Security Automation and Orchestration (SA&O) Implementer Insights

The Integrated Adaptive Cyber Defense (IACD) Community partners with Industry, Government & Academia demonstrating effective Cyber Security Automation, Orchestration and Information Sharing strategies (https://www.iacdautomate.org/aboutiacd/). An increasing number of organizations are exploring and integrating Security Automation & Orchestration (SA&O) / Security Orchestration, Automation & Response (SOAR) strategies and platforms in cyber defense. To assist organizations evaluate and integrate effective SA&O strategies, experienced adopters and vendors offer recommendations and lessons learned, based on experience with use cases, measures and metrics and deployment guidance.

Highlights:

- **Adopting SA&O/SOAR** – Develop proposals and socialize ideas across your organization to drive interest, support and commitment. Demonstrate quick wins and build trust with mature security practices.
- **Applied use cases** – Demonstrate financial, operational effectiveness, and morale improvements by introducing time efficiencies, enforcing consistency in practice and shifting analyst focus to challenging analysis tasks. Common interests include aiding investigations with data gathering & enrichment, integrating threat intelligence with internal security telemetry, and orchestrating actions and system updates across teams and systems.
- **Developing Playbooks & Workflows** – Accelerate development by describing SA&O scenarios as process flow diagrams recognizing where you want staff to influence decisions. Consider early how you plan to organize playbooks & workflows for reference, updates, and dependencies. Beware of unintended effects! Remember to validate data and verify actions with error handling conditions.
- **Deployment** – Commit to process improvements, phase implementation, ingrain development and configuration management practices, and automate/orchestrate system updates to maximize benefits and effects.
- **Architecture** – SA&O solutions are offered as cloud As-a-Service and traditional enterprise hosted platforms. Evaluate which environments you need supported and request vendors demonstrate capabilities across environments. Many security platforms are beginning to incorporate orchestration features. Determine how they will support your organization's SA&O strategy.
- **Measures & Metrics** – Baseline metrics prior to SA&O to quantify benefits. Measure reliability to build trust and confidence in the system. Consider risk, impact & alternatives if highly utilized tools were to become unavailable. Adopters find SA&O dashboards, complemented by traditional infrastructure monitoring tools, sufficient.

Have recommendations or lessons learned to share? Interested in a specific topic? Join the discussion and assist others with achieving SA&O benefits, value, and effects (https://iacdautomate.org). Adopters are interested in connecting communities, diversity of thought, and lessons learned with incentives to encourage participation and acknowledgement.

Contents

EXPERIENCED ADOPTER / VENDOR RECOMMENDATIONS & OBSERVATIONS

ADOPTING SA&O / SOAR

Develop proposals and socialize ideas across your organization to drive interest, support and commitment. Demonstrate quick wins and build trust with mature security practices.

- Develop proposals to assist with identifying, selecting and socializing relevant SA&O scenarios driven by goals and end-states. Proposals should clarify accountability, dependencies and interfaces between departments, tools and staff.
- Include auditors, compliance, IT, Security Engineering and Operations when exploring SA&O scenarios. Start early with multiple perspectives to drive interest and support both in concept and execution.
- Begin by applying SA&O to mature security practices and processes. Cost savings and process improvements are easier to recognize and assist building trust and confidence in an SA&O platform by providing verifiable familiar results.
- Document and refine processes to avoid orchestrating and automating broken processes. Before deploying solutions, identify best practices and address process gaps. Consult professional services if needed. Adopters recognize to fix processes rather than orchestrate broken processes. [1]

1 – IDG Communications CIO Security Orchestration & Automation eGuide - http://idgcommunications.lookbookhq.com/threatconnect/threat-connect-artic-1

APPLIED USE CASES

Demonstrate financial, operational effectiveness and morale improvements by introducing time efficiencies, enforcing consistency in practice and shifting analyst focus to challenging analysis tasks. Common interests include aiding investigations with data gathering & enrichment, integrating threat intelligence with internal security telemetry, and orchestrating actions and system updates across teams and systems.

