SOC Metrics

Cheat Sheet

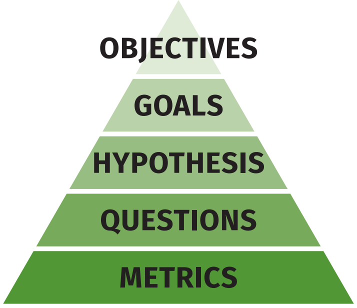
SANS
CYBERSECURITY
LEADERSHIP

Created by Mark Orlando, co-author of
LDR551:™ Building and Leading Security Operations Centers™
sans.org/ldr551

Security Operations Center (SOC) metrics are essential for justifying resource allocation, validating processes, and identifying areas for improvement. This cheat sheet outlines a strategy for creating SOC metrics that are both thorough and aligned with your organization's mission and security goals.

METRICS HIERARCHY

The most effective way to gather comprehensive metrics is through a top-down approach, beginning with overarching business security objectives and translating them into measurable goals for the SOC.


OBJECTIVES
GOALS
HYPOTHESIS
QUESTIONS
METRICS

DOCUMENT

Document each metric's unit of measure, purpose, type, target or threshold, data sources, data sinks, and sampling rate.

EFFECTIVE METRICS ARE:

- Consistently measured
- Inexpensive to collect
- Expressed as a cardinal value or percentage that can increase or decrease
- Based on at least one clear unit of measure
- Actionable and tied to decision-making
- Time-bound

SOURCES AND SINKS

Sources provide the data needed to measure a process.

Sinks are where those measurements are stored.

⚠ TIP

Don't let tools dictate your metrics just because certain data points or reports are easy to extract. Focus on what you need to measure first—then find the best way to gather the data.

⚠ TIP

Measurement frequency should match the process's rate of change, for example, alerts per day or incidents per month.

PITFALLS TO AVOID

- Prioritizing quantity over quality
- Defining metrics without clear action paths
- Using vague or ambiguous measurements
- Misaligning metrics with business objectives
- Using metrics punitively
- Relying on static, non-evolving metrics

TYPES OF METRICS

- Financial
- Percentage-based
- Absolute value
- Timing-based
- Trend (Increasing)
- Trend (Decreasing)
- Key Performance Indicators (KPIs)
- Objectives and Key Results (OKRs)

SOC Metrics

Cheat Sheet

SANS CYBERSECURITY LEADERSHIP

SOC DOMAINS AND FUNCTIONS

The SOC Capability Maturity Model (SOC-CMM) defines five essential domains: business alignment, people, process, technology, and services. Used alongside the SOC functional model outlined in the LDR551 course, this framework supports the development of comprehensive metrics across key SOC capabilities.

BUSINESS

These metrics assess the satisfaction levels of internal stakeholders regarding SOC services, budget planning and expenditures, as well as the alignment of SOC services with key business drivers.

PEOPLE

People metrics track hiring timelines, turnover rates, employee satisfaction, training effectiveness, knowledge management, and how well knowledge, skills, and abilities (KSAs) align with the competencies required for SOC roles.

PROCESS

Process metrics assess case workflow efficiency, playbook completeness and validation, use case management, detection engineering, and the overall effectiveness of automation within the SOC.

TECHNOLOGY

Technology metrics cover the maintenance and optimization of SOC tools, the availability of technology-delivered SOC services, and the overall capacity and performance of the SOC infrastructure.

SERVICES

Service metrics span areas such as monitoring coverage, time-based assessments for alert reviews and incident response, and both qualitative and quantitative measures of detection and response effectiveness. They also include threat hunting coverage and outcomes, as well as vulnerabilities addressed. These metrics can be further broken down by specific technical functions within the SOC, as outlined below.

- DATA COLLECTION
- DETECTION
- TRIAGE & INVESTIGATION
- INCIDENT RESPONSE & FORENSICS
- THREAT INTELLIGENCE
- TESTING & VALIDATION