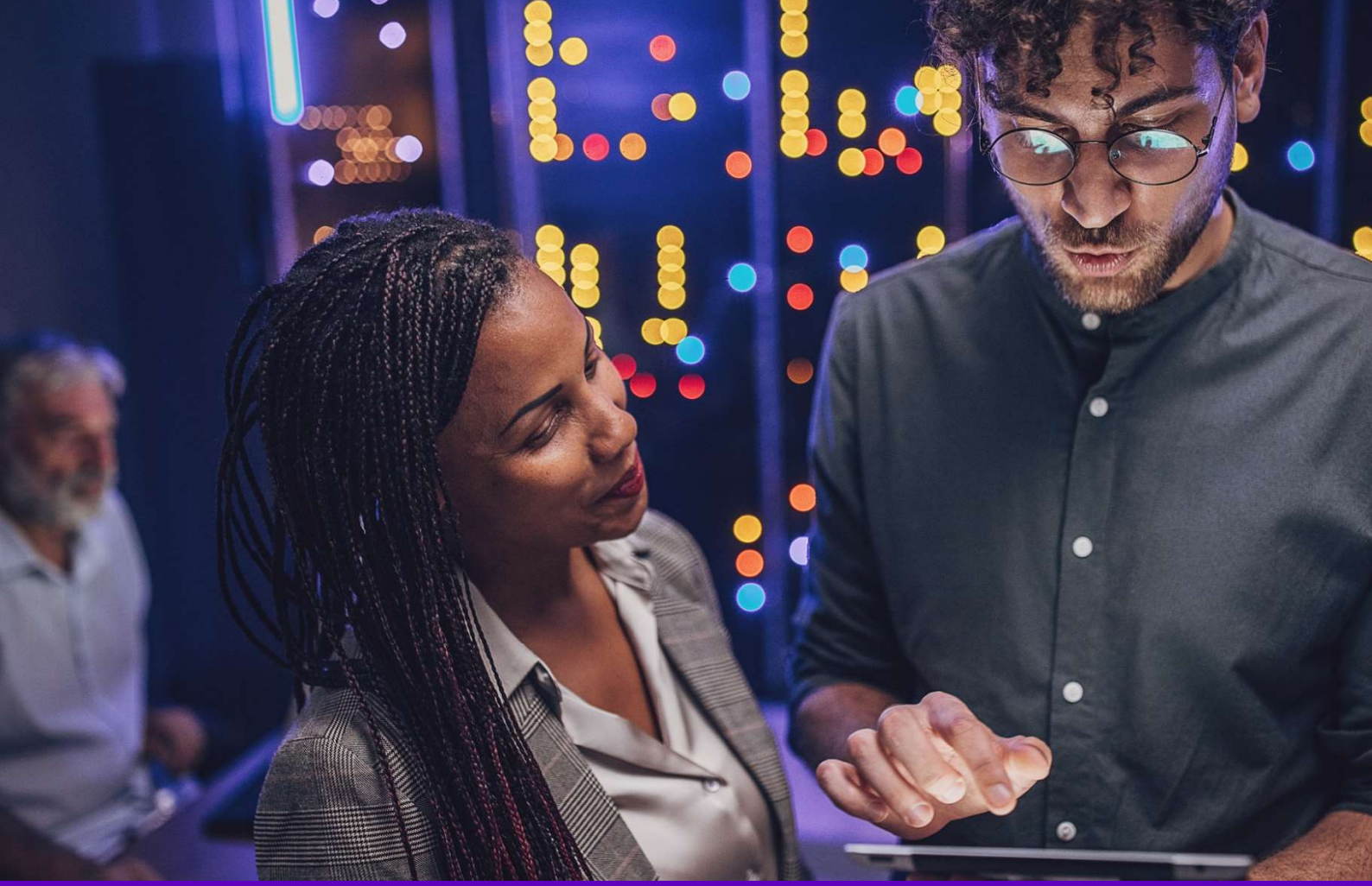

G-Cloud 14 Service Definition

Accenture Cyber Security Consultancy Services

May 2024

accenture

Contents

For your reference, entire catalogue:

