DXC Technology Cyber Defence Threat Detection & Response

G-Cloud 14

Service Definition Document

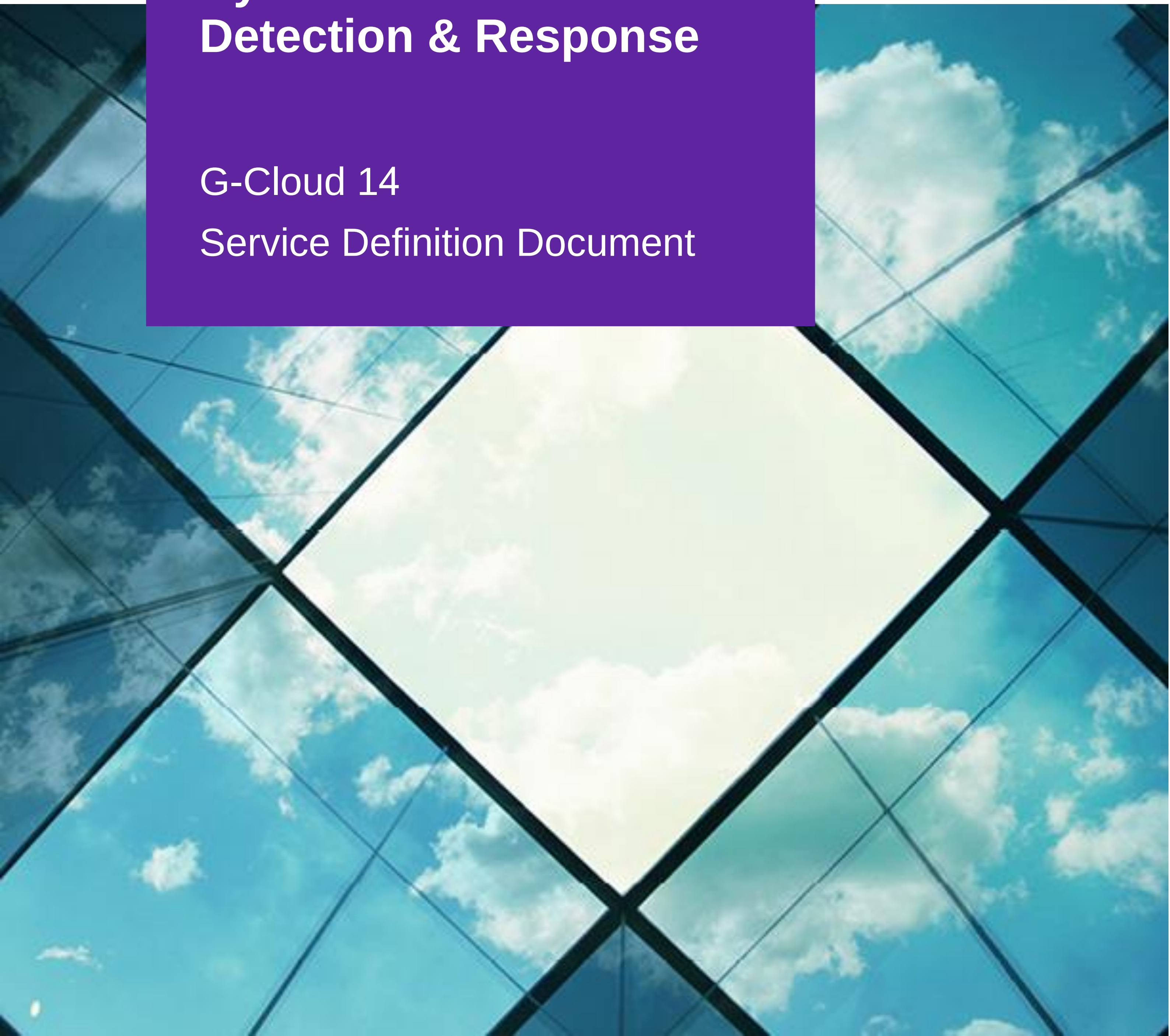
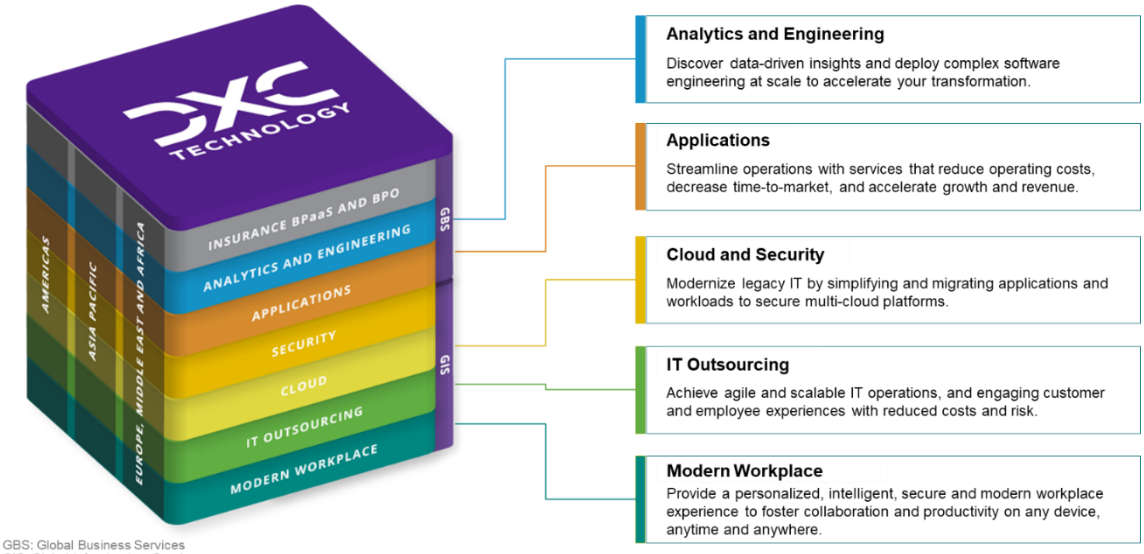


