Unlock The Potential of Your Underperforming SOC

ENHALO

Introduction

Many businesses have established Security Operations Centers (SOCs) as dedicated hubs for monitoring, detecting, and responding to security incidents to counter an ever-growing array of sophisticated cyber threats effectively. However, despite investing significant resources in building and maintaining a SOC, some organizations find their SOC is not delivering the desired outcomes.

This document aims to provide insights on everyday use case challenges and guidance on unlocking your SOC's performance to its full potential to enhance your cybersecurity posture.

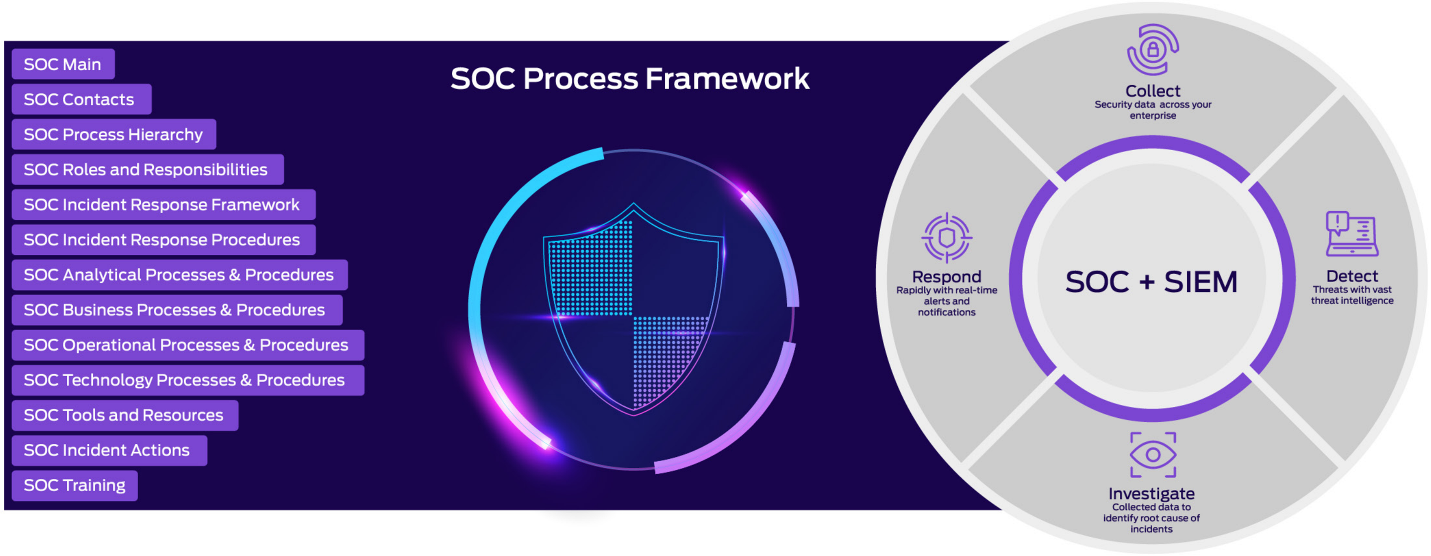
> With 103 days before attacks are even detected, it is clear that there is room for doubt about the effectiveness of SIEMs and how they are staffed.
>
> — Gerhard Conradie, ENHALO
> Co-Founder and Global Head of Solutions Architecture

Understanding The SOC's Purpose

A SOC serves as a centralised nerve center for monitoring and responding to security events.

The SOC uses a Security Information and Event Management (SIEM) system to see what's happening in real-time – analyzing data from different sources and finding patterns to determine the most likely threats. The SIEM then alerts the SOC team about events that might indicate a security incident.

A well-functioning SOC combines skilled personnel, cutting-edge technology, and robust processes operating together to defend against cyber threats, detect potential incidents, investigate security alerts, and mitigate the impact of breaches.



SOC Process Framework

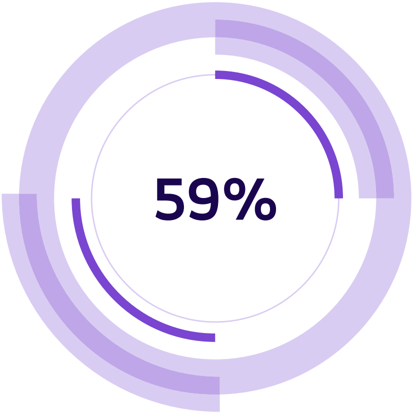
- SOC Main
- SOC Contacts
- SOC Process Hierarchy
- SOC Roles and Responsibilities
- SOC Incident Response Framework
- SOC Incident Response Procedures
- SOC Analytical Processes & Procedures
- SOC Business Processes & Procedures
- SOC Operational Processes & Procedures
- SOC Technology Processes & Procedures
- SOC Tools and Resources
- SOC Incident Actions
- SOC Training

Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence
Investigate
Collected data to identify root cause of incidents
Respond
Rapidly with real-time alerts and notifications
SOC + SIEM

How to Create a SOC Safety Net with SOC Assurance

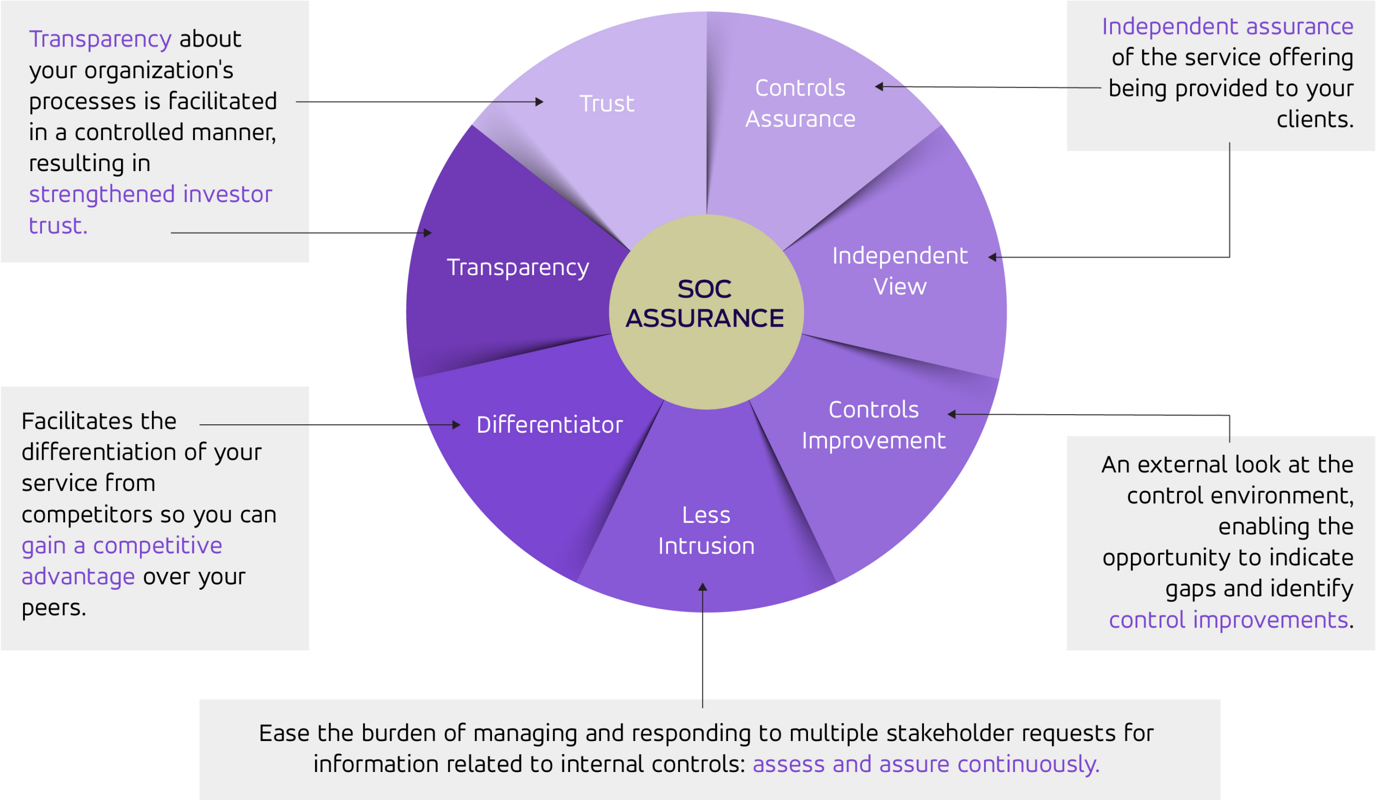
Suppose your SOC lacks defined key performance indicators (KPIs) or monitoring and reporting mechanisms. In that case, it becomes challenging to evaluate its effectiveness, identify areas for improvement, and demonstrate value to stakeholders.

ENHALO's SOC Assurance Service involves simulating various events and scenarios to assess the effectiveness and readiness of a Security Operations Center (SOC). These simulations evaluate whether the SOC can detect, respond to, and mitigate the risk of missed alerts or gaps in the system.



