DATA SHEET

SOC Assessment

Strengthening Security Operations for Resilience, Visibility, and Rapid Response

Deliverables

- ***SOC Capability Maturity Report***

A comprehensive evaluation mapped to global frameworks (e.g., MITRE D3FEND, NIST CSF).

- ***Gap Analysis Matrix***

Actionable insights categorized by criticality and impact.

- ***SOC Optimization Roadmap***

Practical recommendations covering quick wins and long-term initiatives.

- ***Presentation to Stakeholders***

Executive briefing summarizing findings, risks, and proposed improvements.

Key Outcomes for Your Organization

- Improved threat detection and incident response speed
- Aligned SOC operations with business risk and regulatory expectations
- Maximized value from existing security investments
- Clear direction for scaling your SOC, including hybrid or MDR integration
- Enhanced team collaboration and knowledge transfer

You can get more information at Guardians@Trellix.com.

Why a SOC Assessment?

Security Operations Centers (SOCs) serve as the heartbeat of an organization's cyber defense capability. However, with evolving threats, new technologies, and changing business demands, periodic assessments are essential to ensure the SOC remains relevant, efficient, and resilient.

Our SOC Assessment service empowers your organization to:

- Enhance detection and response maturity
- Streamline operational processes
- Integrate threat intelligence and automation
- Benchmark against global best practices (MITRE ATT&CK®, NIST, ISO 27001, CIS Controls)

Our Modernized Methodology

We apply a structured, comprehensive approach to assessing your SOC environment:

1. Pre-Assessment Preparation

Scope definition, stakeholder alignment, and review of existing architecture, tools, and processes.

2. Capability & Maturity Evaluation

Review of people, processes, and technology. Capability benchmarking against industry standards and threat-informed defense models.

3. Operational Deep Dive

Event Intake & Enrichment, Threat Monitoring & Detection, Triage & Escalation, Incident Response Process, Threat Hunting, Use of Automation, Orchestration, and AI/ML, Collaboration and Reporting.

4. Workforce Readiness

Shift scheduling, skills evaluation, and workload analysis. Recommendations for training, certifications, and team structuring.

5. Gap Analysis & Roadmap

Gap prioritization based on business impact and threat exposure. Tactical and strategic roadmap to elevate SOC maturity.