# Security Operation Centre (SOC) Maturity Assessment

Gain a defensible, evidence-based view of your SOC's maturity to guide planning, investment, and operating-model decisions

As cyber threats evolve, SOC performance must continually mature across people, process, and technology. A SOC Maturity Assessment provides a structured, independent review of your detection and response functions, helping you understand current capability, identify uplift opportunities, and reduce operational risk. Lumen's assessments are tailored to meet you where you are today, ensuring you neither overinvest in unnecessary capability nor underinvest in areas that expose your organisation to risk.

## What is the Lumen SOC Maturity Assessment?

Lumen's SOC Maturity Assessment delivers a benchmarked, standards-aligned review of your SOC across the core pillars of people, process, and technology. It identifies gaps, risks, and improvement opportunities, providing a clear roadmap to uplift detection and response effectiveness.

**People**

We assess SOC roles, responsibilities, governance, and escalation ownership, as well as internal skills. You'll gain clarity on whether the SOC's people model is capable of sustaining consistent operations.

**Process**

We review SOC governance, incident response workflows (detect, triage, investigate, contain, recover), and operational routines. You'll gain insight into the maturity and repeatability of your processes and the areas requiring uplift.

**Technology**

Leveraging insights from Lumen's Black Lotus Labs, we evaluate your detection architecture (SIEM, EDR/XDR), orchestration (SOAR), and data quality. You'll gain a practical understanding of alert fidelity, automation maturity, and technology enhancements that offer the greatest return.

## Who is the SOC Maturity Assessment Designed for?

The SOC Maturity Assessment is best suited for:

- Organisations that already have 24×7 monitoring in place but are experiencing deteriorating alert quality, rising false positives, and uncertainty about the value of their SOC and who are seeking a clear, evidence-based view of operational strengths, gaps and risks.
- Organisations seeking alignment to frameworks and regulatory expectations to support board reporting, risk programs, and compliance obligations.
- Leaders assessing internal, hybrid, or Managed SOC operating models.

## Aligned to International Frameworks

Our methodology aligns to industry frameworks, ensuring findings are defensible and meaningful to executives, auditors, and regulators. We leverage:

- **NIST CSF:** Structuring the evaluation across the security lifecycle
- **MITRE ATT&CK:** Using a threat-informed lens to evaluate detection against adversary tactics
- **ASD Essential Eight:** Validating visibility over controls that materially impact response
- **APRA CPS 234:** Addressing governance and resilience for APRA regulated entities
- **ISO/IEC 27001:** Evaluating management system discipline and control effectiveness

LUMEN

## How a Lumen SOC Maturity Assessment Works – Process and Timeline

Our assessment follows a structured, phased process to give you a clear baseline of your SOC maturity while minimising disruption to day-to-day operations.

### Discovery Phase

- Kick-off and scoping session
- Interviews and workshops with SOC leadership and analysts
- Review of processes, playbooks, reports, and configurations
- Technology and detection-logic assessment, including ATT&CK-aligned coverage

### Analysis Phase

- Standards-aligned maturity scoring across people, process, and technology
- Identification of operational gaps and risks
- Validation workshop to confirm findings
- Development of a prioritised roadmap and practical recommendations

## Deliverables

The final report provides a comprehensive, evidence-based view of your operations and is designed for both technical and executive review. You will receive:

- An Executive Summary and Business Case Component tailored for senior stakeholders
- A maturity baseline including current-state ratings mapped to recognised frameworks
- A gap analysis of detection, triage, and response effectiveness
- A Practical roadmap for short, medium and long-term improvements
- Recommended governance and RACI models to support sustained uplift

## Benefits to Your Organisation

- Get Independent assurance and objective validation of SOC maturity
- Gain stronger certainty of your detection and response capabilities
- Achieve clearer accountability and reduce operational risk
- Leverage Data to justify future investment and transformation
- Get Better alignment between SOC services and business expectations

## Why Lumen?

Lumen combines deep operational SOC experience with independent advisory expertise. Our assessments are grounded in real-world SOC operations and enhanced by Black Lotus Labs Threat Intelligence, ensuring recommendations are practical, achievable, and contextual. We deliver honest, evidence-based insights that help leaders uplift performance and demonstrate confidence to regulators.

## Contact us to Schedule a Free Scoping Call

Book a scoping call with Lumen's security specialists to confirm your objectives. This first step gives you immediate clarity on scope and expected outcomes.

lumen.com | apac.mail@lumen.com



LUMEN