

IBM Consulting



G-Cloud 15 IBM – Threat Management Advisory Services Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Contents

Service Overview.....	3
Addressing Business Needs	5
Service Definition	6
IBM Approach	7
Why IBM?	8
Values and Outcomes	9
This is IBM in the UK.....	10

Service Overview

IBM provides comprehensive, vendor-agnostic, advisory services to develop your security operations and make your SOC better. We provide a range of services from SOC maturity assessments, AI SOC adoption strategy, SOC design & transformation, use case development & tuning to improve your security best practices and optimise your operational security.

Features

- Advisory and implementation services to make your Security Operations Centre (SOC) better.
- Perform a capability assessment of your security operations and develop an actionable plan to improve.
- Develop a security operations roadmap against existing investments and/or integrate new technologies.
- Embed AI into your SOC roadmap to capitalise on benefits and manage risks effectively.
- Leverage established Threat Management Framework to mature your SOC/Protective Monitoring capabilities.
- Holistic approach to maturing People, Process, Technology and Governance within a security operations context.
- Tailored, vendor agnostic services aligned to your security operations strategy.
- Demonstrate adherence to industry frameworks and standards to meet UK Government regulatory and compliance requirements.
- Identify areas to reduce risk and drives cost efficiency in your SOC operations.

Benefits

- Develop a security operations programme that balances value and cost.
- Improve the capabilities of your existing security operations team.
- Accelerated time to value through operationalising new and existing tooling.
- Improved preparedness for cybersecurity incidents and breaches.
- Reduce false positives and focus limited SOC analyst resource where it's needed.

Key Differentiators

- Extensive expertise supporting the most business-critical services for UK government, including Critical National Infrastructure across IT and OT.
- Comprehensive experience with an array of UK Government regulatory and industry frameworks for security, privacy and resilience.
- Tailored approach based on your preferred approach, acting as an extension of your team.
- Vendor agnostic, receive advisory services that leverage and optimise your existing tooling and resources.

Addressing Business Needs

IBM – Threat Management Advisory Services supports you in transforming your security operations and maturing your threat management programme.

Our team can help you address key challenges that organisations like yours are facing today:

Technology Optimisation

Organisations have made significant investments in technology and need support to optimise the value of these tools, rather than purchasing additional technology.

Lack of Skilled Resources

Lack of skilled human resources and adequate tools to manage day-to-day security operations and develop new capabilities.

Regulatory Landscape

Constantly shifting regulatory landscape requires continuous review and updates to policies, procedures and control frameworks specific to your industry and regulatory context.

AI Threat Management

The emergence of digital labour and AI agents as a workforce is not just a trend, it represents the fundamental shift in how work must be organized and executed within the Security Operations Center (SOC) to manage today's and tomorrow's threats.

Service Definition

We provide a variety of advisory and implementation services that provide expertise from current state assessment, roadmap development and design and build services.

Threat Management Advisory Services are designed to be tailored to meet business requirements and align with different levels of internal capability, providing commitment to service and quality levels throughout the engagement.

IBM – Threat Management Advisory Services provide a full range of capabilities including:

1. Maturity Assessment

Comprehensive assessment of the current state of your IT/OT security operations against leading frameworks, such as ISO 27001, NIST CSF and MITRE ATT&CK, to address identified gaps or weaknesses. Our experienced cyber security consultants can work with you to:

- Measure current state capabilities, maturity and compliance.
- Identify strategic and tactical recommendations.
- Develop a roadmap to implement recommendations.

2. Technology Optimisation

Design, deploy and optimise your preferred technologies within your security operations.

3. Design and Build Services

Based on your business objectives, compliance requirements, existing investments and current state operational requirements, we will work with you to:

- Transform your security operations programme.
- Leverage existing resources and investments.
- Benchmark your SOC metrics against best practice to improve performance.



IBM Approach

We bring the benefit of having worked with the world's largest organisations, transforming complex, critical services. Our approach is based on robust methods, processes and personalised engagement.

We focus on your business needs and developing trusted long-term relationships, underpinned by industry-leading experience and capabilities.

