G-Cloud 15

Threat Intelligence Services

January 2026

Strictly private and confidential

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.

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 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 them:

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

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

Threat Intelligence Services

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

Threat Intelligence Services

Providing threat intelligence reporting, data and services for your cloud solutions. Our services are designed to enable effective preparation and timely defence against targeted and advanced cyber threats.

Threat Intelligence Services	Threat Intelligence Services Benefits
• Threat Intelligence Subscription Service • Threat Intelligence provider for GBEST • Threat Intelligence directed research • Cyber threat assessment • Cyber threat intelligence monitoring (including Deep & dark web) • Cyber Threat Intelligence Capability & Maturity Assessment • Advisory services helping organisations consume, apply and produce threat intelligence.	• Enables visibility, detection and prevention of cyber threats • Intelligence data shared through multiple platforms, for ease of access and integration • Provides threat profile insight • Contextual analysis tailored towards informing risk-based decisions • Timely insight into a broad range of external threats, including new and innovative techniques being observed. • Garner insights from our highly experienced analysts through collaboration to help you remediate issues faster and with greater confidence • Increased effectiveness in the detection and prevention of threats • Development and design of appropriate mitigations for new threats • Supports regulatory requirements for intelligence-led testing.

Our view on the service features and benefits within this service definition document are presented below:

1. Threat Intelligence subscription service

Our threat intelligence subscription offering can be tailored according to your business requirements, with four levels of service that provide the flexibility to optimise your threat intelligence capabilities as needed. The following components form part of the offering depending on service level selected:

	API	Portal Lite	Portal Plus	Portal Detect
Access to PwC API for atomic enrichment	✓	✓	✓	✓
Access to PwC threat intelligence reporting		✓	✓	✓
Ability to query or access specific PwC intelligence holdings			✓	✓
Access to PwC threat intelligence analysts			✓	✓
Access to PwC detection rules				✓

Threat intelligence reporting is a key component of our subscription services. It is derived from hundreds of global incident response engagements per year, our managed security services, and a wide variety of bespoke collection systems and partnerships.

Our reports cover a wide variety of threat research, from strategic reporting on the threat landscape for specific sectors or geographies to more tactical reporting on a particular threat or campaign, such as new malware families or intrusion techniques.

2. Directed research and assessments, including GBEST

Our directed research service provides direct access to PwC's threat research team for tasks relating to ad-hoc or long-term enquiries and can include both tactical and strategic research into malicious samples, threat actors or analysis support. It is often bought in conjunction with one of the PwC subscription services.

We typically offer threat assessments at two levels of depth:

- **External Threat Assessment:** this comprises a high-level assessment specific to the client's profile, such as analysis of the client's threat profile in the context of the sector in which it operates, analysis of regional-specific threats, and high-level implementable recommendations.

- **Tailored Threat Assessment:** this provides a client with a detailed analysis of their current threat landscape, such as analysis which takes into consideration the client's specific profile, including scope of operations and geographic presence, threat actor analysis (including examples of current tools, techniques and procedures), and pertinent open source intelligence that has been identified.

We are also able to provide clients with Targeting Intelligence, which will look into potential attack surfaces. These threat intelligence reports can be delivered to support red team engagements, such as GBEST, comprising detailed Threat Actor Profiles and Attack Scenarios.

Additionally, we can offer a digital risk monitoring service, which provides ongoing keyword-based monitoring of a wide variety of deep and dark web (DDW) criminal forums, marketplaces, paste sites and messaging services. This service paired with our industry-recognised threat intelligence capability can provide valuable insights into your organisation's risk profile and exposure.

3. Threat Intelligence consulting

We have strong expertise in cyber threat intelligence, as well as capability development, transformation and implementation. Our threat intelligence capability and maturity assessment service provides a blueprint for developing and optimising your organisation's threat intelligence capability based on your organisation's unique needs, operational structure and cyber threat landscape. We can help:

- Review your current cyber threat intelligence capability and needs to provide a high-level assessment and recommendations for improving the utility, efficiency and effectiveness of threat intelligence within your organisation and drive your organisation's cyber strategies.

- Help your organisation make better use of internal data and resources to enrich and contextualise the threat intelligence you are receiving.

- Conduct a structured, multidimensional analysis of your cyber threat intelligence capability and needs to provide a comprehensive maturity roadmap – covering pillars such as strategy, resources, requirements, collection management, integration, analysis, production, dissemination, and continuous improvement – to increase efficiencies and maximise your organisation's threat intelligence capability.

- Provide a bespoke solution to address your threat intelligence needs through additional PwC Threat Intelligence offerings.

Confidential. This document does not constitute a Call-Off Contract for Services with PricewaterhouseCoopers LLP. Where we are engaged to provide Services, our Services will be governed by a subsequent Call-Off Contract that may be entered into between us. If you receive a request under freedom of information legislation to disclose any information we provided to you, you will consult with us promptly before any disclosure. All information contained in this document or otherwise provided or made available as part of any Award Procedure is confidential and may not be disclosed to anyone else without our prior consent.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.