Cybersecurity – Security Operations Centres (SOC) – Design, Build and Accredit

G-Cloud 14

November 2024

Table of Contents

1 Service Overview

Capgemini offers Cyber Security Consultancy that can support strategy development, design, build and management services for clients seeking to implement, enhance or outsource management of their Security Operations Centres (SOCs) for enterprise and cloud environments.

A SOC provides security event monitoring, detection, network defense and incident isolation and management across one or more organisations' distributed networks and critical IT services. A mature SOC capability can help an organization:

- Gain better visibility of security events;
- Develop intelligence on the proximity of threats and attribution of events;
- Inform understanding of risks to mission critical information and operational assets;
- Respond to changes in the threat landscape;
- Prepare for; and coordinate response to cyber security incidents.

Capgemini has experience of helping clients identify their business requirements and translate these into a coherent strategy for SOC services that supports their business objectives. This is particularly important for clients embarking on a digital transformation, where protection of integrated cloud services for clients and employees is critical to achieving business goals.

Capgemini can develop a programme of work to design, build, implement or evolve SOC services, including identification of technology, tools, environments, capabilities and processes that can help demonstrate return on investment in risk management terms.

Capgemini provides third generation, managed live SOC services for public and private sector clients. We can provide management of clients' existing SOC and related technology solutions, including Security Information and Event Management systems (SIEM).

Capgemini SOC service can encompass the following:

- **Identification of Cyber Threats**: the qualification of potential or current cyber threats, involving assessment and analysis with specialist tools, by professionally skilled resources;
- **Clarify options:** Advising clients with their selection processes and the options available to them to protect their business;
- **Strategy Definition:** Collaboratively develop a cybersecurity strategy which supports delivery of clients' business objectives;
- **Design:** Develop blueprints for the technology, tools, capabilities and target operating model (TOM);
- **Build:** Help with procurement selection, configuration and testing of the technology and service architecture required for your Security Operations Centre;
- **Business Change and Transition:** We can provide specialist support to transition and implement new capability and support any existing business change functions;
- **Operate:** Capgemini can advise on operational and governance models that clients can use to manage and mature their Security Operations Centre and services; or provide operational SOC management capability from our own Cybersecurity Practice.

Capgemini can provide skilled resources to perform the service. Our services and practitioners can be delivered as part of a Capgemini or a client led programme. It is estimated that a basic engagement would be of 20-30 working days in duration, subject to the agreed scope being confirmed.

2 Business Need

Adopting and delivering cloud and digital services can provide organizations with new business opportunities and the ability to reach more customers. However, delivering these services may result in the integration of more third party provided enterprise and cloud services, increasing security interfaces and, thus, more cyber security risk to manage.

Cybersecurity breaches can have significant legal, reputational, financial and operational impact on organizations. The prevalence of successful cyber-attacks is clearly evidenced through the media reporting with increasing frequency; what was once an annual occurrence has become weekly, with greater board level awareness than ever of the ramifications following the realization of cyber risks.

Traditional approaches to security are unable to cope with the exponential growth in threats and attack methods. Organizations need to proactively, rather than reactively, respond to new threats and events such as:

- **Identify:** Is the business aware of all cyber threats?
- **Qualify:** Does the event pose a threat to business operations?
- **Communicate:** Interpreting the event into meaningful information for the business;
- **Process:** Bring together relevant areas of the business to decide on appropriate defensive action;
- **Investigate:** Consult with trusted advisers to investigate the root course and remedial action;
- **Respond and Report:** Compile and analyze information to produce business reports on regulatory compliance.

The implementation of a Security Operations Centre (and associated tooling) can provide intelligence-led protective or defensive monitoring capability to detect, alert, defend and respond to near real time events as they occur on a client's distributed networks and mission critical IT services.

Capgemini can assist clients in leveraging their IT investment by helping to bring together security functions, correlating events, ingesting and interpreting threat intelligence and providing actionable intelligence that can help inform an appropriate security stance.

