IACD Reference Team:
Shareable Workflows

Paul Laskowski –Johns Hopkins Applied Physics Laboratory

© 2017 by The Johns Hopkins Applied Physics Laboratory.
Material is made available under the Creative Commons Attribution 4.0 International License.

Shareable Workflows

Sharable Workflows – Background & Concept

- **Background:**
  - ○ **Current Orchestration tools tend to have have proprietary GUI/UX for playbook/workflows.**
- **Concept of Shareable Workflows:**
  - ○ **Promote a common visual/data format which represent sharable workflows that can be imported to and from different orchestration tools.**
  - ○ **Allows sharing of workflows for orchestration, vendor independence of IT cyber systems.**
  - ○ **This would allow greater adoption of workflows that could be shared, uploaded, downloaded, adopted.**
  - ○ **Standardized reference workflows could be hosted by government and other cyber organizations (DHS, ISAC, NIST, CIS, etc.).**
  - ○ **Preference for an non-proprietary standard that are open source and currently in use.**
  - ○ **Support graphical and digital data structure.**

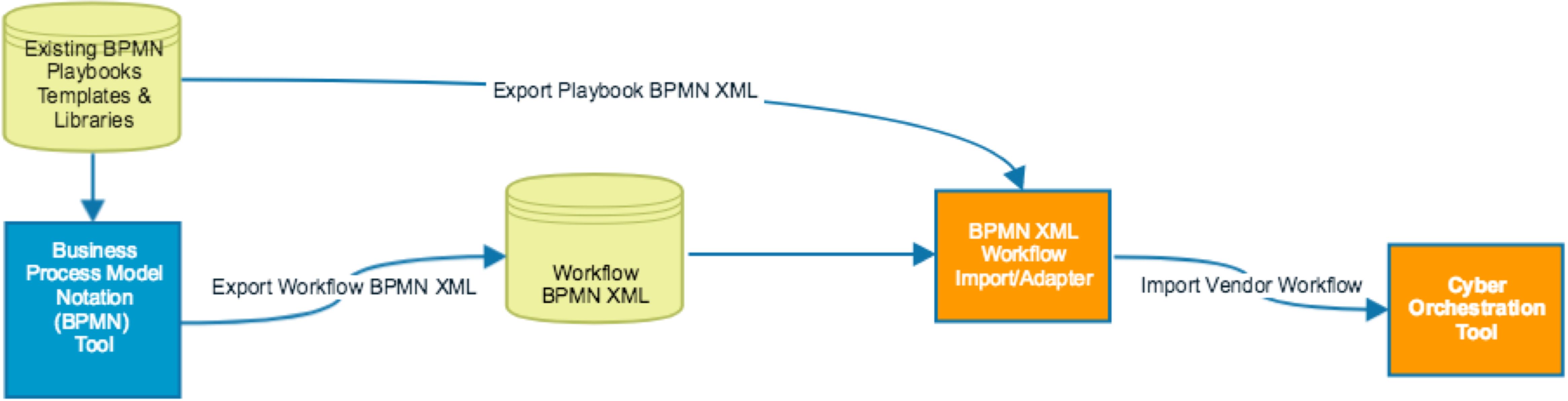
Sharable Workflows – Proposed Solution

- Business Process Model Notation (BPMN) 2.0 is a graphical open source business process modelling language.
- XML based language that is fully interchangeable between BPMN tools.
- 30+ vendors (Oracle and IBM) provide both free and licensed/fee-based BPMN tools.
- Hierarchical structure allows layered workflows to provide more detail as layers of IT are traversed.
- Use STIX, TAXII, Att@ck, OpenC2 and Common Exchange Format (CEF) data integrated into the sharable workflows for passing pertinent data enrichment from orchestration tools to SIEM and other cyber tools.

