A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — SOC Development Optimisation and Sourcing

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner will develop tailored specifications, sourcing strategies and implementation planning for Security Operations Centre (SOC) and Critical Incident Response (CIR) services to enable clients to optimise the implementation and sourcing of these services matched to their operational context, threat exposure and risk appetite. Enterprise-wide digital technologies and services are covered.

Service Description

The work to support SOC and CIR capability implementation or optimisation draws on the following analysis activities:

- Discover and document the ICT and OT landscape and existing security provision to determine the context in which target SOC and CIR services will operate
- Undertake a risk and impact assessment. Assess the critical assets and services to be protected. Appreciate and, if necessary, augment existing risk information. Determine risk appetite, mapped to the assets and services to be protected
- Evaluate and document existing SOC and CIR capability and service provision
- Define a SOC and CIR strategy that addresses the mitigation of the identified risks and directs the achievement of target service and capability levels
- Specify the target SOC and CIR services architecture and operating model, covering the optimal balance of in-house and outsourced capability
- Undertake a market survey and evaluate implementation solutions and service options
- Develop implementation, sourcing and resourcing plans
- Document the transition plan for migration to the target SOC and CIR services

Gartner is uniquely positioned, having a detailed insight into both the demand side and supply side of the market. As a result, we can break down the complexity of the SOC and managed security services market and cloud or on-premises delivery options. The Gartner service optimises the operational impact achieved within budget and operational constraints.

Service Benefits

- Ensures extensible SOC and CIR capability specification
- Optimises the mix of insourced and outsourced services
- Maximises operational impact within budget and operating constraints
- Provides a detailed understanding of products/services minus vendor vapourware
- Accounts for trends in the product and service market
- Provides impartial vendor, product and service analysis
- Delivers what is needed to guide implementation/service procurement
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Service Features

- Specification of operational context, assets and risks to be mitigated

- Evaluation and documentation of current service and capability levels
- Specified architecture and operating model for the target services
- Comprehensive solution and service option identification and evaluation
- Cost analysis to complement service option evaluation
- Evidence-based recommendations for on-premises, hybrid or outsourced services
- Detailed planning to support implementation, transition and operation

Full List of Service Features

Range of Functional Capabilities Covered

The range of functional capabilities covered is outlined in Table 1 below:

Table 1. Range of SOC and CIR Functional Capabilities and Features

Name	Description
Detection	Detection capabilities are designed to identify attacks — via a range of analytical processes, from log analysis to user entity and behaviour analytics and vulnerabilities — using techniques such as network scanning or technical testing.
Response	Response capabilities are about reacting to an identified incident or vulnerability in a coordinated manner, aiming at reducing and mitigating its impact. The capabilities require investigating, containing and remedying issues discovered by detective activities or outside service(s).
Analysis	Analysis capabilities allow the security organisation to explore and analyse the security data and events supporting detection and response. They also allow retrospective analysis of an incident, identifying how it occurred and reviewing the response process to support continuous improvement of prevention and response.
Intelligence	Intelligence capabilities are part of an iterative process and provide the security organisation with a means to identify threats or potential threats. Threat intelligence provides the means to proactively implement countermeasures before an incident occurs or take timely corrective action during an incident.
Data management	Data Management capabilities support the full life cycle of the customer and internal data inside the SOC. This includes logs, referential data, and other data.
SOC architecture, engineering, and implementation	SOC architecture, engineering, and implementation provide the core capabilities required to provide SOC services.
Solutions operation	Solution operation capabilities are required to operate and support on a day-to-day basis the technical solutions and infrastructure supporting the security services.
SOC management and coordination	SOC management and coordination capabilities ensure the SOC is continually aligned with the wider business and has the resources needed to succeed, collaborate and deliver services efficiently. Additionally, it should optimise its own services and respond to offensive and defensive capability trends and changes in the threat, vulnerability and asset landscape.

Market Trend Evaluation

Gartner monitors and often sets the trends within the technology market. We are positioned to ensure analysis and consideration of offensive and defensive capability trends, including:

- Emergent threats and malware evolution
- Security analytics (AI, machine learning)
- Security orchestration and automation
- Mobile security services
- Integration of cloud service security
- IoT/OT security
- Managed detection and response

Threat Intelligence Services Frameworks and Templates for Accelerated Delivery

Gartner supports the analysis with a detailed three-level SOC and CIR service analysis framework. This supports a structured, in-depth and efficient analysis of the functional domains set out in Table 1 above.

Project Approach

Phase 0: Project Initiation

Project objectives, form of deliverables, engagement stakeholder engagement, information sharing and coordination planning set or validated.

Phase 1: Discovery and Current State Definition

Gartner uses predefined templates to rapidly capture and document key aspects of an enterprise's operating context, as well as ICT and OT service architectures. Cyber security and ITSM capabilities and services, focused on those that integrate with SOC and CIR services, are identified and documented.

Key assets and services to be protected are identified. Threat, vulnerability, and risk information are collated to determine exposure and levels of risk appetite and to guide the specification of the target SOC and CIR services.

If SOC and CIR services are in place, their capability maturity levels are assessed.

Phase 2: Gap Analysis and Target Service Specification

A strategy is developed that addresses the mitigation of the identified risks and directs the achievement of target service and capability levels.

Specification of the target SOC and CIR services includes:

- A conceptual-level architecture that covers the following service functions:
  - Detection, Response, Analysis and Intelligence functions
  - Data architecture and management
  - SOC and CIR service architecture and engineering, and SOC operational support and management
- An operating model covering insourced, outsourced and hybrid operation aspects
- A workshop to validate the Target State Definition

Phase 3: Market Survey, Solution Option Evaluation and Planning

Gartner will undertake a market survey and evaluate implementation solutions and service options, develop implementation, sourcing and resourcing plans and document the transition plan for migration to the target SOC and CIR services.

Project Schedule

The time frame for a SOC Optimisation and Sourcing project varies depending on the organisation size and complexity. A typical schedule is shown below.

- Phase 0: 2 days
- Phase 1: Discovery and current state definition: 3 weeks
- Phase 2: Gap analysis and target service specification: 3 weeks
- Phase 3: Market survey, solution option evaluation and planning: 4 weeks