Through continual threat assessment, our clients are able to intelligently evaluate risk, gain insight in the effectiveness of their controls architecture and prioritize focus on controls and interventions that are designed to thwart attacks earlier in the attack lifecycle. This can help provide our clients with the assurance that their assets and critical operations are appropriately safeguarded.

Depending on the options selected the value to the client business may consist of:

- Reduction in the risk that business processes will be impacted by cyber threats;
- Fraud reduction (where appropriate) across the client's business processes and interactions with citizens and suppliers;
- Maintaining 'digital trust' in the client's business processes and services.

3 Our Approach

Capgemini believes that a SOC should be treated as a living entity, with four core elements (tools, processes, perimeter and people) that need to be defined, implemented and then placed within a "cradle to grave" lifecycle services model. Mature SOCs require a robust core of governed processes, capabilities and tools; coupled with the ability to adapt and respond to changes in the tactics, techniques and procedures of those seeking to attack clients' services.

Capgemini offers a consultant led service, using skilled teams of cybersecurity subject matter experts (including CCP certified professionals), architects, project managers and operating model consultants. Capgemini can

collaborate with our client's suppliers and use tried and tested methodologies to support all aspects of a SOC from initial design to ongoing improvements can support the client's critical business objectives.

Typical deliverables of a SOC design would consist of the following elements:

- A programme management plan to support timely and controlled delivery;
- A client-specific SOC Strategy, Vision and Design Principles;
- Creation of a SOC Target Operating Model, incorporating and building on one or more of the following:
  - **Level 0:** Functions: The building blocks of an organization;
  - **Level 1:** Capabilities: The ability to do something and deliver;
  - **Level 2:** Activities: What will be done in target state and enable the capabilities;
  - **Level 3:** Tasks: Procedural maps and roles required in delivery;
  - **Level 4:** Steps: Role descriptions and business scenarios that enable delivery.
- Governance and Management Information;
- A technical architecture for the SOC;
- Advice and assurance around the security of the wider business architecture;
- Vendor and / or product selection and product assurance;
- Business Case expertise;
- Business Change Strategy;
- Transition Plan;
- Security analytics and threat intelligence planning.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The following Buyer responsibilities will apply:

- The Buyer will provide a project/engagement manager to act as a single point of contact and an escalation route for the full duration of the project/engagement;
- The Buyer will make available appropriate subject matter experts (business and technical) as appropriate to support the project or delivery plan;
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date;
- The Buyer will progress the introduction of the service through any internal service introduction/gating process, Enterprise Architecture processes and any other standard processes that are necessary;
- All internal and external user communications will be managed by the Buyer;
- The Buyer will make any network changes to their networks as required for the project;
- Any changes to existing environments required for the service will be Buyer's responsibilities;
- The Buyer will also provide any required test environments and test data reflective of the target implementation environment(s).

- Depending on the service model chosen, the Buyer may have other responsibilities which will be discussed, agreed and then described in the Order Form.
- If these responsibilities do not match your expectations, then please contact Capgemini in order that we can explore options to vary our approach.

5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact Capgemini to discuss which of these fits your requirements. These are:

- **Offshore resources**: Capgemini consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini consultants work from our UK offices. This provides a cost-effective solution for Buyers that require UK delivery.
- **Dedicated resources:** Capgemini consultants work on your sites, embedded as part of your team. This provides a solution for Buyers that require skills augmentation and a high degree of control over the work.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form and an exit plan in line with the Call-Off Contract terms which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognizes that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards

For the 12th year in a row, Capgemini has been recognized as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgment of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Capgemini can provide security delivery professionals with the following industry certifications:

- NIST Cybersecurity Framework (NCSF);
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified ISO/IEC 27001 Lead Implementer;
- Certified ISO/IEC 27001 Lead Auditor;
- Certified Information Systems Security Professional (CISSP);
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Security Manager (CISM);
- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF9, SABSA and other architectural methodologies including Capgemini's own;
- IT security specific MSc or PhD;
- Membership of the Chartered Institute of Information Security Professionals (CIISec)
- Certified in Risk and Information Systems Control (CRIS)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

