Security Automation and Orchestration to Make Data Actionable

There is a belief among some security professionals that the process of searching for Indicators of Compromise (IOCs) is not worth an analyst's time when trying to defend modern enterprises from Advanced Persistent Threats [Asher]. Security professionals are inundated with data: log data, security product alerts, IOCs, vulnerability reports, other forms of cyber threat intelligence, and on and on. The vast majority of this data is not used, for a variety of well-documented reasons (timeliness, applicability or lack thereof, sheer volume). The reality is that it takes too much time and too many resources to turn this flood of data into information that can be acted upon. If this data was more actionable from the beginning, it could and would be used by network defenders. So what does it take to make data actionable? In particular, what makes it such that these defenders can reduce the volume to identify applicable information upon which they can take appropriate actions in cyber-relevant time?

IOCs are a perfect case study to identify what it takes to make data relevant and actionable for network defense. The time spent to manually review, distribute, and determine whether or not to block an IOC often takes longer than the time that the IOC is active. For this intelligence to be usable by a network defender, a dramatically faster process is needed. Because the decision to block an IOC is a risk decision based on organizational policies and risk tolerance, speeding up this process is less about doing the same steps faster, and more about providing the insight necessary to adapt and even "short-cut" the process under acceptable conditions.

The Integrated Adaptive Cyber Defense (IACD) initiative recently completed a pilot demonstrating that it is possible to define a process that optimizes time to mitigation by utilizing Security Automation and Orchestration (SAO) technologies. By combining SAO within the IOC generation and evaluation process with a "low-regret" [Watson] strategy of automatically blocking suspicious IOCs that have no prevalence on the enterprise network, the IACD initiative achieved dramatic improvement in the time required to take action on an IOC as represented in Figure 1. During pilots conducted by the IACD initiative SAO was seen to reduce the median time for the process of creating an IOC for distribution to blocking said IOC down from 14 hours to approximately 9.5 minutes.

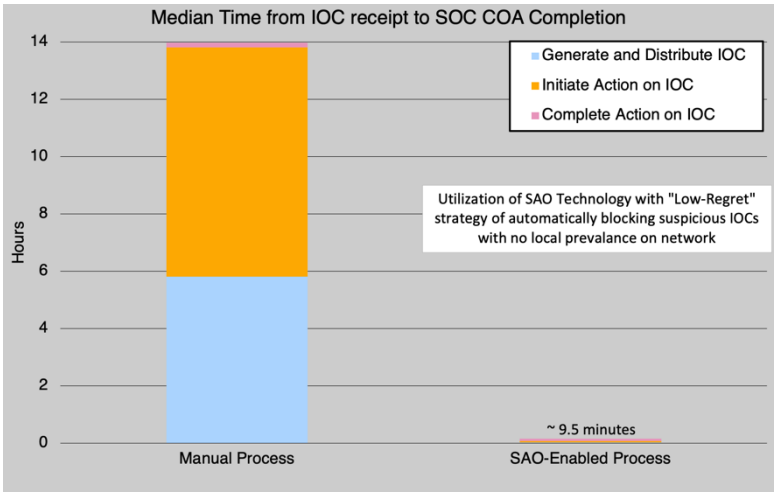

Figure 1: Time to generate and process IOCs

Many organizations have access to one or more automated feeds of IOCs, for example through an Information Sharing and Analysis Center (ISAC) or Threat Intelligence Platform (TIP). As stated earlier, IOCs from these automated feeds are often not incorporated into those organizations' defenses. For those organizations, that data is not actionable: processes do not exist to make decisions based on the information provided and then take appropriate actions within security operations and products.

