INDICATORS OF BEHAVIOR

Indicators of Behavior

Machine shareable objects for representing cyber adversary behavior to enable network defense

Charlie Frick, Johns Hopkins Applied Physics Lab,
OCA IOB Sub-Project Chair
Charles.Frick@jhuapl.edu

Acknowledgement:
Contributions from Dr. Vasileios Mavroeidis, University of Oslo, OASIS CACAO Project

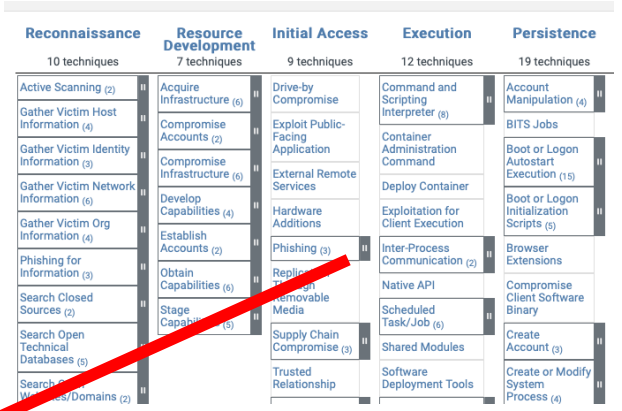
Overview

- In 2021, CISA and JHU/APL partnered with the Open Cybersecurity Alliance in their establishment of the Indicators of Behavior (IOB) Sub-Project
- This presentation will provide an overview of the IOB concept, some examples and information on the Sub-Project
- Links for access to the reference implementation and additional resources are included in this presentation
  - Active collaboration on this research is welcome through the IOB Sub-Project (https://opencybersecurityalliance.org/iob/)

Motivation for the Research

- Network defenders struggle to obtain and use Cyber Threat Intelligence
- STIX provides a useful standard for packaging the data, but the proper context is needed
- MITRE ATT&CK and D3FEND provide a necessary but not sufficient capability
- There is a need for something more general than an IOC and more specific than a high level Attack Pattern that can be shared and utilized by various community stakeholders
  - Automation & Vendor Products
  - Network Defenders
  - Threat Intelligence Analysts

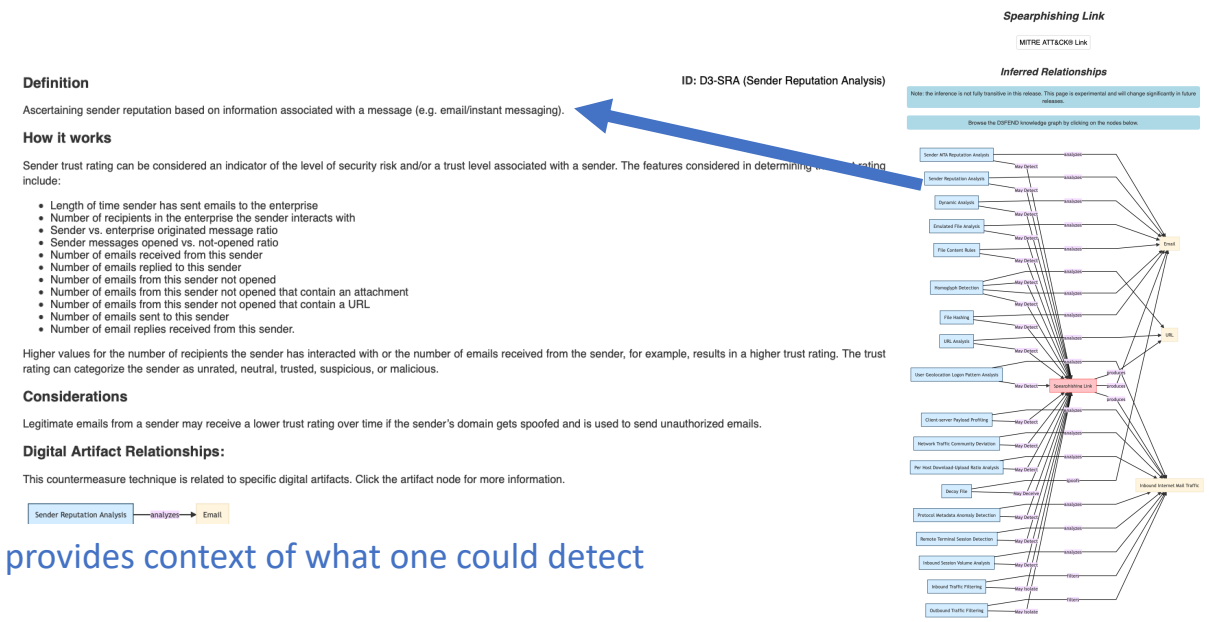
Shareable, machine-readable behavior objects are being developed to bridge this gap



ATT&CK shows what type of data to look for

Application Log

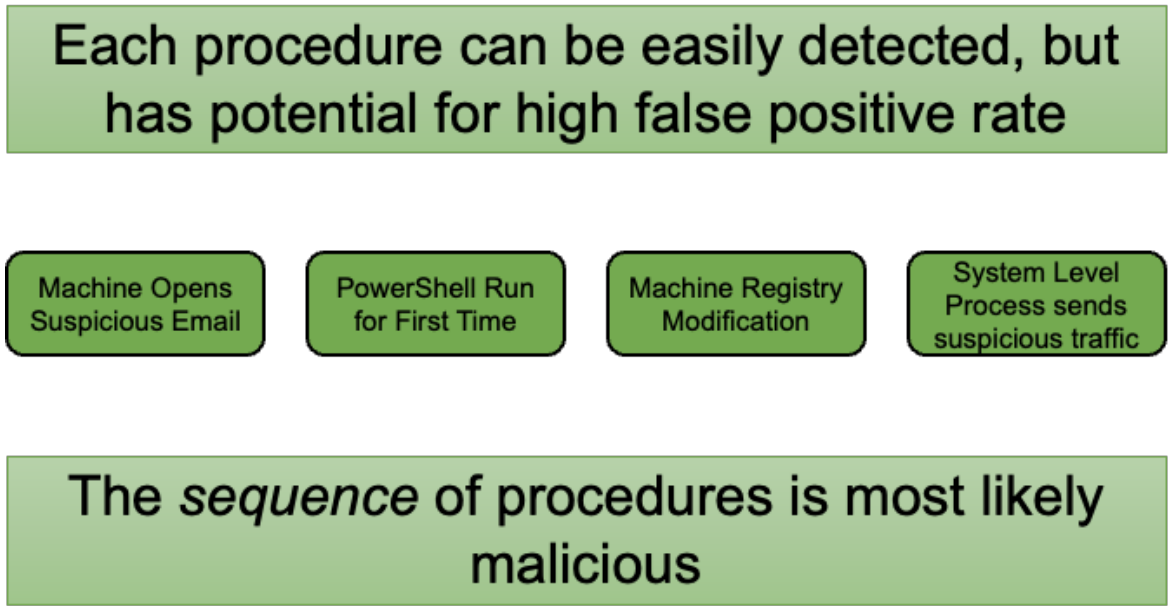
Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)[1]



D3FEND provides context of what one could detect

Indicator of Behavior Concept

- 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



What is STIX?

