D2NA

G-Cloud Service Definition

Security Operations Centre (SOC)

For G Cloud 15

CREST SECURITY TESTING Penetration Testing

CREST SECURITY OPERATIONS Security Operations Centre

CREST SECURITY TESTING Vulnerability Assessment

CYBER ESSENTIALS PLUS

Vanta PARTNER

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS ISO 9001:2015 9940

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS ISO/IEC 27001:2022 9940

Security Operations Centre

Part of D2NA's Cyber Ascend Framework

Who We Are

D2NA is a UK-based cybersecurity specialist with over 20 years' experience supporting public and private sector organisations.

We're trusted by CREST and IASME to deliver Cyber Essentials/Plus, Penetration Testing, SOC and Managed Support Services. We are proud to be one of only 41 UK-based Security Operations Centres (SOCs) accredited by CREST, the gold standard for security assurance.

Our team holds key industry certifications, including ISO/IEC 27001:2022 for information security, ISO 9001 for quality management, and Cyber Essentials Plus. These accreditations demonstrate our commitment to the highest standards of security, quality, and continual improvement.

Our Approach

We know that every organisation is unique. That is why we take the time to understand your organisation, your risks, and your goals. Our approach is proactive and partnership-driven: we do not just deliver technology, we work alongside your team to provide ongoing support, clear communication, and strategic guidance. Our services are designed to be scalable and flexible, so they can and grow with your organisation and adapt to changing needs.

Managed Detection and Response

The core service offered by D2NA's CREST accredited UK Security Operations Centre (SOC) is **Managed Detection & Response (MDR)**, powered by **Microsoft Sentinel SIEM** and **Microsoft Defender XDR**.

Designed for UK public sector organisations, this service provides continuous monitoring, rapid incident response, and proactive threat hunting to reduce risk and ensure compliance with NCSC and ISO standards.

Managed Detection & Response (MDR) included as standard

- ✓ Continuous 24x7 monitoring combining the best of modern security technology
- ✓ and expert human oversight
- ✓ Microsoft Sentinel SIEM
- ✓ Microsoft Entra ID Connector
- ✓ Microsoft Defender XDR Connectors
- ✓ Infrastructure Connectors (Firewalls, Hypervisors, Networking, etc)
- ✓ Application Connectors
- ✓ Threat Intelligence
- ✓ Proactive Threat Hunting
- ✓ Rapid Incident Response
- ✓ Reporting demonstrating evidence of risk reduction and governance

Service Benefits

- ✓ Reduces business risk with 24x7 CREST-accredited UK SOC monitoring
- ✓ Improves detection speed using Microsoft Sentinel SIEM and Defender XDR
- ✓ Accelerates response times; contains threats quickly through MDR analysts
- ✓ Reduces downtime via proactive threat hunting across cloud and endpoints
- ✓ Improves compliance with NCSC, ISO 27001, Cyber Essentials Plus
- ✓ Reduces patch backlog through coordinated endpoint and infrastructure patching
- ✓ Strengthens user resilience with phishing testing and awareness training
- ✓ Provides clear reporting dashboards with evidence of risk reduction and governance
- ✓ Simplifies procurement, integration, onboarding; UK public sector-ready managed service
- ✓ Reduces alert fatigue; automates incident triage with SOAR playbooks automation

Support Levels

Standard Support includes the following: 24x7 access to our UK-based SOC team via phone, email, and secure portal. Incident triage Investigation Remediation guidance Automated reporting	**Enhanced Support includes Standard Support plus the following:** Proactive service reviews Tailored reporting Quarterly Threat Posture Assessment (a structured review of your security posture, including threat intelligence analysis, SOC data trends, risk scoring, and actionable recommendations to strengthen defences and meet compliance, with an executive summary for leadership).	**Premium Support includes Enhanced Support plus the following:** Dedicated Technical Account Manager (TAM) for strategic guidance, escalation management Priority access to senior analysts.

Onboarding, Service Management & Exit

Onboarding and exit are straightforward, with minimal disruption and full data portability.

Onboarding process includes the following steps:

- ✓ Risk Assessment
- ✓ Identification of VIP's (people and assets)
- ✓ Setup of Sentinel and Lighthouse
- ✓ Connectors for Entra ID and Endpoint XDR
- ✓ Connectors for Infrastructure and Applications
- ✓ Syslog Server (if applicable)
- ✓ Setup of Tailored Reporting (if applicable)

Service Management Reviews include the following:

- ✓ Review of Risks, Vulnerabilities and Incidents, with remediation advice
- ✓ Review of Risk Assessment
- ✓ Review of VIP Lists
- ✓ Review of Threat Intelligence
- ✓ Review of Tailored Reports (if applicable)

