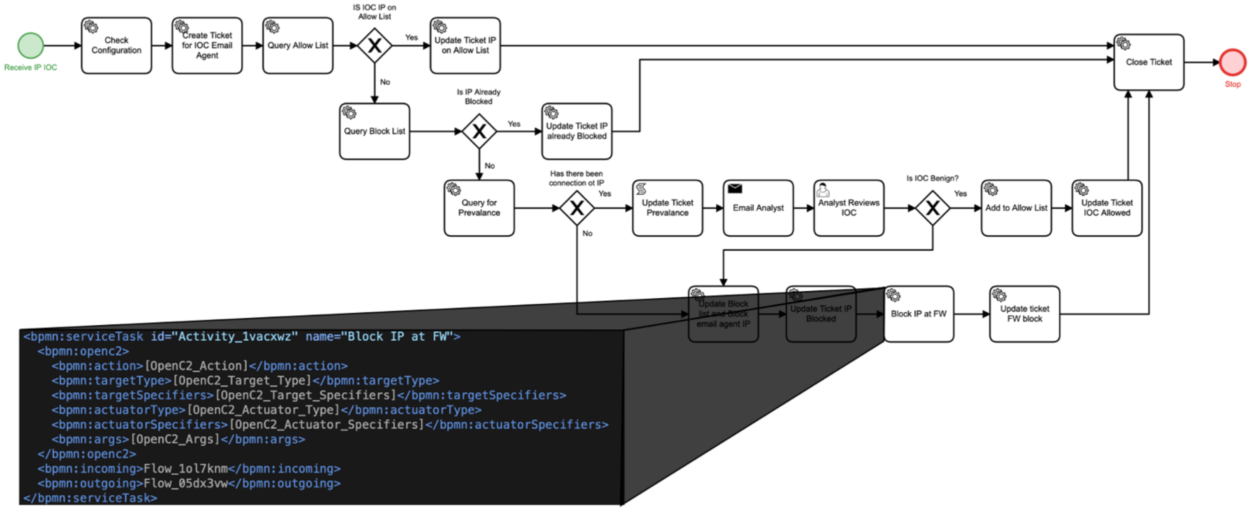
Enriched BPMN Workflows

Cyber defense at speed and scale requires sharing not only the indicators of cyber threats, but also the defensive actions required to respond to those threats. Security Orchestration, Automation, and Response (SOAR) platforms are increasingly being adopted by organizations to respond to attacks with automated, repeatable processes – codifying those defensive courses of action (COAs) within SOAR workflows. Unfortunately, each SOAR product uses its own proprietary format for workflows, which leads to organizations being "locked in" to a particular vendor and making it harder to share workflows of defensive actions with the broader community. The ability to share SOAR workflows in a vendor-neutral, cross-platform manner would enable more effective cyber information sharing and defense.

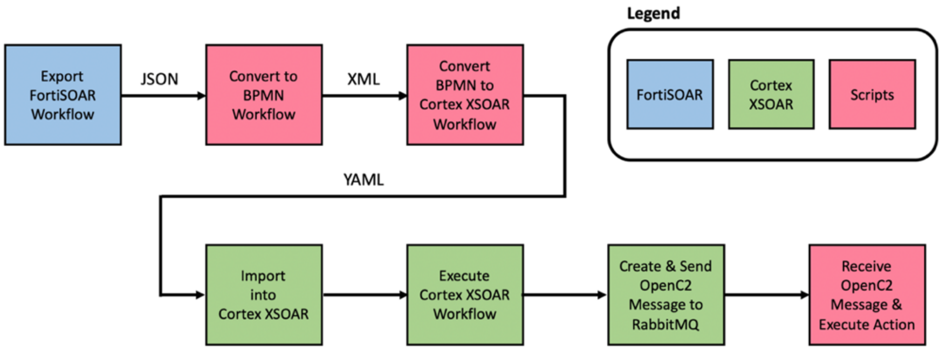
Business Process Model and Notation (BPMN) is a standard for business process modeling maintained by the Object Management Group [1]. BPMN graphically represents sequences of business activities in a standardized manner using a defined set of symbols to facilitate communication and understanding across different process stakeholders. By utilizing an eXtensible Markup Language (XML) base, BPMN is also machine-readable making it directly actionable by a computer. BPMN can be used to describe the structure of a SOAR workflow, but additional enrichment is critical in that it provides the context for the response actions of the security tools orchestrated by SOAR products. To describe the response actions of a workflow, the industry standard OpenC2 (Open Command and Control) is used to enable "machine-to-machine communications for the purposes of command and control of cyber defensive components in a way that is agnostic to products, transport mechanism, and other implementation details" [2]. OpenC2 can be embedded within an enriched BPMN workflow to enable more robust information sharing of cyber defense response actions.