- **S**tructured **T**hreat **I**nformation e**X**change
- Standard language and framework for describing and exchanging cyber threat intelligence (CTI)
- Managed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the OASIS (Organization for the Advancement of Structured Information Standards) consortium
- JSON representation of CTI to enable machine readability and sharing of knowledge graphs
- Often sent via TAXII standard protocol also managed by OASIS CTI TC

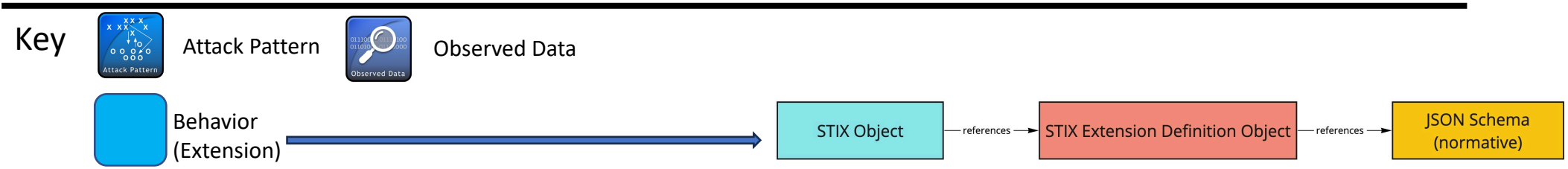
For more information:
https://oasis-open.github.io/cti-documentation/

Example

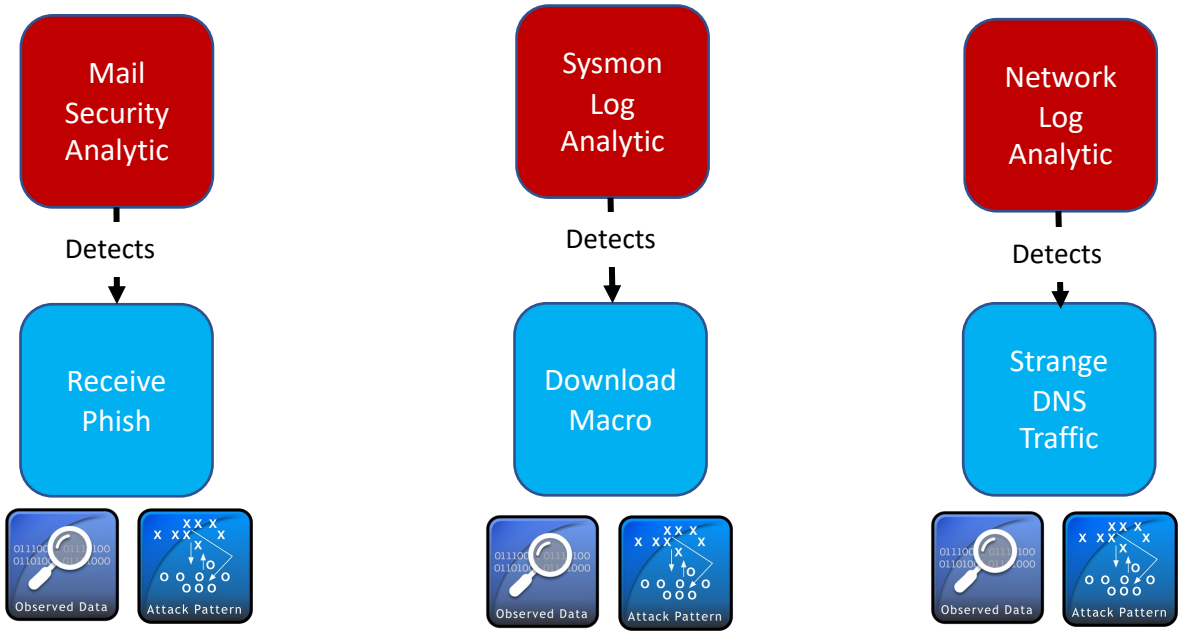
Custom STIX Objects represent a sequence of adversary behaviors

Attack Patterns Linked to MITRE ATT&CK STIX Objects

STIX Observables included for context



Example

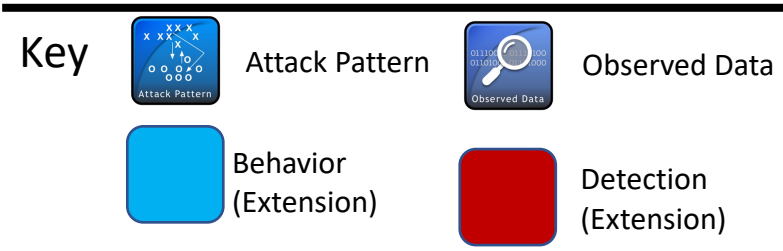


Each Behavior linked to detection analytics (SIGMA, STIX-Patterning, SQL, etc.)

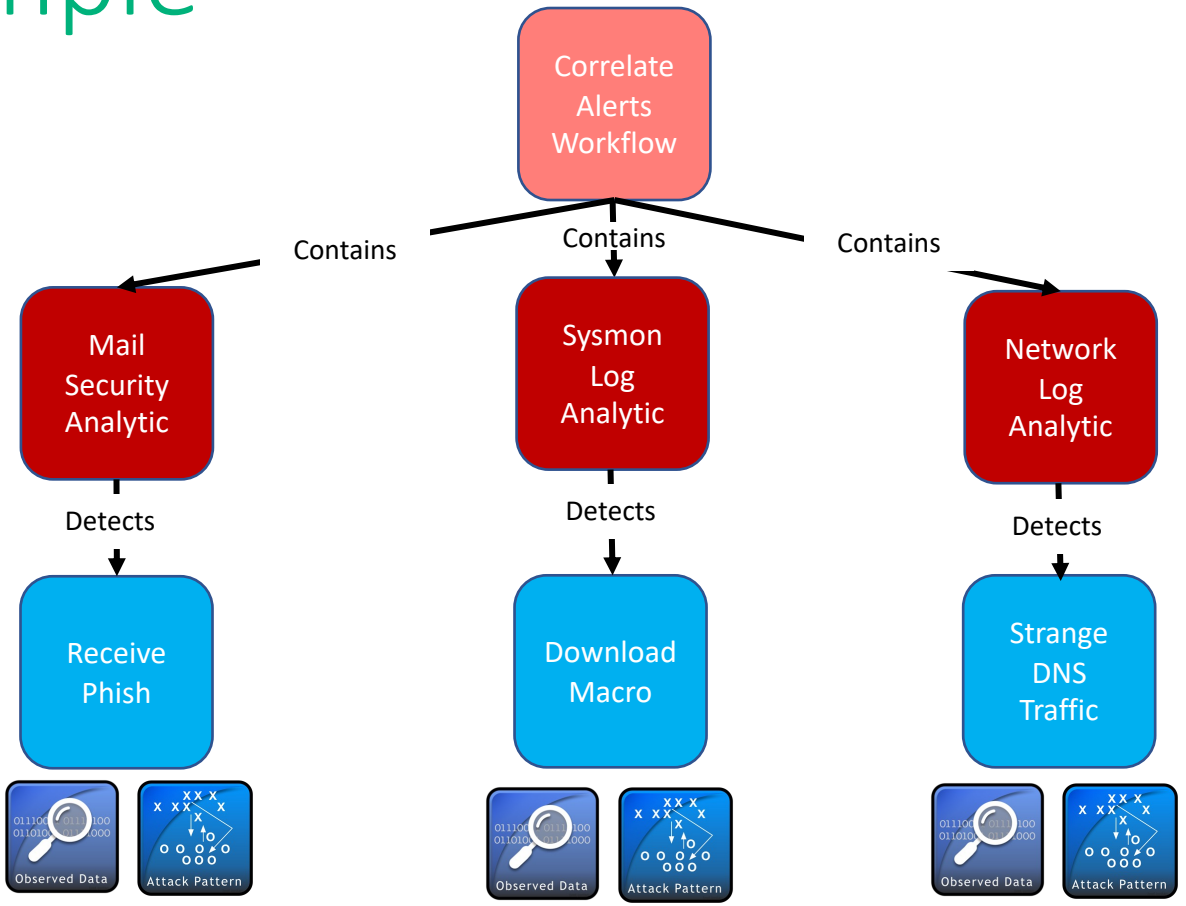
Analytics focus on observed patterns in defender network to compound detection of IOCs

