G-Cloud 15 Service Definition

Accenture Cyber Security Operations and Incident Management for Cloud Services

Jan 2026

accenture

Contents

1.0 Scope of our services

Service introduction

Our service will quickly contain an incident, analyse valuable intelligence on the attacker and help you take appropriate action. We can integrate with your existing operational security functions, or provide on-demand services following a suspected cyber-attack.

Our Security Operations specialists can provide guidance on how to prepare for the worst and ensure you are ready to detect, analyse and respond to a cyber security incident before it occurs. Our services are designed to help your business monitor the network for suspicious or malicious activity and appropriately respond to cyber security incidents to mitigate damage to your business and its reputation. We quickly contain an incident, analyse valuable intelligence on the attacker and help you take the appropriate action. We can integrate with your existing operational security functions or provide on-demand services following a suspected cyber-attack.

Service features

- On shore security cleared teams
- Experience of sovereign services
- Industry leading cyber incident management and response frameworks
- Forensics capability for the preservation of evidence in Cloud services
- Triage and prioritisation of cyber security incidents
- Options for on-demand service or embedded business function
- Static and dynamic incident analysis for cyber-attack modelling
- Integrated with cyber security intelligence sources for realtime updates
- Independent and impartial investigation of security incidents
- Co-ordination of incident response with third parties (e.g. NCSC, CERT UK)
- Support and guidance for existing operational cyber security function
- Extensive tool and process optimisation experience
- Multi-SOC collaboration experience, leading to increased customer maturity

Service Benefits

- Improve incident containment, eradication and recovery timeframes
- Establish effective incident response policies, plans and procedures
- Develop existing operational security capabilities and create new ones
- Quickly recover business systems and return to operationally ready state cleared teams

- Prevent the systemic spread of cyber incidents across cloud services
- Confirmation that the affected systems are functioning within normal parameters
- Proactively monitor your Cloud services for misuse and criminality
- Reduce the frequency of cyber security incidents in your organisation
- Improve response times to reduce business impact and financial loss
- Consistent approach that is dependable, measurable and repeatable

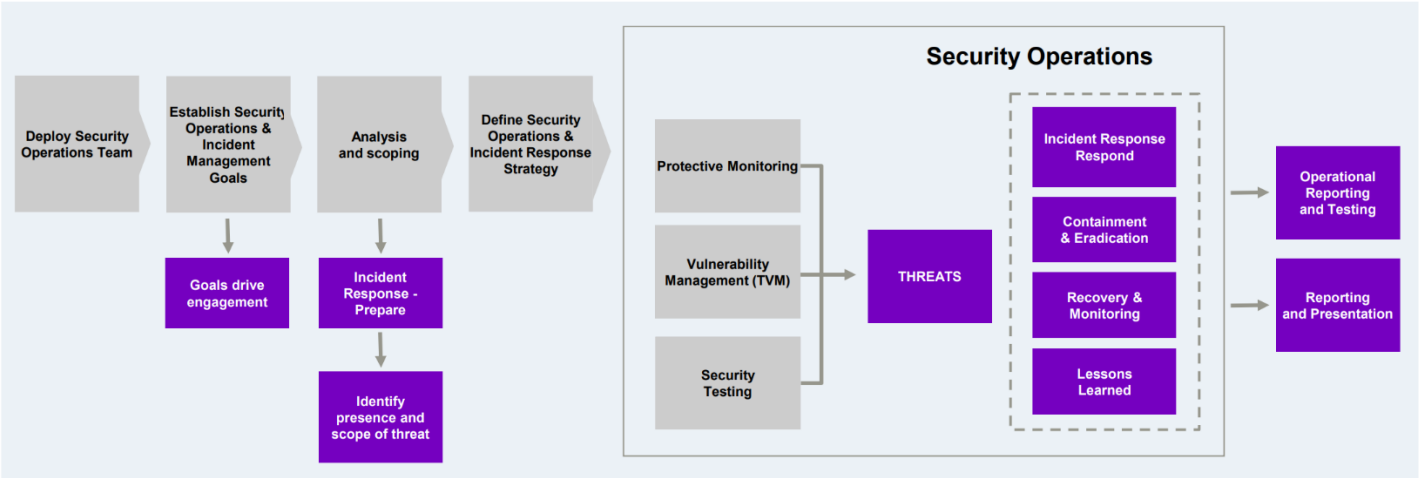
2.0 Service Implementation

Dealing with cyber security incidents – particularly targeted attacks at your organisation can be a very difficult task. We work with you develop processes and procedures based on industry best practice to ensure a systemic and structured approach to Security Operations & Incident Management:

- Identify critical assets and ensure appropriate controls are present
- Establish escalation routes and procedures to allow quick response and decision making when responding to cyber security incidents
- Analyse the threat landscape and outline the required security posture to best protect your business and its most valuable information
- Create an appropriate framework with the necessary strategy, roadmap and procedures to define your Security Operations & Incident Management functions
- Planning and Development of Incident Response rehearsals based on realistic scenarios
- Development and Tuning of Monitoring use-cases to automatically respond to targeted threats to your organisation

What do you get?

- We work with you to define your Security Operations & Incident Management requirements based on the needs and threats to your business.
- We work with you to define your strategy and integrate with your existing security teams to provide effective monitoring and Incident Response procedures.
- Provide Security Testing and reporting



Our Approach to Incident Response

To investigate and resolve security incidents 6point6 respond through 4 phases:

1

Initiation

Review and confirm scope of the engagement.

2

Initial Diagnosis

This is a key step in analysis of the initial symptoms of a cyber security incident. We will look to establish the security posture of the compromised environment, and the detection capabilities within.

3

Root Cause Analysis

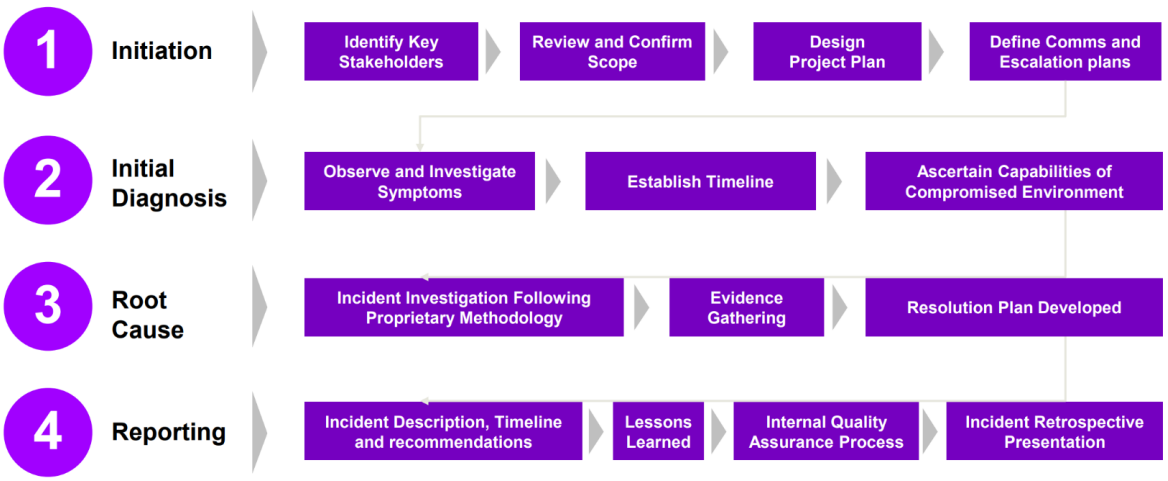
Our experts will perform discovery and monitoring activities that will allow us to determine the extent of a cyber security incident and seek to identify which of your assets may have been affected.

4

Reporting

It is important that no opportunity to improve is wasted. Based on our findings and observations throughout the investigation, our experts will work with you to create an incident report. The report will outline the facts of the root cause analysis and the outcome of the investigation.

Incident Response Methodology



3.0 Pricing

Please refer to the associated pricing document/ rate card relevant for this service.

4.0 Contacts

Email: UK.TenderMonitoring@accenture.com

Telephone: +44 (0) 20 7844 4444

5.0 About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organisations build their digital core, optimise their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 799,420 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities