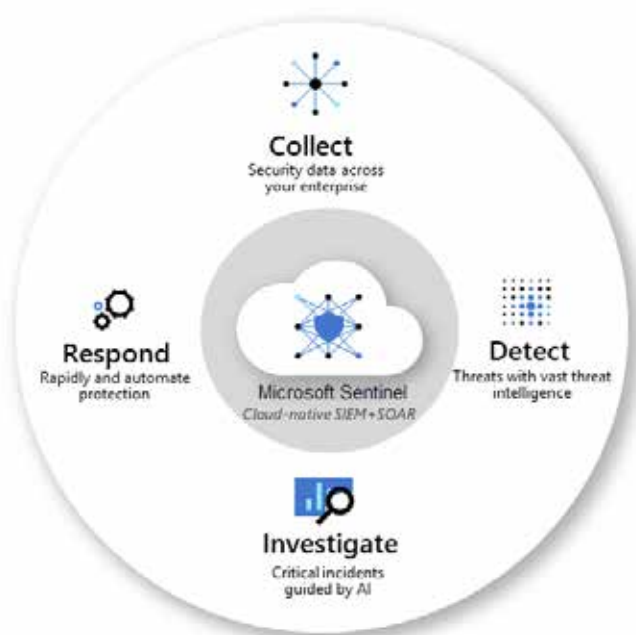# Managed Detection & Response (MDR)

Powered by Microsoft Sentinel

What is Managed Detection & Response (MDR)?

Managed Detection & Response is a service provided to an organisation that allows the IT Security Team to be able to **detect** potential security events and then prioritise and **respond** to them.

The CSA MDR service delivers intelligent security analytics and threat intelligence across the enterprise. Powered by Microsoft Sentinel, you secure a single solution for attack detection, threat visibility, proactive hunting, and threat response.

The CSA 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.

Collect
Security data across
your enterprise

Respond
Rapidly and automate
protection

Microsoft Sentinel
Cloud-native SIEM + SOAR

Detect
Threats with vast threat
intelligence

Investigate
Critical incidents
guided by AI

COLLECT

Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

DETECT

Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft

INVESTIGATE

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft

RESPOND

Respond to incidents rapidly with built-in orchestration and automation of common tasks

cybersecurity
associates

Managed Detection & Response (MDR)

Powered by Microsoft Sentinel

Our **M**anaged **D**etection & **R**esponse (**MDR**) Service

The CSA
Managed Detection &
Response Service

MONITORING & ALERTING

Providing 24/7/365 monitoring of the IT infrastructure across your organisation, alerting you to any security events that have been dealt with or require further action to be taken.

INCIDENT INVESTIGATION

Providing full end to end incident investigation to find the route cause of the security event and help you to reduce the remediation time.

THREAT INTELLIGENCE

Providing you with real-time threat intelligence fed directly into Microsoft Sentinel. Covering key Indicators of Compromise (IoCs).

THREAT HUNTING

Providing threat hunting on your organisations data, identifying new attack vectors and tactics, techniques and procedures (TTPs).

AUTOMATED RESPONSE

Providing automated responses to high risk threats through Security Orchastration, Automation and Response (SOAR).

FULL 24/7/365 SERVICE

RAPID DEPLOYMENT

EASY INTEGRATION

KEEP FULL CONTROL OF YOUR DATA

Managed Detection & Response (MDR)

Powered by Microsoft Sentinel

The CSA **M**anaged **D**etection & **R**esponse (**MDR**) Service Features

REAL TIME LOG INGESTION	**SUPPORTED OPERATING SYSTEMS**	**SINGLE PORTAL & DASHBOARDS**
FULLY COLLABORATIVE WORKING WITH CLIENTS	**THREAT INTELLIGENCE**	**THREAT HUNTING**
USER ENTITY BASED ANALYTICS (UEBA)	**SECURITY ORCHASTRATED AUTOMATED RESPONSE (SOAR)**	**UK BASED GOVERNMENT SECURITY CLEARED CYBER ANALYSTS**
CLIENT HAS FULL TENENT DATA CONTROL	**EXPERIENCED & CERTIFIED SOC TEAM**	**INCIDENT RESPONSE LEADERSHIP SUPPORT**

