A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Cyber Security Function Optimisation

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner‘s cyber security function optimisation service helps clients address current and future cyber security threats and risks by planning for future improvements to the target cyber security operating model. Gartner’s security capabilities and operating model framework are used to modernise a client’s cyber security function.

Service Description

Gartner can help organisations modernise and optimise their cyber security function by addressing evolving and increasing cyber security risks and threats by utilising a consistent and consolidated target operating model.

The cyber security function needs to consider several dimensions, including:

- Organisations' business strategic drivers and programmes
- Existing cyber security-related mission statements, policies, capabilities and already planned initiatives
- Service governance and service delivery to underlying organisational structures
- Impacting regulations, technology trends and opportunities for the cyber security Function
- Industry and market perspectives and best practices on the cyber security function

The service and engagement can be approached in the following manner:

Phase 1 — Discover and evaluate the current cyber security operating model

Gartner will need to understand the critical IT infrastructure and business functions as well as identify key required capabilities in scope according to Gartner’s cyber security capabilities and operating model pillars.

Phase 2 — Determine cyber security target operating model

Gartner will define the client’s cyber security target operating model (TOM) using Gartner’s operating model pillars and security capabilities in scope for the engagement.

Phase 3 — Plan and report the transformation roadmap for the target operating model

Gartner will produce a roadmap outlining the opportunities and activities that are recommended to form the cyber security target operating model over a suggested timeline.

Service Benefits

- Stakeholder alignment on vision, objectives, security TOM and roadmap
- Mature and improve corporate strategy, culture and business drivers
- Improved and optimised cyber security capabilities (function)
- Bird’s eye view on security capabilities and potential gaps
- Confidence that leading practices are baked-in from market insights
- Clear and shared defined accountabilities and priorities
- Optimised resource allocation and demonstrable value for money
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Service Features

- Exposure to Gartner's research-based cyber security capabilities
- Introduction to Gartner's research-based operating model pillars
- Composable services permit the combination of any/all phases/components
- Flexible scope to align with specific business areas
- Industry-leading research for cyber security used in analysis/evaluation
- Enhance the organisation's cyber security ecosystem

Full List of Service Features

Phase 1 — Discover and evaluate the current cyber security operating model

- Gartner will discover the current state and requirements to manage the internal and supplier ecosystem of the cyber security operating model, understanding the needs of the organisation to its business objectives and regulatory and legal requirements
- Gartner will need to understand critical IT infrastructure, critical business functions and applications and to identify key required capabilities (functions/services, technologies, resources) in scope according to Gartner cyber security capabilities and operating model pillars
- Potentially, the organisation may wish to conduct threat modelling exercises to identify relevant cyber threats, most relevant threat actors and threat scenarios. Identify and prioritise Tactics, Techniques, and Procedures (TTPs) of most relevant attacker groups

Discover the current context and security operating model.

- Perform and document an objective SWOT analysis of the current operating model leveraging Gartner cyber security capabilities and operating model framework and best practices for comparison
- Set the cyber security function's target maturity level regarding risk profile and ambitions
- Identify initial recommendations

Phase 2 — Determine cyber security target operating model

Gartner will define the client's cyber security target operating model using Gartner's operating model pillars and security capabilities, which are in scope by:

- Providing Gartner's outside-in perspective on cyber security trends, benchmarks, organisation, key services, and capabilities
- Develop the organisation's target operating model (scope, activities, key functions/services/tech capabilities, sourcing options, organisational structure...)
- Size cyber security function team (roles, number of FTEs required), identify missing resources & skills for in-scope capabilities
- Refine the TOM through workshops with the organisation

Phase 3 — Plan and report the cyber security transformation roadmap for the target operating model

Gartner will produce a detailed roadmap outlining the opportunities and activities that need to be carried out to form the cyber security target operating model over a suggested timeline of 6, 12, 24 or 36 months.

- Identify key projects and initiative
- Create an actionable roadmap over 2-3 years that takes into account already committed projects, resources and initiatives
- Perform a macro-estimate of the implementation cost of the target operating model selected
- Provide a summary of key findings, recommendations and next steps

Project Approach

Project initiation

- Conduct a kick-off meeting to ensure an understanding of the project objectives, scope, schedule, milestones, roles, responsibilities and required resources.
- Discuss and identify any anticipated risks and mitigation plans based on lessons learned from past experience
- Identify key people and stakeholders required for the discovery and analysis phase

Deliverables

- Kick-off presentation and project schedule

Phase 1 — Discover and evaluate the current cyber security operating model

- Perform discovery and scoping workshop
- Create an initial proposal for in-scope cyber security capabilities and a services structure
- The following steps are for threat modelling to establish Tactics, Techniques, and Procedures (TTPs) to be overlayed toward the security capabilities and operating model pillars, which is optional:
  - Gather intelligence through open-source intelligence, social media intelligence, human intelligence and technical intelligence-(this step is optional)
  - Identify specific threats and associated threat actors, including their goals, capabilities and modus operandi (TTP) (this step is optional)
  - Identify and map the threat actors and scenarios specific to critical business functions (e.g., up to 5) (this step is optional)
  - Describe the three most likely attack scenarios and TTPs (this step is optional)

Deliverables

- Cyber threat assessment, including attacker TTP analysis (this is optional)
- Cyber security capability map, services structure and design principles

Phase 2 — Determine cyber security target operating model

- Conduct workshops to define and align:
  - Cyber security strategic focus areas
  - Cyber security services and capabilities
  - For example, required skills/people
  - For example, partner ecosystem and sourcing options
- Document cyber security target operating model covering:
  - Services and capabilities
  - Processes and services
  - Role Model and Responsibilities (RACI matrices)
- Required resources and skills
- Deliver high-level recommendations for mitigating identified gaps

Deliverables

- Target operating model for in-scope cyber security capabilities, including gap assessment (e.g., services, resources, skills, KPIs) with respect to the current state

Phase 3 — Plan and report the cyber security transformation roadmap for the target operating model

- Generate a high-level roadmap and deployment plan for the implementation of the target operating model
- Document and prioritise key initiatives and success and performance metrics
- Deliver final report
- Prepare and present executive briefing
- Deliver final report
- Prepare and present executive briefing

Deliverables

- High-level deployment plan and roadmap for the target operating model
- Executive summary report and briefing presentation

Project Schedule

This schedule is subject to change based on the scope of activities agreed upon engagement:

- Phase 0 — Prepare: One (1) week
- Phase 1 — Discover and evaluate: Three (3) weeks
- Phase 2 — Define target operating model: Four (4) weeks
- Phase 3 — Plan and report: Three (3) weeks