We want you to get the best out of every engagement and to deliver outcomes that matter for your organisation.

Our approach is tailored to your needs and flexible to support all delivery models. We offer established programme and portfolio capabilities that can be aligned with your internal governance and methods, linking to industry recognised standards such as MITRE ATT&CK, NIST and ISO27001.

We bring specific skills and attitudes including:

- Proven delivery track record working in complex environments.
- Access to specialists who understand the lessons and risks for transformation.
- Being able to advise, support and transfer knowledge with your teams.
- Implementing strong governance, defined collaboratively within the context of robust methods and processes.
- Bringing an integrated and controlled planning approach.
- Proactive identification and management of risks and issues based on experience.
- Working across complex existing and new platforms.
- Experience with the latest technologies, tools and delivery methods.

We work to manage the complexity of key business projects, programmes and portfolios, communicating with clarity and helping you make informed decisions.

Why IBM?

IBM provides a unique blend of cybersecurity and business expertise to help organisations through their transformation journey including:

- Extensive expertise supporting the most business-critical services for UK government, including Critical National Infrastructure across IT and OT.
- Comprehensive experience with UK Government, industry and regulatory frameworks for security operations.
- Breadth and depth of experience across regulated industries in co-creating a strategy to implement or enhance security operations programmes.
- Program governance tailored to your organisations needs, including the development and implementation of new and existing technologies, based on your preference.
- Building long-term client relationships based on innovation, trust and service excellence.
- Developing and deploying world-class talent.

Values and Outcomes

IBM can provide you with a comprehensive evaluation of your security operations, and support with remediating against any findings using proven industry standards and best practices.

We focus on your organisational needs and developing trusted long-term relationships, underpinned by industry-leading experience and capabilities so that you can be confident in the support of your critical services.

1. Maturity Assessment

- Independent assessment of your cyber security operations, enabling identification and of gaps and associated remedial measures.
- Includes current state observations and recommendations against industry best practices and best in class tools and models suited to your needs.
- Receive a personalised roadmap that lays out the steps to enhance your threat management capabilities.

2. Technology Optimisation

- Increase value from existing investments.
- Reduce costs from optimised tooling and avoiding potential additional investments.

3. Design and Build Services

- Establish a security operations programme aligned with organisational objectives to effectively manage threats and meet compliance requirements.
- Develop and implement a SOC architecture that reduce disruption costs and recovery times of key business processes.
- Test plans and playbooks against simulated cyber-attacks to improve crisis management.
- Optimise your security operations against best practice and industry benchmarks.

This is IBM in the UK

We have worked together with organisations in the UK for over 100 years, with a rich history of joint innovation and achievements, built on trusted relationships.



Cloud

Together, IBM and Red Hat are working to deliver the world's only **next-generation hybrid multicloud platform**



Economy

IBM has been **integral to the UK economy for >100 years**, and is one of its largest tech employers



R&D

In the UK alone, IBM **invests £170 million in R&D** each year



Quantum

IBM Q, the world's most advanced quantum computing initiative for commercial use, is being used by CERN



Environment

IBM's focus on sustainability began in 1971 with our first environmental policy



Artificial Intelligence

IBM develops **watsonx based generative AI solution** for the Austrian federal armed forces to **provide fact-based evaluation and classification** for the ability to remain capable of acting in the light of risk scenarios.



Changing the world

IBM was awarded **World Changing Company of the Year 2019** by Fast Company



Royal recognition

29 UK IBMers received honours from the **Queen** for contributions to tech and society



Diversity

IBM won the **Global Diversity Award 2019** and the **ENET's Gold Standard**



Graduates

IBM is committed to developing future talent – we are **Target Jobs' Graduate Employer of the Year 2019**



Volunteering

IBM dedicates **>20,000 volunteering hours every year** for a better society



Tech talent

IBM runs P-TECH schools in 18 countries, helping **>100,000 students build skills for careers of the future**



Inventors

IBM UK is home to many Master Inventors, with **>250 patents filed last year alone**