1. Accenture CHECK IT Health Check (ITHC) Services
2. Accenture Application Security Assessment Services
3. Accenture Infrastructure Assessment Services
4. Accenture Mobile Device Security Assessment Services
5. Accenture Mobile Application Security Assessment Services
6. Accenture Wireless Testing Services
7. Accenture Red Teaming, STAR, CBEST and GBEST Testing Services
8. Accenture MDM Configuration Review Services
9. Accenture Build and Configuration Review Services
10. Accenture Firewall Review Services
11. Accenture Cloud Security Assessment Services
12. Accenture Code Review Services
13. Accenture Managed Phishing Services
14. Accenture Incident Response Retainer (NCSC CIR Level 1) Services
15. Accenture Emergency Response and Investigation (NCSC CIR Level 1) Services
16. Accenture Simulated Attack and Respond (Purple Team) Services
17. Accenture Compromise Assessment Services
18. Accenture Cyber Hygiene Assessment Services
19. Accenture Managed Detection and Response (MDR) Services
20. Accenture Incident Response Plans
21. Accenture Threat Assessment Services
22. Accenture Cyber Maturity Assessment Services
23. Accenture Cyber Advisory Services
24. Accenture Compliance Programme Support Services
25. Accenture Incident Preparedness / Exercising Services
26. Accenture SOC Maturity Assessment Services
27. Accenture ACSC IA Audit and Review Services
28. Accenture Security Awareness Training Services
29. Accenture Security Target Operating Model Services
30. Accenture ACSC Risk Management

1. Accenture CHECK IT Health Check (ITHC Services)

The CHECK IT Health Check is a technical risk assessment that identifies vulnerabilities in HMG IT systems and networks to assure the confidentiality, integrity, and availability of information. The testing methodology is largely determined based on the risks raised and agreed on by the Accreditor and the testing CHECK team.

Features

- NCSC CHECK-based assessment aligned with system Accreditors' key risks
- Established methodologies for understanding infrastructure and applications
- Reconnaissance, network mapping, and core network architecture analysis
- Automated vulnerability assessment
- Manual issue verification
- Authentication, authorisation, and session-related testing
- Local storage, information leakage and server configuration analysis

Benefits

- One of the largest pools of NCSC CHECK certified penetration testers
- Multifaceted testing providing thorough analysis of data and configurations
- Active exploitation of vulnerabilities and root cause analysis
- Scenario-based attacks for real-world applications

2. Application Security Assessment

Application security assessments identify security weaknesses in applications and provide mitigation recommendations. Our methodology is aligned to industry standards such as the OWASP testing guide, supplemented by our research into application security vulnerabilities.

Features

- Pre-engagement scoping services to ensure both coverage and cost-effectiveness
- Assessment of web-based and thick-client applications
- CREST certified consultants
- Threat ratings based on impact and ease of exploitation
- Proven testing methodology to ensure both coverage and depth
- Cross-discipline research and response expertise providing assurance against emerging threats
- Reporting includes common vulnerability metrics (e.g., CVSS, CWE)
- Recommendations for remedial actions and strategic management of vulnerabilities.

Benefits

- Identification of vulnerabilities affecting bespoke and COTS applications
- Accurate threat ratings to assess vulnerability risk to the business
- A tried-and-tested, evolving methodology covering major and emerging application technologies
- Penetration testing includes detailed inspection of web content and functionality

3. Infrastructure Assessment (Internal and External)

External infrastructure testing simulates a hacker carrying out malicious activities from across the internet. It surveys network services, probing for vulnerabilities, aiming to extract data or compromise the network. Internal testing, typically on-site, considers scenarios like insider threats from employees or contractors, assessing associated risks and consequences.

Features

- Pre-engagement scoping services to ensure both coverage and cost-effectiveness
- Identifying internet-facing “footprint” and attack surface for external infrastructure assessments
- Identification of vulnerabilities affecting systems
- CREST certified consultants
- Proven testing methodology to ensure both coverage and depth
- Cross-discipline expertise to provide assurance against emerging threats
- Reporting includes common vulnerability metrics (e.g., CVSS, CWE)

Benefits

- Assurance that critical internet-facing systems are secure (external)
- Assurance that the risk of internal attack is mitigated (internal)
- Identification of vulnerabilities
- Accurate threat rating to assess vulnerability risk to the business
- Recommendations for remedial actions and strategic management of vulnerabilities

4. Mobile Device Security

Mobile device security assessments provide assurance that a device is safe to use in the home or workspace and provide recommendations for secure configuration. Our approach includes assessment of a pre-configured device to identify issues in the device's configuration, which may increase the likelihood of a successful compromise.

