Security Operations Centre as a Service (SoCaaS)

Service description details

Security Operations Centre as a Service (SoCaaS)

Methods' SOC-as-a-service is a powerhouse of cybersecurity vigilance, featuring 24/7 threat detection, proactive monitoring, and swift incident response. Anchored by certified NCSC expertise and advanced SOC management, our SOC ensures robust security architecture and compliance for public sector and CNI clients, fortified by our deep government/industry SOC experience.

What is the Service

Methods is an NCSC Assured Cyber Consultancy who has been assured to the highest standards as defined by NCSC and professional bodies such as UK Cyber Security Council. With a proven track record of delivering cyber security consultancy expertise, we pride ourselves on working closely with our clients - often augmenting in-house capability.

A Cyber Security Essentials Plus certified company, the services provided by the Cyber Portfolio align with ISO/IEC 20700 family of information security management standards, ensuring work is appropriately scoped, planned and delivered to the highest standards.

Methods provide a holistic approach to the provision of Security Operations Centre (SOC) services with work undertaken by industry qualified Cyber security experts, many holding CCP Lead Practitioner else qualified to Chartered status, able to offer approved guidance and support to both public and private sector clients, covering the entirety of the Security organisation.

Our team provides customers access to industry-recognised experts with proven experience supporting organisations to achieve a risk-appropriate security posture with Defence in Depth approach. We adhere to security standards and frameworks in line with industry best practice, including NSCS, CIS, OWASP, ISO 27001x, NIS, and NIST CSF.

Methods has a team of experts that proactively monitor an organisation’s ability to operate securely, averting cyber-attacks 24 x 7. Our services include:

- Protective Monitoring
- Incident response (EDR, NDR, XDR, SIEM, SOAR)
- Vulnerability management
- Threat Hunting and intelligence
- Security Operations consulting
- Compliance and coordination and context.

We assist the operational component of enterprise information security by collaborating with organisations to detect, analyse, respond to, report on, and prevent cybersecurity incidents. Additionally, we provide capabilities in root cause analysis.

We incorporate the organisation's security operations services to identify a strategy that incorporates business-specific goals from various business units, as well as input and support from senior management. We understand typical SOC infrastructure and can design and implement architectures and platforms to collect telemetry data via multiple sources. This data is then analysed and prioritised based on severity, risk, and impact.

Contact details

bidteam@methods.co.uk
020 7240 1121
www.methods.co.uk

Service description details

Our service offerings include a series of Security services that make up specific areas of a Security Operations centre. These Include, teams for a range of services such as EDR, vulnerability management, protective monitoring (SIEM), threat Intelligence, and incident response. These services work collaboratively to protect the organisations assets, and sensitive data as well as comply with industry or government regulations.

Methods' SOC capabilities provide organisations with:

- Security automation
- Effective technology
- Current threat intelligence.

Our methodology is agile and integrates seamlessly into the organisation, complementing and innovating current working practices. Whether the organisation requires ad-hoc support or a long-term partner, our team can help identify and implement best-in-class solutions.

Collaboration is one of our core tenets. We adopt principles of openness and knowledge transfer to empower people and build impressive, sustainable governance around complex multi-cloud solutions. Our consultants have a strong background in both public and private sectors, quickly adapting to environments and providing specialist expertise to design innovative and risk-based solutions.

We provide pragmatic and proportionate risk-based guidance as trusted consultants covering compliance, architecture, and design assurance. Our experienced consultants have proficiency working on various Government projects with different divisions, including critical national infrastructure, defence, policing, justice, education, healthcare, border control, central government, local authorities, and government digital services.

In line with HMG requirements, Methods is certified to Cyber Essentials Plus, ISO/IEC 27001, ISO 27017, and ISO 9001 standards. We adopt certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above. Methods has a large pool of SC and DV cleared UK personnel and experience in designing, building, and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET, and ABOVE SECRET classifications.