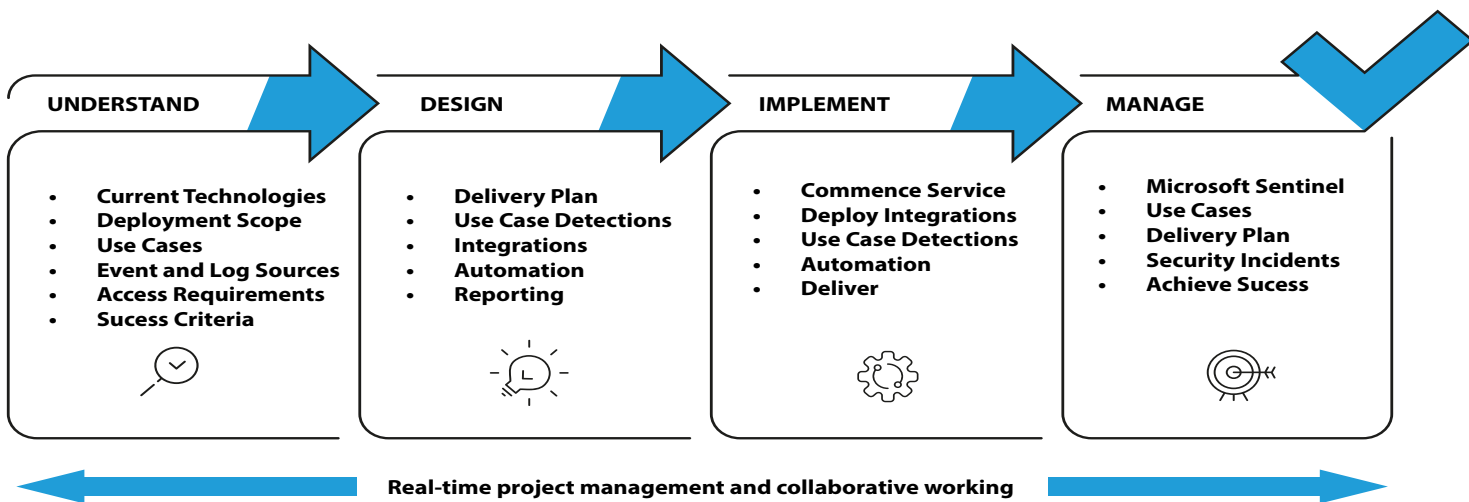# Managed Detection & Response (MDR)

Powered by Microsoft Sentinel

Our MDR Service On-Boarding Process

Built and delivered on a tried and tested process

CSA, through the use of Microsoft Teams and SharePoint has developed a streamlined on-boarding process that gives you all the information that is required to ensure success. Through our collaborative working approach the CSA team are able to keep the client updated at every step of our process.

Our collaborative project management approach not only keeps you updated on the progress of each step of the on-boarding process, but is proven to increase communication flows and ensure information is shared continuously and accurately.

UNDERSTAND
- Current Technologies
- Deployment Scope
- Use Cases
- Event and Log Sources
- Access Requirements
- Sucess Criteria

DESIGN
- Delivery Plan
- Use Case Detections
- Integrations
- Automation
- Reporting

IMPLEMENT
- Commence Service
- Deploy Integrations
- Use Case Detections
- Automation
- Deliver

MANAGE
- Microsoft Sentinel
- Use Cases
- Delivery Plan
- Security Incidents
- Achieve Sucess

Real-time project management and collaborative working

To book a demonstration of our MDR Service or for more information please contact us on +44 (0)300 303 4691 or email us at info@csa.limited

cybersecurity associates

Managed Detection & Response (MDR)

Powered by Microsoft Sentinel

Why choose Cyber Security Associates Ltd?

Built on experience and expertise to offer robust cyber security services

Established in 2013, Cyber Security Associates Limited (CSA) provides cyber consultancy and cyber managed services which help to detect, protect and educate against the ever-changing cyber threat. CSA has built their team from a foundation of Government (ex-Military) and Commercially experienced specialists all holding current and relevant cyber certifications.

Today our cyber services are built around a 24/7 SOC based within the UK's cyber hub in Gloucestershire.
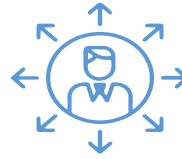
Experience

We are cyber warriors with more than 50 years' experience

Trusted

By the world's largest brands and government organisations

Proactive

Approach to security strategies

Insight

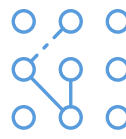Into all of the Latest cyber threats and trends

Service Led

Customer first approach to all solutions

World Renowned

Partnerships and accreditations

Flexiblity

Not tied to one single tool or solution

Ambitious

We have ambitious growth plans supported by our investors

Innovation

Leading technology and service capabilities for the future