Features

- Experience and expertise in assessing all major mobile device platforms
- Methodology aligned to NCSC guidance for remote end-user device deployment
- Advances in mobile device management feed back into assessment methodologies
- Threat ratings based on impact and ease of exploitation
- Authentication, configuration profiles, patching, encryption, application scrutiny, connectivity, and jailbreaking/rooting

Benefits

- Advice on secure deployment of mobile devices in the workplace
- Assurance of risk mitigation relating to lost/stolen devices and data
- Analysis of the emerging risks to mobile devices including malware
- Advisory for policies relating to mobile device integration in workplace
- Proven track-record in performing these assessments for clients across industries
- Cross-discipline expertise to provide assurance against emerging threats

5. Mobile Application Security Assessment

Mobile application security assessments identify security weaknesses in applications running on mobile devices. Modern mobile applications often re-implement the functionality of traditional web-based applications, which can lead to repetition of security mistakes. Additionally, modern mobile operating systems open new attack vectors, including cross-application attacks, and accidental disclosure of sensitive data.

Features

- Manual assessment of the mobile application's functionality included
- Builds upon the OWASP mobile security checklist including:
  - Application footprint & binary analyses
  - Data storage
  - Authentication & authorisation
  - Inter-app communication and input validation
  - Application permission analysis
  - Cryptography analysis
  - Application defences
  - Server components & communication analysis

Benefits

- Identification of vulnerabilities affecting bespoke and COTS mobile applications
- Assurance that sensitive application data is securely stored on-device
- Accurate threat ratings to assess vulnerability risk to the business
- Recommendations for remedial actions and strategic management of vulnerabilities
- Knowledge transfer from mature web-application testing pedigree and methodology
- Extensive expertise in the field of mobile security

6. Wireless Testing

Wireless connectivity is now an expectation for many: at home, in public places and the workplace. Our proposed methodology will consist of the following steps:

- Wireless network discovery
- Encryption and authentication
- Services and admin interfaces
- Key management and policy
- WPA Enterprise configuration
- Network segregation
- Client security
- Rogue access point detection

Features

- Extensive experience in all types of wireless, RF-enabled technologies
- Identification of rogue devices on wireless networks
- Analysis of wireless network segregation and passive information leakage
- Threat ratings based on impact and ease of exploitation
- Proven testing methodology to ensure both coverage and depth
- Cross-discipline expertise to provide assurance against emerging threats
- Reporting includes common vulnerability metrics (e.g. CVSS, CWE)

Benefits

- Identification of threats affecting corporate and guest wireless networks
- Assurance that wireless networks are appropriately segregated
- Assurance that sensitive wireless data is appropriately encrypted
- Accurate threat ratings to assess vulnerability risk to the business
- Recommendations for remedial actions and strategic management of vulnerabilities

7. Red Teaming, STAR, CBEST and GBEST

Red team engagements emulate real-world attacks in a controlled manner. From email phishing to data exfiltration, mirroring daily threats countered through the NCSC/CPNI CIR scheme. These exercises provide valuable insights for continuous improvement, enhancing incident response capabilities and fostering a culture of security awareness.

