Cybersecurity Automation and Threat Intelligence Sharing Best Practices

April 2021

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

ENABLING AUTOMATION IN SECURITY OPERATIONS

Strategy for Efficient Process Automation

Kimberly K. Watson

The single most valuable piece of advice for organizations automating security processes is: Do NOT automate your existing process. Manual processes are optimized for a very limited resource whose specialty is inference and decision making – your analysts. Automated processes should be designed to leverage what automation does well, which is consistent, rapid, and repetitive execution of conditional logic. This makes automation perfect for implementing triage and prioritization tasks, allowing analysts to quickly focus on the information and events that are associated with the most risk. Figure 1 provides an overview of how to effectively utilize automation for security operations.

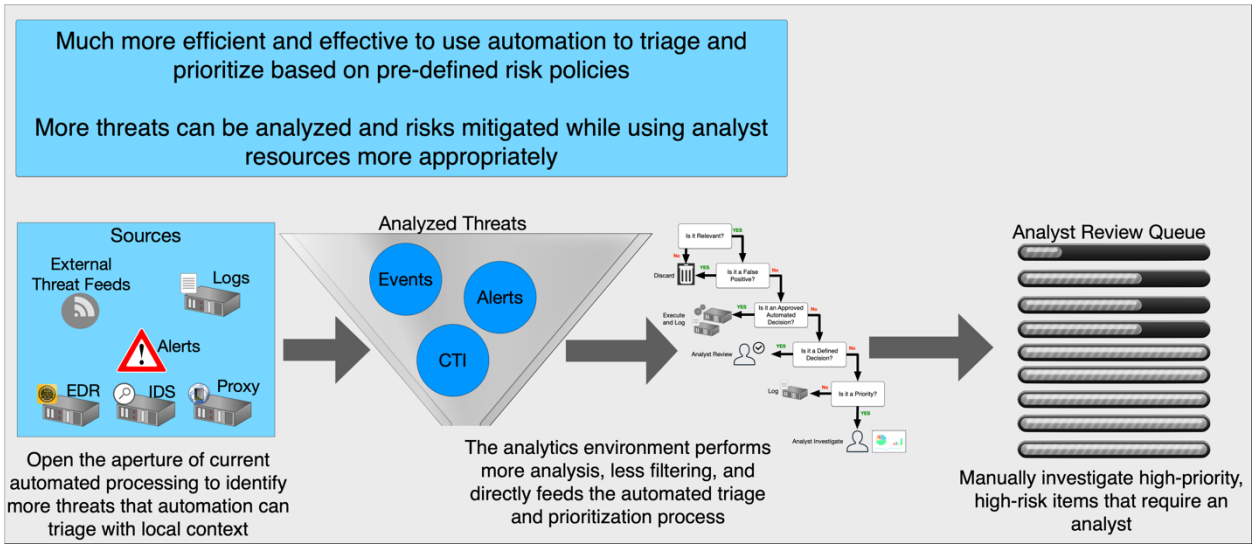

Figure 1 Effective Use of Automation in Security Operations

The Basic Approach

The idea is to identify the conditions that will allow security operations to handle the alert, event, or externally provided Cyber Threat Intelligence (CTI)[1] in an automated manner according to local risk policies. This may mean discarding the item, executing automated response actions, or making an automated recommendation for an analyst to review. The key is to identify as many items as possible, as quickly as possible that do not require analyst investigation.

