Security Automation and Orchestration (SA&O) Metrics & Measures

Background

SA&O metrics and measures assist organizations in recognizing and refining how SA&O capabilities and techniques introduce benefits, value and effects. This document identifies metrics and measures that organizations may find beneficial to collect, assess, and compare over time.

Metrics and Measures Groupings
1. **Operational Performance - evaluate & recognize SA&O value, benefits, issues and effects as it relates to security operations and performance.**
2. **System Performance - evaluate & recognize value, issues and effects as it relates to your Cyber security infrastructure, practices and SA&O support.**
3. **Process Performance – evaluate & recognize value, issues, and effects as it relates to organizational, practice and process dependencies that directly impact SA&O value.**
4. **Workflow Execution - assist organizations to design, develop, monitor, tune, troubleshoot and maintain SA&O capabilities.**
** The groupings are general to highlight types of metrics and measures and are not comprehensive*

As organizations apply SA&O capabilities, there is value in collecting information to help assess utility, applicability, (in)efficiency, and reliability of the implementations. It is also useful to collect information that identifies dependencies, opportunities for improvements, or changes in performance. Lastly, it may be important to collect audit information to support deployment testing or compliance verification.

Metrics and Measures may be tailored for performance indicators as: [1]

- Quantitative – measure of value (number, time, $, ratio)
- Qualitative – measure of acceptability or health
- Thresholds – when an index reaches set targets or falls into set ranges
- Milestones – when a specific condition is reached
- Trends – results analyzed over time and volume

Metrics and Measures

The following tables provide insight into metrics and measures that can be captured or produced by SA&O systems. Each entry includes a description and rationale/utility examples.

SA&O Operational Performance measures and metrics

Assist organizations to evaluate and recognize SA&O value, benefits, issues and effects. They offer insights for how SA&O has been applied, efficiencies gained, cyber security operations effectiveness and overall Return on Investment (ROI) context. Because they are directly related to reasons that organizations invest in SA&O, most of these metrics and measures are already "provided" by orchestration providers and described in industry resources.

Measure/Metric	Description	Rationale/Utility *Identifies or Informs*
Operational Performance		
1. Mean time to notification	Time between a potential malicious activity detected and an alert is provided to the person or system responsible for investigating. [2]	• Summarize operational value when compared with prior practices • Example: Time lapse notifying SOC tier 1 support
2. Mean time to investigation	Once an alert has been sent, how much time passes before the investigation begins and what is the duration of the investigation? [2]	• Throughput • Summarize operational value • Ability to handle higher volumes of investigations, alerts and data • Example: Time lapse between notification and when an automated workflow or analyst begins investigating
3. Mean time to remediation	From alert to investigation to remediation, total elapsed time.[2]	• Summarize operational value • If organization achieving quicker detection and response • Example: Average time to resolve a number of major vs. minor incidents
4. Remediation summary statistics	Statistics tracking manual, semi-automated and automated remediation	• Characterize the level of automation applied in operations • Track progression for each type of remediation • Summarize operational value • Example: Summarize the types of incidents aided by workflows for remediation
5. Percent Investigated vs. Alert Volume	Investigations vs. alert volume [3]	• Security Operations risk gap • How SA&O aids investigations compared to the volume of alert data
6. Performance Improvements	Information collected to show how automation is improving processes and resource utilization.	• Operational value in terms of performance • Resource savings • Examples: speed of decision/resolution, resource utilization improvement (e.g., devices run faster due to less malware, increased network bandwidth due to blocking malware related traffic)

System Performance measures and metrics

Assist organizations to evaluate & recognize value, issues and effects as it relates to your cyber security infrastructure, practices and SA&O support. They offer insights for how SA&O has been implemented, orchestration management, and cyber security product/service value as related to automation in operations.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
System Performance and Utilization		
7. Workflow utility	Track how many incidents and types of incidents were aided by workflows.	• Utilization trends • Operational value for incident and alert triage • Operational practices and dependencies • Example: Identify if workflows are or could address common incidents/alerts in part or whole.
8. Sensor utilization	Track playbook/workflow dependencies on sensors, threat feeds and data sources.	• Potential impact of compromised or unavailable sensor(s) • Heavily vs. underutilized sensor(s) • Which sensors aid investigation and/or remediation actions • Example: Which workflows rely on real-time packet capture analysis? Impact if it were to become unavailable?
9. Sensor value	Track which sensors, threat feeds and data (sources) aided an investigation or remediation	• Potential impact of compromised or unavailable sensor(s) • High valued vs. underutilized sensor(s) • Sensor tuning effectiveness • Which sensors aid investigation and/or remediation actions • Example: Types of logs or threat feeds and indicators proven effective
10. Threat Indicator or IOC value	Track which threat indicator(s) aided an investigation or remediation	• Types and sources of indicators aiding security operations
11. Queued workflows or actions	Number of playbooks, workflows, investigations queued	• Ability to scale and support demand • Identify system bottlenecks • Throughput • System failures • Examples: Understanding if the system is capable of supporting operational demand
12. Concurrency / Parallel workflows	Number of playbooks, workflows or investigations executed per time period	• Ability to scale and support demand • Examples: Comparing workflow executions with Incident triage in peak

		time periods
13. Workflow interface dependencies	Track which product integration interfaces were used in or are required for workflow execution	• Security infrastructure dependencies • Common, duplicative vs. purposely separated system interfaces • Example: Common dependency on a logging interface and impact if it were to become compromised or unavailable.
14. Performance Degradation	Information collected to show how automated processes are negatively impacting system or process performance.	• Counterproductive operational impact • Example: boundary protection devices run slower due to increasingly large blacklists or decreased network bandwidth due to queries to support internal enrichment of IOCs
15. Custom Measures & Metrics	Enable admins and users to create and save measures or calculations for use in analysis	• Performance measures and Key Performance Indicators differ by organization, culture and goals. Offer the flexibility for organizations to define and analyze performance and results. • Examples: unauthorized software/devices identified in investigations, percentage of devices with current patches, detected non-compliance with business conduct policies, and number of reported vs. detected security incidents