For cyber threat intelligence to be actionable, it must be generated in a manner that makes it easily understandable, usable, and consumable by the receiving organization in an automated manner. In general, actionable information will possess a number of key characteristics:

- The content must be indicative of an attack phase, activity, or technique.
- The content must be specific and granular such that any response actions and have very low probability of unintended side effects.
- The context must enable evaluation and adaptation to the consumer's environment, to include their policies and risk tolerance.
- The data must be contextualized, shared, and then processed in a timely fashion (which varies depending on the type of indicator being shared).
- There must be confidence and trust in the source, provenance, and integrity of the data at a level commensurate with acceptable risk to business operations.
- It must be possible to ingest and correlate the data with information from the local enterprise environment in an automated manner.

SAO technology can assist with some of these characteristics to make cyber threat intelligence actionable. An example of this process compared to a more traditional manual one is provided in Figure 2.

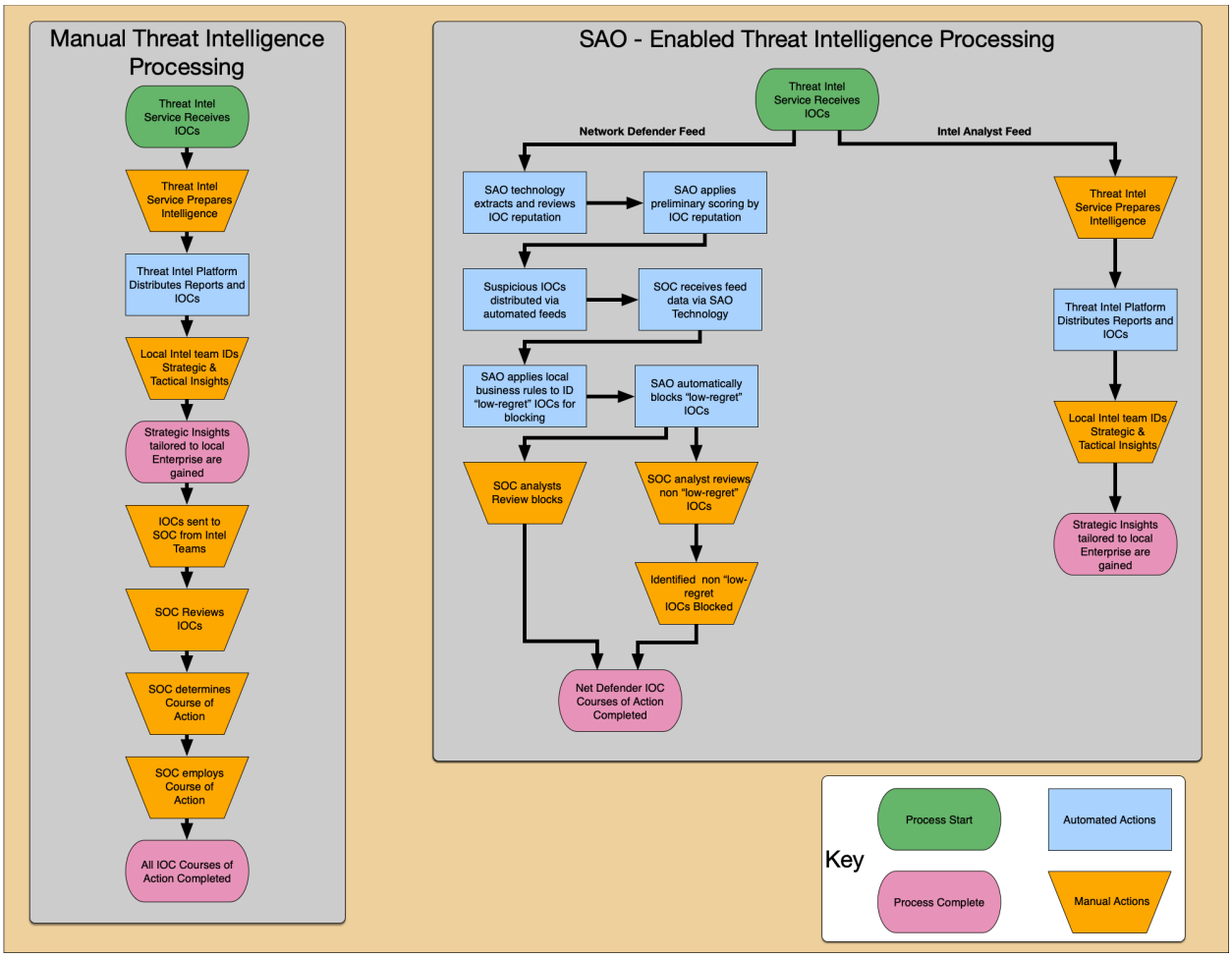

Figure 2: Manual versus SAO-Enabled IOC Processing

In particular, security orchestrators provide a mechanism for processing data in an automated and timely fashion based upon rules and workflows that are defined by the organization. Security orchestrators can connect the server that receives the data (e.g., a TAXII server) with the rest of an organization's security infrastructure to enable correlation (via a Security Information and Event Management server), provide additional context (via cyber threat intelligence sources), and/or effect appropriate responses (via other security products such as firewalls or endpoint security). ***Security orchestrators can do more than just integrate products and services to automate manual tasks – they also implement a manageable, auditable, and reliable decision-making process that will consistently apply mitigations in accordance with local risk policies.***

Conceptually, SAO technology provides the ability to make IOCs actionable by viewing automation and information sharing as a combined ecosystem. Through its pilot development efforts, IACD has demonstrated techniques for making IOCs actionable in the necessary timeframe and format needed by network defenders.

