Cybersecurity Automation and Threat Intelligence Sharing Best Practices

April 2021

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

CYBERSECURITY ORCHESTRATION

Information-Centric Automation and Orchestration

Kimberly K. Watson

As organizations develop workflows in Security Orchestration, Automation, and Response (SOAR) products, they often include data normalization routines for each resource they access. They may also design the workflows to handle the creation and storage of accessible information about state, interim results, and cross-references for other organizational capabilities to use. The problem with performing these normalization, standardization, and information management functions with SOAR is that whenever a resource is added or upgraded, or a new capability deployed, they have to modify all associated workflows. It is worth considering an Information-Focused Automation Framework (Figure 1) to handle these functions allowing your automation to be source- and capability-agnostic.

An Information-Focused Automation Framework keeps your automation information-centric, allowing you to change sources without having to redesign workflows and analytics

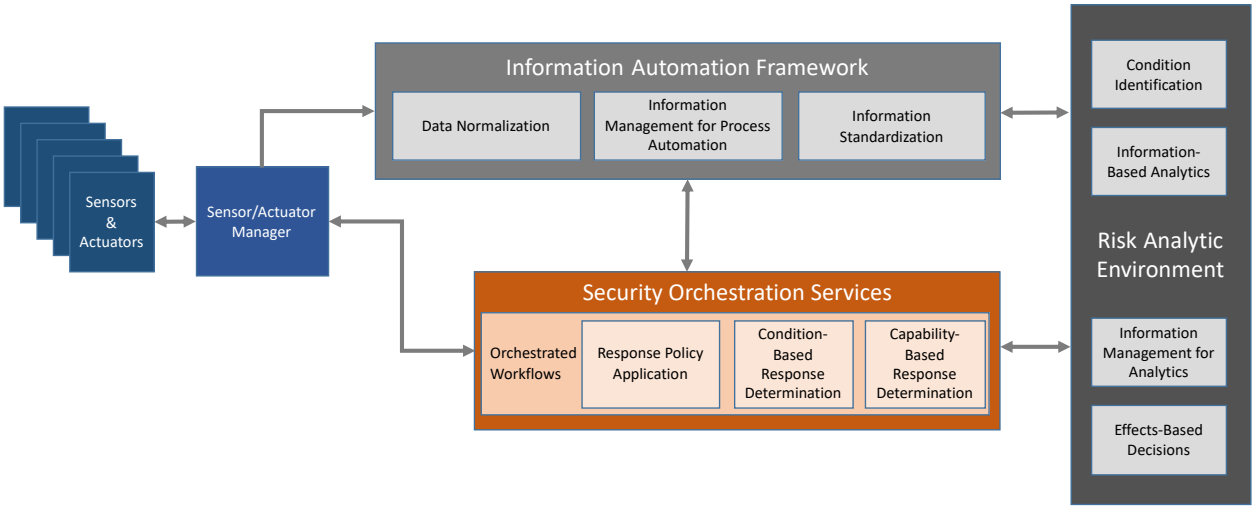

Figure 1 Information-Focused Automation Framework and Security Orchestration

Many products designed to perform advanced analytics or automate analysis of cyber threat information separate the data normalization and information standardization functions from the automated workflows and analytics engines. This way they are working on information in a specific, defined, and understood context, allowing them to

add, modify, and delete sources and analytics without impacting existing core functionality. In essence, they have deployed an Information-Focused Automation Framework for the organization.

As organizations mature their analytic environments, security orchestration, or automation capabilities, they should consider including functionality that allows them to perform information-centric instead of product-centric operations. This enables organizations to orchestrate automated capabilities via SOAR instead of orchestrating integrated products.

Information-Focused Automation Framework Functionality

The intent of deploying this type of framework is to enable information-centric automation. Information-centric automation emphasizes developing workflows and analytics based on standardized pieces of information made accessible by local resources instead of inconsistent data provided by products and services. This framework provides information management functionality that is explicitly designed to enable automation.[1]

Relationship to Risk-Analytic Environment

Most organizations currently invest in a security-analytic product or service. More resourced or mature organizations have started investing in security-analytic environments, using advanced analytics to try to identify, prioritize, or recommend mitigations for cyber threats. The expectation is that these environments will continue to advance, resulting in risk-analytic environments where model-based analytics will help to identify, quantify, and mitigate cyber risk.

The success of such investments is directly related to the existence of the functionality provided by the Information-Focused Automation Framework. The risk analytics will be too complicated to redesign every time a new data or information source is made available. There will also be a desire to add and upgrade analytics into the environment without having to assess and modify or redefine information collected, normalized, and stored by the organization.

The three primary functions provided by the framework to support the analytic environment are as follows:

- **Information Standardization**. The framework needs to define key information elements for use by any automated workflow or analytic. This means that the

[1] Watson, K., “Enabling Automation in Security Operations: Increasing Automation Potential of Processes”, March 2021.

representation of the information element must be consistent, unambiguous, and machine-readable.

- **Normalization**. The framework needs to provide a way for data accessed, generated, or used by the organization to be normalized and turned into the appropriate information elements without modifying the content.
- **Information Management for Automation**. There are certain information management practices that are required strictly to support the automation of processes. These include:
    - Consistent location, application, and mechanisms for cross-referencing different identifiers for the same or associated pieces of information.
    - Consistent (in format and existence of) historical data and metadata (e.g., timestamps) to support conditional logic, decision making, and measurements.

Information-Centric Operations and Security Orchestration Services

Current SOAR workflows tend to include rule and algorithm based decision logic to identify, prioritize, or respond to cyber threats. These types of logic work for basic response actions, but start to fail quickly when those actions need to be tailored based on attributes of the asset affected or the risk being mitigated. As analytic environments become more pervasive and reliable, security orchestration will need to evolve to be about determining what it takes to implement a particular response type or effect in the operational environment using existing technologies.

Conclusion

Enabling automation is a critical component of every organization that wishes to address the speed and scale of modern cyber attack. As automation and orchestration continues to evolve and organizations begin extensive investments in analytic environments, a shift to information-centric operations from product-centric integrations will become critical. This type of shift requires some sort of Information-Focused Automation Framework, which enables new and improved data sources and analytics to be rapidly integrated into the operational environment without having to redesign existing automated workflows.[2]

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

[2] Elder, Matthew. “Effects Based Courses of Action.” Integrated Adaptive Cyber Defense, IACD, 2020, www.iacdautomate.org/s/Assessing-Cyber-Threat-Intelligence-Feeds.pdf.

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