- Applying SA&O to cyber investigations results in financial, operational and morale benefits. It accelerates investigations, improves quality with fewer resources in less time, and enforces consistency in practice while minimizing mundane tasks. Organizational risk is perceived lower with the demonstrated ability to handle a higher volume of alerts.
- Assist investigations with data gathering and enrichment. Security analysts shift focus to analyzing data while the system gathers and enriches data. Benefits realized include time efficiencies, consistency in practice, improved analyst motivation, challenge and analysis skills.
- Improve or enforce consistency and compliance with your organization's preferred methodology. Orchestrated playbooks and workflows guides analyst actions and offer an easy method to audit actions for compliance and regulatory reporting.
- Assess the ability for service providers to meet Service Level Agreements (SLAs). Identify opportunities for which your organization can improve upon services offered.
- Improve morale by balancing workloads and acknowledging analyst strengths in processing events. Avoid the early temptation to measure and report analyst effectiveness through the platform.
- Enterprise Strategy Group (ESG) observes organizations want to merge threat intelligence with their internal security telemetry, add custom functionality for security operations and automate remediation tasks. [1]

APPLIED USE CASES (Continued)

- According to ESG research, 19% of enterprises have already deployed technologies for security automation and orchestration extensively, 39% have done so on a limited basis and 26% are engaged in a project to automate/orchestrate security operations. [1] CISO interests include:
    - Advanced Automation – Beyond triggering remediation action, SOC teams are automating their Standard Operating Procedures (SOPs) aligning runbooks with automated actions in an easy intuitive way. Vendors offer scripting, Graphical UI based configurations, templates and canned runbooks. Advanced automation includes analyst activities for triage, prioritization, and investigations among other activities. [1]
    - Process orchestration across heterogeneous tools. Leading products have opened APIs, established developer support and are making use of technology ecosystem partners. [1]
    - Case management – Large organizations need central management capabilities to initiate, monitor and communicate SOC activities through event lifecycles. Case management needs strong communication functionality to enable processes requiring multiple individuals and shared processes between security and IT. Many organizations try to use generic case management and ticketing systems, but often find the tools are inadequate for cybersecurity needs. [1]
- ESG asked 412 cybersecurity and IT professionals to identify their organization's SA&O priorities:
    - 35% want to use SA&O technologies to integrate external threat intelligence with internal security data collection and analysis. (streamline investigation workflows) [1]
    - 30% want to use SA&O technologies to add functionality atop existing tools. Typically orchestrating workflows as part of things like security investigations, incident response or remediation tasks. [1]
    - 29% want to automate basic remediation tasks – things like generating firewall rules upon receiving a list of Indicators of Compromise (IOCs). [1]
    - 28% want to correlate and contextualize data resulting from the output of several tools for a holistic picture of security incidents. [1]
    - 22% want to integrate security and IT operations tools. Enable security analysts to access asset databases, configuration management, trouble ticketing systems and other tools and systems. [1]
- Review how an SA&O solution may influence Privacy Act disclosures and the role it will play as a System of Record for incidents.

DEVELOPING PLAYBOOKS & WORKFLOWS

Accelerate development by describing SA&O scenarios as process flow diagrams recognizing where you want staff to influence decisions. Consider early how you plan to organize playbooks & workflows for reference, updates and dependencies. Beware of unintended effects! Remember to validate data and verify actions with error handling conditions.

- Document SA&O scenarios as process flow diagrams to speed development. Many organizational security practices and policies, intended for SA&O, are not well documented, which slows playbook definition and development. Documenting existing processes prior to executing in a SA&O platform is key.
- Improve playbook quality and speed development efforts by recognizing how staff will influence decisions. Know where you intend or are required to have staff in your processes. Understand which actions they will take.
- Validate and Verify. Validate needed data is available. Verify, in playbooks & workflows, data arrives as expected. Run test cases and confirm all playbooks execute as intended. Learn from mistakes; for example a contributor accidentally updated a firewall rule blocking all traffic instead of an intended subset. Beware of unintended effects. Look for recommendations on how to improve data validation in playbooks.
- Plan how to organize playbooks and workflows for reference, general updates and interdependencies. Playbooks are often customized with slight revisions, which may lead to duplication and confusion of intent.
- Assess how easy and flexible an SA&O platform supports data normalization to map common fields that may be defined differently between systems. This is a tedious task that can slow integration efforts if fields are not easily mapped and referenced.

IACD offers a playbook template to identify SA&O relevant practices and implement them as playbooks & workflows in SA&O platforms. https://www.iacdautomate.org/playbooks/

DEPLOYMENT

Commit to process improvements, phase implementation, ingrain development and configuration management practices and automate/orchestrate system updates to maximize benefits and effects.

