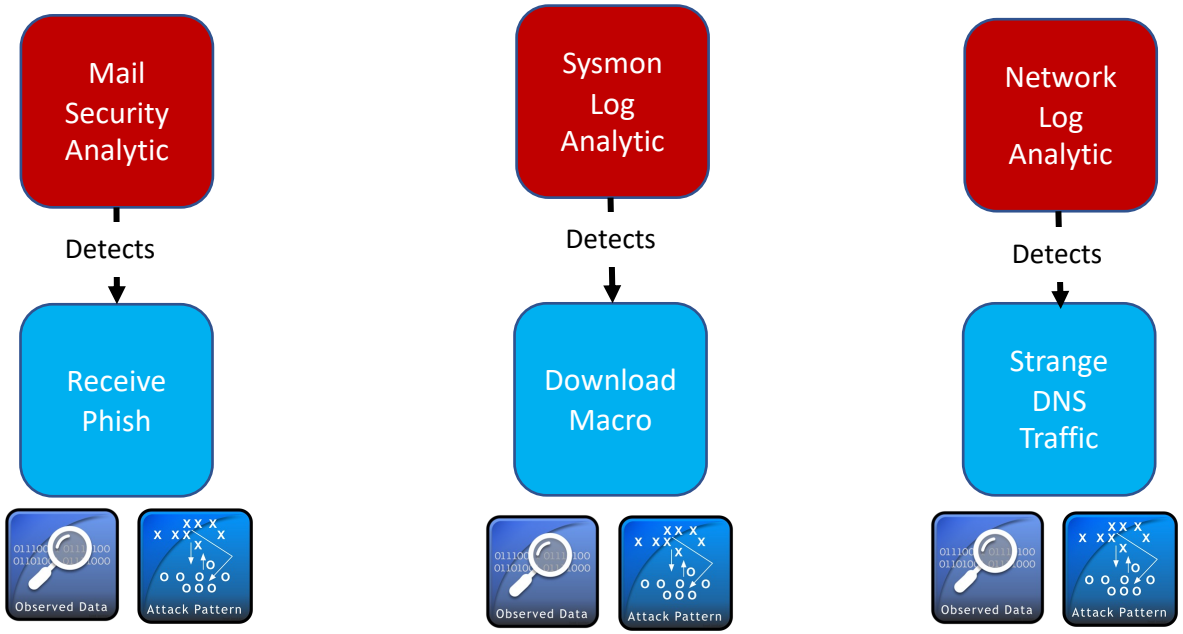
Custom STIX Objects represent a sequence of adversary behaviors

Attack Patterns Linked to MITRE ATT&CK STIX Objects

STIX Observables included for context



Example

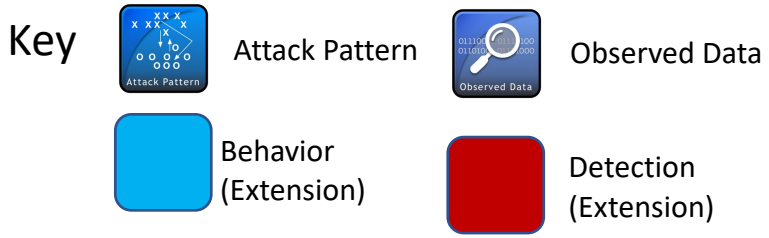


Each Behavior linked to detection analytics (SIGMA, STIX-Patterning, SQL, etc.)