A Ponemon Institute study showed that 59% of respondents had data breaches caused by one of their third parties, and 42% of those had been in the last 12 months.

The summary below highlights some of our customers' advantages when participating in this independent assurance service.



Transparency about your organization's processes is facilitated in a controlled manner, resulting in strengthened investor trust.

Independent assurance of the service offering being provided to your clients.

Facilitates the differentiation of your service from competitors so you can gain a competitive advantage over your peers.

An external look at the control environment, enabling the opportunity to indicate gaps and identify control improvements.

Ease the burden of managing and responding to multiple stakeholder requests for information related to internal controls: assess and assure continuously.

Use cases for “my SOC is not working”	What causes the use case challenge most of the time	What are the best practice solutions
The SOC fails to detect security incidents promptly or consistently misses critical alerts.	Ineffective or slow incident detection: There is a problem with the monitoring tools, detection mechanisms, or the expertise of the SOC analysts.	Threat scenario development: ENHALO’s SOC Assurance Service starts by developing realistic threat scenarios that reflect potential risks and attack vectors relevant to the organisation. These scenarios can be based on known threats, emerging trends, or industry-specific risks.
Analysts suffer from alert fatigue as the SOC is inundated with many false positive alerts, distracting them from focusing on legitimate threats.	High false positive rates indicate a need for fine-tuning detection rules or improving correlation and filtering mechanisms.	Simulated attack execution: Once the threat scenarios are defined, the SOC Assurance Service executes simulated attacks to replicate the behaviour and techniques of real-world threats. These attacks could include phishing campaigns, malware infiltration, network breaches, or other common attack vectors.
The dwell time between the initial compromise of the system and its detection is too long, and breaches are going undetected.	Limited integration and automation: If your SOC lacks proper integration of tools or fails to automate routine tasks, it can result in inefficiencies and increased response times. Threats go undetected for an extended period, potentially resulting in data breaches or significant damage because SOC is not minimising dwell time through proactive monitoring and swift incident response.	Monitoring and detection: During the simulation, the SOC analysts and monitoring tools actively monitor the network, systems, and relevant security devices to detect any signs of the simulated attack. This phase assesses the SOC’s ability to identify suspicious activities, anomalies, or indicators of compromise associated with the simulated attack.
The SOC team solely relies on automated alerts, leaving emerging or novel attack techniques undetected until the automated system updates.	Inadequate incident response: Gaps in processes, procedures, or resource allocation leads to prolonged system compromise, data loss, or further spread of threats.	Alert handling and analysis: As the simulated attack progresses, the SOC analysts receive alerts generated by the monitoring tools. SOC Assurance evaluates how well the analysts handle the alerts, including their ability to triage, investigate, and determine each alert’s severity and potential impact. This stage assesses the analysts’ expertise, response times, and decision-making capabilities.

SOC analysts are not knowledgeable about the latest threats and technologies.	Insufficient staff training and expertise: SOC analysts not receiving regular training hinder the effectiveness of incident detection, response, and overall security operations.	Incident response and mitigation: If the simulated attack is successfully detected and escalated as an incident, the SOC Assurance Service evaluates the SOC's incident response capabilities. This includes analysing how effectively the SOC responds to the incident, coordinating different teams, and applying incident response procedures and playbooks.
Insufficient collaboration and communication between IT, incident response, and management leads to missed incident and remediation action.	Inadequate collaboration and communication: Lack of coordination or siloed information leads to missed opportunities for timely incident response and remediation. A well-functioning SOC requires seamless collaboration and communication among various teams, including IT, incident response, and management.	Communication and Reporting: SOC Assurance also examines the communication and reporting practices within the SOC. This involves evaluating the clarity and timeliness of communication between the SOC and relevant stakeholders, such as IT teams, management, or external incident response partners. Reporting mechanisms and documentation of the incident response process are also assessed.
There are never any post-incident analysis investigations.	Failure to learn from incidents: SOC team does not conduct post-incident analysis, share insights, and implement necessary improvements and may very well repeat the same mistakes and fail to adapt to evolving threats.	Post-simulation analysis: The SOC Assurance Service gives a detailed event analysis after the simulation. The SOC's performance is reviewed, strengths and weaknesses are identified, and actionable recommendations for improvement are provided. This analysis will include evaluating the effectiveness of tools, detection rules, processes, and training programs. Based on the findings, the organisation can implement necessary improvements and enhancements to the SOC's infrastructure, processes, and training. The simulation process should be repeated periodically to track progress, verify the effectiveness of implemented changes, and ensure continuous improvement.