Features

- Customised engagements delivered by certified and suitably cleared consultants
- Tailored attack plans based upon real world threat scenarios
- Cross-discipline engagements to uncover vulnerabilities across people, process and technology
- Mature risk management and delivery approach
- CREST STAR certified for Threat Intelligence and Penetration Testing phases
- Certified to deliver under the Bank of England CBEST scheme
- Certified under regulatory led initiatives including GBEST and NBEST schemes
- SC/DV cleared delivery and support personnel

Benefits

- Replicates a real-world, persistent attack upon your organisation
- Assessment of the business mitigations against real-world scenarios
- Identification of weaknesses arising from publicly available information
- Identification of weaknesses arising from security vulnerabilities
- Accurate threat ratings to assess vulnerability risk to the business
- Recommendations for remedial actions and strategic management of vulnerabilities
- Enables focused budgeting and increased ROI on cyber security spend
- Experience delivering high-value/low-risk simulated targeted attacks via a dedicated team

8. MDM Configuration Review

MDM configuration reviews are performed to address risks from increasing use of mobile devices to access sensitive enterprise data. Accenture assess the deployed MDM solution configuration, the supporting network architecture as well as the mobile device security policies and management processes.

Features

- Consultancy for personnel selection and document review pre-testing
- Audit of MDM-related documents, including security and device policies
- Review of MDM server configurations for compliance and best practices
- Testing mobile devices to ensure security policy compliance
- Configuration review: policy enforcement, data separation and encryption, device interface
- Remote device management and application management assessment
- Update management, compliance actions, reporting, and logging evaluation
- Analysis of MDM network architecture and device policies and processes

Benefits

- Assurance that corporate MDM systems and BYOD set-ups are secure
- Risk mitigation relating to lost or stolen devices and data
- Advisory for MDM system integration into the wider client Infrastructure

9. Build and Configuration Review

Build and configuration reviews ensure that laptops, workstations, and servers are configured securely. Insecurely configured environments can allow malicious users to obtain unauthorised access, and if a standard build containing weaknesses is deployed across hundreds or thousands of servers, the impact can be significant.

Features

- All mainstream operating systems covered (Unix, Linux, Windows etc.)
- CREST certified consultants
- Engagements carried out on-host or remotely via a delivered script
- Threat ratings based on impact and ease of exploitation
- Proven testing methodology to ensure both coverage and depth
- Cross-discipline expertise to provide assurance against emerging threats
- Reporting includes common vulnerability metrics (e.g. CVSS, CWE)

Benefits

- Assurance that specific business-critical systems are configured in a secure manner
- Provides defence-in-depth assurance that systems are secure
- Accurate threat ratings to assess vulnerability risk to the business
- Recommendations for remedial actions and strategic management of vulnerabilities

10. Firewall Base Review

Many organisations have come to rely on firewalls as a keystone of their network defences. It is important that they are fit for purpose and delivering optimum performance. The device review is based on checklists derived from NSA hardening guidelines and other best-practice sources.

Features

- Tried-and-tested methodology covering all firewall vendors
- Both rule sets and device configuration are assessed
- Ensures rules account for bidirectional filtering (ingress and egress)
- Ensures adequate logging and process for information retention
- Devices analysed for unnecessary services, default credentials and outdated OS
- CREST-certified consultants
- Reporting includes common vulnerability metrics (e.g. CVSS, CWE)

Benefits

- Ensures devices align with industry best practices for configuration
- Assurance that firewall implementation adheres to design
- Recommendations for remedial actions to ensure bare minimum security exposure

11. Cloud Security Assessment

Our cloud security assessment analyses cloud systems from multiple perspectives, employing a largely manual approach to auditing cloud implementations. Using a range of techniques dependent on the hosting provider, instance type and service running, our methodology aligns with industry best practices and is supplemented by research into misconfigurations and weaknesses.

Features

- External application and infrastructure penetration testing of cloud environments
- At a high level, our methodology consists of the following:
  - Account, access, policy and permissions
  - Encryption and locks
  - Logging, monitoring and data location
  - Network configurations and firewall
  - Storage and disks
  - Extensions and third-party applications
- Scenario testing of cloud node segregation
- Architecture review
- Cloud VM hardening assessment
- Remote administration review

Benefits

- Gain assurance over cloud environment security
- Multi-perspective assessments covering a range of potential attacks

12. Code Review

Code reviews aim to provide assurance of complex software where coverage from a ‘black box’ perspective cannot be guaranteed. During a code review, consultants combine targeted manual code inspection and automated analysis to identify security risks in software. Code review is often undertaken in support of application security assessments.