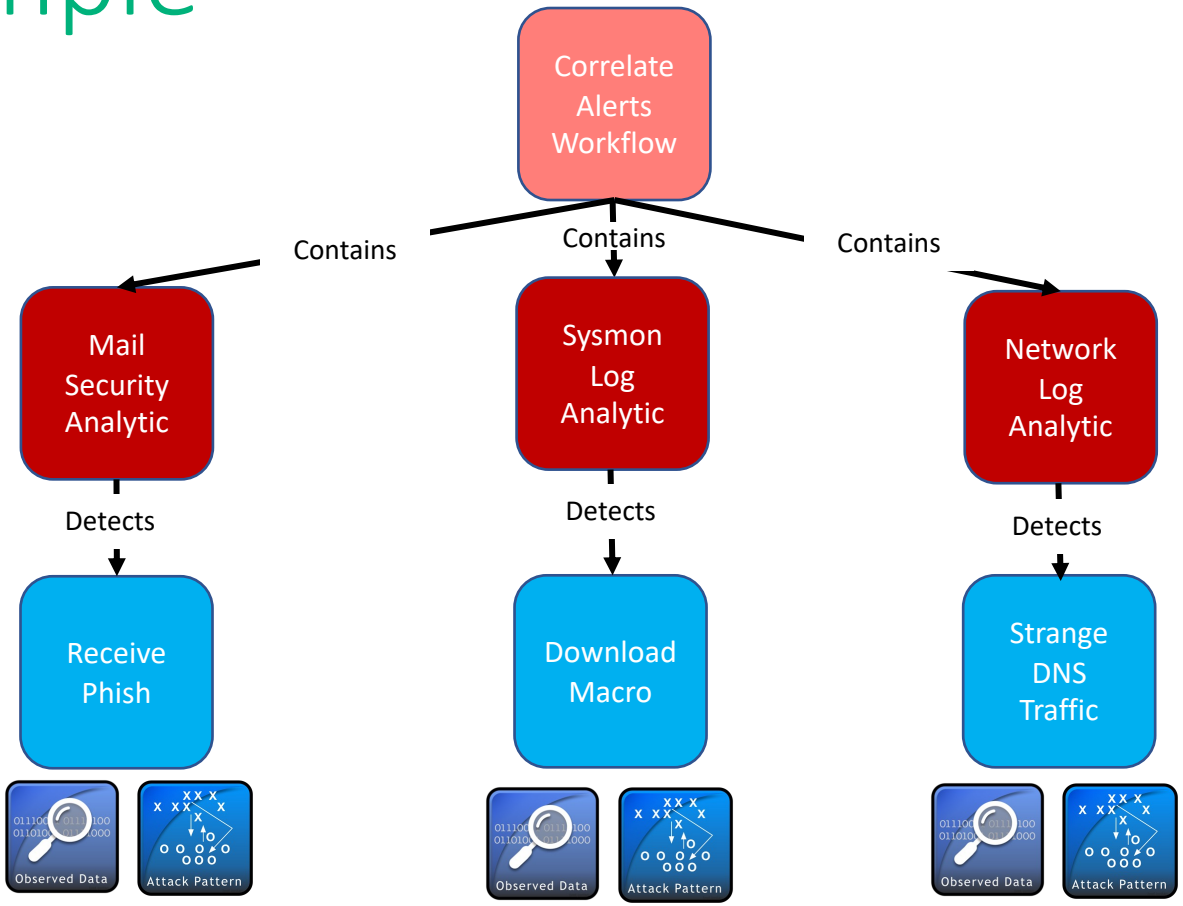
Analytics focus on observed patterns in defender network to compound detection of IOCs

Meant to be repeatable across campaigns

Analytics meant to run by automation in background (high false positives)



Example



Alert Correlation Workflow shares which fields between alerts will be common to support correlation and detection of threat activity with low false-positive rate

