Siemplify

The No-Nonsense

Guide to Security Operations Metrics

WHITE PAPER

The No-Nonsense Guide to Security Operations Metrics

KPIs That Actually Work for Assessing Your SOC Progress and Driving Executive Support (Plus Actionable Advice for Improving Those Metrics)

As the saying goes, there are two types of companies: Those that know they have been hacked – and those that just haven't discovered it yet. The adage admittedly isn't perfect, nor fair, as there are countless companies practicing defense in depth and performing due diligence by continuously assessing the threat landscape and effectively putting people, process and technology to work to address them.

But because every organization in the world is a target for cyber threats and data breaches, information security is a rare discipline in which what should be the traditional hallmark of success – "Nothing bad happened!" – isn't an option.

As a result, success becomes more difficult to define and measure, and companies must think long and hard about the appropriate metrics for their business and technical goals. Still, metrics are an important part of cybersecurity and security operations programs. Being able to measure your progress shows how well your security program is functioning and helps justify to executive leadership and other stakeholders the security operations center (SOC) resources you require.

Security teams are constantly asking for more budget for resources to improve their day-to-day operations. Yet, the SANS Institute found in its 2018 Security Operations Center Survey that just 54% of SOCs collected metrics, and most weren't "business-relevant effectiveness metrics." SANS said that without clear measurements, SOCs may run into funding resistance due to their inability to communicate to management the value of the SOC and overall security program.

Knowing that securing more funding for additional hires and new technologies rests on providing data-based proof raises an obvious question: Why aren't more SOCs diligently tracking their performance? For starters, many security operations teams say the reporting they provide requires a significant amount of work to pull together. Between non-stop alerts, burned-out analysts, an overdependence on manual processes, skills shortages and security tools that don't interoperate, defining success – never mind approaching metrics from a business perspective – can seem virtually impossible.

But for security operations to grow within your company, attesting to its value both internally and across the greater organization will be tantamount to your individual success.

BEFORE YOU MEASURE

The first step to building your enterprise cybersecurity metrics and security operations KPIs is setting clear direction as to what you are collecting and why. You will need a vision, long-term objectives and strategy before you can achieve executive stakeholder buy-in for your metrics program.

Going the reverse route will result in a barrage of questions and little in the way of support. Reduce the friction and expedite approvals by clearly articulating a solid plan and the concrete role leadership support plays. (In case you are wondering, yes, not only are you ultimately seeking executive-level support for your SOC, but also endorsement for collection of data related to it.)

Outside the executive suite, some stakeholders within the IT department may feel a metrics program adds pressure to their teams because of the added visibility into their day-to-day operations. No one enjoys feeling like another group within the organization is keeping tabs on them.

Building and presenting your program to alleviate this concern is paramount to minimizing pushback. Framing the process and rationale as a way you are assisting with tightening processes and technology for the organization as a whole is often a good starting point. Also, go in prepared with a clear outline of stakeholder roles and responsibilities. You'll need to answer questions like:

1. If an issue is determined via the metrics program, what is each stakeholder's responsibility with regard to remediation efforts?

2. How will information be reported to stakeholders?

3. Will there be service-level agreements (SLAs) for solving and correcting concerns within the metrics?

BUSINESS-ORIENTED METRICS

Earlier, we established that no organization is immune from a successful cyberattack. But that doesn't mean catastrophe is inevitable. Those businesses that can reduce the harm that a successful compromise can impose will be able to stave off costly consequences and revert to normal operating conditions in a timely manner. Here are a few metrics that will help support your risk mitigation strategies, as well as convey risk to senior leaders and the board.

Time to Detection, Containment and Eradication

KPIs in this category include mean time to detect, or MTTD, which reflects the amount of time it takes your team to discover a potential security incident. Mean time to respond, or MTTR, is the time it takes to control, remediate and/or eradicate a threat once it has been discovered. And dwell time captures the entire length of a security incident, reflecting the duration from when an attacker first enters your network to the time they are removed and you have returned to a known-good state.

The impact of dwell time cannot be understated: It is during this window that adversaries have unrestricted access on your environment, allowing them not just lateral movement but also the ability to commit any number of damaging actions, including data theft, network and user reconnaissance, and additional malware infections.

