G-Cloud 15

Managed Cyber Defence

January 2026

Contents

Transforming Business using the Cloud

Enabling business and enterprise transformation using cloud is a complex, strategic consideration facing many private and public sector organisations. We have worked with many Central and Local Government clients to support the implementation of their business objectives using cloud technology. En

Cloud technology and services have the potential to reduce cost, remove technology bottlenecks, and facilitate rapid business innovation. As a result, for most organisations globally, adopting cloud technology has become a question of "when and how" rather than "if".

Opportunities for enterprises generally include a combination of one or more of the following:

- Implementing private and/or hybrid clouds for infrastructure and applications
- Smarter use of public cloud infrastructure for optimising existing business functions
- Using cloud for implementing new business services or digital operations
- Reducing cost by moving to consumption-based pricing models that only charge for the actual IT capacity and services used.

Migration or adoption of cloud must be properly choreographed for success. We understand the realities and the business and technical risks that should be fully considered, understood and mitigated before such a move.

Critical considerations include:

- **Alignment of business and technology objectives.** This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions
- **Availability and reliability of services.** The avoidance of operational downtime to mitigate in lost revenue, unnecessary operational cost or reputational damage that can disrupt a business' operations
- **Decentralised support structures.** The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information.

- **Data handling practices.** Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data

- **Data privacy.** Compliance with GDPR to understand where and how information can be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out of office experiences

- **Future Technology Trends.** Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

A careful assessment of an organisation's needs and different cloud service provider's controls is required, enabling concerns to be addressed and the correct path to the cloud to be selected.

As a trusted advisor PwC provides the framework, and the wealth of private and public sector experience, to consider the combination of Business, customer experience and Technology activities outlined above. There is no single answer that covers each and every client organisation; we tailor our frameworks to client circumstances to support clients:

- As a partner through the complete lifecycle of strategy through to execution

- With point business issues encountered during implementation or running the business.

Managed Cyber Defence

This section describes in more detail the service features and benefits included within this service definition document.

Managed Cyber Defence Service

Our range of managed security operations services, powered by PwC's Threat Intelligence and a follow the sun SOC model, provides clients with instant access to advanced capabilities, including:

- Managed detection and response
- Managed cloud security

Managed Detection & Response

PwC's Managed Detection & Response service is a 24/7 managed threat hunting, protection, detection and response service. It is built on PwC's Threat Management platform and features integration with leading detection and response tooling such as:

- Palo Alto Networks Cortex XDR & XSIAM
- Microsoft Defender XDR & Sentinel
- CrowdStrike
- Stamus ClearNDR
- Google SecOps.

Threat Intelligence also includes a NCSC Enhanced Incident Response retainer as standard.

Using PwC's global incident response insights combined with our threat intelligence in real-time means we are hunting for new threats as they emerge. Our automation playbooks and expert hunting skills improve threat visibility, reduce white noise and analyst workload with response times in minutes, as such breach probability is greatly reduced.

We combine unique Incident Response insights from our global network managing >600 significant events annually. Our threat intelligence gleaned from our network of 220,000 clients and our expert threat hunters into proprietary detection rules will comprehensively protect your organisation round the clock.

Managed Cloud Security

PwC's Managed Cloud Security is a 24/7 managed Cloud Native Application Protection Platform (CNAPP) service and provides full visibility across multiple cloud providers. To provide a comprehensive cloud security solution, from code to cloud, our manged cloud is powered by Palo Alto Network's Prisma Cloud platform which is enhanced with PwC's:

- Proprietary threat intelligence
- In-house analyst expertise and
- Sophisticated automatic remediation of threats and integration.

With support for all major cloud infrastructure providers, including AWS, GCP, Microsoft Azure, Oracle Cloud & Alibaba Cloud, our CNAPP based offering provides flexible access to several core cloud security capabilities including Cloud Security Posture Management, Application Security and Cloud Workload Protection.

Backed by our follow the sun SOC model, our fully managed service will provide support in identifying exposures, 24x7 incident response capability and call-off support to remediate findings.

Our Managed Cyber Defence services can be deployed in any mode - as a standalone end-to-end detection and response service; enhancing your existing capabilities or as an overlay service to complement traditional MSSP services.

Managed Cyber Defence Service Features	
Managed Detection & Response	**Managed Cloud Security**
• Fully managed support for market leading security tools: Microsoft Defender XDR / Sentinel, Palo Alto Networks Cortex XDR / XSIAM. Google SecOps, Stamus ClearNDR & many more • Proactive threat hunting and intelligence-led targeted hunting • Integrated PwC threat intelligence with daily updated behavioural rules • Security Orchestration, Automation and Response using PwC's Threat Management Portal • Automation and orchestration playbooks deliver improved detection and response	• Integration with market leading cloud infrastructure providers, including AWS, GCP, Azure, Alibaba, Oracle & IBM • Cloud Security Posture Management with regular reporting of cloud exposure • 24x7 alerting on new critical exposures • A single pane of glass and consistent control for all your cloud providers • Automated remediation of cloud misconfigurations • On demand access to cloud security architects on a retained basis

- Access to incident response and crisis management expertise
- Endpoint protection blocks known and unknown threats in real time.

Managed Cyber Defence Service Benefits

- Stops threats before they damage the targeted system
- Reduce the time between detection and response to minutes
- Significantly reduced analyst workload through validated and enriched data
- Visibility into endpoint, network and cloud for improved detection
- Leverage IT investments through easy integration with existing technologies
- Reduce operational costs with automation of routine tasks
- Real-time threat intelligence delivers ultimate detection and response capability
- 24/7 SLA backed access to world-class incident response experts
- Threat intelligence gathered by Europe's leading cybersecurity consultancy
- Fast service deployment to reduce cyber threats within days.