G-Cloud 15 Service Definition

Accenture Security Operations Centre Advisory and Design for Cloud Services

Jan 2026

accenture

Contents

1.0 Scope of our services

Service introduction

Our service focuses on the effective strategy, design, deployment, accreditation and operational running of a Security and Network Operations Centre (SOC / NOC) by, on shore security cleared, teams. This service will enable you to proactively control activities and incidents taking place across your estate.

- Definition of the SOC (Security Operations Centre) Strategy.
- End-to-end design and implementation of the on-premise/cloud-hosted SOC/NOC
- End-to-end design and implementation of the SSDLC (Secure-Software-Development-Lifecycle).
- Security gap assessment and remediation planning.
- Design and implementation of the Threat and Vulnerability Management.
- Design and implementation of the SIEM (Security Information and Event-Management-System).
- Design and implementation of the CD/CI pipeline and container security
- Adaptation and optimisation of the CSP-provided native security controls.
- Automation and optimisation of the existing SOC processes.
- Design and implementation of the Threat and Vulnerability Management.

A SOC strategy aligns with the specific business and IT needs of the client. A security operations centre will be the centre point of all Security Engineering capabilities, be a point of contact for identifying all security incidents and provides defence in depth for your Enterprise

Service features

A Security Operations Centre is an environment in which computer logs are monitored in real time. Endpoints, applications, databases and websites can have their activity records centralised in one secure location including other security tools. This centre is engineered to be the most secure possible and enables efficient response to Security events

Strategy

- On shore security cleared team
- Centralised Single pane of glass management collating results of all security tooling
- Log normalization and parsing for streamlining events
- SaaS or On prem cloud deployment
- People, Processes and Technology

- Access control and hardening
- Can meet sovereign demand

SIEM

- Dashboards visualise patterns over time
- Assist with technical forensic investigations
- Data storage and retention
- Correlation of multiple event types
- Data presentation for stakeholders
- Anomaly detections not possible using traditional tools
    - Threat and Vulnerability Management and SDLC Management
- Direct reporting of vulnerabilities for catalogue and remediation
- Tooling can be on prem or SaaS based
- Signature based and misconfiguration detection
- Integrations with internal ticketing processes
- Fits directly into host infrastructure
- Visibility across the IT Estate
- Tooling can include SAST, DAST, IAST and RASP

Service benefits

Strategy

- Visibility of all services in a single secure environment
- Uncover potential unknown resources and service limitations
- Defence in depth
- Monitor live threats

SIEM

- Real time event detection and alerting
- React to future threats with improved forecasting

- Increased efficiency
- Better breach handling
- Reduced incident response time
    - Threat and Vulnerability Management and SDLC Management

- Secure code creation is mandated as part of lifecycle in a shift left
- Simplified reporting for remediation
- Reduced bottleneck in QA and Pentest SDLC stages
- Vulnerabilities identified at the earliest point are substantially easier to remediate than Live codebases
- Prioritised remediation plan
- Reduced cost in remediation
- Mandate secure releases through forced blocking of code which does not meet policy requirements

Service Implementation

- Tool integration process for the SOC strategy and all tool capabilities
- Cyber maturity assessment outlines the risks that an organisation faces and how resilient the organisation is.
- The use cases a product must meet are identified and a market review of suitable vendors is conducted. A PoC of these requirements takes place to confirm the market review before procurement.
- HLD and LLD documents define precisely how the tooling will be setup within the client environment and will be subject to authorisation prior to implementation.
- The tool will be integrated with host infrastructure will all necessary technical processes. This includes ticketing, automation, hardening and configuration.
- Internal teams will be onboarded into the new tooling, with training and roles and responsibilities assigned.

2.0 Pricing

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

3.0 Contacts

Email: UK.TenderMonitoring@accenture.com

Telephone: +44 (0) 20 7844 4444

4.0 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