Features

- Expertise reviewing code in all major languages, both compiled and interpreted
- Extensive industry experience in finding and exploiting flaws in code
- Identification of critical areas of code

Benefits

- Vulnerability-free software with secure coding and design principles
- Ensuring adherence to secure code principles during development
- Added assurance to ‘black box’ application security assessments
- Remediation recommendations for long-term code improvement
- Threat ratings based on impact and ease of exploitation

13. Managed Phishing Service

Accenture's managed phishing service allows organisations to send simulated phishing emails to their users in a controlled manner. User actions are tracked safely, user awareness is benchmarked, and trends can be analysed across regular assessments. This assesses an organisation's resilience to these attacks, from a technical and staff awareness perspective.

Features

- Our approach to delivering phishing exercises comprises the following five phases:
  - Pre-staging workshop (optional)
  - Staging
  - Execution
  - Analysis & reporting
  - Post-engagement workshop (optional)

Benefits

- Phishing attacks are modelled on real world techniques including:
  - Spoofed email addresses
  - Links to 'typosquatted' domains
  - Filter evasion techniques (e.g. cross-site request forgery and scripting)
  - Attachments contain simulated malware
  - Spam filter evasion techniques (e.g. throttling of email sending)
- Both non-targeted and targeted email options available

14. Incident Response Retainer (NCSC CIR Level 1)

The retainer-based incident response investigation support service provides access to Accenture's response capability within guaranteed timeframes, ensuring experienced incident responders are on the ground when they are needed most. This service enhances, and integrates with, existing incident response plans.

Features

- NCSC/CPNI Cyber Incident Response (CIR) scheme Level 1 certified
- Incident response and readiness consultancy
- Telephone hotline available up to 24/7
- Response times bound by Service Level Agreement (SLA)
- CREST and GIAC certified incident handlers
- CREST and GIAC certified analysts
- Threat intelligence led investigation capability

Benefits

- Guaranteed response times as defined by SLA's
- Reliable access to experienced incident responders
- Reliable access to vital rare skills and toolsets
- Proven incident response capability
- Expert advice and guidance

15. Emergency Response and Investigation

Accenture has one of the largest NCSC CIR accredited incident response teams in the UK with expertise spanning malware, network traffic, forensics, and threat intelligence. With proficiency in IT and OT response, crisis management, and recovery, we ensure swift restoration with minimal disruption and maximum resilience.

Features

- NCSC/CPNI Cyber Incident Response (CIR) scheme Level 1 certified
- CREST and GIAC certified analysts
- CREST and GIAC certified incident handlers
- Analyst centred; intelligence led detection
- Best-of-breed analysis and detection technologies
- Highly experienced investigation team
- UK security cleared personnel

Benefits

- Proven incident response capability
- Expert advice and guidance
- Wide range of technical and analytical competencies
- Technology agnostic

16. Simulated Attack and Response (Purple Team)

Accenture offers a range of services under the Simulated Attack and Response banner. Our response focussed approach utilises our Incident Response specialists to both review and coach the client Incident Response teams (typically SOC and IT Security) during carefully tailored simulated attack activities.

Features

- Services based off real-world case studies and experiences
- Led by highly experienced incident response consultants
- Flexible scenarios that can be tailored to specific organisational requirements
- CREST and GIAC certified consultants

Benefits

- Improved incident readiness and detection of incidents
- Increased confidence in handling of incidents
- Proactive identification of possible issues
- Reduced risk and impacts from major incidents
- Compliance with regulatory and audit requirements
- Improved resilience to incidents across the estate

17. Compromise Assessment

Advanced adversaries challenge traditional security measures. Static detection and COTS technology often fall short, leading firms to invest in dedicated threat-hunting capabilities. As a UK NCSC “Cyber Incident Response” (CIR) scheme member, Accenture integrates proprietary threat intelligence and tooling with niche skillsets, supporting risk management and upskilling of in-house teams.