The figure below depicts an example of an enriched BPMN workflow with an embedded OpenC2 command. The SOAR workflow uses the product-agnostic BPMN to describe a set of defensive actions to perform when receiving an IP address Indicator of Compromise (IOC), and the embedded OpenC2 command to describe how to block that IP address at the firewall.



```
<bpmn:serviceTask id="Activity_1vacxwz" name="Block IP at FW">
  <bpmn:openc2>
    <bpmn:action>[OpenC2_Action]</bpmn:action>
    <bpmn:targetType>[OpenC2_Target_Type]</bpmn:targetType>
    <bpmn:targetSpecifiers>[OpenC2_Target_Specifiers]</bpmn:targetSpecifiers>
    <bpmn:actuatorType>[OpenC2_Actuator_Type]</bpmn:actuatorType>
    <bpmn:actuatorSpecifiers>[OpenC2_Actuator_Specifiers]</bpmn:actuatorSpecifiers>
    <bpmn:args>[OpenC2_Args]</bpmn:args>
  </bpmn:openc2>
  <bpmn:incoming>Flow_1ol7knm</bpmn:incoming>
  <bpmn:outgoing>Flow_05dx3vw</bpmn:outgoing>
</bpmn:serviceTask>
```

The Integrated Adaptive Cyber Defense (IACD) initiative demonstrated the utility of a BPMN shareable workflow enriched with OpenC2 commands for sharing across multiple SOAR platforms. IACD conducted experiments with enriched BPMN workflows using two SOAR products: FortiSOAR and Cortex XSOAR. In the first scenario, IACD extracted a workflow from FortiSOAR, converted it to BPMN, and then imported it into Cortex XSOAR, as depicted in the figure below.


Export FortiSOAR Workflow
JSON
Convert to BPMN Workflow
XML
Convert BPMN to Cortex XSOAR Workflow
YAML
Import into Cortex XSOAR
Execute Cortex XSOAR Workflow
Create & Send OpenC2 Message to RabbitMQ
Receive OpenC2 Message & Execute Action
Legend
FortiSOAR
Cortex XSOAR
Scripts

To achieve the conversion of a workflow between the proprietary formats of SOAR products, IACD was required to employ custom scripts in a BPMN Adapter, handling conversions for FortiSOAR-to-BPMN, BPMN-to-Cortex XSOAR, and Cortex XSOAR-to-BPMN. These scripts were also the primary vehicle to embed OpenC2 messages, providing an abstracted, vendor-neutral description of the corresponding response actions. For this experiment, an analyst was required to fill in additional values in the OpenC2 command to provide context for the originating action and then map those actions to the actuators in the second enterprise environment. When the second SOAR platform executed the workflow, OpenC2 messages were sent to a RabbitMQ message broker, and IACD developed an OpenC2 client that subscribed to the messages and performed the appropriate action (e.g., a firewall blocking an IP address).

IACD also implemented a second scenario in which a workflow that included an OpenC2 task was exported from Cortex XSOAR into an enriched BPMN format. When the BPMN enriched workflow was imported back into another instance of Cortex XSOAR, no additional analyst input was required because the OpenC2 task was already defined, and OpenC2 enabled the workflow to be reusable even with different actuators.

These scenarios demonstrated that it is possible to convert workflows from one SOAR to another while using approved standards for both the workflow (BPMN) and the commands issued within the workflow (OpenC2). IACD believes that the community will have to move past scripting requirements in the future and is recommending that the vendor community embrace the export and import of workflows in standardized formats. Also, more research is needed with respect to embedding actuator profiles as well as OpenC2 commands within the workflows so that a SOAR platform could alleviate the burden on the operators for the configuration of shareable workflows once imported within the platform.

For more information on BPMN shareable workflows, SOAR technologies, and other experiments, please visit https://www.iacdautomate.org. For examples of BPMN workflows, please visit https://www.iacdautomate.org/playbook-and-workflow-examples.

References

[1] Object Management Group. (2020). Object Management Group Business Process Model and Notation. Retrieved from: http://www.bpmn.org/

[2] OASIS Open Command and Control (OpenC2) TC. (2019, November 24). Open Command and Control (OpenC2) Language Specification Version 1.0. (J. Romano, & D. Sparrell, Editors). Retrieved from OASIS: https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs02/oc2ls-v1.0-cs02.html