Table of Contents

1 Company Overview

DXC Technology helps global companies run their mission critical systems and operations while modernising IT, optimising data architectures, and ensuring security and scalability across public, private and hybrid clouds.

The world's largest companies as well as mid-sized clients and public sector organisations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. We have a long heritage in data centre services and management, operating over 320 global data centres and supporting 1,300+ customers. DXC provides innovative solutions to customers by leveraging strong domain capabilities and by applying leading technologies as represented in the DXC Technology stack below.



Analytics and Engineering
Discover data-driven insights and deploy complex software engineering at scale to accelerate your transformation.

Applications
Streamline operations with services that reduce operating costs, decrease time-to-market, and accelerate growth and revenue.

Cloud and Security
Modernize legacy IT by simplifying and migrating applications and workloads to secure multi-cloud platforms.

IT Outsourcing
Achieve agile and scalable IT operations, and engaging customer and employee experiences with reduced costs and risk.

Modern Workplace
Provide a personalized, intelligent, secure and modern workplace experience to foster collaboration and productivity on any device, anytime and anywhere.

GBS: Global Business Services
GIS: Global Infrastructure Services

Figure 1. DXC Technology stack

DXC is one of the few IT services providers that can orchestrate mainframes, servers, private and public clouds as an effective whole. We manage the complexities of your cloud migration strategy and apply modern operating models, practices and capabilities to build and optimise cloud for the unique needs of your enterprise. We leverage deep cloud expertise and intelligent automation to run and maintain your infrastructure, and enable business agility, resilience, and continuous improvement.

1.1 Why DXC?

WIth DXC knowledge, experience and breadth, the enterprise can be rapidly secured both inside and out.

Security operations centers on **5** continents

3,000+ DXC security professionals

1M+ cyber incidents managed per month

24x7 monitoring, detection and response

Figure 2. DXC credentials

As enterprises adapt to changing business models, security is now top of mind to protect and grow your business with confidence.

Defend against today’s cyberthreat landscape with a recognised leader in managed security and data protection services. DXC works quickly to help you:

- Automate processes to prioritise threats, incidents and vulnerabilities
- Validate and respond to security gaps quickly through orchestrated workflows
- Protect against growing threats through comprehensive threat hunting

Build a secure digital foundation that accelerates detection and response of security incidents, ensuring efficient management and visibility into the enterprise’s security posture.

2 Service Overview

The priority is to implement a 24x7x365 Security Detection service to get visibility into the threat landscape, detect attacks or intrusions and to support timely response. The solution shall be flexible to enhance it with additional services as needed.

DXC has an extensive portfolio of security services and is therefore well suited to provide the initial services on short notice and to support ACME on its mid- and long-term journey to improve their cyber defence.

2.1 What the service is

DXC Cyber Defense services help clients detect and respond to security incidents to minimise breach impact. DXC advise on and implement solutions for gathering, correlating, and analysing security data to deliver actionable information about security events, incidents or threats.

Based on the response to clarification questions and environment investigation the resultant solution will include ingestion of logs within our Cyber Threat Analysis Centre (CTAC).

