G-Cloud 14
Service Definition

Cyber Security Operations and Incident Management for Cloud Services

May 2024

accenture

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.

Service features and benefits

Service Features

- 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 real-time 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

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
- 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

Security Operations and Incident Management

Failing to prepare is preparing to fail

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.

Working with You

Dealing with cyber security incidents – particularly targeted attacks at your organisation can be a very difficult task. At 6point6 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.

Why Prepare?

There are many benefits in ensuring your strategy for Security Operations & Incident Response is well-defined and effective:

Having a Security Operations and Incident Management capability is of utmost importance in times of crisis to help you deal with an incident when the worst happens.

Produce an effective monitoring strategy so that your business-critical information and assets are monitored and protected against cyber threats

Considers the implications of people, process, technology and information

Create, maintain and test Incident Response Plans as part of an effective Security Operations function to understand your preparedness to respond to a cyber security incident.

Align the Incident Management capabilities across multiple teams within your organisation to ensure the effective management of cyber incidents

Our Services

Security Operations

We will integrate with your existing security functions or provide on-demand services to monitor your network identifying suspicious traffic, malicious activity or indicators of misuse.

Incident Response PREPARE

A service to help you prepare for the worst, ensuring your business can respond effectively to a cyber attack. We conduct a criticality assessment to define your business-critical assets, identify threats to your business and conduct a full technical assessment of your network.

Incident Response RESPOND

We help you recover from the impact of a live cyber incident and get your business back and running. Utilising our proprietary methodology based on the CREST Framework we will work with you to define an incident through initial diagnosis, investigate through root cause analysis, eradication and recovery.

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

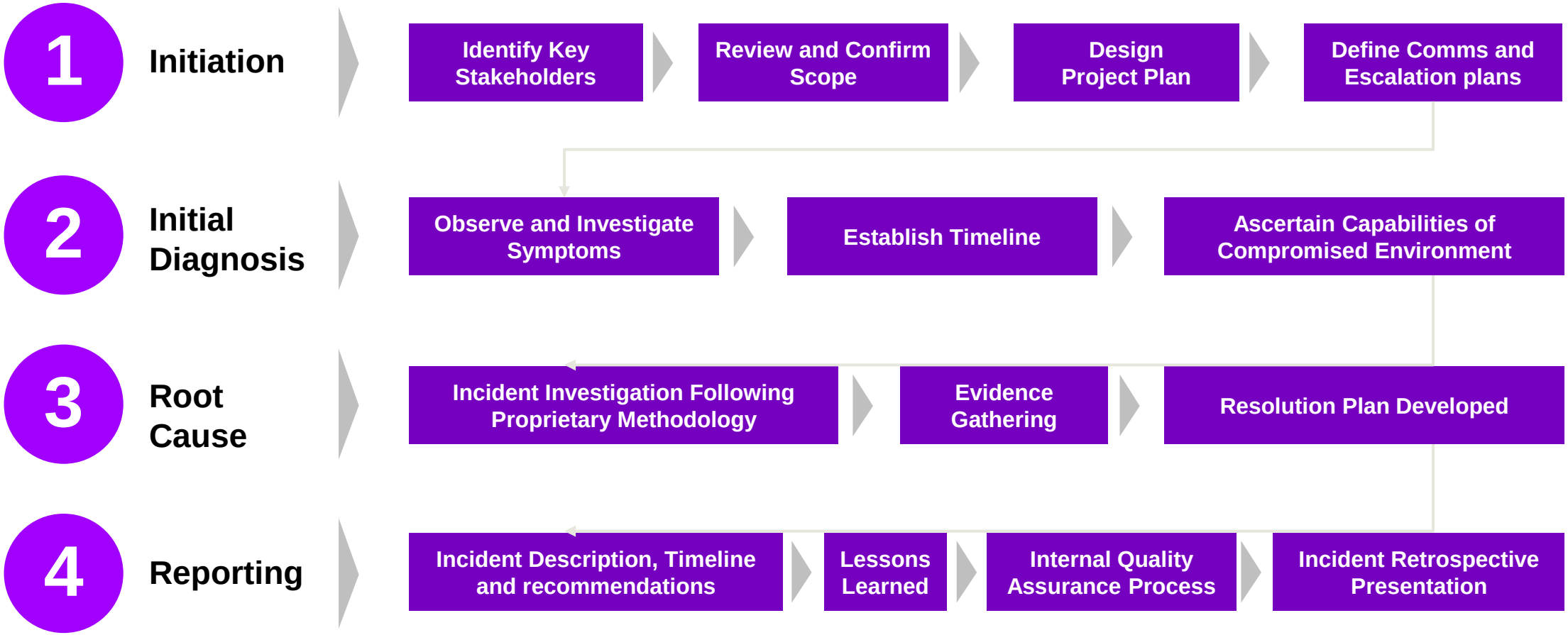
Our experts will perform discovery and monitoring activities that will allow us to determine the extent of a cyber security incident and seek to identify which of your assets may have been affected.