Features

- Tailored approach based on risk appetite and focus
- Conducted by NCSC CIR Level 1 certified team
- Intelligence-led approach to compromise assessments
- Uses a range of unique hunting techniques and toolsets
- Expertise in forensics, reverse engineering, penetration testing and threat intelligence
- Often include coaching or training on threat hunting skills

Benefits

- Identify hostile activity and provide recommendations on managing the risk
- Provide an understanding of historic bad-actor activity
- Identify opportunities to improve defensive monitoring and controls
- Identify opportunities for improvement in future Incident Response investigations

18. Cyber Hygiene Assessment

A cyber hygiene assessment is a proactive evaluation of an organisation's network and identifies artefacts contributing to compromise. As tool deployment and log data is shared, the exercise is also a dry-run for a live incident. This makes it a valuable technical rehearsal that improves coordination during a complex investigation.

Features

- Carried out by a certified NCSC CIR Level 1 team
- May expose significant cyber hygiene, infrastructure, technical and operational challenges
- May identify the presence of persistent adversaries necessitating further investigation
- Tailored approach based on risk appetite and focus
- Toolset deployment based on threat profile and technologies
- Analysis uncovers malware, unwanted programs, and risky administrative practices
- Immediate escalation of compromise indicators; detailed technical and executive reporting

Benefits

- Reduced risk of an undetected persistent compromise impacting key assets
- Improved capabilities ready to meet the demands of a complex threat landscape
- Identify unwanted programmes, poor hygiene and unusual administrative practices
- Technical dry-run to ensure tooling and data accessibility during incident

19. Managed Detection and Response

Accenture delivers SOC capabilities from a Government Accredited facility. This includes threat intelligence led 24/7 proactive threat hunting, monitoring and investigations, by UK-resident security cleared analysts, supported by NCSC CIR Level 1 certified Incident Responders. Clients benefit from our industry-leading knowledge and experience maximising the value of existing security technologies.

Features

- Analysis of security-rich data from Cloud, on premise and hybrid.
- Utilising our established SOAR platform realising automation and efficiency gains.
- Threat intelligence sourced through OSINT, closed groups and technical discovery.
- SIEM tool agnostic - deep technical knowledge of market leading tools.
- Comprehensive 24/7 reactive monitoring with tailored proactive threat hunting
- UK based service with SC analysts within Government Accredited facilities.
- Secure UK data centres capable of holding OS data.
- Service management adhering to ITIL framework delivering high level engagements.
- Capability of tool integration or leveraging customer's existing technical investments
- Continual development of use-cases (detection logic) and tuning requests. to combat emerging threats and evolving attacker techniques.

Benefits

- Capability designed to go beyond traditional managed security services providers.
- The most comprehensive proactive approach for identifying threat actors.
- Coherent and complete monitoring protecting against external and internal threats.
- Fully flexible and scalable service that adapts to client requirements.
- Independent assurance that client response plans are appropriate and effective.
- Clients benefit from knowledge and experience from across functions.
- Identification of high value log sources reducing too many alerts
- Assisting clients in risk management, minimising the risk of compromise
- Experienced support to UK Government and Defence Supply Chain
- Formerly known as Context, a trusted supplier by Cyber Regulators

20. Incident Response Plans

Cyber-attacks threaten organisations with severe financial and reputational damage. Without an incident response plan, responses may be chaotic and inefficient, amplifying organisational impacts. Effective incident response plans are essential to mitigate impacts by ensuring a coherent and coordinated approach to dealing with a cyber incident.

Features

- Bespoke incident response plans tailored to the organisation
- Key elements that are considered and outlined within the plan:
  - How the organisation utilises threat intelligence
  - How Incidents are notified and escalated
  - Communication channels (internal and external), and information requirements
  - Roles and responsibilities across the organisation
  - Regulatory reporting
  - Media management
  - Linkages to BCP/DR and Crisis Management functions

Benefits

- Reduced impact from any cyber incident
- Improved ability to respond and recover from cyber incidents
- Faster and more efficient response to cyber incidents
- Identifies cyber incident response risks, prioritised and managed accordingly
- Clarifies communication channels, responsibilities and decision-making authorities

21. Threat Assessment

Understanding the threat landscape is crucial for building effective security architectures. Organisations recognise the importance of detailed threat knowledge in optimising cyber defense and risk management. Threat assessments provide deep insights into the threat environment, supporting regulatory compliance, incident response, vulnerability management, and cybersecurity strategy development.

Features

- Tailored threat assessment
- Strategic intelligence analysis fused with deep tactical intrusion set knowledge
- Threat assessments aligned to CREST STAR standards and methodology
- Deep technical and business discovery tailored to organisation. Including:
  - Strategic threat analysis outlining key drivers of business threats
  - Consideration of supply and value chain risks
  - Tactical analysis of intrusion sets presenting most significant threat
  - MITRE alignment with offensive heat mapping
  - Detection and threat hunting recommendations
  - Detailed technical threat scenarios aligned to an organisation’s environment

Benefits

- Comprehensive understanding of organisational threats, prioritised against business objectives
- Understanding of likely targeted assets and critical paths of intrusions
- Visibility of exposure to adversaries
- Can use as the baseline for continuous threat intelligence monitoring

22. Cyber Maturity Assessment

Emerging threats, vulnerabilities, and regulatory obligations make it crucial for organisations to demonstrate effective management and protection of the information entrusted to them. Accenture's CMA evaluates your capacity to safeguard critical assets, utilising policies and controls, such as NIST ISO27001 and CIS, to identify and prioritise areas for improvement.

Features

- A tried and tested methodology reviewing your organisation's security maturity
- Bespoke or standards-aligned assessments, e.g., NCSC Cloud Security Principles
- Collaborative, face-to-face approach between Accenture consultants and your team
- Assurance of support from an independent trusted partner

Benefits

- Provides real-world insight into the efficacy of your maturity controls
- Comprehensive expertise from a full range of cybersecurity consultancy domains
- Actionable, pragmatic advice for problem-solving and increasing baseline security
- Detailed reporting that includes feedback accessible to all departments

23. Cyber Advisory

In an ever-changing cyber risk landscape, Accenture's Cyber Advisory practice can help you ensure that you are aware of your current cyber risk posture across all domains and can support you in achieving your desired future state of cyber security.

Features

- Extensive experience of supporting clients across complex cybersecurity domains
- Offering both standards-aligned services and bespoke, tailored approaches
- Track record of service delivery
- Five 'pillars' of Advisory service offerings:
  - Cloud and Security Architecture
  - SOC Transformation
  - Security Governance, Risk and Compliance
  - Cyber Resilience
  - Human Factors

Benefits

- A holistic overview of your cybersecurity posture
- Real-world advice on both remediation and future growth
- Multi-skilled and experienced cybersecurity practitioners

24. Compliance Programme Support

In a rapidly changing compliance landscape, Accenture can help ensure that you have the correct standards and governance in place. We can help you meet a range of compliance processes with the ultimate aim of allowing your business to use compliance credibly and effectively as a driver of growth.

Features

- Extensive experience of supporting the delivery of ISO27001 conformity
- Experience enabling other security frameworks
- Supporting security compliance with relevant regulations and legislation
- Bespoke, tailored approach
- Track record of service delivery

Benefits

- Gap analysis of your existing compliance programme
- Roadmap to compliance
- Align IS function with business needs

25. Incident Preparedness / Exercising Services

Our tabletop exercises are a highly valuable and efficient way to both practice response and identify potential gaps, which can be addressed prior to a real incident. We draw on our front-line incident response, threat intelligence, and consultancy expertise to develop and run realistic scenarios which draw out key challenges and issues in real incidents.

Features

- Realistic incident scenarios and exercises facilitated by IR and advisory experts.
- Draws on experience from our NCSC Cyber Incident Response (CIR) scheme certified IR team.
- Post exercise report with observations and prioritised recommendations.
- Core IR stages from detection to recovery including critical decision making
- Communications and incident management
- Diverse team engagement from technical through to strategic level responses

Benefits

- Simulates real scenarios, challenging teams in a safe, structured, environment
- Clear prioritised recommendations to inform business cases for improvement
- Understanding potential challenges or gaps you may face in incident
- Testing of existing incident response processes and capabilities

26. SOC Maturity Assessment

Most organisations are on a maturity journey with regards to the effectiveness of their SOC (Security Operating Centre). Accenture can bring its world class knowledge and experience to bear to help you evaluate your capability, looking at People, Process, Technology, but also at key business drivers and relationships.