DXC provide 24x7x365 monitoring and management, including:

- Protective Monitoring
- Application Monitoring
- Proactive threat analysis
- IT and OT monitoring
- Threat feeds
- Security Orchestration, Automation and Response (SOAR)
- User & Entity Behaviour Analytics (UEBA)
- Varied delivery locations, dependant on requirements
  - Near-shore or offshore
  - DXC UK Secure 24/7/365 SOC feeds into DXC CTAC in Aldershot
  - Staff Vetting – SC (mainly) with DV staff for specific roles/security domains

The service will enable identification of suspicious activities falling outside of the expected baseline. Identified anomalies will be investigated by our skilled analysts.

The team will use the alerts alongside the available threat data to;

- Categorise incidents based on most commonality relevant to client threats
- Establish efficient lines of communication and escalation criteria for serious incidents with the type and severity
- Provide advice and remediation recommendations on the observed threats

If required DXC will provide a service for end to end co-ordination of security incidents raised from various sources such as the Security Detection service.

The service includes:

- additional triage and assessment of severity

- Communication with key stakeholders to allow further investigation in order to inform and resolve.
- Further evidence collection and collation to allow deeper analysis and ensure threats are contained and eliminated when necessary .
  - Following the investigation, a report can be provided that documents the root cause and advising the client of any corrective and preventive measures that may be required.
  - DXC can also assist in the preparation of security incident metrics for reporting to the client.

2.2 Business Continuity and Disaster Recovery

DXC will ensure that the deployed solution is both resilient and highly available.

DXC also has Business Continuity plans in place for its delivery locations. These plans are regularly reviewed and tested.

2.3 Onboarding and Offboarding Support

Before using DXC Technology G-Cloud Services, a sale representative or account manager will work with you to identify the service on the Digital Marketplace that best aligns to your digital transformation objectives.

DXCs consultants can assist with the definition of G-Cloud Service architecture, service wrapper and advise you on making sure your transition runs smoothly and without disruption.

These services are available via DXC’s Lot 4 Offerings on the Digital Marketplace. When you make an order or ask for a quote, our sales support desk will acknowledge your request and give you a reference number you can use to track its progress. For quotes, our sales support desk will keep you regularly updated on progress.

Once we have agreed the service design our consultants and sales staff will work with you to develop the Call-Off Contract, during this process, DXC will confirm the required order details.

Once we have processed your order, DXC will advise you of the service start date

2.4 Service constraints

DXC endeavour to minimise any restrictions on our services. Certain specific requirements may incur additional charges and these will be detailed in the Client agreed contract and SLA.

2.5 Service Levels - Performance, Availability and Support Hours

The DXC services are provided 24x7x365.

Specific details can be negotiated and are contained within the Client agreed contract and SLA.

2.6 After Sales Support

Details contained within the Client agreed contract and SLA.

2.7 Technical Requirements

Details contained within the Client agreed contract and SLA.

2.8 Outage and Maintenance Management

Details contained within the Client agreed contract and SLA.

2.9 Hosting Options and Locations

The DXC can be managed and monitored from on shore, near shore or offshore locations. This is all dependent on the client requirements.

2.10 Access to Data (Upon Exit)

Specific details can be negotiated and are contained within the Client agreed contract and SLA.

2.11 Security

- **Staff security clearance** : Conforms to BS7858:2012
- **Government security clearance** : DXC Cyber Defence staff are cleared up to SC and can call upon Developed Vetting (DV) resources if required.

3 Service Definition

3.1 Service Features and Benefits

The Cyber Defence Detection and Response services are designed from the ground up to be flexible, agile and scaleable.

We are vendor agnostic and have experience in many different technologies.

The services are performed by highly experienced and skilled teams of consultants, analysts, and engineers.

Service features

- 24x7x365 resource locations available across the globe to provide the service, onshore, nearshore and offshore
- Integrated Threat Intelligence from DXC, 3rd party suppliers and vendors allow for greater visibility into the data stream and allow for proactive analysis and threat hunting
- Tailored Detection Use Cases and Playbooks to align to client requirements
- Cloud or on-premises based platforms depending on data residency and security requirements
- Alignment to MITRE ATT&CK framework
- End to end security incident investigation, handling and coordination
- NIST aligned processes

Service benefits

- Service provided in an agile manner on a cost-effective security detection platform
- Assistance to achieve/maintain regulatory compliance
- Vendor agnostic, allowing us to use industry leading SIEM technologies including Azure Sentinel and ArcSight
- Vendor agnostic, allowing us to use industry leading EDR technologies including Defender, Crowdstrike and Carbon Black
- Expert assistance and advice for security incident investigation, classification and coordination
- Identification and protection against new, stealthy, advanced threats and zero day malware