Key

Attack Pattern

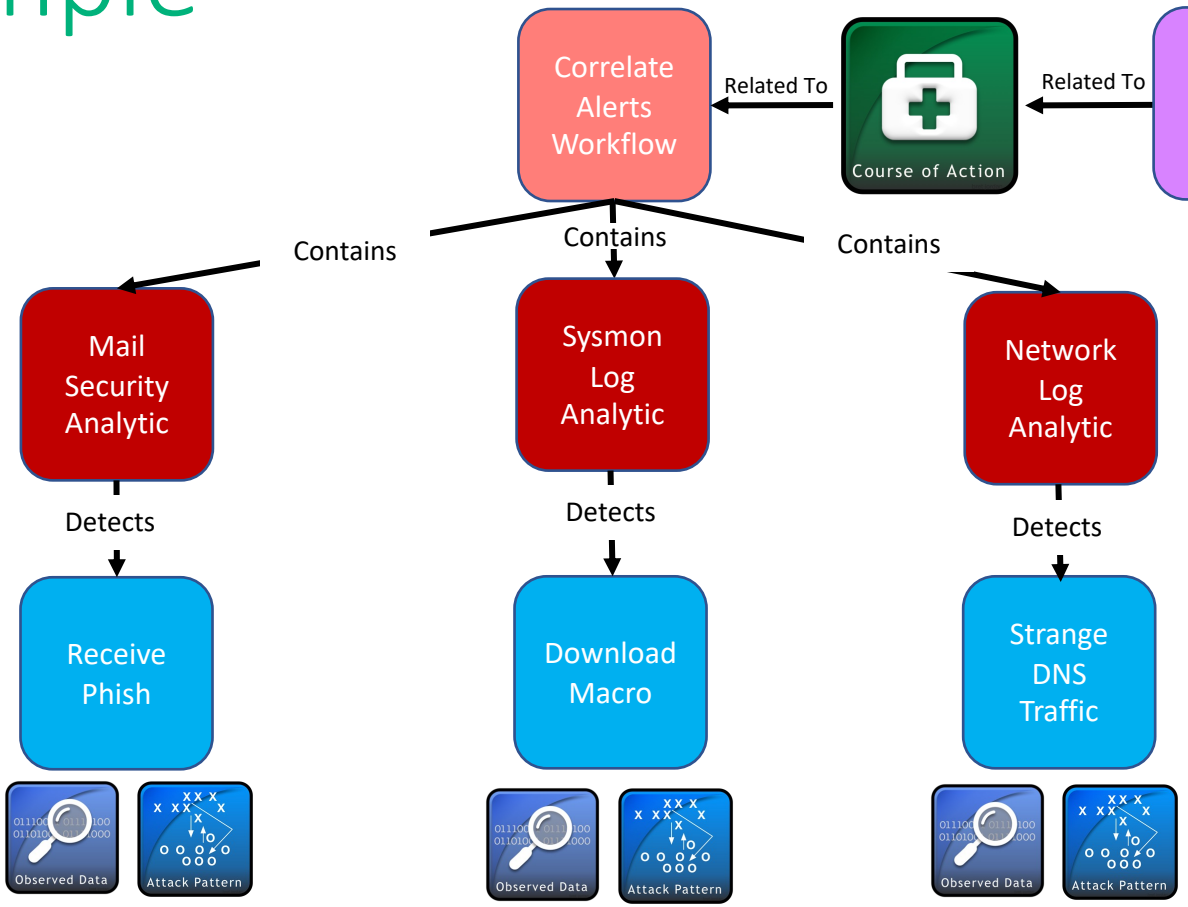
Observed Data

Detection Group (Extension)

Behavior (Extension)

Detection (Extension)