Meant to be repeatable across campaigns

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

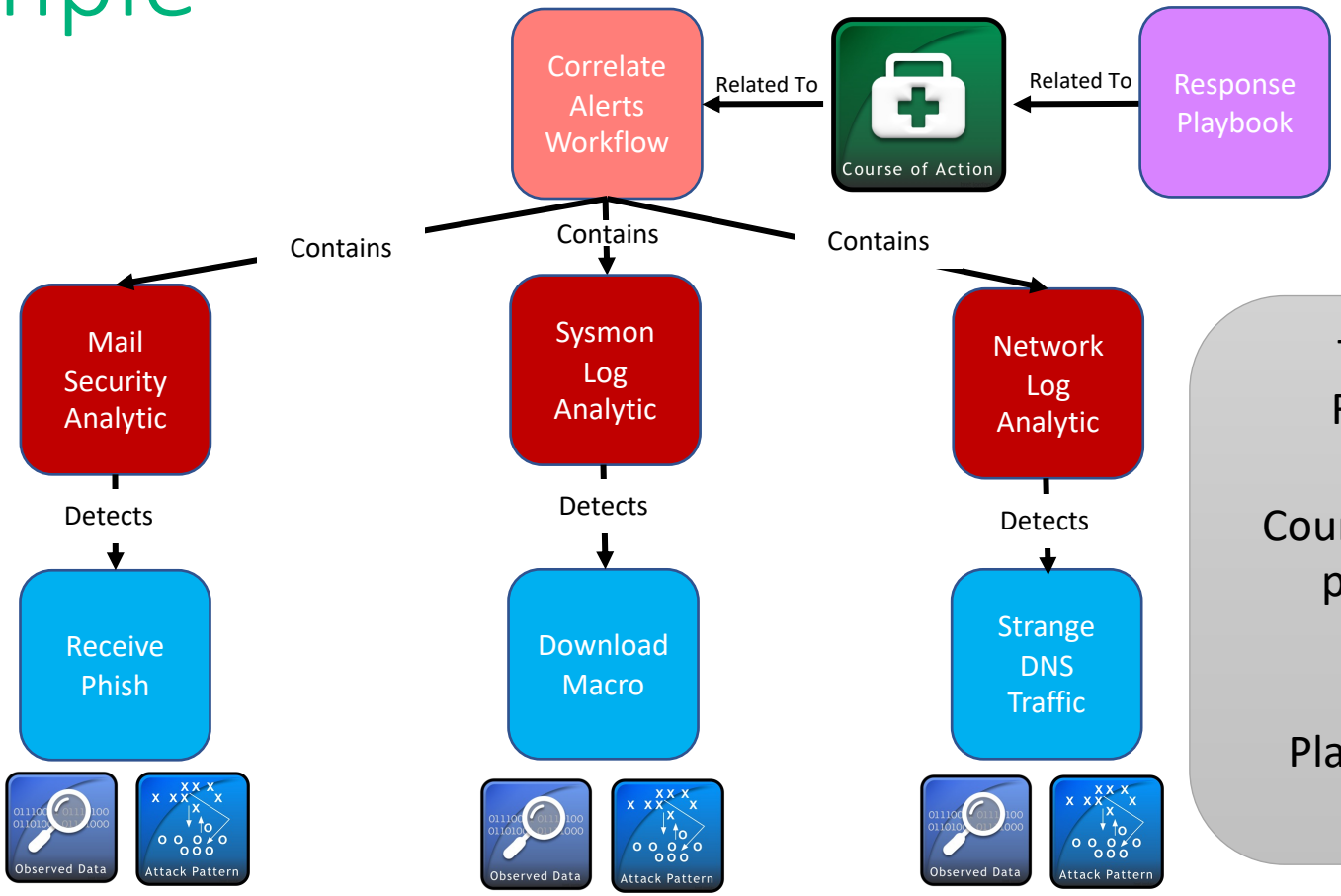


Example



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

Example



Threat detection can also trigger Recommended Courses of Action

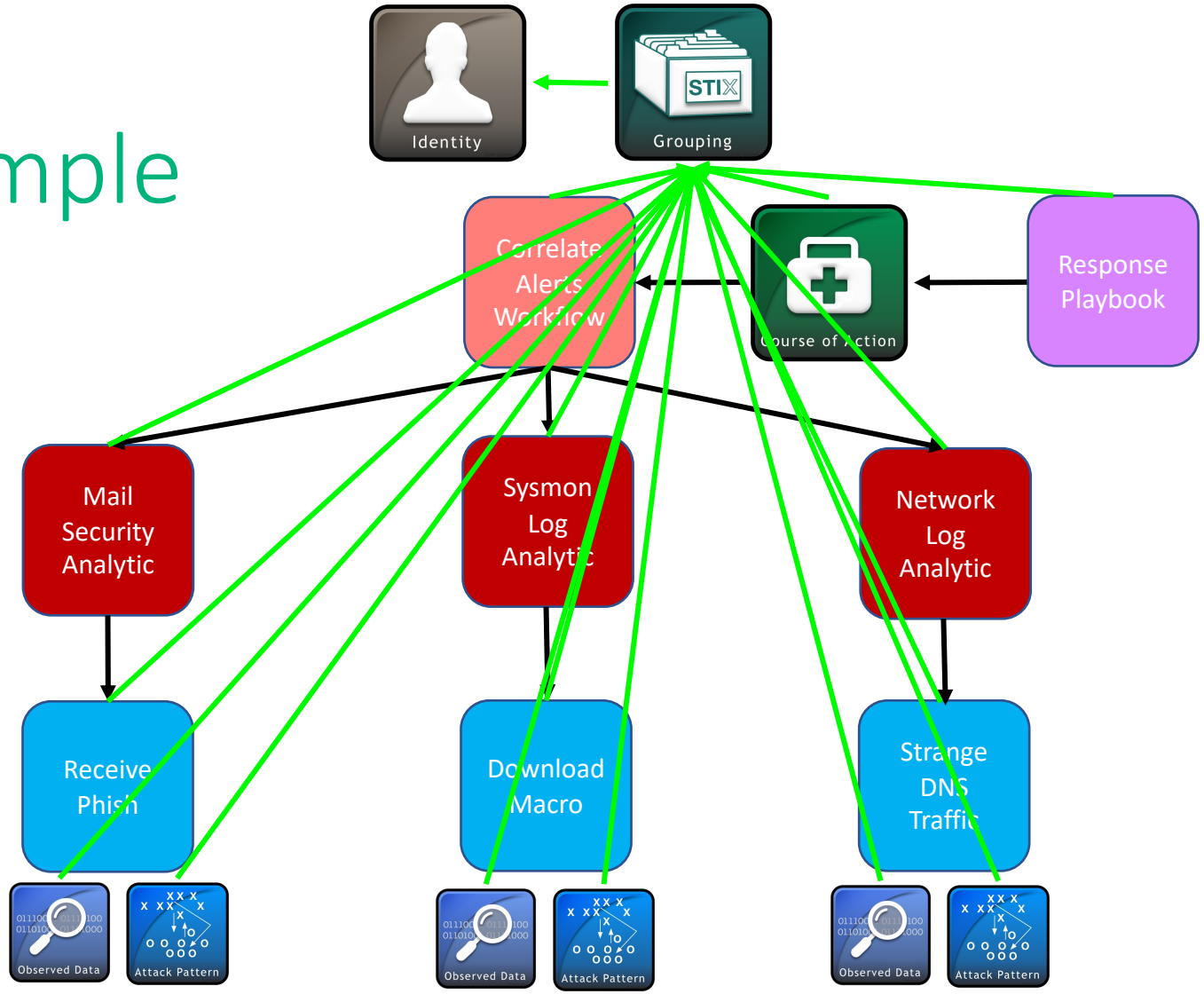
Courses of action can reference multiple playbooks in standardized formats (CACAO, BPMN, etc.)

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



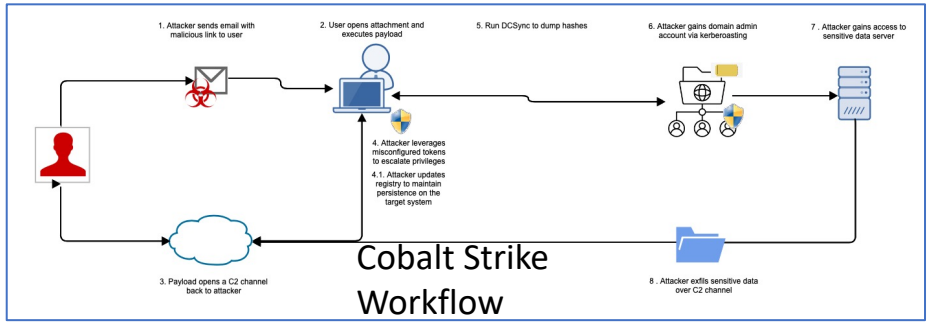
Entire set of sequence, detection, correlation, response, and associated observables / intelligence objects combined into STIX 2.1 grouping and bundle JSON format

