Security Automation and Orchestration Capabilities Supporting Intra-Organizational Collaboration

Security Automation and Orchestration (SAO) provides many benefits in addressing security use cases with greater speed and efficiency. SAO technologies can also be used to enable intra-organizational collaboration for activities that require different teams within an organization to coordinate in a consistent and repeatable manner. The Integrated Adaptive Cyber Defense (IACD) initiative demonstrated this capability through research via use cases on the applicability of SAO in the context of an Insider Threat Analysis and Response program and techniques for Security Operations Center (SOC) analysts to collaborate with IT asset managers. IACD found that SAO technologies provide mechanisms for ensuring that the disparate team processes within these use cases are coordinated and applied consistently.

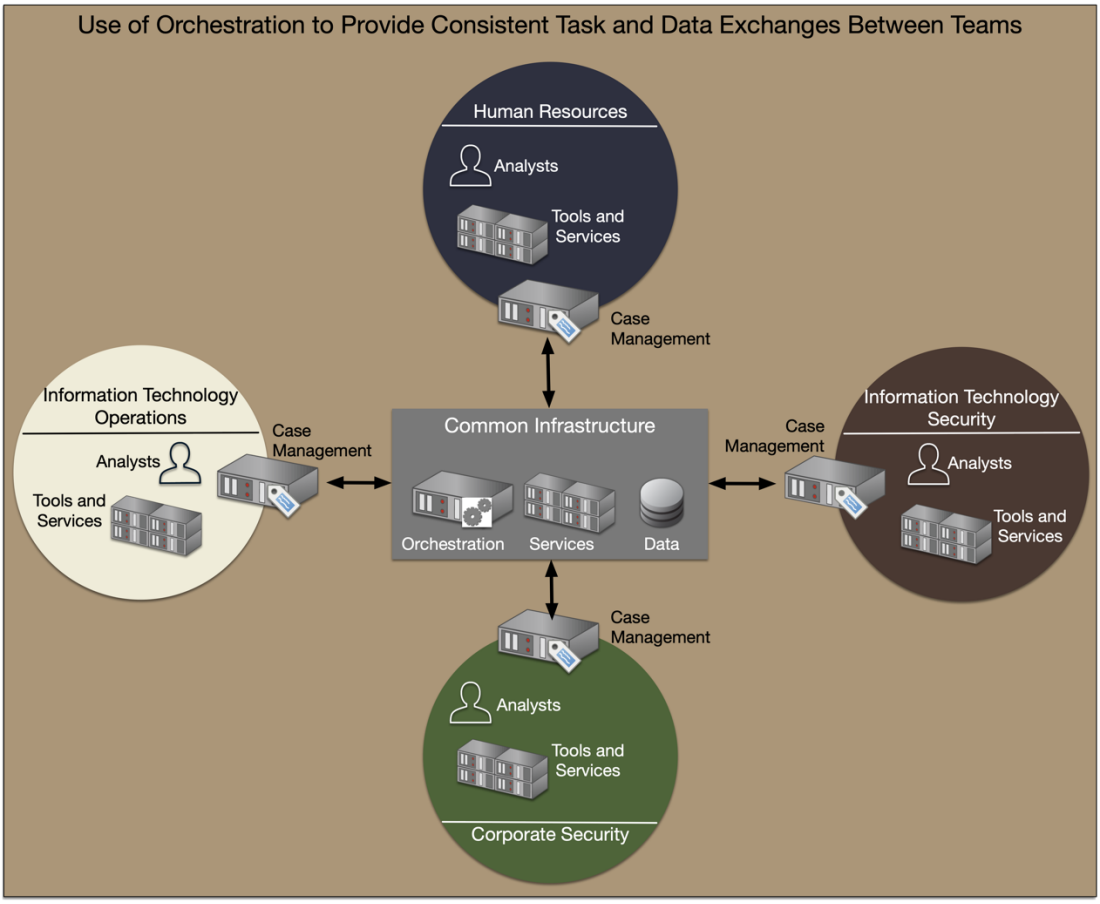
An insider threat with respect to Information Technology (IT) is “a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems” [NCCIC]. While the insider threat has typically focused on malicious insiders acting intentionally, more recently the scope of the insider threat sometimes includes unintentional harms caused by insiders (e.g., activities occurring on an employee machine compromised by malware) [CMU/SEI], and even insider threats to physical security and safety.
Insider threat investigations are conducted by cross-functional teams within an organization. Many different teams are typically involved, including Human Resources (HR), Legal, Corporate/Physical Security, Information Technology (IT) Operations, and IT Security teams, among others [CMU/SEI]. A specific organization might have different combinations of teams that perform these roles, but at a minimum there are operations that must be provided across all these areas.

For the SOC/IT use case, there are several tasks with respect to incident remediation and system hardening that require tasking across organizational boundaries. In many organizations, SOC analysts and IT asset managers are in different departments and each have their own tools, processes, and priorities. Once a course of action (CoA) has been selected which impacts an IT asset, the changes to the IT asset typically must be adjudicated via existing change management processes prior to being implemented. In many enterprises the availability of assets is a priority, so these processes tend to rely heavily on administrators to make decisions and authorized modifications are queued and executed at regularly scheduled intervals.