Example



Threat detection can also trigger Recommended Courses of Action

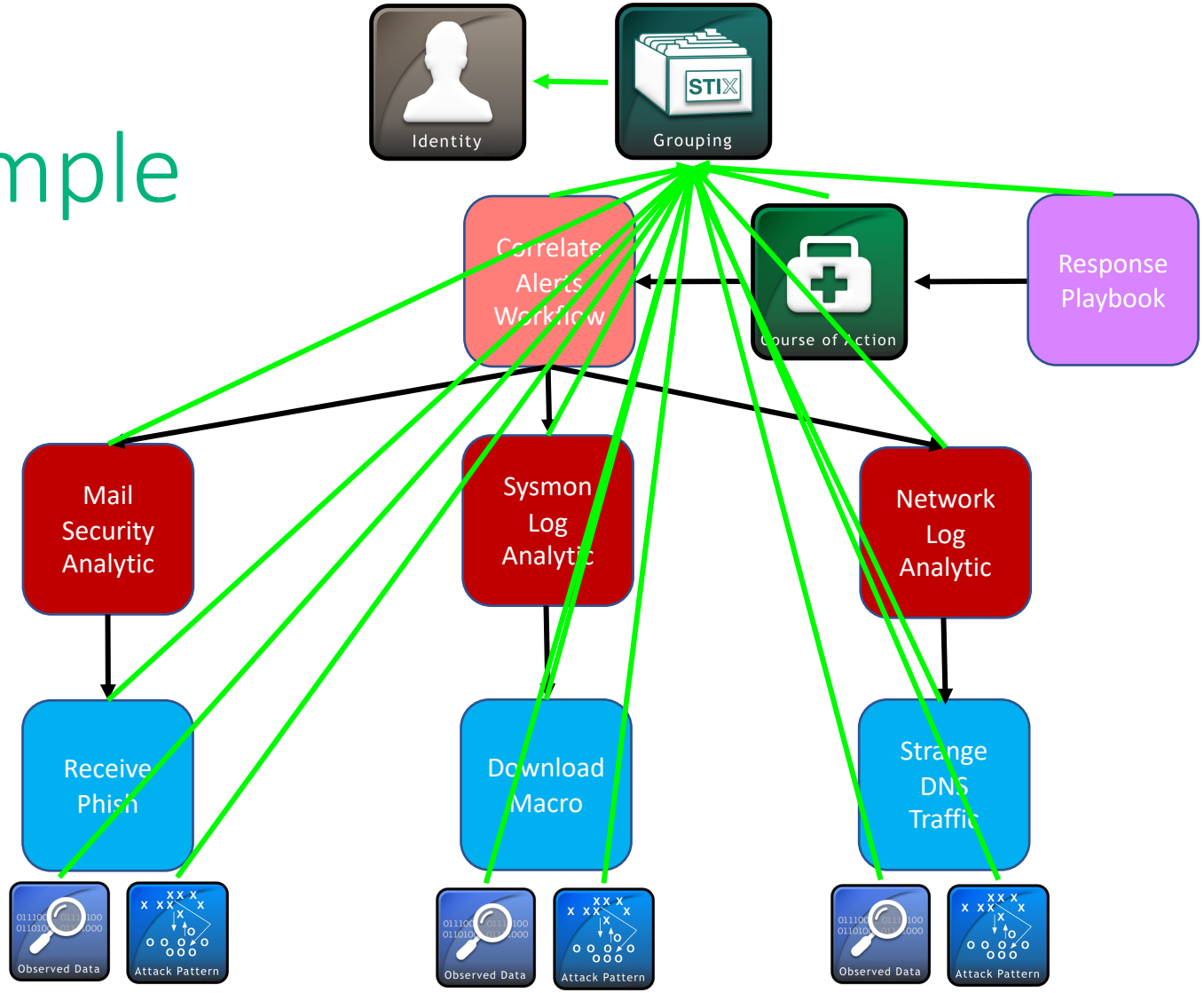
Courses of action can reference multiple playbooks in standardized formats (CACAO, BPMN, etc.)

Playbooks can rapidly be executed for manual and automated action

Key

- Attack Pattern
- Observed Data
- Detection Group (Extension)
- Playbook (Extension)
- Behavior (Extension)
- Detection (Extension)
- Course of Action

Example




```
{
  "type": "bundle",
  "id": "bundle--9edb6354-d73f-4ba2-b774-3d76c6474b14",
  "objects": [
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-iacd-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Spearphishing Link Behavior",
      "tactic": "INITIAL ACCESS",
      "technique": "T1566.002 Spearphishing Link",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
```