10 Sub-contractors

Capgemini can offer these services using either onshore UK resources or offshore resources. Should the Customer choose an offshore service from India, then Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

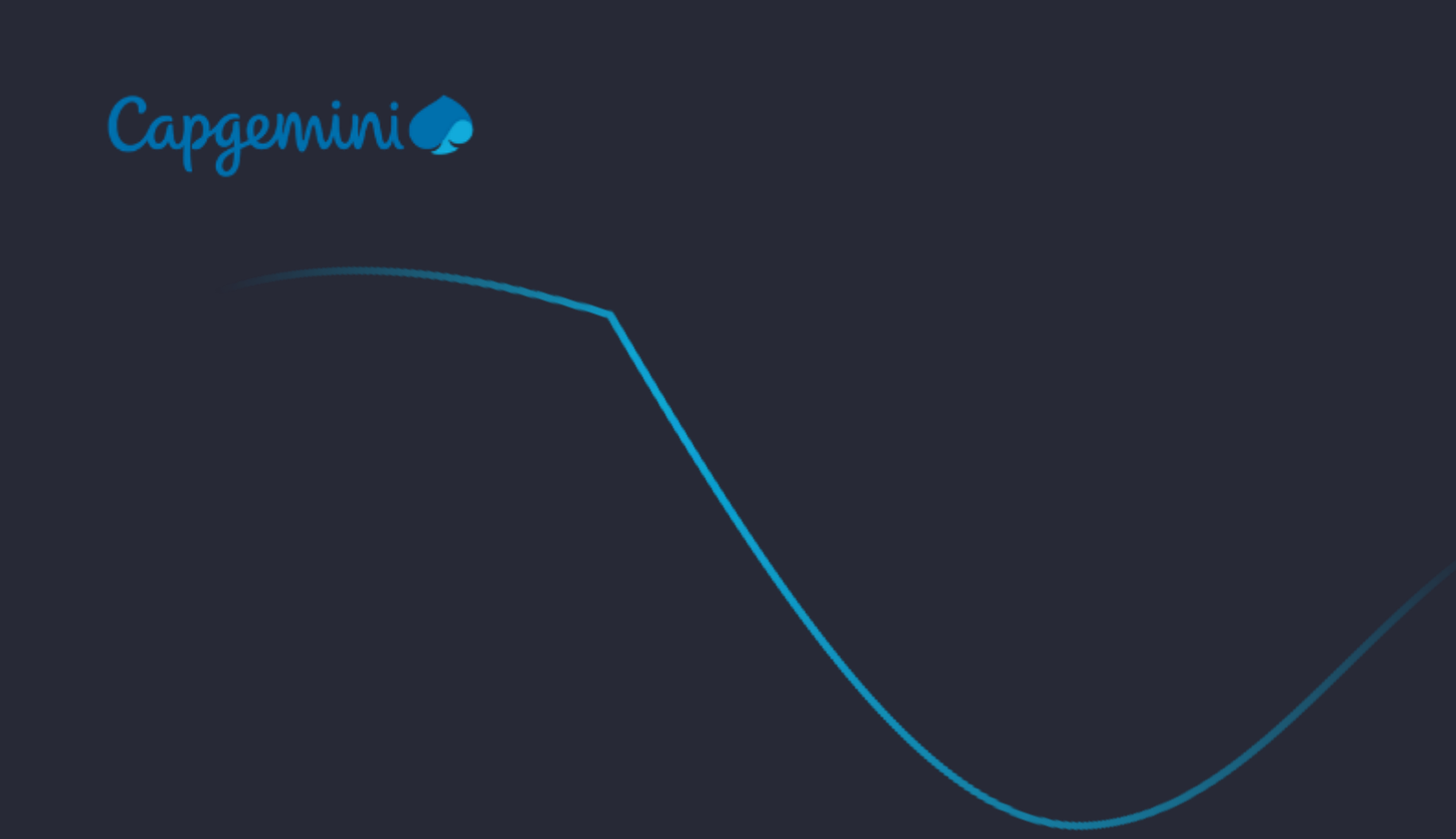
15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.



About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com