Unit 42 SOC Assessment

Modernize your SOC with strategic insights and expert guidance for proactive cyber resilience.

SecOps Challenges

Security Operations Centers (SOCs) are the core component defending your organization against today's complex and rapidly evolving threats, but they face many challenges. These obstacles can limit visibility, delay response, and drain valuable resources. Understanding these hurdles is the first step toward building a more resilient, high-performing SOC.

Operational Burden

SOC teams are dealing with a significant operational strain. They're overwhelmed by manual, repetitive tasks, from maintaining disparate tools and integrating systems to sifting through a constant influx of uncorrelated alerts. Furthermore, Issues with security tools and management were a contributing factor in nearly 40% of cases[1] seen by Unit 42, allowing attackers to establish footholds and escalate privileges undetected. This drains valuable resources, stifles innovation, and leaves little to no time for strategic planning or proactive security initiatives.

Expanding Attack Surface & Visibility Gaps

The rapid adoption of new technologies - driven by business innovation - is escalating your attack surface, introducing critical vulnerabilities and dangerous blind spots that fall outside existing detection funnels. In 75% of incidents, critical evidence of the initial intrusion was present in the logs but wasn't readily accessible or effectively operationalized, leading to attackers exploiting these gaps, undetected.[2] Without a comprehensive view of these expanding risks, SOCs remain reactive, scrambling to integrate data and address gaps often only discovered during an incident.

Evolving Threats & Adversary Automation

Attackers aren't just evolving. They're automating their attacks and leveraging AI to continuously refine their tactics, techniques, and procedures (TTPs). This places immense, sustained pressure on your SecOps teams. Many SOCs lack the critical time and resources to validate and update playbooks or proactively tune detections. This significantly hinders their ability to effectively keep pace with attackers and prioritize critical risk, leaving them one step behind.

Unit 42 SOC Assessment Benefits

Develop a Formidable Defense

Enhance visibility, reduce complexity and streamline detection and response to support secure innovation.

Outpace the Adversaries

Equip your SOC with insights and strategies to stay ahead of continuously evolving threats and tactics.

Drive Strategic Cyber Transformation

Transition your SOC from reactive firefighting to proactive cyber resilience, aligned to your organization's business goals.

1. Unit 42 2025 Global Incident Response Report, February, 2025
2. Unit 42 2025 Global Incident Response Report, February, 2025

A Better Approach: Unit 42 SOC Assessment

The Unit 42 SOC Assessment is more than just an evaluation. It's your accelerated path to a resilient and proactive cyber defense. We combine our extensive experience in building high-performing SOCs with unparalleled real-life incident response insights to deliver a proven framework that radically enhances your technology and processes.

A Strong Foundation for the Modern SOC

Comprehensive SOC Evaluation	Our experts conduct a deep dive into every facet of your SOC capabilities to precisely identify strengths and opportunities. We benchmark your SOC maturity against proven best practices and cutting-edge AI-driven defense. You receive immediate, actionable recommendations to strengthen your posture.
Holistic Visibility & Data Unification	Evaluate how your SOC ingests, normalizes, and uses security data across all tools – from endpoint and network to cloud and identity. Pinpoint critical gaps, eliminate complexity, and get a clear roadmap to consolidate your security telemetry into a unified platform to maximize threat detection.
AI-Driven Detection & Automation Roadmaps	We meticulously review your SOC workflows—across detection tuning, alert triage, and incident response—to uncover prime opportunities for transformative efficiency gains using intelligent automation and AI-enabled tools. This equips your SOC with the strategies and capabilities to stay decisively ahead of rapidly evolving threats.
Custom Strategic Vision & Action Plan	Partner with us to define a clear strategic vision for your modern SOC. Explore cutting-edge SOC capabilities powered by AI and automation, aligning them to your unique business goals, and get a detailed action plan to transition your SOC from reactive firefighting to proactive cyber resilience.

About Unit 42

Unit 42® brings together our world-renowned threat researchers and hunters with an elite team of security consultants to create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections offered by our products and services to stop advanced attacks. As threats escalate, Unit 42 is available to advise customers on the latest risks, assess their readiness, and help them recover when the worst occurs. For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

unit42_ds_unit-42-SOC-assessment_061825