



SOCaaS Provider Evaluation Checklist

Key criteria to assess when selecting a Security Operations Center as a Service provider

Coverage Scope

- Network monitoring & threat detection
- Cloud workload protection (AWS, Azure, GCP)
- Endpoint detection & response (EDR)
- Identity & access management (IAM) monitoring

24/7 Monitoring and Response

- Round-the-clock security operations coverage
- Dedicated SOC analysts assignment
- Real-time alert triage and investigation
- Incident escalation protocols

SLAs and Response Times

- Initial response SLA (Critical: <15 min)
- Resolution timeframes by severity
- Uptime guarantees (99.9%+)
- Escalation path and procedures

Compliance Support

- SOC 2 Type II certification support
- ISO 27001 compliance assistance
- NIS2 directive requirements
- GDPR data handling & privacy

Technology Stack

- SIEM platform (Splunk, Sentinel, etc.)
- SOAR automation capabilities
- Threat intelligence feeds integration
- EDR/XDR tool compatibility

Transparency & Reporting

- Real-time security dashboards
- Monthly executive summary reports
- Incident documentation & forensics
- Threat landscape briefings

Pricing & TCO Elements

- Transparent pricing model (per asset/user)
- Contract flexibility and scalability
- Hidden costs and fee transparency
- ROI and cost-benefit analysis support

Evaluation Best Practice

Use this checklist during vendor demos and RFP processes. Request evidence, references, and proof points for each category to ensure the provider meets your organization's specific security requirements.