ENABLING AUTOMATION IN SECURITY OPERATIONS

Assessing Automation Potential of Products and Services

Kimberly K. Watson

As organizations automate operational security processes, they are discovering that not all products and services support these initiatives. The main issue is that the functionality and information available via the Application Programming Interface (API) may be different than what they have access to via the user interface. It is important to assess products and services, those already deployed as well as those under consideration, to determine if they have limited automation potential. This assessment requires more detail than just making sure there is an API, and is not easily discernable from a typical vendor demonstration.

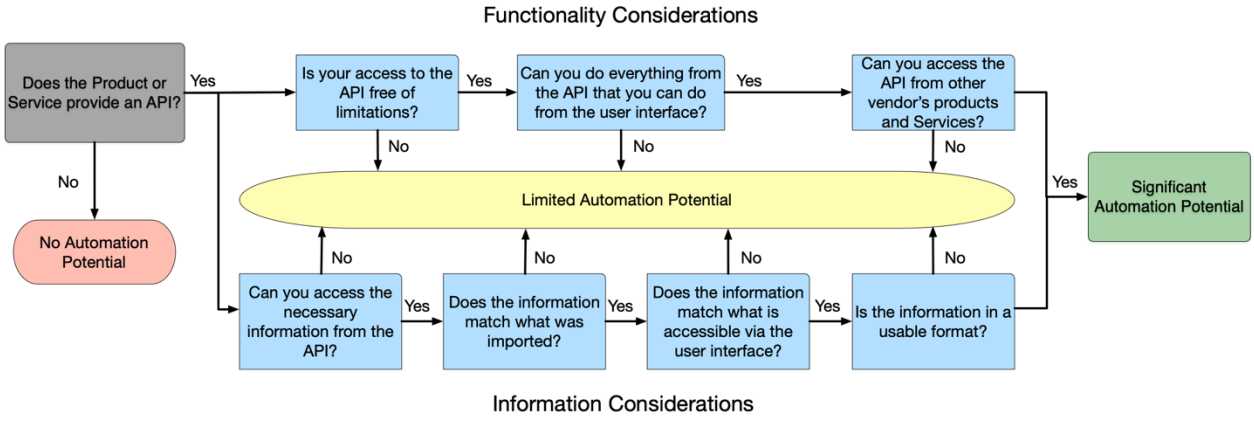

Figure 1 Flowchart for Assessing Automation Potential

The flowchart in Figure 1 walks through a set of questions that will identify the most common issues with products and services that organizations encounter when automating operational processes. When evaluating a product's ability to support automation, it is critical to assess the availability of the API, the functionality of the tool from the API, and how information is presented through the API as opposed to the tool's general user interface.

API Availability

First and foremost, the product or service must have an API that is intended for use at scale by the customer organization. Prior to the emergence of the Security

Orchestration, Automation, and Response (SOAR) market, not all products provided their customers with direct API access. The expectation was that users would interact with a dashboard or console, and that the application would internally handle all API requests. When organizations begin receiving thousands of alerts from dozens of products, this approach is no longer plausible to enable survivable network defense. Most products now expect and support some level of automation from customer organizations, but this initial design principle of users manually interacting with the application via the provided graphical interface has resulted in varying degrees of automation support.

Many products now have two distinct APIs available, one designed for interaction with typical users and one designed for the support organization to manage the capability and associated information. In this paper, the former will be referred to as the frontend API and the latter the backend API.

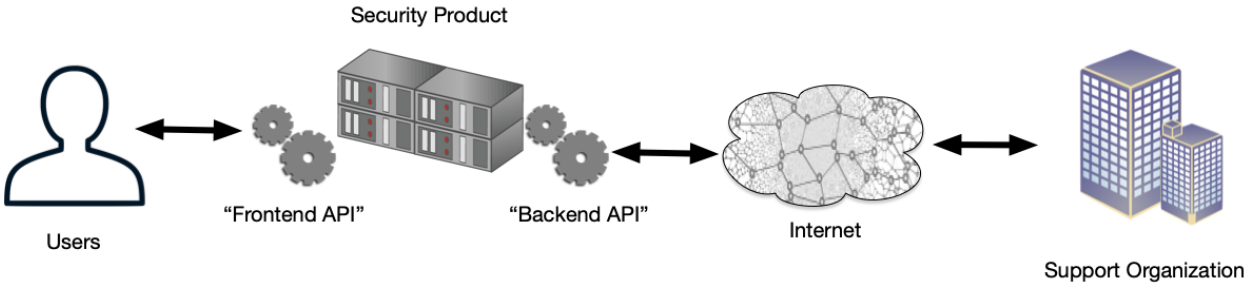

Figure 2 "Front End" and "Back End" APIs

This distinction is important because the different APIs often expose different types of information and functionality, and as such, they can be subject to different licensing restrictions. These differences in capability and access options may impact automation of conditional or complex operational processes, requiring some combination of calls to both the frontend and backend APIs to implement.