- Successful SA&O/SOAR results come from a commitment to process improvement, a deliberate phased implementation plan and partnerships with technology vendors who posses deep security operations experience. [1]
- Integrate development and configuration management practices. Playbooks, similar to developed code, require updates, testing, verification and version control. Organizations typically establish several environments (development, staging & production) to develop, test and deploy playbooks.
- Invest in DEVOPS practices and tools to streamline playbook and workflow updates. Without them, your security operation teams will be unable to handle the frequency of changes and testing desired. SA&O platforms provide development tools yet require manual steps to transition and maintain playbooks across environments. Creation, updates, vetting, testing, approving and deploying across environments are all considerations. Several adopters noted experimenting with GitHub.
- Review your security infrastructure tool and license support for SA&O. Licenses may limit the number of actions or functionality accessible via API. SA&O platforms can assist in tracking utilization of your tools and projecting license costs and requirements. Initial efforts should closely monitor tool integration and resource consumption with safeguards to mitigate inflating costs and inadvertently impact system and network performance.
- Establish vendor support agreements, in addition to professional services, to assist integrating SA&O solutions with your infrastructure. Defined APIs assist, but may require updates to achieve full functionality desired.

ARCHITECTURE

SA&O solutions are offered as cloud As-a-Service and traditional enterprise hosted platforms. Evaluate which environments you need supported and request vendors demonstrate capabilities across environments. Many security platforms are beginning to incorporate orchestration features. Determine how they will support your organization's SA&O strategy.

- Consider SA&O cloud and traditional enterprise hosted solutions. Similar to IT, security teams are encouraged to operate in cloud environments; with their corporate infrastructure having already migrated.
- Determine if you need SA&O to support enterprise and /or cloud environments. Request vendors demonstrate capabilities across environments. Review how a solution may support interfacing with local infrastructure and cloud orchestration services. For instance, does the approach support querying and executing actions across local and distributed proxied systems?
- SA&O platforms, within enterprise networks, are usually deployed in segmented protected networks co-located with SIEMs and other protected security infrastructure services. Network and application proxies, sometimes log consolidation systems, facilitate and meter connectivity with devices.
- Evaluate how SA&O platforms scale storage. Are they limited to local storage or extensible to cloud storage? Which features protect data and how are liability concerns addressed?
- IT, Development and Security orchestration platforms remain distinct yet are converging in capabilities and necessity for linking processes and capabilities.
- Many threat intelligence and other platforms are beginning to incorporate orchestration features. Determine how these features will support your organization's SA&O strategy.
- Plan for how your organization will react to a suspected SA&O compromise. Many organizations plan to revert to manual processing, but need to consider how staff will reference preferred organizational practices, access tools previously accessed through system interfaces and prioritize activities at a slower pace. SA&O platforms offer high availability configurations for scaling and failover with recovery guidance.

MEASURES & METRICS

Baseline metrics prior to SA&O to quantify benefits. Measure reliability to build trust and confidence in the system. Consider risk, impact & alternatives if highly utilized tools were to become unavailable. Adopters find SA&O dashboards complemented by traditional infrastructure monitoring tools sufficient.

- Baseline metrics, prior to SA&O, to assist in quantifying benefits achieved. Begin by observing practices in current operations or during a pilot; specifically examine comparable manual and semi-automated steps.
- Measure workflow reliability to build trust and confidence in the system. These are important to track for production readiness and reliability.
- SA&O reports, with the ability to export data, reduces the time required to prepare for audits and demonstrate capabilities.
- Monitor which security tools and infrastructure components aid investigation and remediation activities. Consider risk, impact and alternatives if highly utilized tools or infrastructure were to become unavailable. Few organizations are evaluating this today.
- Tracking analyst click counts, pre and post SA&O, assisted to quantify reduced analyst actions required.
- Adopters monitor standard investigation performance metrics including number investigated, mean times to notification, investigation and remediation. Experienced adopters track and tune types of investigations aided through automation and orchestration.
- Track analyst efficiencies through your SA&O platform. Consider investigation timelines pre and post adoption and pay particular attention to differences in averages depending on event type and time of event occurrence.
- Adopters and vendors find SA&O dashboards, complemented by output from traditional infrastructure monitoring tools, as sufficient for monitoring SA&O platform performance and scale. Queueing and parallel playbooks/workflows are not routinely monitored in deployments.

IACD identified a set of metrics and measures to assist organizations recognize SA&O benefits, value and effects within their organization.
https://www.iacdautomate.org/integration-strategies/?rq=metrics