Cybersecurity Automation and Threat Intelligence Sharing Best Practices

April 2021

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

CYBERSECURITY ORCHESTRATION

Orchestration of Information Technology (IT) Automation Frameworks

Kimberly K. Watson

The Security Orchestration, Automation, and Response (SOAR) market has matured considerably over the last few years, but many organizations still have a hard time differentiating between SOAR and IT automation frameworks. Those with investments in IT automation often question the need for extending SOAR deployments outside of the Security Operations Center (SOC), while others wonder how to effectively combine the two technologies to mitigate cyber risks. Some organizations may worry about SOC updates changing IT assets, but as explained in this paper, using approved frameworks can ensure any changes align with existing priorities and policies. At the heart of both of these scenarios is the question "What does it mean to orchestrate IT automation frameworks?" Figure 1 provides a visualization of these relationships.

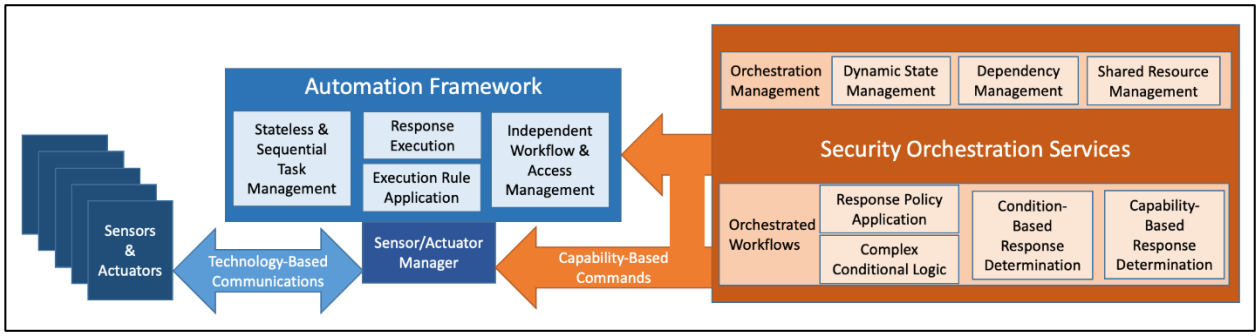

Figure 1 Security Orchestration Services Supporting Automation Frameworks

Key Differences

The best way to explain what it takes to orchestrate automation frameworks is to characterize the key differences in functionality between the two capabilities. These differences fall into two general categories: management functions and workflow characteristics.

Management Functions

Orchestration products and services usually implement a more complex set of management functions than traditional automation frameworks. This is because the *coordination* required to automate complex dynamic processes is considerably more

than what is required to schedule, deconflict, and automate sequential tasks. The following are primary areas in management functionality that distinguish security orchestration services from IT automation frameworks:

- **State**: Most IT automation frameworks are stateless while one of the primary functions of orchestration is to manage dynamic state information within and between workflows.
- **Dependencies**: While IT automation does support parallel task execution, these paths are usually independent of each other. SOAR, on the other hand, is designed to manage dependencies between workflows, decision logic, states, and resources.
- **Resource Management**: IT automation frameworks manage access to resources as required to execute tasks. Orchestration services manage not only access to, but also the sharing of, resources within and across workflows.

Making the above security orchestration functionality a native part of IT automation frameworks would require adding significant complexity to the existing products and services. For this reason, organizations will need to invest in orchestration capabilities to automate operational processes that include decision logic based on dynamic variables or state information that may be shared between workflows. This is true even if they currently use an IT automation framework.

Workflow Characteristics

Both SOAR and IT automation products and services have automated workflows at the core of their capability. They both provide the ability to develop, approve, and deploy workflows. There are minor differences in both workflow execution and workflow management, with security orchestration tending to provide more robust capabilities to version, validate, instrument, and monitor workflows. The major differences have more to do with workflow purpose and complexity. The following areas are key discriminators between the two technologies:

- **Response**: Security orchestration workflows represent the logic used by an analyst to determine the appropriate response. In contrast, IT automation workflows generally represent the series of tasks that need to be executed to implement a selected response action.
- **Policy**: SOAR workflows implement operational policies for responding to a security-related condition while IT automation workflows implement rules to enforce execution policies.
- **Decision Logic**: All security orchestrators support complex conditional logic in their workflows. IT automation workflows sequentially chain together tasks that must be completed in order to accomplish a particular job.

IT automation frameworks may find it productive to expand their capabilities to provide workflows with characteristics more indicative of SOAR products and services in order to provide the same level of features for IT operations.

Orchestrating IT Automation Frameworks

IT automation frameworks enable organizations to more efficiently and effectively manage IT assets. SOAR products and services enable organizations to more efficiently and effectively implement local security procedures to defend against cyber-related threats. Because cyber threats compromise organizational assets, there is value in leveraging both SOAR and IT automation to mitigate cyber risk. This can be done by using security orchestration to manage the dependencies, complexities, and dynamic decision making related to response investigation and selection, while relying on existing IT automation workflows to execute the responses. By using the approved IT automation frameworks and existing authorized workflows, the responses are aligned with local priorities and subject to applicable execution policies. This helps alleviate certain concerns organizations have about security operations making changes to IT assets.

Conclusion

Enabling automation is a critical component of every organization that wishes to address the speed and scale of modern cyber attack. This is true for all security-related processes regardless of whether they are the domain of IT administrators or the SOC. There are differences between security orchestration products and IT automation frameworks that make them optimal for the types of processes they automate. As organizations invest in SOAR, or some other form of security orchestration capability, they need to develop orchestrated workflows that leverage existing automation frameworks, particularly those used for IT asset management. Combining the functionality of these different technologies can result in more timely and comprehensive mitigation of cyber risks.

Acknowledgement

This material is based upon work supported by the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency under Grant Award Number DHS-19-CISA-128-SLT-001 (State, Local, Tribal, and Territorial Indicators of Compromise Automation Pilot).

Disclaimer

The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

✉ Kimberly Watson
Kimberly.Watson@jhuapl.edu