Complimentary Services

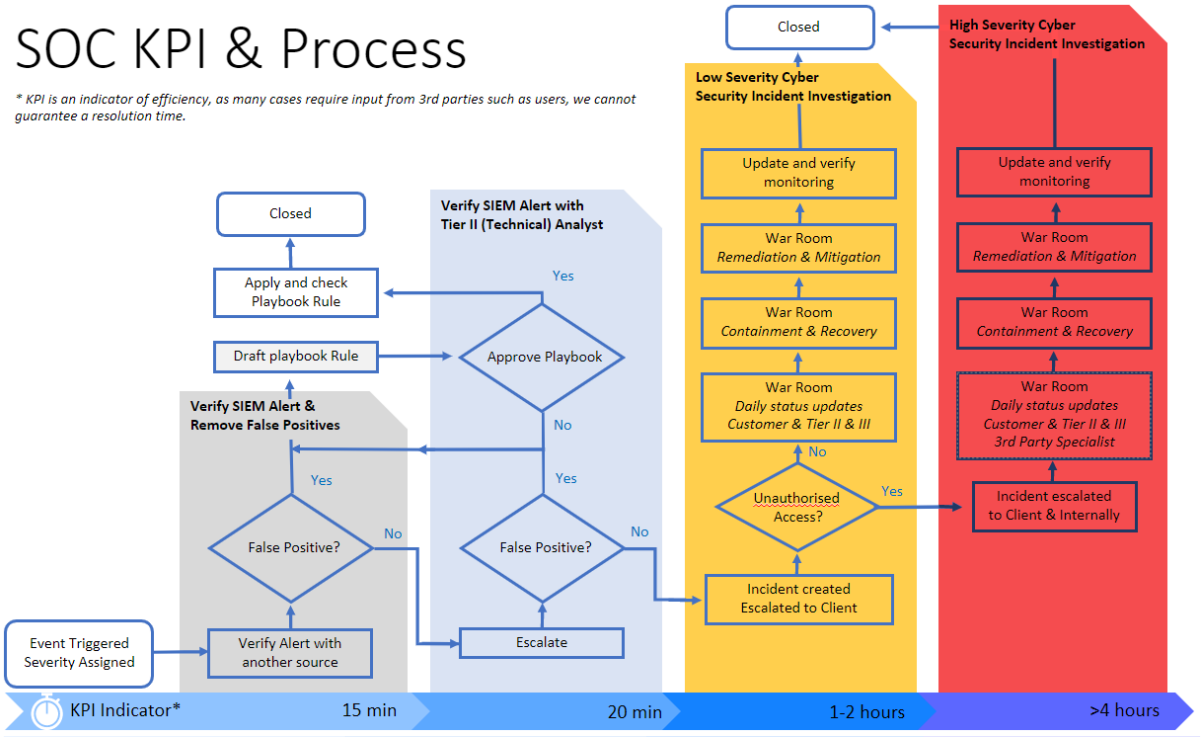
In addition to the core MDR service, our SOC also offers the following complimentary services to further strengthen your security posture.

- ✓ Vulnerability Management
- ✓ Endpoint Patching
- ✓ Infrastructure Patching
- ✓ Governance, Risk & Compliance
- ✓ Phishing Testing & User Awareness Training (D2Aware)
- ✓ Virtual Chief Information Security Officer (CISO)

Managed Detection & Response SLA's, KPI's & Process

Our CREST-accredited SOC is made up of three distinct levels, Tier I Analysts, Tier II Analysts, and our SOC manager. The entire team is UK based and work on a rota basis to ensure round-the-clock coverage.

The chart below indicates how our OLA's (described as a KPI) and processes are defined:



Tier I Analyst

KPI 15 min *True Positive* - An Alert is received in the SIEM and verified against another data source to confirm a True Positive and escalate as soon as possible. Alerts can have multiple data points to verify and some may require input form a 3rd party such as a user or partner.

KPI Up to 14 hours *False Positive* - These should be removed from any future Alerts with a Playbook Rule. This is authorised by a Technical Tier II Analyst to ensure accuracy of alerts going forward. The Alert is closed as False Positive.
Eg: legitimate email attachment

Tier II Technical Analyst

KPI 20 min Verify *True Positive* - The Alert is double checked against the second data points and escalated to a Cyber Security Incident as quickly as possible.

False Positive – Alerts are passed back to the Tier I Analyst and discussed for further training and addition to the Playbook.

Tier II Technical Analyst & SOC Manager

KPI 1-2 hours *Investigate* - This is escalated to the client in the agreed method. The investigation aims to identify as much information to apply mitigations for future Cyber Security Incidents and ensure these are correctly implemented and monitored.
Eg: Phishing attempt caught before any payloads executed (likely relies on user input).

False Positive – This is used to improve Alert Detection and training.

Tier II Technical Analyst & SOC Manager

KPI >4 hours *Investigate* - This Cyber Security Incident involves Unauthorised Access of any kind and is escalated to the client in the agreed method. The investigation aims to identify as much information to work with partners on containment and recovery.
Eg: 2-4 hours - Phishing link clicked & credentials harvested. 6-8 hours - Ransomware recovery of 4 PCs with backups.

False Positive – This is used to improve Alert Detection and training.

TIME: Times are based upon an average from an event being triggered. For Alerts generated from Threat Hunting the first alert is manually generated.
ALERTS: It is possible for a Cyber Security Incident to occur WITHOUT generating an alert. For Example: the attack vector is so new, the SOC has no Alert to Trigger.
RESOLUTION: Events will likely require input from 3rd parties for investigation and resolution, therefore we do not recommend MTTR (Mean Time to Resolve) as a measure of efficiency.
** KPI is an indicator of efficiency, as many cases require input from 3rd parties such as users, we can NOT guarantee a resolution time.*