CNS
at Six Degrees

MANAGED DETECTION AND ALERT

Protect your organisation with Six Degrees' Security Operations Centre (SOC), offering 24x7 security monitoring, detection and alerting around your infrastructure and technical solutions for full security event visibility and incident management.

With Six Degrees' Managed Detection and Alert service, you can secure your platforms through our experienced SOC team that will monitor and manage your infrastructure 24x7. Our experienced SOC Analysts will identify potential cyber security breaches and incidents and alert you and provide guidance on how to isolate and contain threats.

The Managed Detection and Alert 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 SOC Analysts who are continuously trained and certified to identify and contain increasingly advanced and sophisticated threats.

Managed Detection and Alert Service Benefits

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

Managed Detection and Alert Service Features

A SOC 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 SOC 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 SOC Analysts will conduct further investigations across priority incidents to identify possible causes, indirect associations to other indicators and scale of potential breach. The SOC 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 Detection and Alert service also helps you align to your chosen compliance frameworks. The service can be provided as an HMG accredited service, and can be delivered to assist with your own HMG, ISO, PCI DSS or other information security standards.

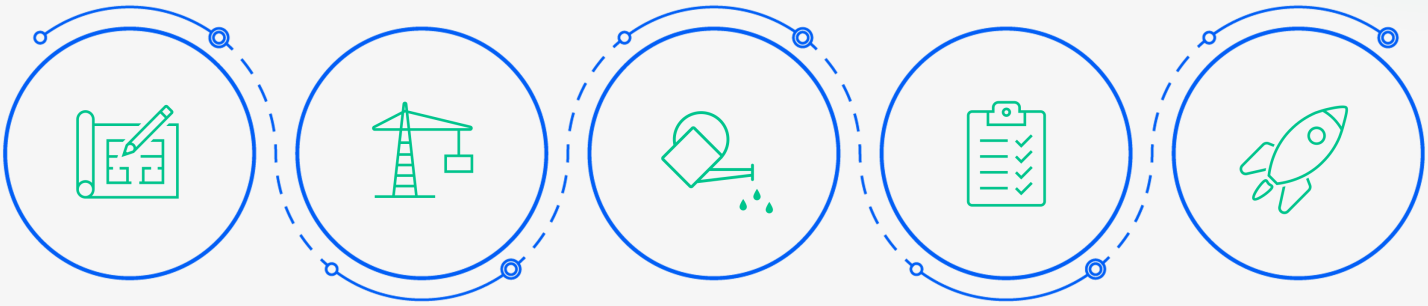
Develop your cyber security maturity with monthly reports.

We will provide you with a monthly report on key findings and issues detected by our SOC. 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 SOC IMS, and will be prioritised by the SOC analysts based on the incident severity. All event logs are stored and retained for up to 24 months in immediately accessible storage and can be accessed retrospectively for security investigation or used to identify activities around events after they occur. Archived storage options are available for storing log data for up to 7 years.

Managed Detection and Alert Service Onboarding



Initiation and Planning

Transition and Build

Tuning and Optimisation

Staging

Go Live

- All Managed Detection and Alert services must be individually scoped. This assures we meet your business' exact requirements.
- All Managed Detection and Alert services are comprised of a consultancy onboarding element followed by the managed service element.
- Our Managed Detection and Alert services are powered by Microsoft Sentinel SIEM technology. This solution is a cloud based system and will generate usage and storage fees. These fees are estimated for you during the pre-sales process so that there are no hidden costs.The service is designed to meet your individual needs.
- Onboarding requires assistance from the client and commitment to work with the onboarding team to achieve quality service results.
- Onboarding will require some assistance and commitment from you to assure the onboarding team achieves quality service results.
- There is a choice of contract length from 12 months to 10 years; initial contract length is typically 3 years.

Our Credentials

Microsoft Partner | Azure Expert MSP

Member of Microsoft Intelligent Security Association

Microsoft Solutions Partner – Infrastructure Azure – Specialist Infra and Database Migration

Microsoft Solutions Partner – Modern Work – Specialist Calling for Microsoft Teams

Microsoft Solutions Partner – Security – Specialist Cloud Security, Threat Protection

Microsoft Solutions Partner – Digital & App Innovation Azure

Microsoft Solutions Partner – Data & AI Azure – Specialist Infra and Database Migration

Certification Body Cyber Essentials Plus

PCI Security Standards Council Qualified Security Assessor™

ISO 27001 | 9001 | 22301

CNS at Six Degrees

For more information about the Managed Detection and Alert service, speak to your Account Manager or contact us.