Security Operations Center (SOC) Assessment & Training Service

Optimizing Security Operations Performance

What is the SOC Assessment & Training Service?

SOC Assessment & Training is a tailored service to effectively assess an organization's SOC team skills and procedures, properly train it and make sure it is fully skilled and capable of acting as the organization’s guard dog, detecting cyber vulnerabilities on time, and putting in motion the proper prevention procedures.

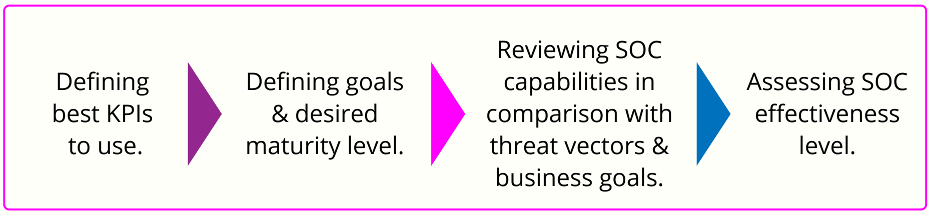
This service allows organizations to quickly mature their security monitoring and incident response capabilities to take them to the next level. HolistiCyber's method is based on years of nation-state-grade cyber defense, SOC consulting, front-line incident response experience, and threat intelligence expertise. We are uniquely positioned to provide organizations with an industry-leading approach to defining their SOC program.

A strong SOC allows security teams to detect threats and data breaches before they escalate into serious security hazards. By identifying events that require security teams' attention and receiving alerts, they are in a stronger position to respond to attacks before they cause widespread damage.

SOC Assessment

HolistiCyber's nation-state-grade domain experts conduct an optimization assessment, including key performance indicators (KPIs) definitions and assessments of program maturity levels. They provide enhancement and optimization recommendations for processes and technological tools to support the SOC's daily operations.

The SOC Assessment involves a review of documentation, discussions with staff, and a manual review of the organization's SOC. A detailed, tailored report is provided with the issues discovered and their impact, along with recommended steps for improvements.
Meetings - experts gather information on existing SOC operations and share best practices.
Detailed reports - a detailed, tailored report, documentation analysis, and follow-up discussion.
Prioritized areas for optimization - The assessment includes a roadmap of prioritized recommendations to strengthen and optimize the SOC’s ability to detect and respond to cybersecurity incidents quickly and effectively.



Defining best KPIs to use.

Defining goals & desired maturity level.

Reviewing SOC capabilities in comparison with threat vectors & business goals.

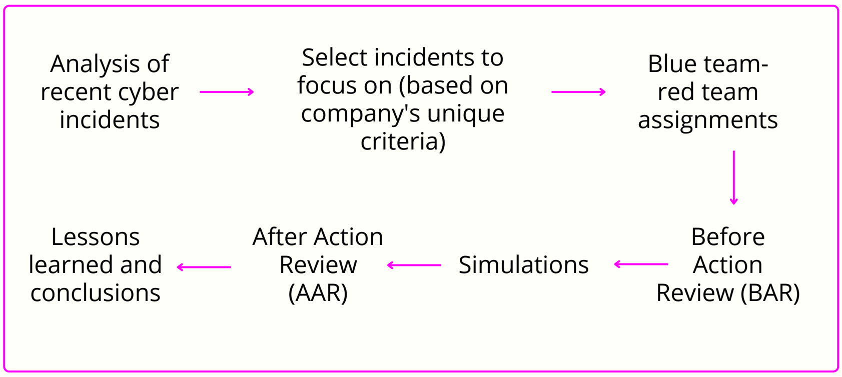
Assessing SOC effectiveness level.

WHAT SHOULD YOU EXPECT?

- **A better trained, better prepared, more vigilant, and more aware SOC team.**
- **Improved detection and response times to cyber threats and breaches.**
- **Increased automation in alerts, detection and response processes.**
- **Optimized processes, procedures and technological tools to support the SOC in its daily operations.**
- **Alert workflow creation.**
- **Establishing proper logging processes and procedures.**
- **Training for continuous monitoring and collecting relevant logs.**
- **In-depth assessment and identification of gaps in cybersecurity operations and incident response programs.**
- **Determining maturity levels and receiving guidance to achieve the desired effectiveness of security operations.**
- **Detailed, prioritized plan to reduce organizational security risks with optimization of operations.**

SOC Training

Our domain experts will serve as the organization's SOC trainers, building a customized training plan to close any detected gaps in skills, knowledge, processes, or procedures. They provide simulations and training using repetitive and new scenarios deployed periodically. The result is creating a better trained, better prepared, more vigilant, and more aware SOC.



Analysis of recent cyber incidents → Select incidents to focus on (based on company's unique criteria) → Blue team-red team assignments → Before Action Review (BAR) → Simulations → After Action Review (AAR) → Lessons learned and conclusions

How can enterprises keep up with today's cybersecurity threats? By staying ahead of them.

According to a recent survey, 8 in 10 organizations have suffered at least one breach they can attribute to a lack of cybersecurity skills or awareness. The survey also shows that 64 percent of organizations surveyed experienced attempted cyber attacks that resulted in the loss of revenue, recovery costs, and fines.

The increased volume and sophistication of security events, incidents, and false positives mean security teams are already over-extended, wading through a sea of alerts, and unable to afford the time to review their procedures and skills and to implement positive changes. The lack of security resources makes assessing SOC capabilities and current effectiveness challenging. When embedded in a daily routine of alert fatigue, it's challenging to see the gaps that may exist or train personnel to deal with them. Simply keeping up with the latest trends, technologies, processes, and threat intelligence becomes a luxury few can afford.

A vigilant SOC team is crucial in today's ever-evolving cyber threat environment. However, building and maintaining a SOC is both complex and expensive. These are why organizations seek to proactively engage with experts who can assess, train, and advise them on the best approach to implement an effective SOC.

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.

"HolistiCyber brought a very rarely seen holistic capability versus other offerings. From day one, they understood the "big picture" risks of our business processes and practices, strategic assets, physical security, and internal and external threats."

CISO, Financial Services Company, USA