MEASURING EFFECTIVENESS AND RETURN ON INVESTMENT OF A MANAGED SOC SERVICE

Contents

	Page
• Abstract	3
• The Problem	3
• The Metrics	4
• Incident Volume	5
• Time to assignment (MTTA)	5
• Time to triage (MTTT)	6
• Time to Closure (MTTC)	8
• Incident severity ratios	8
• Number of incidents escalated to the customer	9
• Reason for escalation	9
• Real incidents vs false positive incidents	10
• Conclusion	11

Abstract

Metrics, when employed in a Security Operations Centre (SOC), are vital for ensuring adherence to Service Level Agreements (SLAs) and for evaluating the effectiveness and efficiency of cybersecurity efforts.

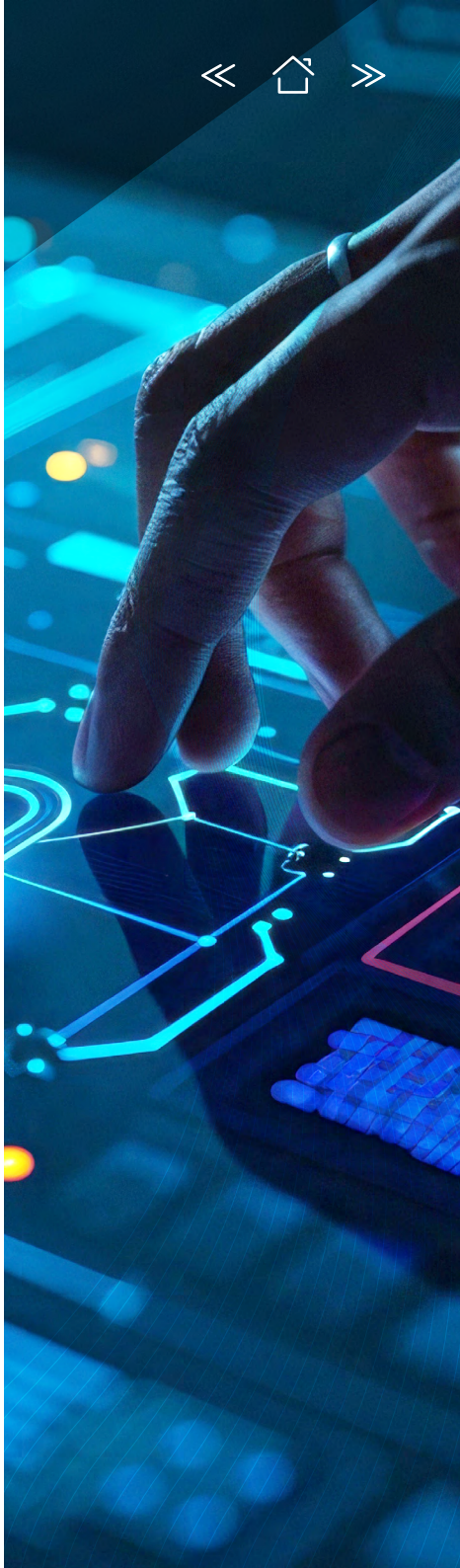
They help in proving the value of investment in cybersecurity to customers and their stakeholders, and in identifying potential areas for improvement. Through analysing specific metrics, SOCs can optimise their operations, enhance security postures, and provide tangible evidence of their contribution to the organisation's overall security strategy.

This White Paper discusses some of the metrics that can be used for these purposes.

The Problem

Without clear metrics, it is difficult to measure the effectiveness of a SOC, identify areas of improvement or demonstrate return on investment for the customer. However, poorly designed metrics can inadvertently lead analysts to focus on improving those metrics rather than actual performance, potentially causing a decline in the quality of their work as they aim to meet these misleading benchmarks.

It should also be noted that some metrics may not be fully in the control of the SOC provider, but the organisation as a whole.



The Metrics

Some metrics that can be used to measure the effectiveness and return on investment of a SOC include:

- Incident volume
- MTTA (mean time to assignment)
- MTTT (mean time to triage)
- MTTC (mean time to closure)
- Incident severity ratios
- Incidents escalated to customer
- Reason for escalations
- Real incident vs false positive ratio (either absolute number, or time spent triaging)

Incident Volume

At the start of any SOC engagement, incident numbers are often high due to the initial, unrefined state of security settings and lack of precise tuning to accurately detect genuine threats. But as the SOC team refines and optimises the security environment (through tuning and adding new detection rules based on identified security gaps, for example) the number of false positive incidents typically decreases. Introducing new data sources and analytical tools might temporarily increase incident volume, but a well-tuned system should, over time, exhibit a downward trend in the number of incidents, indicating an effective and maturing security posture.

This number is then also used to record effectiveness of the SOC as a ratio of 'Incidents escalated to customer' or 'True Positives'

Time to assignment (MTTA)

This is the time it takes an analyst to get initial eyes on an incident; from when an incident is reported until an analyst first reviews it. This metric, known as MTTA (mean time to assignment), captures the time to the initial assessment, but *not* the full investigation time.

It includes confirming the incident's priority level and is used to gauge the speed of a SOC's response, measured as an average across all incidents to reflect overall responsiveness. It's also reported as Mean Time to Respond (MTTR).