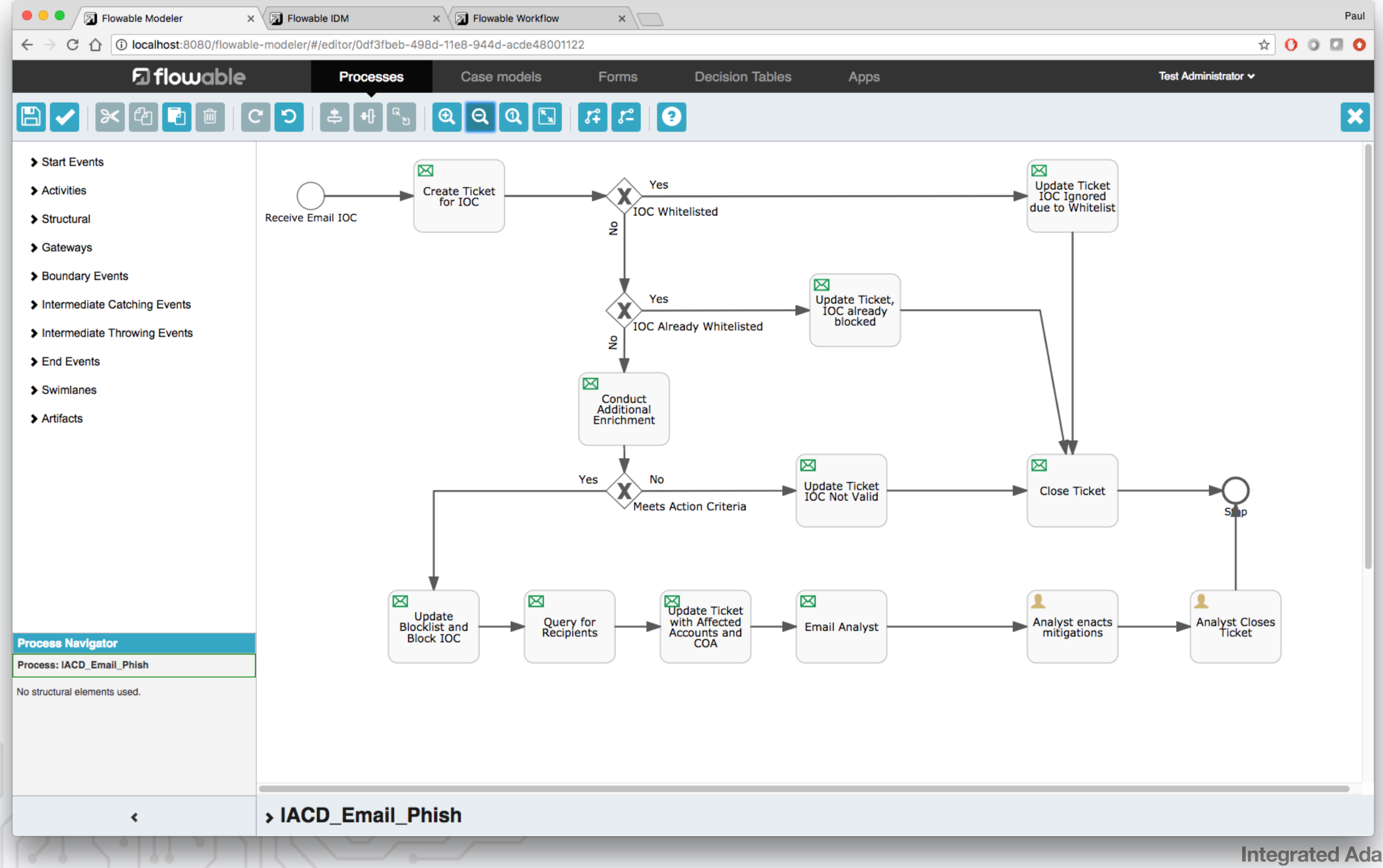
Sharable Workflows – Major Accomplishments

1. **Created Simple Phishing Email example for Sharable Workflow**
   - ✓ Created XML and JSON files to represent a Phishing Email workflow.
2. **Success During Integrated Cyber (IC) Conference in May 2018:**
   - ✓ Demonstrated concept of Sharable Workflow with Cybersponse
   - ✓ Cybersponse imported the XML into their tool with some manual user data manipulation
3. **Building More Relationships with Key Industry Partners**
   - ✓ IBM’s Resilient, Phantom, and Demisto have expressed interest in working with APL IACD on Sharable Workflows