Security orchestrators can process IOCs from a threat feed to automate a number of actions. What action depends on a number of factors such as applicability of the information, confidence in the source, or severity of the risk. One important question that an organization wants to answer when ingesting an IOC is “has this IOC been seen in my environment?” If the particular IOC has not previously been seen, then a “low-regret” action that can be implemented using SAO technology would be to block that IOC using existing security defenses. For example, if a particular IP address is identified as malicious and it has never been seen in firewall logs, incoming or outgoing, then there is very little reason not to block that IP address going forward. Even if the IOC is not confirmed malicious or you are not confident in the source, you can take this action with little risk of impact to operations, hence the term low regret. This decision process involves the orchestration of multiple security products, first to check for the presence of the IOC, then to implement the blocking action in the appropriate security product(s).

Another potential application of SAO technology to improve actionability and decrease time to mitigation is to enrich the data with other sources of cyber threat intelligence. Depending upon the data source, IOCs might be provided with little confidence, or evidence of confidence, that the IOC is malicious. In general, one will have more confidence that an IOC is malicious if that IOC has been confirmed by other sources. There are many sources of cyber threat intelligence available, some free and some via paid subscription, such as blacklists for IP addresses and file hashes. Many security products already purchased and deployed by an organization contain or provide access to cyber threat intelligence and reputation services. A security orchestrator can enable correlation of a particular IOC against one or more of these cyber threat intelligence sources to enable calculation of a confidence score, tuned to the particular organization’s risk tolerance and threat model. Blocking IOCs that one has high confidence are malicious is a high-value response action enabled by SAO technology in this application.

By utilizing SAO across the combined ecosystem of generating IOCs and responding to them merged with SAO workflows focused on expediting “low-regret” actions, SAO technology can make cyber threat intelligence more actionable in an organization’s environment. This in turns provides more value to the organization from their existing security investments. IACD has demonstrated the synergy between security orchestration, automation, and information sharing through its pilot development efforts. For more information on SAO technologies and Cyber information sharing concepts, please visit https://www.iacdautomate.org .

References

[Asher] Asher, Mor (2016, April 28). IOCs are dead. Stop chasing MD5s or SHA256s and start working seriously on your application logic rules. [Web Page]. Retrieved from: https://www.linkedin.com/pulse/iocs-dead-stop-chasing-md5s-sha256s-start-working-seriously-mor-asher/

[Watson] Watson, Kimberly (2018, October). High-Benefit/Low-Regret Automated Actions as Common Practice [Web Page]. Retrieved from: https://www.iacdautomate.org/s/Low_Regret_Automated_Response_072018.pdf