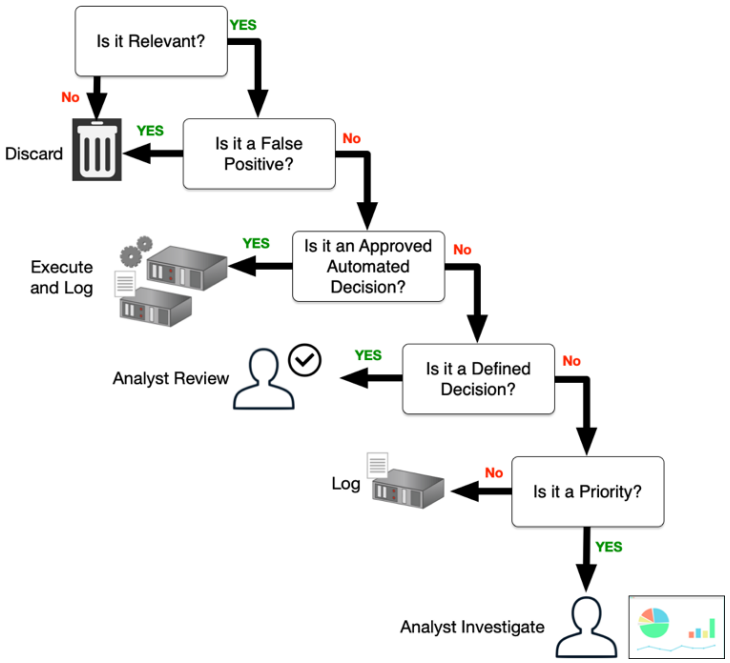

Figure 2 Automated Triage and Prioritization

What piece of information is necessary to determine that something is not relevant or is a false positive? Automating the logic that your analysts repeatedly use to make these determinations saves both time and resources. Examples include an Indicator of Compromise (IOC) that is already on the block list implemented by your security vendor, or an alert from your Intrusion Detection System (IDS) that a Windows exploit was attempted against a Linux asset.

Under what conditions has your organization defined and approved a fully automated response? For many active threats, the operational value[2] of responding is directly related to how fast you detect and respond. Being able to process more alerts, events, or CTI, and quickly identify when conditions are met for authorized automated responses, is a critical step in defending against those threats. Examples include blocking IOCs derived from IDS alerts that meet low-regret criteria[3,4] or adding a file hash to application block lists when a reliable source flags it as malware.

Under what conditions are other responses authorized, even if not automated? Automation can efficiently build enriched tickets for analyst review or approval. The

[1] In an effort to stay technology and implementation agnostic, “item” will be used to represent any combination of alert, event, and/or external CTI that is flagged for analysis or response.
[2] Watson, K “Deploying Indicators of Compromise for Network Defense.” February 2021
[3] Frick, C. “Applying Low-Regret methodology for cyber threat intelligence triage.” April 2021.
[4] Frick, C. “Applying Low-Regret methodology for response to indicators.” April 2021

ticket can contain preapproved recommendations, the information used to make the recommendations, and even the code to execute the response if selected. Examples include quarantining a compromised device or resetting an administrator credential. Previous experience has shown that using automation to recommend a response for analyst review and approval has resulted in gains in operational efficiencies, despite not being fully automated. Over time, you can identify conditions that can result in a fully automated response.

What characteristics make this either a high or low priority item for your organization? Examples include using the severity rating associated with a signature or the criticality level of the asset. Automating the logic used by your analysts to make these determinations saves time and resources. Most of your current sensor configurations and filters, as well as operational analytics, are designed to identify high-priority alerts or events. Automating your process to implement this logic at the end instead of the beginning enables your organization to handle more alerts and events and focus your analysts on investigating and mitigating the highest risk items.

Primary, Authoritative, and Corroborative Information

Often the source of the information determines if the response is authorized to be fully automated or requires analyst approval. Many conditions, characteristics, or attributes used to make the response decision are not uniformly available from a single reliable source. It is very valuable to identify primary sources of information, which are sources that consistently have the same information available for all objects of a certain type, even if that information is not always accurate to the desired level. Often your analysts have already figured out what other pieces of information (e.g., corroborative information) in your environment can be used to determine when this source is accurate enough for a particular response decision.

Most organizations have identified authoritative sources of information that are required to make response decisions, but have not considered when it may be more appropriate or reasonable to use a primary source instead. Authoritative sources rarely contain timely insight for all objects because of the extra resources required to make the more accurate determinations. Waiting until the source can obtain the insight into a particular object may delay the timeliness of the response, impacting the effectiveness. It is recommended to consider what response decisions can rely on primary and corroborative sources instead of always requiring limited or inconsistent authoritative information.

An example of these types of sources for a given attribute is using a software management server as the primary source, an endpoint agent as a corroborative

source, and the output of a credentialed vulnerability scanner as an authoritative source for identifying assets vulnerable to a particular exploit.

Certain software application versions or patches may be clearly linked to certain vulnerabilities, allowing the software management server information to be more than appropriate for some decisions (e.g., a device running Red Hat is not vulnerable to an exploit against Windows Server). Sometimes the details about whether a vulnerable library is present on a device with a particular application installed may be available from an endpoint management server. Sometimes the only way to determine if an asset is vulnerable is from a credentialed scan.

Thinking about primary, corroborative, and authoritative information sources allows an organization to more efficiently automate triage and prioritization decisions in alignment with local policies.

Conclusion

Enabling automation is a critical component of every organization that wishes to address the speed and scale of modern cyber attacks. This is why most organizations are investing in automation of their security operations. When developing automated workflows, it is important to remember that manual processes are optimized for analysts. Redesign the process to leverage automation to perform triage and prioritization, allowing more alerts/events to be processed with less analyst engagement. The basic approach identified in this guide will help an organization develop and deploy automation that is more efficient and effective for their operations. This approach is easily extended to support the inclusion of more advanced analytics into the detection and response process.

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