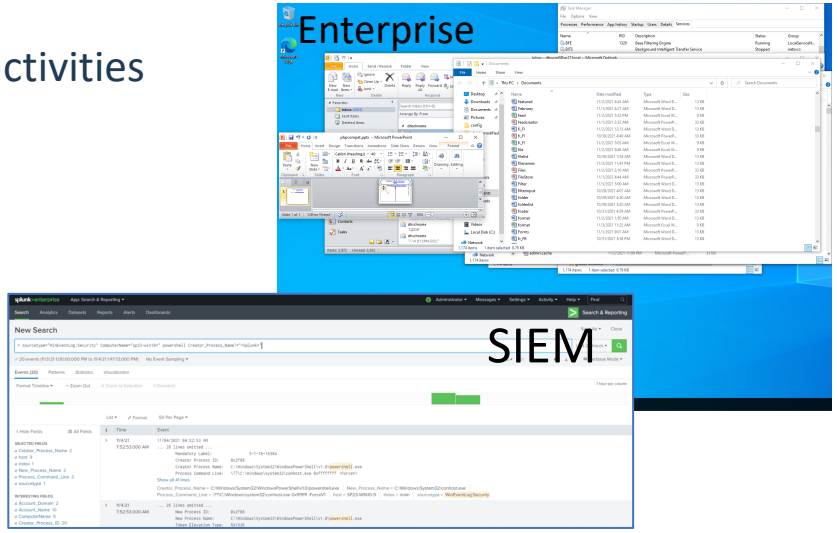
Key

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

Current Reference Prototype

- A 1800+ line JSON “bundle” compliant with STIX 2.1 spec
- Represents observed behaviors from an emulated attack based on APT 37 / “Reaper”
- Includes behaviors and detections in shareable Sigma rule format
  - Detections tested against emulated enterprise network with a SIEM, endpoint, and network sensors
  - Enterprise machines conduct general user activities so analytic false positives can be reduced





To exercise this new approach, we have created and tested a bundle for an example APT attack

STIX


```
{
  "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"
        }
      ],
      "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-b2d4-1234567890aa",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Execution Behavior",
      "tactic": "EXECUTION",
      "technique": "T1059.001 Command/Script execution - VBA",
      "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-b2d4-1234567890bb",
      "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",
```

STIX2NEO4J Script

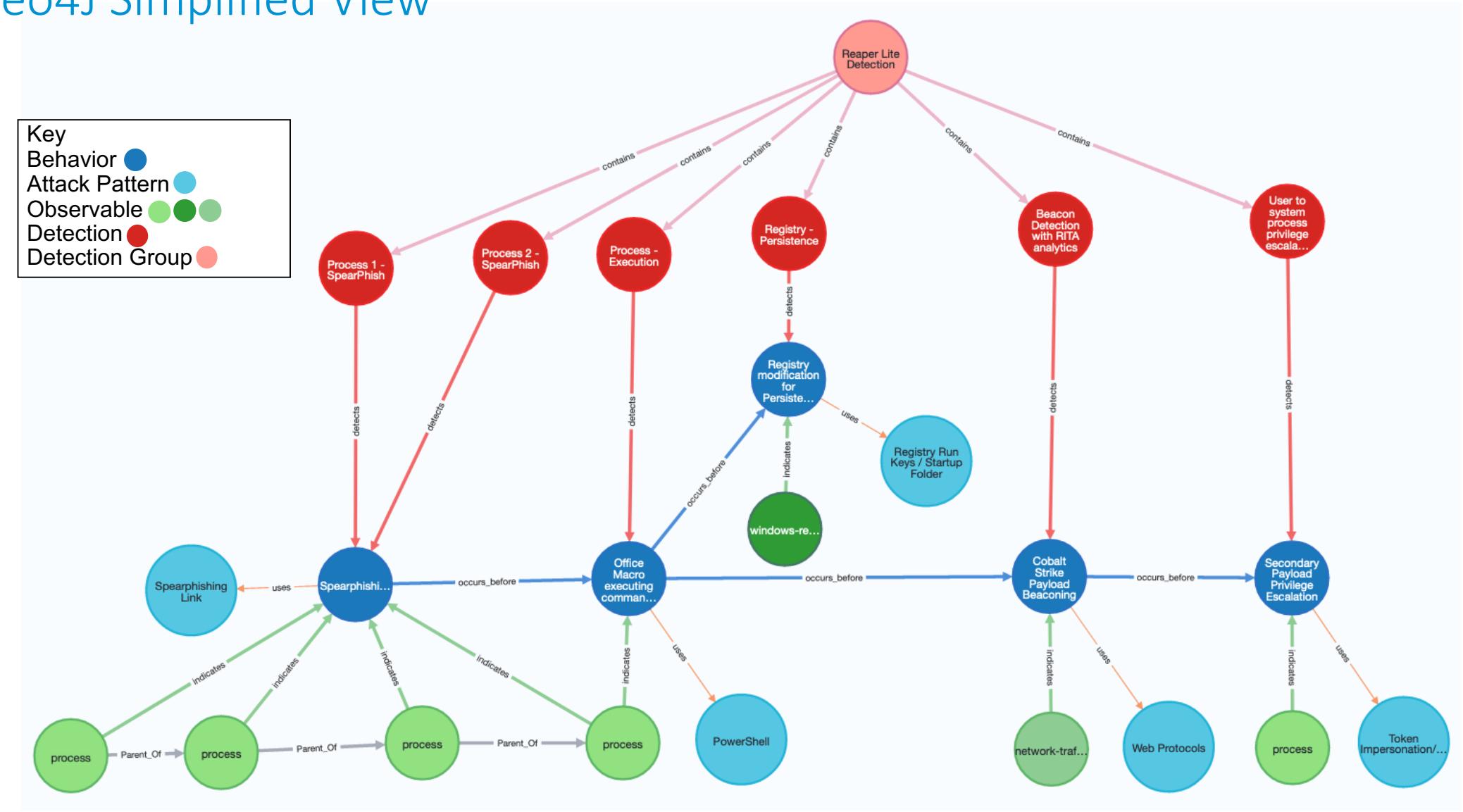
- Python script for analyzing STIX 2.x bundles in a neo4j graph database
- Provides additional analytical capabilities for investigating raw STIX messages without major modification of the data
  - Threat Intel Platforms often make significant changes to data model upon import
- Released on an Apache2 license through the Open Cybersecurity Alliance Indicator of Behavior Sub-Project
- Script repository link on GitHub:
  - https://github.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter

SCAN ME

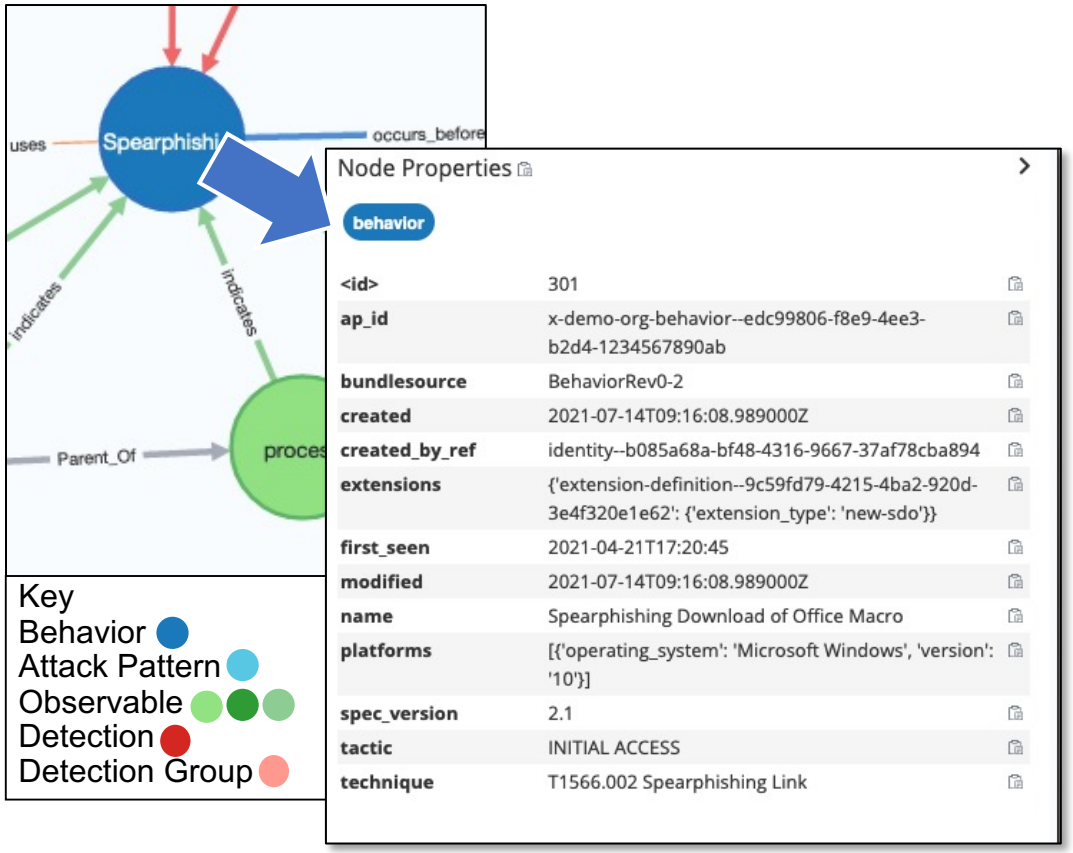
INDICATORS OF BEHAVIOR

Visualization of Bundle

Neo4J Simplified View

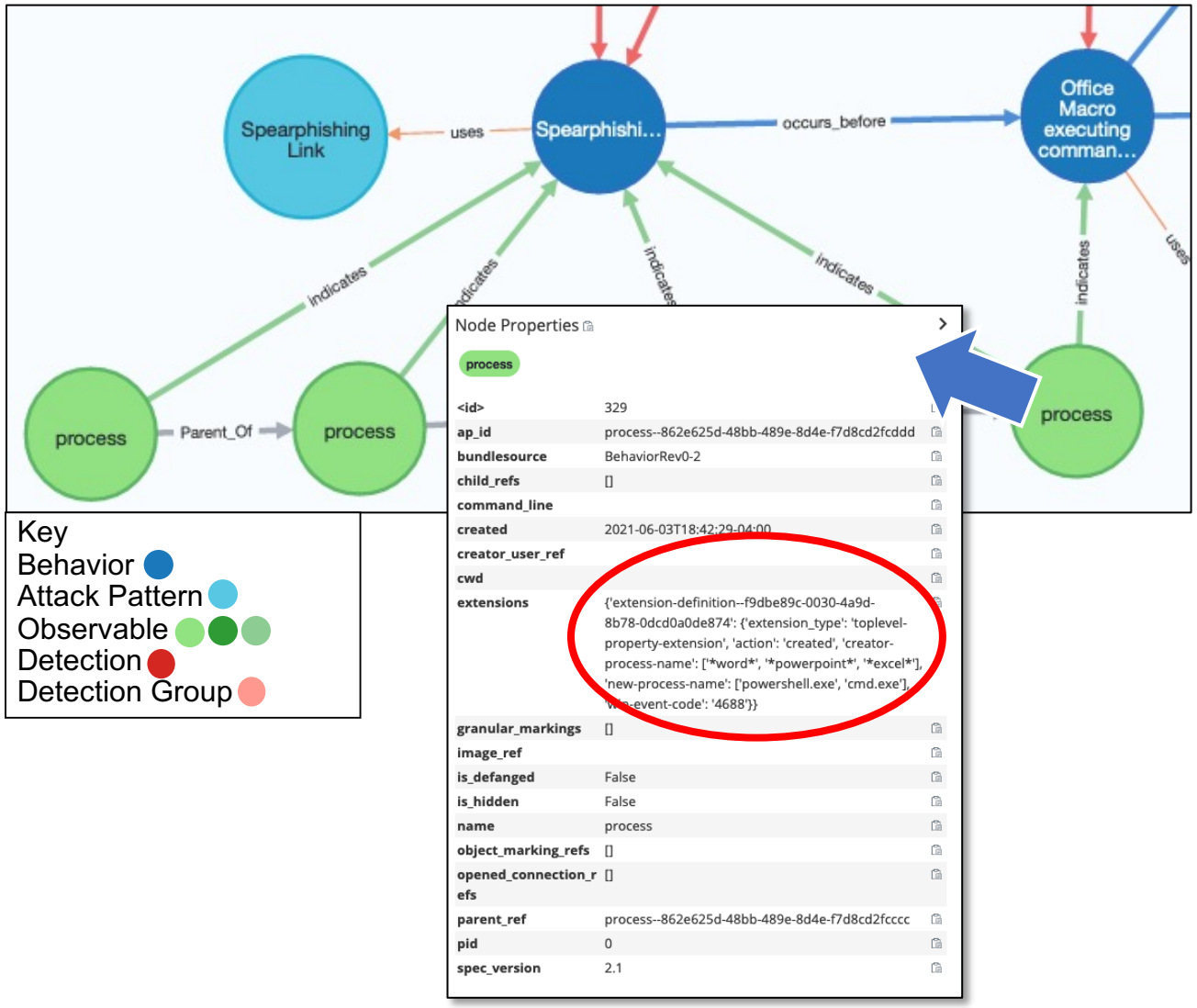


Visualization of Bundle – Behavior Object



- Each Behavior Object summarizes one of the behavior steps in the overall sequence
- Object metadata contains links to relevant MITRE ATT&CK entries
  - Multiple behaviors and behavior sets could map to these ATT&CK techniques
- As will be seen on the following slides, multiple node types will link to the Behavior Object node to define the overall behavior
  - Observables
  - Detection analytics
- Multiple Behavior Objects are linked together to represent the overall sequence of the behavior set

