MANAGED CSOC/ SIEM SERVICE

Protect your organisation with Six Degrees' government-accredited Cyber Security Operations Centre (CSOC), offering 24x7 security monitoring, detection and alerts around your infrastructure and technical solutions for full security event visibility and incident management.

With Six Degrees' Managed CSOC/SIEM service, you can secure your platforms through our UK-based CSOC team that will monitor and manage your infrastructure 24x7. Our experienced CSOC Analysts will identify potential cyber security breaches and incidents and actively work to isolate and contain threats.

The Managed CSOC/SIEM service leverages a Security Information Event Management (SIEM) platform that receives event log data from devices and services within your technical infrastructure including on-premises, SaaS, PaaS, public and private cloud, and hybrid-based environments, which ensures your organisation's infrastructure is fully monitored and protected.

The service is provided by knowledgeable and professional Security Cleared (SC) CSOC Analysts who are continuously trained and certified to identify and contain increasingly advanced and sophisticated threats.

Managed CSOC/SIEM Service Benefits

- Tailored to your organisation's requirements for optimal performance.
- Proactive and effective response to mitigate potential threats and breaches.
- A cost-effective alternative to building a specialised in-house cyber security operations centre.
- Reassurance that your organisation is protected 24x7x365 by experienced and Security Cleared (SC) CSOC Analysts.
- Access guidance on strategic decisions through monthly reports that track incidents.
- Assistance with compliance and regulations.

Managed CSOC/SIEM Service Features

A CSOC service that is designed and configured to your environment.

Six Degrees will design a solution that is tailored to your security monitoring requirements. Highly experienced and certified Security Consultants and Engineers will configure and test the solution to assure correct configuration and that event information and feeds are provided to the SIEM platform correctly, providing reassurance that all threats and breaches can be detected and offering guidance to assist and remediate effectively.

Proactive triage and alert analysis to inform you of all potential threats.

The CSOC Analysts will monitor your environment 24x7 and will review and triage all incidents and provide mitigation guidance, issuing a prioritised notification to you via the Incident Management System (IMS). If incidents are connected, they will be linked together for clarity and focused effort.

Threat analytics and investigation enables quick response to threats.

The CSOC Analysts will conduct further investigations across priority incidents to identify possible causes, indirect associations to other indicators and scale of potential breach. The CSOC will provide you with further mitigation guidance relevant to the incident, allowing quick actions to be taken and for threats and risks to be remediated promptly.

Assurance with meeting important compliance regulations.

The Managed CSOC/SIEM Service also helps you align to your chosen compliance frameworks. The service is provided as an HMG PSN accredited service, and can be delivered to assist with your own HMG, ISO, PCI DSS or other information security standards.

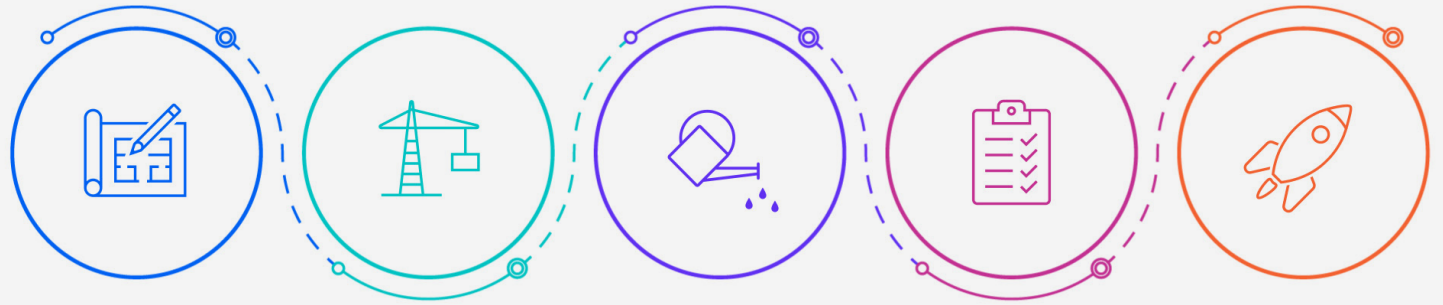
Develop your cyber security maturity with monthly reports.

We will provide you with a monthly report on key findings and issues detected by our CSOC. The reports will assist in tracking security performance, identifying common issues, and allowing strategic decisions to be made for developing your security maturity.

Provide a full understanding of the importance and impact of incidents.

As part of the deployment, your solution will be tuned to a baseline – establishing rules and policies to suppress false positives and filter out irrelevant events and data emanating from your monitored assets. Any alarms from suspected incidents will automatically generate an incident ticket in the CSOC IMS, and will be prioritised by the CSOC analysts based on the incident severity. All event logs are stored and retained for 12 months, and can be accessed retrospectively for security investigation or used to identify activities around events after they occur.

Managed CSOC/SIEM Service Onboarding



- All Managed CSOC/SIEM services must be individually scoped. This scope is checked at the start of the onboarding process and changes to scope may impact the onboarding and service costs.
- All Managed CSOC/SIEM services are comprised of a consultancy onboarding element followed by the managed service element.
- Sentinel-based solutions will create an additional usage-based cost for the client.
- The service is designed to meet individual client needs.
- Onboarding requires assistance from the client and commitment to work with the onboarding team to achieve quality service results.
- Onboarding typically takes around 6-8 weeks; smaller environments may be onboarded in 4 weeks, while larger onboards may be phased over several months.
- Contract length is typically 3 years.

Our Credentials

Gold Microsoft Partner | Azure Expert MSP

Member of Microsoft Intelligent Security Association

CYBER ESSENTIALS PLUS

ISO 27001 | 9001 | 22301

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

For more information about the Managed CSOC/SIEM service, please contact sales@6dg.co.uk or call 0800 012 8060.