D2NA™

G-Cloud Service Definition

Managed Detection and Response

For G-Cloud 14

Security Operations Centre

A Security Operations Centre (also known as a SOC) is a centralised location where our team continuously monitors, analyses, and responds to cybersecurity incidents and threats. The primary goal of the SOC is to protect a business from live threats before they cause any problems and this is done by monitoring multiple areas including network traffic, login information, applications, and information usage.

Bad Threat Actors do not just operate during business hours. Implementing an outsourced SOC means that you have the peace of mind that your environment is being monitored 24/7 by experts. In a world where more cyber threats are being discovered daily; having a SOC can help detect and prevent damage to your organisation in the earliest stages, helping you sleep a little easier at night knowing that you are being kept safe.

Microsoft Sentinel SIEM

Our SOC is powered by Microsoft Azure Sentinel which is an industry-leading SIEM platform. Microsoft Sentinel gives us a platform for attack detection, threat visibility, proactive hunting, and threat response. Sentinel raises instant alerts to our UK based team who can react 24/7 to any threats or concerns.

Threat Monitoring

Continuous monitoring of your company's IT systems to identify potential security issues or anomalies.

Incident Response

Promptly identify and contain security incidents, followed by remediation and recovery efforts to minimize impact to the business.

Threat Intelligence

Gathering and analysing information about emerging threats, attack sources, and threat actors to improve the company's security posture.

Vulnerability Management

Identify, assess, and prioritize weaknesses in the company's systems and processes, and work with your team to address them.

Security Analysis

Examine a wealth of security data and logs to identify patterns and features that may indicate potential threats or areas for improvement.