What it can do for you

Methods is an NCSC certified consultancy, boasting CCP Lead Practitioners in Cyber Security & IA Architecture. Our central aim is to establish a centralised function for detecting, containing, and remediating IT threats within your organisation. We specialise in identifying, analysing, communicating, investigating, and reporting events, alerts, and incidents round the clock 24X7, ensuring maximum transparency to your business. Additionally, we can facilitate a hub-and-spoke architecture, enabling continuous monitoring and enhancement of your organisation's security posture.

Service Features

1. 24x7 SOC strategy, design, build, and management
2. Advanced threat detection with human-led proactive hunting analytics
3. Incident containment with SOAR and emergency support capabilities
4. Continuous network and endpoint monitoring with expert alert analysis
5. Comprehensive cloud security across AWS, Azure, and Google Cloud
6. Certified cybersecurity consultancy ensuring optimal threat disruption and response
7. Real-time threat intelligence integration for pre-emptive security measures
8. Robust cybersecurity event management with SC cleared monitoring
9. Agile SOC services for cloud, network, and infrastructure integration
10. Dynamic threat prevention, detection, and response for enterprise protection

Service Benefits

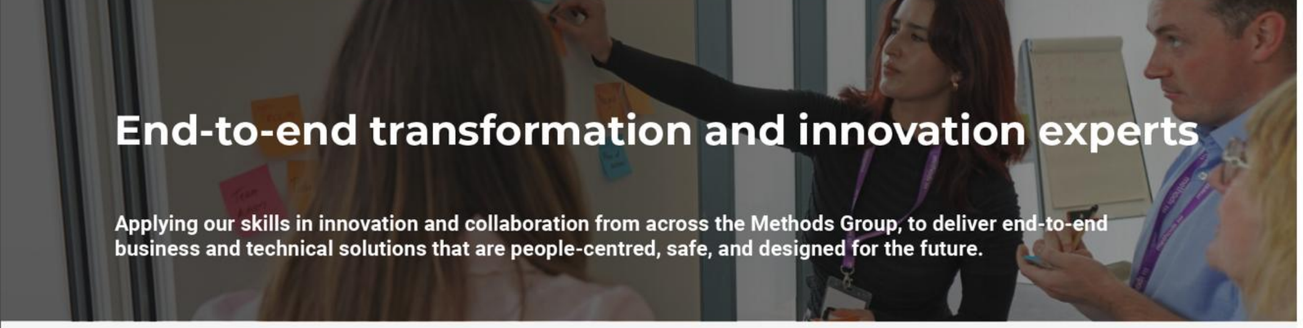
1. 24/7 centralised monitoring, proactive threat management and incident response
2. Comprehensive investigation, triage, and post-incident analysis and alert reporting
3. Advanced Machine Learning for behaviour analytics and threat hunting
4. Optimising SOC with tailored use cases, rules, and response playbooks
5. Efficient log management for optimal storage cost-saving strategies
6. Digital forensics support for thorough investigative processes
7. Robust protection techniques from incident detection to resolution
8. Integrates seamlessly with existing service desk operations
9. Delivers regular performance reviews and real-time security insights
10. Certified and experienced cybersecurity team ensuring compliance and reduced risks

Contact details

bidteam@methods.co.uk

020 7240 1121

www.methods.co.uk



End-to-end transformation and innovation experts

Applying our skills in innovation and collaboration from across the Methods Group, to deliver end-to-end business and technical solutions that are people-centred, safe, and designed for the future.

Methods provide collaborative and innovative solutions to help Central Government adapt to the changing landscape and deliver better outcomes for citizens.

With a focus on driving interoperability and innovation in UK Central Government, we have helped multiple organisations in the sector modernise their IT architecture, systems, strategy, and operating models to improve organisational resilience and service delivery.