A similar situation may occur when comparing on-premises tools to a cloud-based offering. Many vendors remove, constrain, or modify API access policies and functionality when migrating to the cloud. If an organization is reliant upon the API access, this must be evaluated when considering a vendor's offer to migrate to a cloud-based version of the tool.

Functionality Considerations

As organizations automate operational security processes, they encounter a common set of issues related to the functionality exposed by APIs. The following considerations are intended to help organizations assess products and services to ensure they enable automation as appropriate.

Unconstrained

It is important that the product or service provides API access at a scale that supports automated processing. The first issues usually encountered when automating manual processes are licensing constraints. Frontend API keys, which are used to access these APIs in an authorized manner, may not be included in initial licensing agreements. Likewise, there are many services that are free when manually accessed by an analyst, but require a for-fee upgrade to support automated access. Even when an organization has paid for API access, it is often associated with a maximum number of requests or a limited set of services that are based on current manual operations. In all these cases, access to the available API is constrained in some manner that impacts the organization's opportunity to employ desired automation.

Comprehensive

Every function that can be performed by an analyst in the application needs to be available via the API. The next issue that organizations encounter when automating manual processes is that the API only exposes a subset of the functionality that the analysts use in operations. Even when a set of functions are available via the API, there may be differences between the application supported capability that uses those functions and what can be automated. This is because the application may implement proprietary methods for advanced functionality that cannot be implemented by chaining together available API calls. Any action or task that an analyst performs during operations that cannot be consistently and accurately implemented through API calls limits the efficiencies that can be gained via automation.

Externally-Accessible

Every function that can be automated needs to be exposed by the API to sources external to the application. Certain vendor packages or application suites have APIs that only their official products can access or that can only be called using information generated internal to the suite. Operational processes can receive the same core pieces of information from multiple sources both internal and external to their organization. The same automated process should be able to perform the same operation on the same type of information, regardless of the source of the information. If different automated processes need to be developed for different sources or different capabilities need to be deployed to access the same information via different APIs, then the effectiveness of automated operations will be limited.

Information Considerations

As organizations automate operational security processes, they also encounter a common set of issues related to the information exposed by APIs. The following considerations are intended to help organizations assess products and services to ensure they support automation as appropriate.

Accessible

The information that is made available to analysts using the application must be available via an appropriate API. Many products restrict what can be exported or returned using an API call, making certain pieces of information only available internal to the application. There is often a difference in what information is available via the frontend API as opposed to the backend API, and accessibility to each API is limited according to legal or service agreements and security policy. Products and services that generate or provide information used by operations personnel must provide API access to that information or opportunities for automation are significantly impacted.

Consistent

Any product that imports information used in operational processes needs to make that same information available in a consistent fashion via an API. Many products and services offer comparable information (e.g., severity score, prioritization) but that piece of information can mean very different things. Even if they have the same meaning, how that information is derived can be very different. Sometimes certain data fields are deleted or modified during the import process. This results in inconsistent information being exported via the backend API. While a person can use context to infer the meaning of a piece of information, automation usually cannot.

Expected

The information accessible via the API must match the information provided to the analyst using the application. Graphical user interfaces are designed for people to look at and are visually optimized to support inferencing. They support analysts customizing visible fields, labels, and the display order of results. APIs are designed for responding to requests and optimized for processing considerations using a very specific structure. This leads to a situation where the information as requested and seen in the application may vary from the information returned via the API. The ability to automate manual processes is directly tied to the ability to reproduce analyst derived information via the API.

Consumable

The information exposed via the API has to be provided in a format that can be used by other products and services in an automated manner. In certain instances, custom code has to be developed and maintained to parse, translate, normalize, or reformat information received from an API call before it can be used in operational processes. The more processing that has to be performed, the more the efficiency of automated processes may be impacted. This impact may become more critical as the usage of automation is scaled up by an organization.

Conclusion

Enabling automation is a critical component of every organization that wishes to address the speed and scale of modern cyber attack. Without orchestrated automated response via security tools, it is often not possible to respond to cyber threat intelligence in a timeframe that enables network defense. However, organizations often find themselves struggling to understand which of their security tools can leverage these capabilities. Merely having an API to a product is not enough. The factors identified in this guide will help each organization assess whether or not their tools can leverage the significant benefits of automated responses and identify features that they can request from their vendors to support their operational needs to assure business continuity while under cyber attack.

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