CSACyber | G-Cloud

CSA Managed Security Operations Centre (SOC) Service

The CSA Managed Security Operations Centre (SOC) Service provides 24/7/365 monitoring, detection, investigation, and incident response to protect organisations against evolving cyber threats.

Delivered by UK-based, security-cleared analysts, the service combines advanced tooling, behavioural analytics, automation, and threat intelligence to ensure rapid identification and containment of attacks. CSA operates a CREST-accredited SOC backed by proven operational processes, strong governance, and deep expertise in Microsoft Sentinel, endpoint security platforms, and threat-hunting methodologies. The service includes continuous tuning, custom detection rules, dashboards, and collaborative communication channels to integrate seamlessly with customer environments.

CSA's SOC enhances resilience through proactive threat hunting, automated enrichment and response workflows, and structured reporting for technical teams and senior stakeholders. With compliance alignment across ISO 27001, Cyber Essentials Plus, and industry-specific requirements, the service provides a scalable, future-ready security capability suitable for public sector, critical national infrastructure, and regulated organisations.

The CSA Cyber MDR service is your bird's-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

References and case studies can be provided on request.

BENEFITS

Monitoring, Detection & Alerting
Providing 24/7/365 monitoring of network activity and systems for security threats, promptly identifying anomalies, and triggering alerts to enable swift response, protecting against potential cyber attacks and data breaches.

Incident Investigation
Analysing security breaches or suspicious activities to determine their root cause, impact and method of occurrence, aiming to prevent future incidents and enhance existing security measures.

Threat Intelligence
Combination of Microsoft, NATO, Mandiant and OT threat intelligence feeds, fed directly into Microsoft Sentinel SIEM.

Threat Hunting
Providing threat hunting on your activities at scale, tapping into decades of organisations data, identifying new attack vectors and tactics, techniques and procedures (TTPs).

CREST Security Operations – Security Operations Centre
CREST Incident Management – Incident Response
CREST Security Testing – Penetration Testing
CREST Red Teaming – Intelligence-led Pen Test
CREST Security Testing – Vulnerability Assessment

Assured Service Provider – in association with National Cyber Security Centre – CHECK Penetration Testing

Assured Service Provider – in association with National Cyber Security Centre – Cyber Incident Response: Standard Level

Cyber Essentials

Cyber Essentials Plus

hello@csacyber.com
csacyber.com
0300 303 4691