Features

- Delivered by experienced and security cleared consultants.
- Helps you identify and focus on specific areas of improvement
- Allows for the independent assessment of your capability
- Allows you to plan and plot a journey of improvement for your SOC

Benefits

- Reduces enterprise risks
- Upskills your SOC
- Increased visibility into your SOC’s efficacy
- Helps meet compliance requirements

27. ACSC IA Audit and Review

Our Assured Cyber Security Consultancy (ACSC) IA Audit and Review service is part of our NCSC assured services to Commercial, CNI, HMG and the supply chain. It is designed to provide clients with support and guidance in achieving and maintaining compliance with relevant legal, regulatory, contractual, standards and policy requirements.

Features

- Advice relating to the relevance of policies and procedures
- Advice to clients in maintaining assurance or compliance frameworks
- The review of existing cybersecurity policies and procedures
- Review of artefacts, such as risk assessments and reporting findings
- The performance of checks, reviews and audits, supported by reports

Benefits

- Assured service quality through NCSC oversight
- Providing clear routes to improvement, compliance and certification
- Tailored to varying sectors and needs
- Providing or supplementing a cyber assurance function

28. Security Awareness Training Services

We go beyond traditional training, using behavioural science to foster a security-conscious culture. We aim to instil a sense of commitment to the mission and inspire action, encouraging employees to embrace secure behaviours. Our approach not only builds a cyber-resilient workforce, it cultivates genuine buy-in for our collective security objectives.

Features

- Security awareness and culture change programmes
- Upskilling for teams
- Strategy for attracting, retaining, and developing security talent
- Security organisational change management
- Strategic Cyber Threat Briefing
- Staff Cyber Awareness Briefing
- Senior Executive Situational Awareness
- Gold Team - Senior Executive Exercise
- Incident Response Consultation
- Effective Log Management Briefing

Benefits

- High impact, low-cost method of improving organisational security posture
- Modules based off real-world case studies and experiences
- Led by highly experienced consultants
- Flexible scenarios that can be tailored to specific organisational requirements

29. Security Target Operating Model

A TOM is informed by an understanding of the organisational cybersecurity threats, and it serves as a blueprint for aligning operational capabilities to strategic objectives. It also outlines a roadmap to achieve target state, incorporating controls review, maturity and threat assessments for evidence-based investment in security capabilities.

Features

- This methodology assesses all aspects of an organisation's estate including:
  - Roles and responsibilities (RACI)
  - Process and capabilities
  - Organisational structure
  - Location considerations
  - Suppliers that support the processes and capabilities
  - Management systems
- Experience providing target operating models for global and governmental clients
- Insight from Accenture's core Advisory and Threat Intelligence functions

Benefits

- Understanding where the cybersecurity team is today
- Understanding the target state for next three to five years
- Demonstrating to the wider business how cybersecurity will evolve

30. ACSC Risk Management

Our Assured Cyber Security Consultancy (ASCS) offers comprehensive risk management solutions. With expert guidance, we identify, assess, and mitigate cyber risks, ensuring robust protection for your organisation's digital assets.

Features

- Threat-led tailored risk assessments
- Expert analysis of vulnerabilities and security gaps
- Customised risk mitigation strategies for proactive defence
- Compliance with HMG standards, policy and regulations
- Staff training and awareness programmes for enhanced risk management
- Regular security audits and reviews as part of 3LOD model
- Partnership for long-term security strategy alignment

Benefits

- Enhanced cyber resilience against evolving threats
- Proactive risk management for business continuity
- Compliance assurance for regulatory requirements
- Reduced likelihood of data breaches and financial losses
- Improved trust and reputation among stakeholders
- Solutions tailored to organisational needs
- Increased stakeholder awareness enabling risk-based decision making
- Scalable services for organisations of all sizes and complexity

31. Pricing

Please refer to the associated Pricing Document relevant for this Service, which are our Maximum rates.

32. Contacts

Sarita Sudera

(Accenture Health & Public Services – Sales Lead)

Email: UK.TenderMonitoring@accenture.com

Telephone: +44 7815 100009

33. 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 700,000+ people serving clients in more than 120 countries.