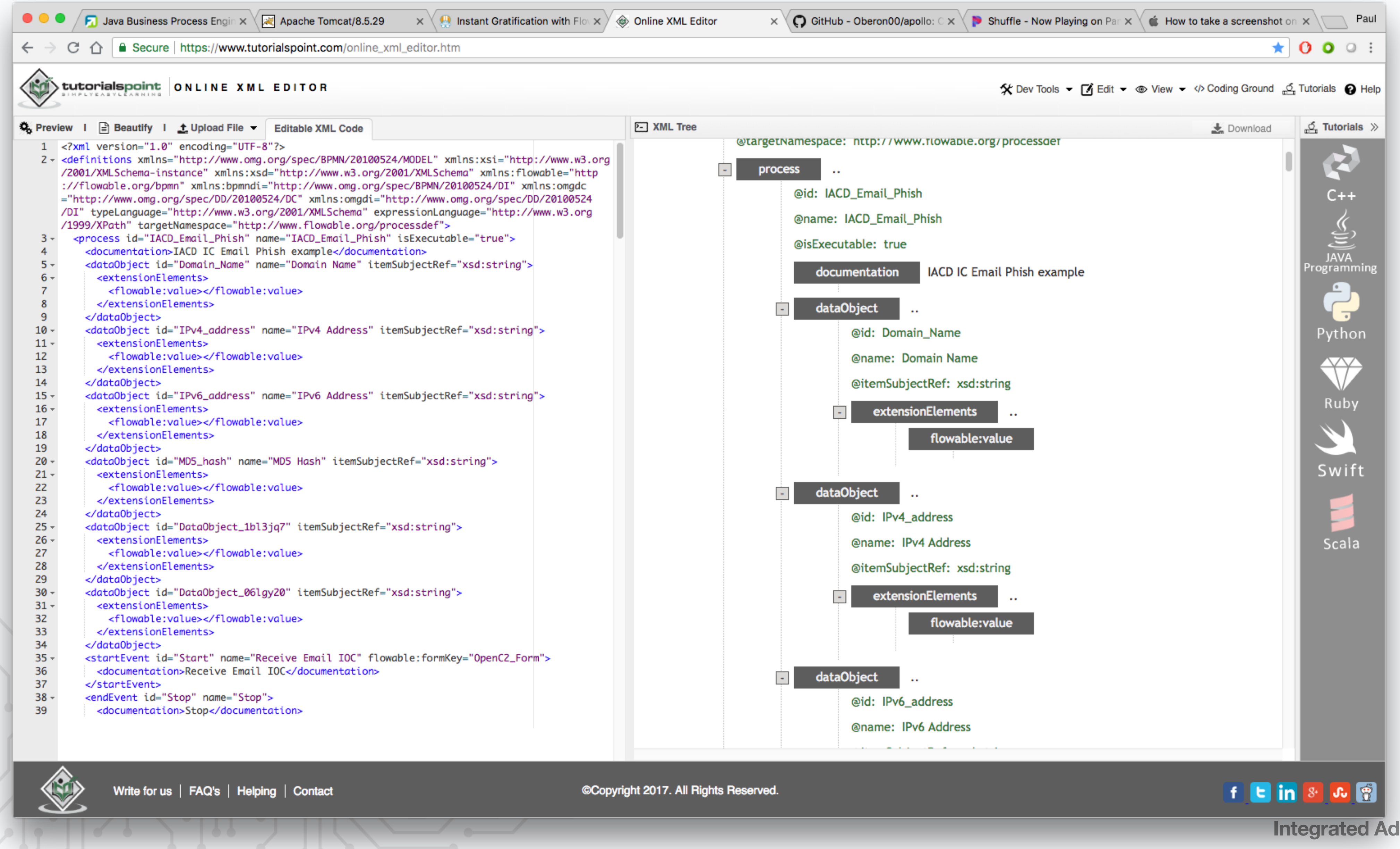
Sharable Workflows – Flow


Existing BPMN Playbooks Templates & Libraries
Export Playbook BPMN XML
Business Process Model Notation (BPMN) Tool
Export Workflow BPMN XML
Workflow BPMN XML
BPMN XML Workflow Import/Adapter
Import Vendor Workflow
Cyber Orchestration Tool