MTTA helps in assessing a SOC's efficiency and responsiveness in initiating the incident response process. By tracking MTTA, a SOC can identify bottlenecks in the incident response workflow and improve procedures to ensure timely intervention, ultimately minimising potential damage from security threats.

Time to triage (MTTT)

The Time to Triage (Mean Time to Triage) metric in a SOC is a crucial indicator of how efficiently security analysts assess and address incidents. It accounts for the time from an incident's identification to its initial management, focusing on prioritisation without being affected by external delays, such as customer response times.

MTTT measures the time an analyst takes in deciding whether to close an incident as false, initiate containment or escalate it for more information or customer action.

This metric does not include the time it takes for the customer's response, as this is outside of the SOC's control.

A lower MTTT indicates a faster conclusion on the potential threat has been achieved, which could include containment, which is essential for minimising the impact of genuine threats. Of course, this metric benefits from thorough environment knowledge, streamlined procedures, automation and adequate resourcing.

Time to Triage is important as in the case of a real security threat, the lower this number the quicker containment actions can occur.

This metric is highly correlated with the incident volume metric, the lower the incident volume the less chance an incident will sit in a queue before it can be triaged. For this reason, it is also highly influenced by tuning activities.

MTTT can be improved by:

- Maintaining a knowledge base of a customer's environment, reducing the need to search for information
- Playbooking and streamlining response actions
- Automated enrichment of Indicators of Compromise (IOCs)
- Scripting and automated repetitive analyst actions
- Improving incident layouts to better present information to analysts

Many of these actions can be greatly enhanced using Security Orchestration, Automation and Response (SOAR) platforms.

An increasing MTTT rate may signal the need for greater process optimisation or additional staffing.

Time to Closure (MTTC)

The Time to Closure (MTTC) indicates the overall time to close an incident. This measurement includes all the time taken to resolve and close a security incident, including the time taken by the IT teams of the client's organisation.

This allows an organisation to identify where they need to strengthen response within their own teams, to ensure that rapid identification of malicious activity by the SOC is not then hampered by lack of priority within supporting teams.

Incident severity ratios

An incident severity ratio allows the SOC team to prioritise which incident needs to be triaged first, especially in the scenario where multiple incidents emerge simultaneously.

Ensuring incidents are correctly classified by severity is crucial for effective response, necessitating well-tuned tools. Though not a direct measure of return on investment, appropriate severity classification enhances SOC responsiveness. Ideally, there will be more low-severity incidents than high-severity ones, allowing for prioritised handling of more critical threats.

As a target for this metric, the expectation is a higher count of low-severity incidents, as it allows the SOC to focus resources on addressing the most critical threats first, enhancing overall security posture and response efficacy.

Number of incidents escalated to the customer

An effective SOC should quickly distinguish false positives from genuine incidents. In the early days, incident clarification might require customer engagement, but over time, building a comprehensive knowledge base reduces this need. Similar customer input is also needed when new security monitoring rules are put in place,

Streamlining processes to identify duplicate incidents prevents redundant escalations. Genuine incidents with no significant impact, subject to customer agreement, may not need escalation. However, impactful incidents, or those requiring further response actions, still require escalation for further action.

An Incident Escalation Metric can track the percentage of total incidents that require direct customer intervention for clarification, additional context or further action. Such a metric helps assess the SOC's efficiency in handling incidents independently - and the effectiveness of its knowledge base in reducing dependency on customer input over time.

Reason for escalation

Recording the reasons for escalation is worthwhile. Incidents escalated due to additional knowledge being required, or where customer response actions are required, can be reduced over time by building an effective knowledge base, and by securing the ability to carry out response actions within the SOC.

Reasons for escalation can typically be:

- Information required
- Response actions needed
- Customer awareness

As a trend, you should expect a shift over time towards “customer awareness” being the dominant reason for escalation.

Real incidents vs false positive incidents

The effectiveness of SOC tuning can be assessed by recording and comparing the ratio of actual incidents to false positives. When tuning to reduce false positives isn't feasible, measuring time needed to triage real versus false incidents becomes a valuable alternative metric, as well as tracking the reason for closing.

Better closure categorisation can help see where effort is being used in investigating alerts and identifying improvements, for example adding resolution reasons such as Confirmed Activity, Expected Activity, Rule Logic Error, or Third-Party Error can provide better visibility of how efficiently the SOC is operating.

To compensate for the inability to tune away false or benign positives, SOCs can implement automation, playbooks and processes. These tools expedite false positive dismissal, allowing analysts to concentrate on genuine threats, optimising SOC efficiency and response times to real incidents. A good example of this would be by automatically checking if there was a supporting, approved service request for the activation of a privileged administration role, which would mean the alert could be automatically closed as 'Confirmed Activity'. This of course leads to other metrics, such as number of incidents closed by automation and time savings through automation.

Conclusion

Metrics, when applied in SOCs, are crucial for assessing effectiveness, guiding improvements and demonstrating value. They enable proper tracking of incident response times, accuracy in threat identification and efficiency in resource allocation.

By analysing the metrics, SOCs can fine-tune their operations and optimise security posture, underscoring the continuous evolution required to tackle emerging cybersecurity challenges.

And as cybersecurity threats evolve, metrics must adapt, focusing on more sophisticated detection methods and incorporating AI-driven analytics for deeper insights.

This evolution promises to enhance current capabilities and anticipate future threats, ensuring SOCs remain a step ahead in protecting digital assets.

CREST