Process Performance measures and metrics

Assist organizations to evaluate & recognize value, issues, and effects as it relates to organizational, practice and process dependencies that directly impact SA&O value. They offer insights for how SA&O efficiency and effectiveness may be impacted by dependencies on external, manual, poorly-defined, and/or cross-organizational processes.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
Process Performance		
16. External process dependencies	Identifies workflows that have a dependency on an external process or system	• Operational dependencies across organizations, systems, tools and practitioners Examples: Third party service or cloud providers, inter-organizational relationships NOC/SOC/IT
17. Workflows requiring human intervention (as designed)	Track playbook/workflow dependencies on human interaction	• Workflows that require an approval or human interaction as part of execution • Workflows that can execute without human interaction • Classifying how different types of workflows may benefit by manual or automated validation, verification and/or audit. • Example: Identify frequently executed workflows with a history of high confidence execution still requiring human interaction.
18. Workflow effectiveness	Track which workflows were effective for their intended goal vs. required additional investigation or analysis.	• Poorly defined processes that cannot be automated consistently • Opportunities to enhance workflows and reduce manual processing required • Additional sensors, sources and/or analysis techniques relevant to the task • Example: Percentage or number of investigations and workflows which required unanticipated analyst investigation support.
19. Analyst/Practitioner/ Organization interactions	Track which organizations and staff were required to interact with a workflow to facilitate an end goal. Track within and across connected workflows	• Organizational dependencies • Opportunities to streamline operations across organizations • Inform service level agreements between organizations • Examples: SOC, NOC, IT, Helpdesk, and Legal

Workflow Execution measures and metrics

Assist organizations in verifying that SA&O performance is achieving intended effects. As part of that, these metrics and measures assist organizations in the design, development, monitoring/auditing, tuning, troubleshooting, and maintenance of SA&O capabilities.

Measure/Metric	**Description**	**Rationale/Utility** *Identifies or Informs*
Workflow Execution		
20. Frequency of workflow revisions	Statistics tracking the frequency of workflow/playbook revisions	• Stability of workflows • Complexity of workflows • Controlled administration, configuration & tuning • Audit authorized & verified changes • Automated tests to verify and validate results and intent. • Example: Stable workflows suddenly revised or unapproved changes to operational practices.
21. Frequency of workflow execution	Statistics tracking the frequency of workflow/playbook execution	• Potential impact to operations if compromised or unavailable • Frequency of initiating condition or alerts • Example: Identify how often the workflow executes during business hours
22. Frequency of remediation actions taken	Statistics tracking the frequency of actions taken to remediate threats/risks	• Audit changes made to operational assets • Frequency of changes made to certain operational assets • Example: Identify how often the workflow executes different actions in response to same trigger
23. Workflow utilization	Track how many times a workflow is selected manually vs. automated and runs.	• Utilization trends (heavily vs. underutilized) • Operational practices and dependencies • Example: Identify if and how analysts and/or automated responses are applying workflows.
24. Workflow value	Savings estimate by multiplying the cost of performing repetitive tasks manually by the estimated number of times the system performs those tasks automatically during a specific date/time range. [4]	• Estimated time and/or cost savings • Return on Investment (ROI)
25. Workflow confidence level	Statistics tracking the frequency automated recommendations are	• Confidence in semi-automated/automated COA recommendations

	confirmed for execution	• Potential workflows to enhance with automation • Example: Workflow confidence score increases given the frequency analysts concur with recommendations.
26. Workflow idle time	Statistics tracking times workflows were paused waiting for data, a decision, action or approval.	• Efficiency opportunities for processes and workflows • Throughput/efficiency constraints • Sources of bottlenecks • Example: SOC workflow commonly requires network operations center (NOC) concurrence which is taking 24-48hrs. Opportunity to accelerate between departments?
27. Workflow reliability	Track successful vs. unsuccessful executions. (success, failure, error rates)	• Reliability trends • Failures common across workflows • Example: Workflow A is highly reliable while workflow B commonly requires unplanned manual intervention and should be considered for revision.
28. Workflow decision processing	Capture triggering condition, key values/decision points, and end state	• Verify that certain actions are taken if and only if certain conditions are true. • Example: provide evidence that a critical server is not taken offline and reset unless another service is verified as online first.
29. Workflow dwell time	Statistics tracking workflow execution times	• Performance (typical vs. abnormal) • Change in system or capabilities • Example: A workflow typically requires 1 minute to complete and is noted taking 2+ mins. Intended or unintended change?
30. Workflow deployment readiness	Evidence verifying and validating workflows are defined by compliant practices and execute as intended.	• Workflow dependencies • If workflows can be verified, audited and validated • Examples: verification that initiating feeds are working, timing information on how long certain paths or steps take, responses from sensors or actuators tasked

References:

1. Deloitte KPI and Measuring Security - https://www.scribd.com/doc/37150665/Deloitte-KPI-and-Measuring-Security
2. Hexadite – A comprehensive guide to evaluating security orchestration and automation solutions - https://www.hexadite.com/resource/comprehensive-guide-evaluating-security-orchestration-automation-solutions/your-download-is-ready/
3. Fidelis - Transforming Security Operations with Automated Detection & Response - http://go.fidelissecurity.com/E0I0Z0OgRAj080YZ3f04w04
4. ServiceNow Operations Management and ROI - https://docs.servicenow.com/