Shareable Workflows Quick Information Guide

What is a shareable workflow?

Security orchestration, automation, and response (SOAR) platforms provide connectivity to, and orchestrate activities between, enterprise security tools and network devices. This allows for increased speed of resolution when resolving indicators of compromise (IOCs) as well as managing of an organization's IT environment. The SOAR platform operates by running documented processes known as workflows that allow for consistent and repeatable application of an organization's policy and procedures in response to a trigger. Often times, these workflows are proprietary to a specific vendor's SOAR platform, which limits sharing between organizations and often time leads to vendor lock-in.

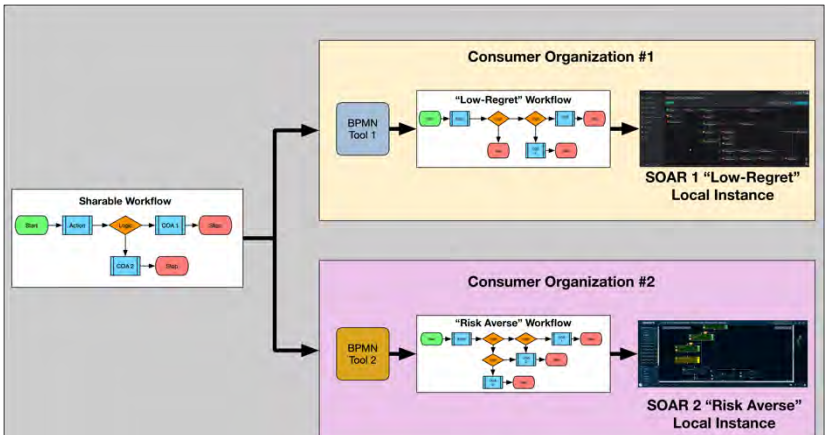

Figure 1 Sharable Workflow concept

Shareable workflows are a technique for members of a community to share the process that they wish to automate in a platform-agnostic way so that it can be tailored to their own needs, risk profiles and business logic. Sharable workflows are developed utilizing open source tools that are standards based so that companies can easily and readily share their best practices with other members within a community of trust to speed up the collective cyber defense efforts. Workflows are high-level documentation of technical steps that an organization's IT components and devices carry out in response to triggering conditions, primarily focused on machine interactions.

The sharable workflow is enabled through the use of the Business Process Model and Notation (BPMN) standard when developing workflows to provide consistent, easily understandable graphical representations of a workflow. These graphical representations aid in the analysis and improvement of business processes. BPMN is an open standard, and many available open-source BPMN editors/tools exist. Figure 1 demonstrates how two organizations can utilize BPMN to tailor a shareable workflow and import that tailored workflow into their own SOAR local instance.

For more information on shareable workflows, please visit the IACD website, or view the IACD video on the concept via the IACD YouTube channel.

© 2019 The Johns Hopkins University Applied Physics Laboratory LLC.
This document is made available under the Creative Commons Attribution 4.0 International License.

How to create a shareable workflow

The following steps are provided as a preliminary guide to the process of creating shareable workflows.

Step 1: Create a high-level cyber defense sharable workflow by using a BPMN editor tool (e.g. Flowable and Camunda)

Step 1a: Download a workflow from a certified sharable workflow repository

Step 1b: Create a new sharable workflow based on the downloaded workflow

Step 2: Choose proper organization's corporate business and security policies for cyber defense

Step 3: Use as is or customize the sharable workflow based on the selected policies to fit the specific organization's conditions within the BPMN tool

Step 3a: Add, remove, and modify tasks within the sharable workflow to fit specific business conditions
Step 3b: Export the updated sharable workflow from a BPMN tool to an external file (BPMN XML format)

Step 4: Input the customized sharable workflow into a SOAR platform (e.g. Cybersponse, Demisto)

Step 5a: Convert the workflow data format into a SOAR recognizable format (e.g. JSON or YAML)

Step 5: Corporate cyber analysts use the imported workflow tasks and connect them into lower level IT local instances of the workflow (e.g. firewall, email server, etc.)

Step 6: Execute the workflow with the SOAR platform controlling the local instances of the cyber infrastructure (e.g. Firewalls)

Step 7: Verify that the proper cyber defense course of actions are deployed

Please feel free to contact the IACD team with any questions at icd@iacdautomate.org

© 2019 The Johns Hopkins University Applied Physics Laboratory LLC.
This document is made available under the Creative Commons Attribution 4.0 International License.