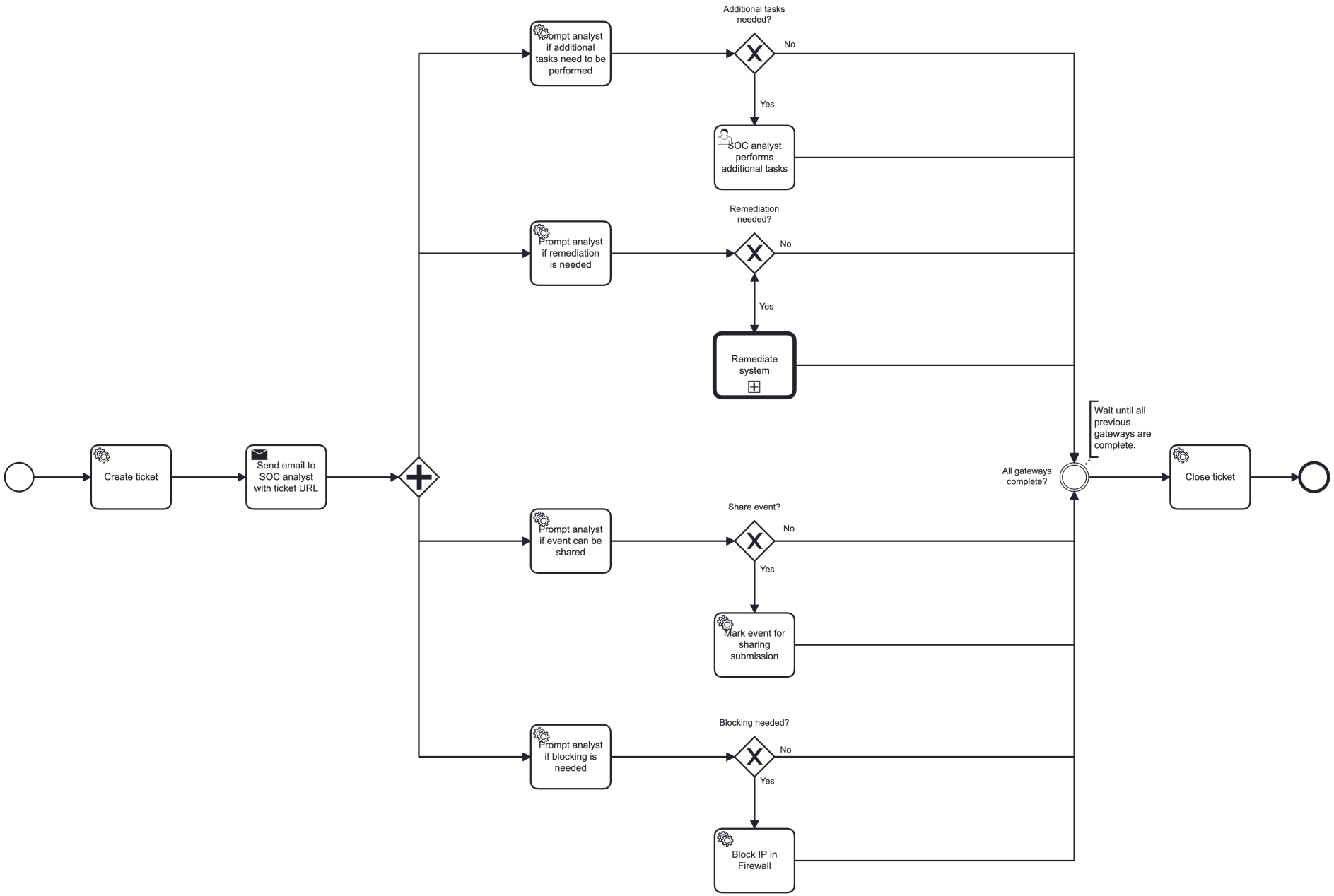

Entire set of sequence, detection, correlation, response, and associated observables / intelligence objects combined into STIX 2.1 grouping and bundle JSON format


```
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-iacd-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "C2 Behavior",
      "tactic": "Command and Control",
      "technique": "T1071.001 - Application Layer Protocol - Web Protocols",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-iacd-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
```


Key

- Attack Pattern
- Observed Data
- Detection Group (Extension)
- Playbook (Extension)
- Identity
- Behavior (Extension)
- Detection (Extension)
- Course of Action
- Grouping

Playbook example



Links for references and examples

- IOB Project page: https://opencybersecurityalliance.org/iob/
- CACAO Project page: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao
- IOB GitHub for documentation, use cases, reference implementation https://github.com/opencybersecurityalliance/oca-iob

Discussion / Q&A

Charlie Frick, Johns Hopkins Applied Physics Lab, Charles.Frick@jhuapl.edu
Vasileios Mavroeidis, University of Oslo, vasileim@ifi.uio.no