Alert Reduction

With the average company receiving tens of thousands of threats per week, not only are SOCs overwhelmed, they are also experiencing alert fatigue. Two types of investigations generally occur in the SOC: alert-based and threat-centric. Alert-based represents a one-to-one relationship between case and alert. An alert comes in, enrichment and automation happen for the alert, and the analyst completes the investigation. Analyst efficiency may improve, but the biggest problem in the SOC, the volume of alerts, is left unresolved. To address alert volume as well as meet the SOCs objectives, you must do more than simply enrich alerts and automate some tasks. This involves leveraging a threat-centric approach to investigations that looks for contextual relationships in the alerts and, if identified, groups these alerts into a single case. This will help you reduce the huge numbers of alerts you must regularly confront.

Service-Level Agreements

Have you been meeting the SLAs as jointly defined with the business? For the SOC to win executive support, it must show it is aligned with business goals, including risk posture and compliance requirements. SLAs help provide supervised accountability and ensure that the SOC is adequately communicating with key departments, including compliance, legal, IT and human resources.

Staff Retention

The security operations center is a pressure-packed place, home to sophisticated threat assaults, disparate detection tools firing off countless alerts and a widening skills chasm. But for as active a hub it is, your SOC can be home to great disaffection and mental exhaustion due to the humdrum tasks involved with working individual alerts. No analyst wants to be stuck doing the tedious stuff for long, and you shouldn't want that either. The goal is to get your analysts partaking in more specialized disciplines, like threat hunting and eradication. And because of the much-maligned skills shortage, you'll want to ensure you offer a thriving environment in which to work. Remember: if the burnout doesn't get them first, a competing employer could.

Other Business-Oriented Metrics to Consider

Metric	Questions it can help answer
False Positive Rates	How many false positives is your SOC experiencing in general or, more specifically, per product? This will help determine overall effectiveness in deployment and configuration of tools.
Distribution of Root Causes	What are the causes of incidents? Root cause analysis can help you determine what needs to change in terms of people, processes or technology.
Threat Attribution	This is likely the most sophisticated of assessment options for the SOC, reserved for those security hubs experiencing elite proficiency. How well you understand the details of a threat can be a strong indicator of the proficiency of your security operations, and it's no surprise that certain organizations will want to add this metric to their measurement repertoire. But bear in mind that threat attribution is complex and involves organizations using advanced intelligence and forensic evidence to determine the origin, motivations and sponsors of attacks.

OPERATIONAL METRICS

Number of Alerts and Incidents Handled

Documenting the number of alerts and incidents your team confronts is an obvious bellwether metric. Is the number increasing or decreasing? What types of tickets and cases are coming through? And what are their severity levels?

In addition to helping to determine the overall success of your program, tracking alert and incident counts and closures will help determine false positive rates, decision-making speed, and whether you are operating with an appropriate headcount (i.e. are there too many events being handled per SOC analyst?), as well as other bottlenecks.

In addition, it will allow you to pinpoint specific areas of the business from which a lopsided number of issues may be emanating. Isolating threat distribution will enable your team to help the company determine which departments may be ripe for remedies, such as additional security awareness training.

You should also document who beyond the SOC was needed to respond to incidents, as well as the escalation level required and how the response played out. SIEM and log data will help discern incidents, but security automation, orchestration and response (SOAR) can help centralize the work by providing full visibility into your detection tools. In addition, SOAR will help make your team more effective by lending more efficiency to your caseload.

If you're feeling inspired, you can stretch this metric to include how many alerts were closed per shift, offering a gauge of your individual team's adeptness. More later on some other metrics that specifically can be used to evaluate SOC team performance.

Other Operational Measurements to Consider

Metric	Questions it help answers
Distribution of Products	From which products are the most alerts originating?
Distribution of Cases by Tier	How many cases are handled per tier (1, 2 or 3)?
Distribution of Outcomes	How many false positives are being marked as real issues and vice versa?
Distribution of Alert Types	What types of alerts occurred over a given time period?