Methods deliver wide-ranging services and thought leadership to support delivery including:

Onboarding and offboarding process

1. **Understand Requirements**

   It is essential that we work with you to understand the requirement so that we provide the right resources with directly relevant experience at an appropriate level of seniority

2. **Protect Team Availability**

   Having the right team on board from the start and maintaining continuity throughout the project ensures timely delivery of desired outputs

3. **Work Synergistically and Innovatively**

   Drawing from our past experiences, we can frequently recommend optimal delivery methods and/or alternative solutions which will deliver benefits (or cost-savings) over time

4. **Service Scope**

   Ensuring that the scope of the service to be delivered is properly quantified involves agreeing on logistics (e.g., deliverables, timelines, quality criteria, etc.) and understanding your constraints, sensitivities, and key drivers to match your expectations accurately

5. **Review/Agree Engagement**

   After initial discussions and planning, you'll review and amend a draft Statement of Work(s)/Services to ensure mutual agreement and alignment of objectives before starting the assignment. We may iterate the Statement of Work(s) with you to finalise the requirements

Ordering and Invoicing

Once we have agreed a Statement of Work(s) we will sign the appropriate agreement and complete a Call Off contract with an attached Statement of Work(s), and submission of a Purchase Order. We will then set up a mutually acceptable start date and commence work.

Payment terms are 30 days or less as may be agreed.

Please note - we are unable to accept Government Procurement Card (GPC) payments.

Customer Responsibilities

For any given requirement, we will identify any dependencies on the customer (e.g. access to key stakeholders, facilities, documentation, etc.) and agree these at the start of the work.

Making a difference

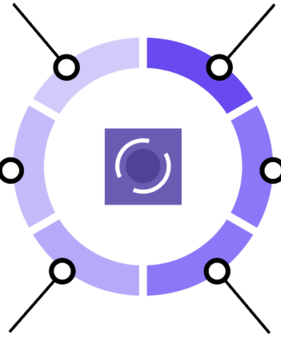
The work we do each day is focused on delivering a positive difference for the public sector for the benefit of society as a whole.

Environment

We use the 'recycle, reuse, repair, refuse' approach to waste reduction to minimise landfill waste, support climate initiatives, and enhance biodiversity, creating a sustainable environment for our colleagues and community

Volunteering

We continue to support charitable causes that align with and support our values including our charity partner and VCSE initiatives



Investment in Talent

We cultivate young talent through our GRAVITATE programme, championing vibrant apprenticeship and graduate schemes while aiding tech career exploration for individuals aged 14-24

Diversifying our Supply Chains

We diversify our local supply chains, promoting small business enterprise and engaging local people, SME, and micro-business suppliers

Staff Wellbeing

We support colleague wellbeing through clear career pathways, strengthened PDPs, and our continued commitment to the Armed Forces Covenant, including achieving Gold Employer Status. Moreover, we continue to support our colleagues holistically, considering them as complete individuals at every career stage with Methods

Safeguarding Services

We continue to provide insightful thought leadership on leveraging modern technology to secure our public services for future generations. This involves speaking at industry events, educating youth on tech career paths, and offering pro-bono advice to senior policymakers

Customer stories

Cloud Hosting & Service Modernisation
Modernised digital services using secure cloud hosting, streamlined legacy workflows, and improved data insights. Delivered faster decisions, reduced manual effort, and a more transparent, **user-friendly experience** for internal teams and external users.

Cloud-Based ITSM Consolidation
Unified multiple service desks onto a cloud-based ITSM platform, standardising processes and automating workflows. Improved incident, change, and problem management, **boosting** overall **service reliability, efficiency, and organisational visibility**.

Large-Scale Cloud Migration (100+ Apps / 120TB)
Delivered cloud migration of **100+ legacy applications** and **120TB of** data with **100% availability**. Strengthened compliance, improved transparency, and significantly enhanced operational resilience across critical digital services.

Azure Migration & Modern Workplace Enablement
Migrated data centres to Azure and deployed modern workplace cloud services, delivering secure, scalable infrastructure. Achieved improved user experience, strengthened security posture, and **£1m savings** - all with zero service disruption.

Cloud ITSM Migration (ServiceNow SaaS)
Successfully migrated from a legacy ITSM tool to a modern, cloud-based ServiceNow platform. Delivered scalable, robust service operations, strengthened governance, and enabled faster, more consistent digital service delivery across the organisation.

Cloud-Native Data Pipelines (Azure Integration)
Built automated Azure Data Factory pipelines into a Lakehouse architecture, using Bronze/Silver/Gold layers and Delta with CI/CD. Delivered secure daily refreshes, improved data quality, lower manual effort, and more efficient reporting.