Sharable Workflows – Phishing Email Example


Flowable Modeler
Flowable IDM
Flowable Workflow
Paul
localhost:8080/flowable-modeler/#/editor/0df3fbeb-498d-11e8-944d-acde48001122
flowable
Processes
Case models
Forms
Decision Tables
Apps
Test Administrator
Start Events
Activities
Structural
Gateways
Boundary Events
Intermediate Catching Events
Intermediate Throwing Events
End Events
Swimlanes
Artifacts
Process Navigator
Process: IACD_Email_Phish
No structural elements used.
Receive Email IOC
Create Ticket for IOC
Yes
IOC Whitelisted
No
Update Ticket IOC Ignored due to Whitelist
Yes
IOC Already Whitelisted
No
Update Ticket, IOC already blocked
Conduct Additional Enrichment
Yes
No
Meets Action Criteria
Update Ticket IOC Not Valid
Close Ticket
Stop
Update Blocklist and Block IOC
Query for Recipients
Update Ticket with Affected Accounts and COA
Email Analyst
Analyst enacts mitigations
Analyst Closes Ticket
IACD_Email_Phish

Sharable Workflows – Phishing Email XML


Java Business Process Engir
Apache Tomcat/8.5.29
Instant Gratification with Flo
Online XML Editor
GitHub - Oberon00/apollo: C
Shuffle - Now Playing on Par
How to take a screenshot on
Paul
Secure | https://www.tutorialspoint.com/online_xml_editor.htm
tutorialspoint SIMPLYEASYLEARNING
ONLINE XML EDITOR
Dev Tools
Edit
View
Coding Ground
Tutorials
Help
Preview
Beautify
Upload File
Editable XML Code
XML Tree
Download
Tutorials
C++
JAVA Programming
Python
Ruby
Swift
Scala
Write for us | FAQ's | Helping | Contact
©Copyright 2017. All Rights Reserved.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns="http://www.omg.org/spec/BPMN/20100524/MODEL" xmlns:xsi="http://www.w3.org
/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:flowable="http
://flowable.org/bpmn" xmlns:bpmndi="http://www.omg.org/spec/BPMN/20100524/DI" xmlns:omgdc
="http://www.omg.org/spec/DD/20100524/DC" xmlns:omgdi="http://www.omg.org/spec/DD/20100524
/DI" typeLanguage="http://www.w3.org/2001/XMLSchema" expressionLanguage="http://www.w3.org
/1999/XPath" targetNamespace="http://www.flowable.org/processdef">
  <process id="IACD_Email_Phish" name="IACD_Email_Phish" isExecutable="true">
    <documentation>IACD IC Email Phish example</documentation>
    <dataObject id="Domain_Name" name="Domain Name" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <dataObject id="IPv4_address" name="IPv4 Address" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <dataObject id="IPv6_address" name="IPv6 Address" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <dataObject id="MD5_hash" name="MD5 Hash" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <dataObject id="DataObject_1bl3jq7" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <dataObject id="DataObject_06lgy20" itemSubjectRef="xsd:string">
      <extensionElements>
        <flowable:value></flowable:value>
      </extensionElements>
    </dataObject>
    <startEvent id="Start" name="Receive Email IOC" flowable:formKey="OpenC2_Form">
      <documentation>Receive Email IOC</documentation>
    </startEvent>
    <endEvent id="Stop" name="Stop">
      <documentation>Stop</documentation>
```

```
@targetNamespace: http://www.flowable.org/processdef
process ..
  @id: IACD_Email_Phish
  @name: IACD_Email_Phish
  @isExecutable: true
  documentation   IACD IC Email Phish example
  dataObject ..
    @id: Domain_Name
    @name: Domain Name
    @itemSubjectRef: xsd:string
    extensionElements ..
      flowable:value
  dataObject ..
    @id: IPv4_address
    @name: IPv4 Address
    @itemSubjectRef: xsd:string
    extensionElements ..
      flowable:value
  dataObject ..
    @id: IPv6_address
    @name: IPv6 Address
```

Shareable Workflows– Way Forward

- Template document on Sharable Workflow standard.
  - Model after Oasis OpenC2 format.
- Engage other Orchestration tool vendors to gain feedback and advice on importation of Sharable Workflows into their tools.
  - Vendor community approach to driving the standard.
- Incorporate additional OpenC2 data commands structures to pass to SIEM tools.
- Produce concept of Sharable Workflow repositories for IACD and ISAC community dependent.

Integrated Adaptive Cyber Defense is sponsored by the Department of Homeland Security and the National Security Agency in collaboration with The Johns Hopkins University Applied Physics Laboratory.

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

IACD
Accelerating the Speed and
Scale of Cyber Defense

http:// https://secwww.jhuapl.edu/iacd

@IACD_automate

https://www.linkedin.com/groups/8608114

icd@jhuapl.edu