IMPROVEMENT METRICS

Analyst Improvement

Whether they are Tier 1, 2 or 3 – or grouped by functional expertise, a personnel structure that is becoming more common according to a recent Cyentia Institute-Siemplify report - analysts are the bedrock of any SOC. Not only are they the frontline responders and coordinators to alerts and events, they also must bear other responsibilities for the wider organization. This includes assisting with compliance requirements, helping to establish companywide security policies and staying up to date on the latest threats. Be sure to create individual metrics that can track your analysts' progress to determine their composite impact.

For example, which Tier 1 analysts are most commonly escalating to Tier 2 analysts? This can help to identify analyst performance, capacity issues and analysts who require additional training (on specific topics or in general).

Other Improvement Metrics to Consider

Metric	Questions it can help answer
False Positive Rates Per Product	Are you utilizing your coveted higher-tiered resources only when necessary because Tier 1 analysts (combined with automation technology like SOAR) is handling anything that they can and should?
Handling Time Per Alert	Which type of alert/product is taking the longest to properly address? This will help you determine where you should spend time optimizing and building new processes/ playbooks moving forward.
Handling Time Per Stage	Are your analysts moving alerts in a timely manner across common stages: queue, false positives, escalation, review, opened case, closed investigation, resolution?
Handling Time Per Analyst	What are the response times and counts for individual analysts?
Playbook Usage Rates	Which best practice workflows are you most commonly leveraging to help handle and investigate alerts and respond to incidents?
Most Common Entities	What are the most prevalent hosts/IP addresses/users that appear in malicious cases? This could indicate they deserve special attention.

AFTER YOU MEASURE

Once your cybersecurity metrics program is in swing, you'll have to aggregate the data you collect to output metrics reports. The reports should be sent to stakeholders and include a clear representation of what is being measured, its priority, what its baseline was and how it has changed over time. Producing these reports requires analysis to get a full understanding of the numbers to have the ability to explain progress, shortfalls and fluctuations.

Be prepared for your reports to take into account exceptions, adjusting variables and areas where combining data may muddy the waters. Often these arise from manual and inconsistent processes. The ability to automate response and remediation processes can limit skewed metrics, streamline reporting, improve predictability and allow for better data hygiene when speaking with stakeholders. SOAR technology can lend a big assist here.

Your deltas between a current metric and the established baseline – either positive or negative – will show change within your organization and should be reviewed by your key constituencies. Positive improvements should get just as much attention as negative metrics, with the goal of applauding the hard work of those who are improving the security of the organization. Not only can this go a long way toward building confidence with stakeholders and boost morale among analysts, metrics improvements in one area can shed light on how to make improvements in others.

Remember: Metrics are an important part of your cybersecurity and security operations programs and being able to measure your progress shows how well your team is functioning. Having key stakeholders brought to review your vision and strategy will assist with getting other teams to cooperate in your data collection. The more you can automate metric collection, as well as in broader security operations processes, the quicker you can respond and produce reports.

FINAL CONSIDERATIONS

If you outsource security operations to an MSSP...

If you're relying on a managed security services provider for some or all of your security operations, make sure you are in regular communication with the vendor and that your metrics program takes into account the fact that an outside partner is handling many of the things that need to be measured. Work to centrally document this interaction process, keeping back-and-forth limited to a single channel if possible.

Security automation, orchestration and response (SOAR)

Earlier we mentioned SOAR, but it's worth referencing again. Most security managers and CISOs likely have been introduced to SOAR solutions by now, but if you haven't here is the basic rundown of what a SOAR is designed to do.

SOARs take alerts from a detection/alerting tool, generally a SIEM, and using APIs gathers data from a variety of sources to "enrich" alerts. It then follows predefined playbooks (aka runbooks) to take automated or semi-automated actions to either fully investigate and respond to an alert or get the alert ready for analyst investigation. SOAR solutions are not intended to replace detection/alerting technologies – or even SIEMs for that matter. Instead, they act as a virtual analyst with the intent to improve analyst, and thus SOC, efficiency.

You should rely on SOAR platforms that deliver robust reporting and business intelligence. Security operations teams no longer need to rely on lengthy, manual efforts for reliable metrics. KPI dashboards provide a clear view of cases being worked, as well as SOC mean time to detect, mean time to respond and dwell time so teams can more easily identify ways to improve productivity and effectiveness. And perhaps most importantly, security orchestration gives SOC management the tools they need to demonstrate the value security operations brings to the organization overall.

For more information, visit siemplify.co.