While these different teams each play a role within these use cases, each team has different policies, procedures, and priorities associated with their function, and each team requires different levels of access to data to support their role in operations. The application and coordination of

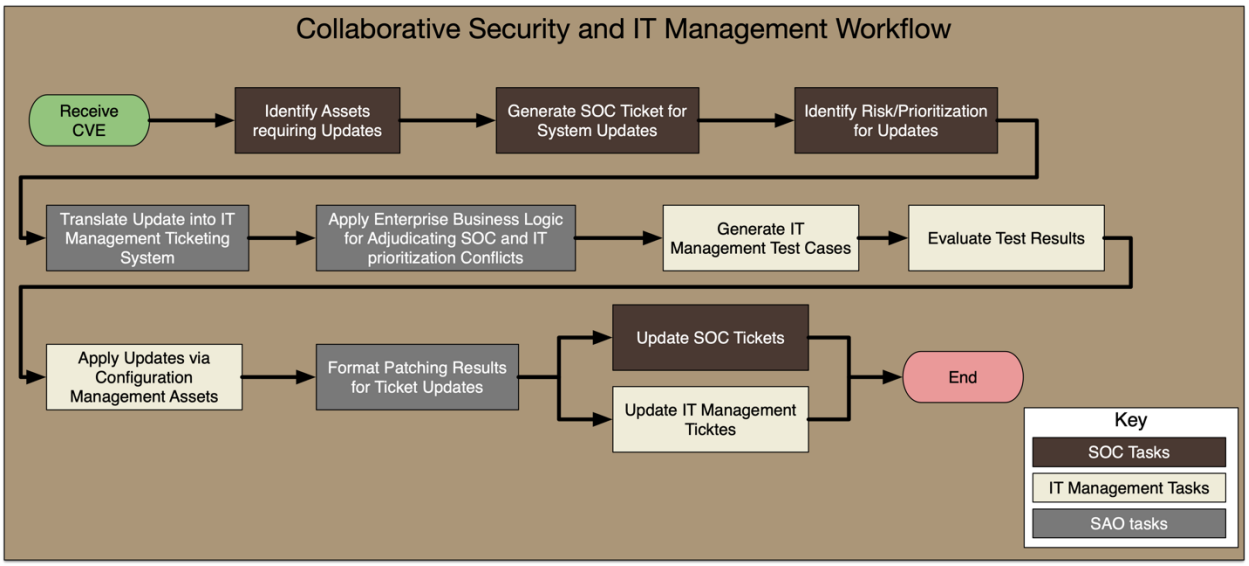
these different policies and procedures is where Security Automation and Orchestration technologies can improve operations by adding consistency and reducing the need to translate tasks and priorities between teams. Security orchestration is a method of connecting security tools and integrating disparate security systems to support automating security Standard Operating Procedures. Each participating team will have its own procedures, often utilizing its own set of systems accessing its specific relevant data. An orchestrator enables more seamless and consistent integration between the systems of each disparate team, including analysis systems and case management/ticketing technologies.

The figure below depicts a notional architecture for insider threat analysis and response with the data and command flows between the relevant teams within an organization. It provides a general description of how an organization can structure SAO to augment collaborative tasks.



An orchestrator can codify the interactions between teams, enabling an efficient and consistent flow of commands and data, while maintaining appropriate separation of roles and responsibilities. An orchestrator also allows each team to work with its own current systems without having to adjust their internal processes related to insider threat investigations, while facilitating the required coordination between teams across the organization.

The following process is an example of the types of actions that may be taken in a collaborative effort augmented by SAO. This particular process is for the application of software patches in response to a Common Vulnerabilities and Exposures (CVE) message received by a SOC that requires configuration management updates via the IT manager.



The use of automation and orchestration has additional benefits for consistency in application across cases. By documenting relevant processes more formally for automation, inconsistencies can be clarified and avoided. Playbooks can augment typical natural language text policy documents, enabling description of more formal workflows of the actions associated with policies. These workflows provide a foundation for consistent application of policies and processes, with particular attention paid to important requirements such as protection of sensitive data including Personally Identifiable Information (PII), limitation of access to investigation data to protect the confidentiality and reputation of employees, and maintenance of chain of custody for investigation evidence.

There are many other activities requiring coordination between teams within an organization that could similarly be improved via SAO. For example, electronic discovery (or e-discovery) in the context of legal proceedings requires coordination between legal, IT, and data owners to ensure that required data is identified and preserved for litigation or Freedom of Information Act requests. SAO can formalize and coordinate processes originating from legal department requests, implemented by IT using data management products, and ultimately reaching into teams owning the relevant data. Compliance with legal requirements requires that these processes be applied correctly and consistently across cases, and SAO technologies enable formalism and execution of these activities.

In summary, the use of security automation and orchestration enables coordination between the different teams within an organization and consistent application of policies and procedures, as demonstrated for insider threat investigations and applicable for other intra-organizational activities.

References

[CMU/SEI] Matthew Collins, Michael Theis, Randall Trzeciak, Jeremy Strozer, Jason Clark, Daniel Costa, Tracy Cassidy, Michael Albrethsen, and Andrew Moore. "Common Sense Guide to Mitigating Insider Threats, Fifth Edition". CMU/SEI-2016-TR-015. Software Engineering Institute, Carnegie Mellon University. 2016. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484738

[NCCIC] National Cybersecurity and Communications Integration Center. "Combatting the Insider Threat". 2014. https://www.us-cert.gov/security-publications/Combating-Insider-Threat