Visualization of Bundle – Observables



- Our spearphishing behavior also includes relationships to a chain of Process STIX Cyber Observables
- Process metadata includes information on data sources to search for the process
- Also defines which process calls it
- Highlighted example is a common process for searching/correlating 2 behaviors in the set

Visualization of Bundle – Detection

Decoded

```
---
title: Registry Run Keys
id: registry persistence
status: experimental
description: Detects new
registry run key created event.
tags:
- attack.persistence
- attack.t1547
author: demo
date: 2021/06/07
logsource:
  product: windows
  index: main
  category: registry_event
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
    - Run
    - Shell Folders
  condition: selection
falsepositives:
- High
level: high
```

- The information in the STIX Cyber Observables allow us to create a shareable detection analytic linked to the behavior
- Highlighted example shows a detection for web browser downloading and opening a macro-enabled MS Office file in Sigma rule format
- Rule is stored as base64 string to preserve formatting

Visualization of Bundle – Note on Sigma

Sigma YAML

```
---
title: Registry Run Keys
id: registry persistence
status: experimental
description: Detects new
registry run key created event.
tags:
- attack.persistence
- attack.t1547
author: demo
date: 2021/06/07
logsource:
  product: windows
  index: main
  category: registry_event
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
    - Run
    - Shell Folders
  condition: selection
falsepositives:
- High
level: high
```

Splunk Query

```
(EventCode="4657" (Object_Name="*Run*" OR
Object_Name="*Shell Folders*"))
```

Elastic Query

```
(EventCode:"4657" AND
Object_Name.keyword:(*Run* OR *Shell\
Folders*))
```

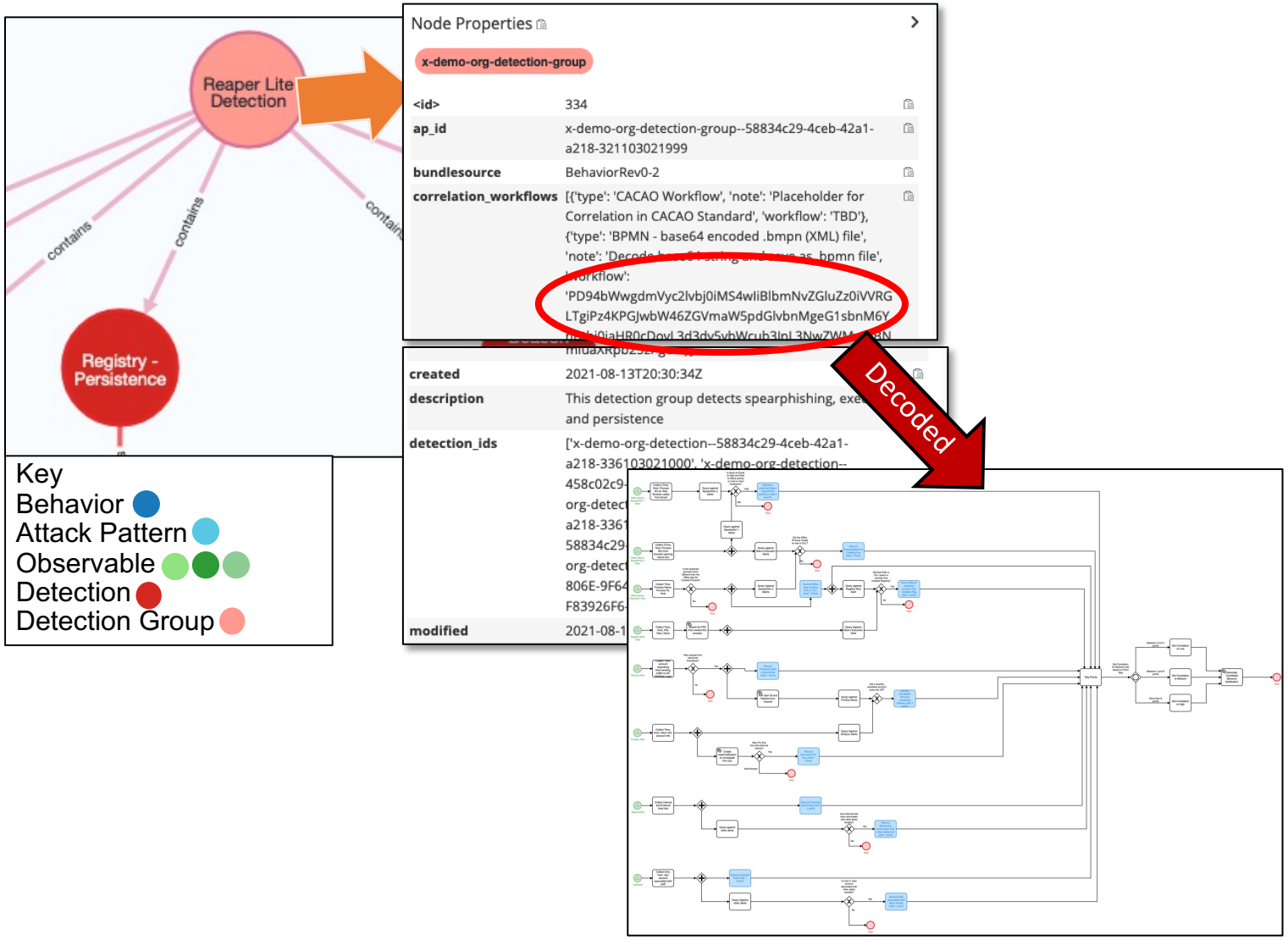
Azure Sentinel Rule

{"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#", "contentVersion": "1.0.0.0", "parameters": {"workspace": {"type": "String"}}, "resources": [{"id": "[concat(resourceId('Microsoft.OperationalInsights/workspaces/providers', parameters('workspace'), 'Microsoft.SecurityInsights'),'/alertRules/registry persistence')]", "name": "[concat(parameters('workspace'),'/Microsoft.SecurityInsights/registry persistence')]", "type": "Microsoft.OperationalInsights/workspaces/providers/alertRules", "apiVersion": "2021-03-01-preview", "kind": "Scheduled", "properties": {"displayName": "Registry Run Keys by demo", "description": "Detects new registry run key created event. Technique: T1547.", "severity": "high", "enabled": true, "query": "Windows | where (EventCode == \"4657\" and (Object_Name contains 'Run' or Object_Name contains 'Shell Folders'))", "queryFrequency": "PT30M", "queryPeriod": "PT30M", "triggerOperator": "GreaterThan", "triggerThreshold": 0, "suppressionDuration": "PT2H30M", "suppressionEnabled": true, "tactics": ["Persistence"], "incidentConfiguration": {"createIncident": true, "groupingConfiguration": {"enabled": false, "reopenClosedIncident": false, "lookbackDuration": "PT2H30M", "matchingMethod": "AllEntities", "groupByEntities": [], "groupByAlertDetails": [], "groupByCustomDetails": []}}, "eventGroupingSettings": {"aggregationKind": "SingleAlert"}, "alertDetailsOverride": null, "customDetails": null, "templateVersion": "1.0.0"}}]}

- Sigma is not a SIEM, but it is a common format for SIEM rules
- Free and open source tools exist to automatically translate the rule into multiple SIEM formats

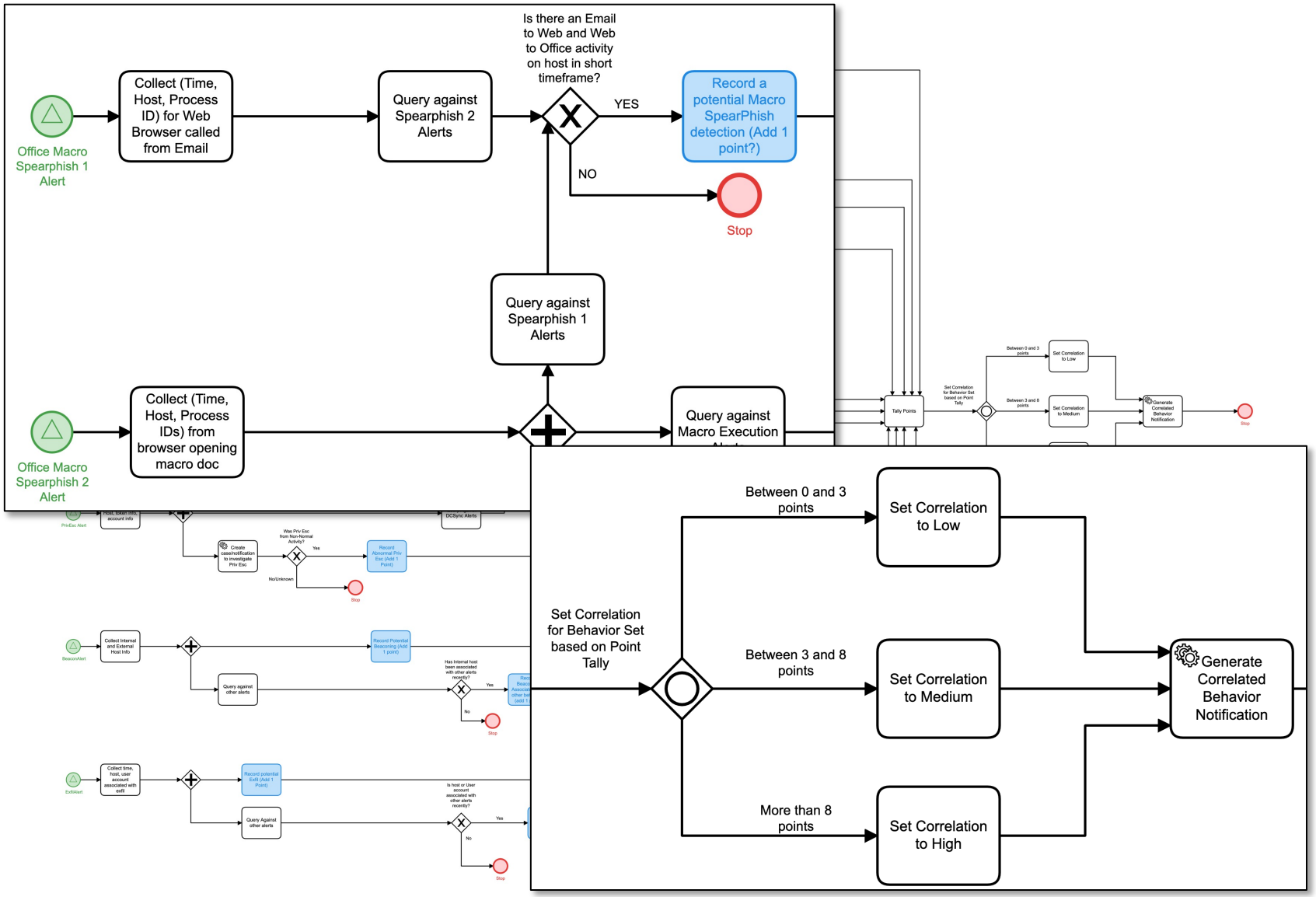
Use of Sigma format for defining detection analytics allows it to be shared and easily consumed through automation for various organizations regardless of their SIEM choice

Visualization of Bundle – Detection Group



- Any single detection analytic within the bundle is prone to false positives
- The Detection Group Object exists in the bundle to help correlate the detections and explain which fields should be common between queries
- Includes base64 encoded Business Process Model Notation (BPMN) for visual and planned support for Collaborative Automated Course of Action Operations (CACAO) standard workflow

Sample Detection Group Correlation Workflow



- Provides logic for how to correlate alerts from the set of detections shared in the bundle
- Any single alert may have multiple false positives
- Correlated alerts allow for higher fidelity of detections
- Can be run with automation or manually

Conclusion

- The IOB Sub-Project wants to drive the use of shared CTI to support network defense operations
- The behavior bundle construct via STIX provides a start for a format that allows sharing deeper context as well as actions to take
  - Current revisions will also include “triggers” for response workflows
- For more information:
  - IOB Project page: https://opencybersecurityalliance.org/iob/
  - IOB GitHub for documentation, use cases, reference implementation https://github.com/opencybersecurityalliance/oca-iob