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.

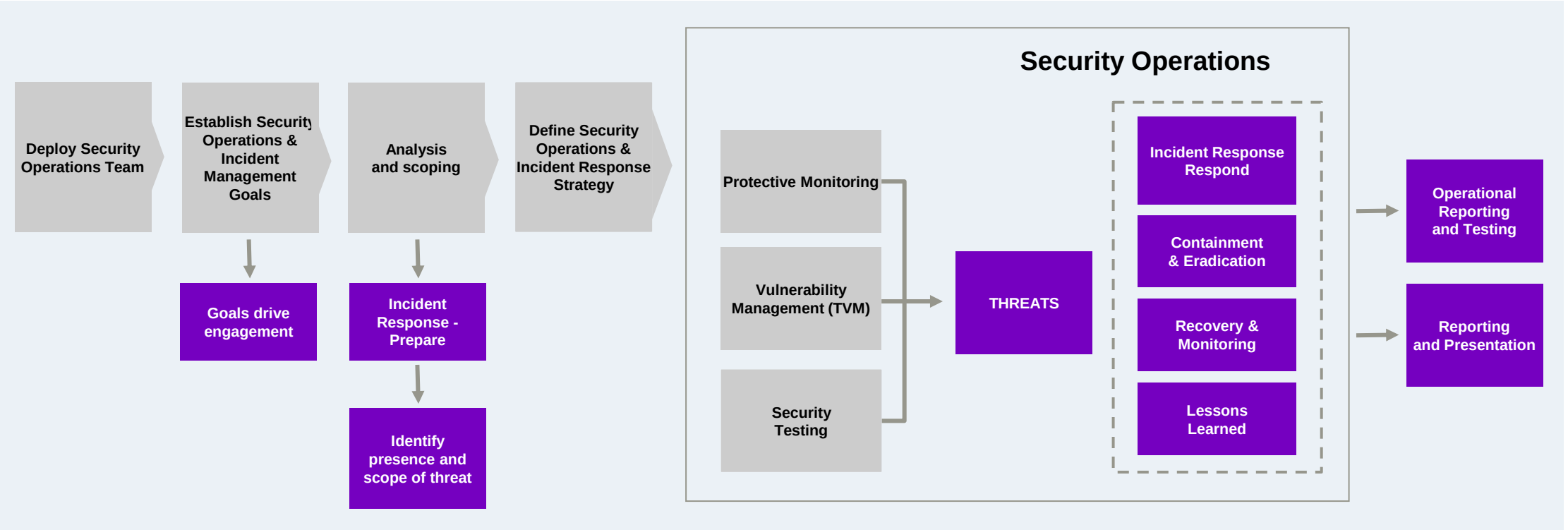
Incident Response Methodology



Service implementation

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



Why 6point6?

Technology agnostic and outcome driven

We mobilise quickly and deliver at pace

Integration and support capabilities around the UK

Our people are proven experts

Transformation secured

We work to

Create innovative new digital products to keep your business ahead

Transform the way you do business with focused insight and analytics

Strengthen your operations, supporting and developing your team and infrastructure

Secure your data and your technology investments

6POINT6
Part of Accenture

“6point6 is my go-to supplier if I need advice or support with regards to cyber security. We see them as our trusted partner, and they have been helping us in our journey to build a secure bank.”

Daniella Somerscales CISO, ClearBank

Pricing

Please refer to the associated Pricing Document relevant for this Service.

Contacts

Sarita Sudera

(Accenture Health & Public Services – Sales Lead)

Email: UK.TenderMonitoring@accenture.com

Telephone: +44 7815 100009

About Accenture

Accenture is a leading global professional services company that helps clients build their digital core, transform their operations, and accelerate revenue growth—creating tangible value across their enterprises at speed and scale. We are uniquely able to create these outcomes because of our broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched industry experience and specialised capabilities across more than 40 industries and all business functions. With 743,000 people serving clients in more than 120 countries, and a net revenue of $64.1 billion USD for the financial year ending on 2023, Accenture drives innovation to improve the way the world works and lives.