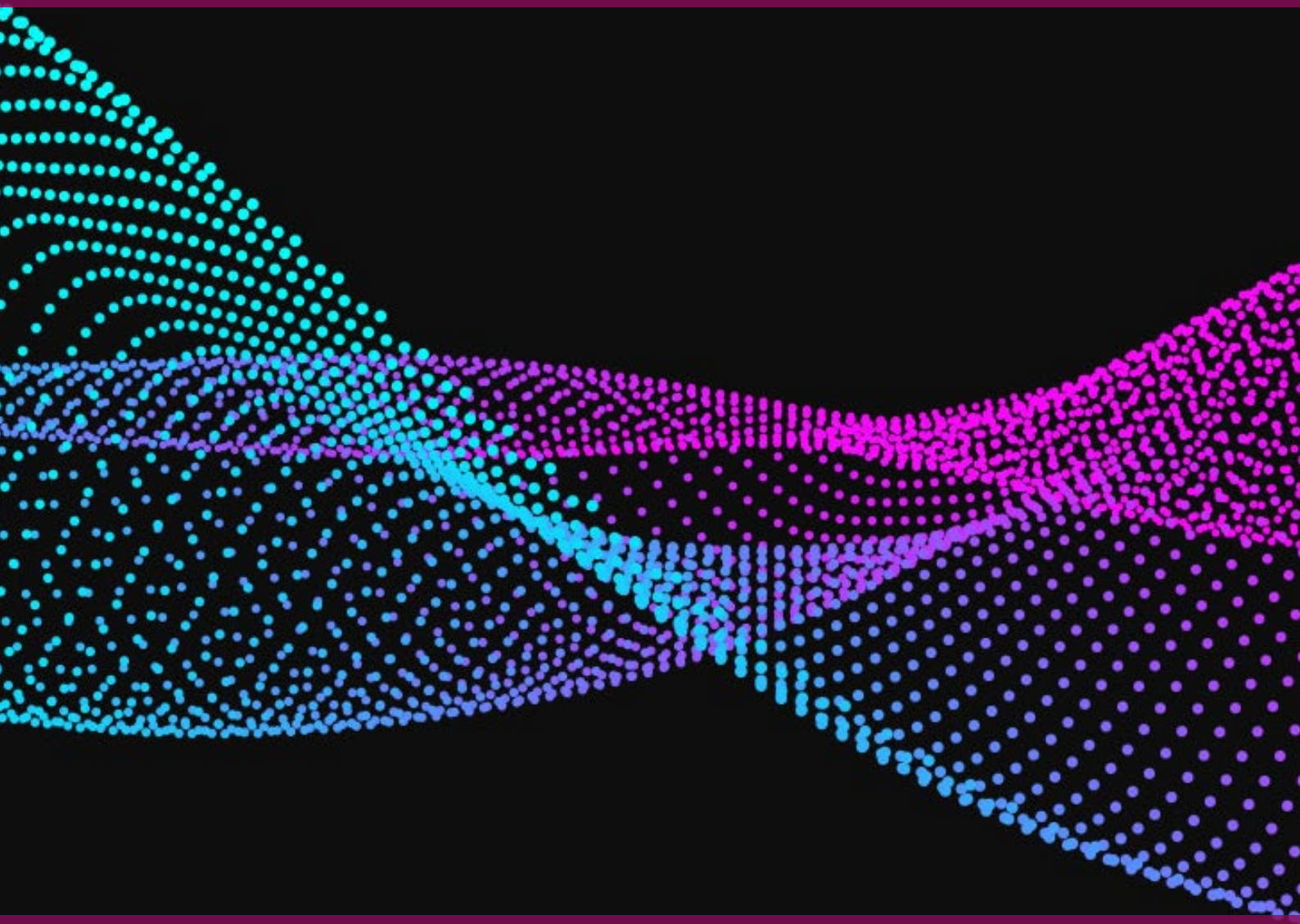
CYBERSEER

XDR as a Service

Extended Detection and Response

Better Protection Together



Your innovative partner for
cybersecurity solutions & expertise

THE VISION TO PROTECT


NODE 01
BLOCK 01
NODE 03
NODE 05
NODE 04
NODE 01
BLOCK 01

NAVIGATING THE SECURITY LANGDSCAPE

Let's face it, it's a pretty tough gig for CISOs right now. With an explosion of traffic from new and evolving sources; corporate estates that are sprawling and fragmented; and hackers who have upped their game – it's not a surprise that most Security Operation Centres (SOCs) are overwhelmed. We're all familiar with the headlines of eye-watering amounts companies have paid to recover their data, and while this has helped get security to the top agenda, it still leaves many teams grappling with how they improve their security posture alone.

THE TOP CHALLENGES FACING CISOS TODAY:

1. The rise of the malicious insider: Boosting SOC teams with better threat detection and response efficacy to identify employees, former employees, contractors and business associates you already trust going rogue.

2. Demands from the digital workplace: Providing your remote workforce needs with safe access while proactively stopping any potential attackers who seek to exploit weaker controls on home IT.

3. Getting a clear picture of threats: Integrating and optimising existing security technologies to get central visibility into data across networks, clouds and endpoints.

4. Greater telemetry is required: Despite a high number of deployed point solutions, many are too narrow and it's a heavy lift (in tools and expertise) correlating threat data.

5. Data ingestion needs to happen at scale: Data issues plague most organisations. It's exhausting searching for important signals in huge data sets; security teams face alert fatigue, and worse, miss critical alerts.

INTRODUCING XDR - A NEW APPROACH TO ENTERPRISE SECURITY

With frustrated SOC teams at breaking point, what's the answer to these forces? Cue XDR – Extended Detection and Response, a new approach to threat detection and response. It is a cloud-native platform that unifies endpoint detections with telemetry from security and business tools. So you can rapidly detect and respond to threats across your whole enterprise.
XDR is designed to deliver intelligent, automated, and integrated security across domains to help security teams connect disparate alerts and get ahead of attackers. Crucially, it provides visibility across many important data sources — including endpoint, network, cloud, and others — to find threats missed by individual point solutions.

Gartner[1] defines XDR as follows:

> **"Extended Detection and Response describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components.**

As a SaaS-based turnkey solution, security teams can switch XDR on and immediately focus on threat detection and response. Offering powerful automation across all touchpoints, it provides a path forward for security teams looking to rapidly increase efficiency and reduce complexity.

> **"XDR is a path for organisations helping them detect, identify, and understand complex attacks across the kill chain.**

DELIVERING SECURITY AT SCALE - XDR AS A SERVICE

XDR has a central role to play in SOC modernisation. Not only can it reduce the number of alerts and help you find threats faster with machine learning and analytics, but it can optimise your SOC team's time and talent. However, for many security operations teams, building an XDR solution in-house isn't an option – it's too time-consuming, costly and staff may lack the right skillset. That's where a Managed Security Service Provider (MSSP) like Cyberseer can help navigate the threat landscape and find active threats.

"Extended Detection and Response as a Service" from Cyberseer is specifically designed for businesses with stretched security resources. Fusing advanced automation technologies with hands-on forensic expertise, we help you gain 360-visibility into user and entity behaviour and find important signals in large data sets. The result? Priority alerts are rapidly identified, time-to-detection is reduced, and your team gets back to doing the work they love.

THE BENEFITS

Collecting threats is one thing, getting ahead of them is another. You need to find meaningful signals in the noise, fast. But it's hard doing this alone. Our advanced enrichment platform and Exabeam's XDR technology, coupled with our deep threat expertise help you proactively protect your data and your reputation, 24/7. So you get the context and automation to stop even the most sophisticated attacks.

Here are some of the enterprise-wide benefits of XDR as a Service:

1. Dramatically improve your security posture and better protect your business with 360-visibility across your critical data, suppliers, staff and clients. Cyberseer can detect modern attacks and insider threat behaviour on-premise, in the cloud and in SaaS applications.

2. Reduce the time-to-detection and fallout of cyber damage with up-to-the-minute threat intelligence. We find important signals in large data sets and quickly prioritise alerts, reducing your business risk.

3. Improve your team's productivity by prioritising their focus on the threats that matter. We reduce alert fatigue and take all the heavy lifting out of threat detection. We are with you every step of the way, so your team can get back to doing the work they love.

4. Augment your current technologies and reduce human error with an automated 24/7 alert escalation platform enforcing a standardised, efficient workflow each time, every time.

5. Save money against expensive in-house resources and have certainty of spend with a fixed, transparent fee. On day 1 we get you up and running, by day 14 we've established comprehensive user behaviour patterns to rapidly detect threats.

6. Speed up threat hunting and make rapid informed decisions with highly visual and intuitive dashboards. Save time on collating comprehensive audit reports and provide tangible evidence of proactive threat prevention to your board.

> **"Organisations can increase business agility when threats are better understood and controlled. Rapidly and effectively correlating threat data across multiple threat vectors leads to increased threat visibility, more rapid and automated response and mitigation, and a reduced dependence on highly skilled security analysts**
> Enterprise Strategy Group


Ai

TOP FEATURES

1. Advanced enrichment platform – Our fully automated, anonymised platform ASPECT, enriches machine learning outputs with additional threat intel before applying proprietary scoring techniques to deliver priority alerts. Enforcing a 24/7 standardised, efficient and effective workflow, each and every time.

2. Expert team of forensic analysts on-hand 24/7 – Our team of experienced cyber experts will help you cut through the clutter of alerts and false positives. As an enterprise-class MSSP, we expertly triage and prioritise incidents and provide context-specific remediation advice.

3. Award-winning XDR technology – We wrap ASPECT and our team of forensic experts around Exabeam's state-of-the-art technology. Utilising machine learning Exabeam XDR automatically creates an in-context, smart timeline of security incidents, connecting the involved assets, communication, and users.

4. Operational consultancy based on MITRE ATT&CK – We map detection methods and event labels to the MITRE ATT&CK framework. Tactics and techniques across all attack stages are visually presented in an easy-to-understand and actionable format.

5. Transparent, fixed costs – Our pricing model and contract is simple, cost-effective and transparent with no hidden costs and no surprises.

6. Making it easier to evidence compliance – From our UK-based SOC, our analysts produce a range of accurate and comprehensive reports to satisfy regulator, auditor and management requirements.

XDR AS A SERVICE – PRIME USE CASES

We help you find threats missed by other tools with behaviour analytics, and automated detection, investigation, and response. Threat detection is an always-moving target, and every organisation has blind spots. Here are the prime use cases we can help you with:

External Threats

Techniques employed by **adversaries** to deceive users, gain access to valud credentials, or exploit corporate assets.

Compromised Insiders

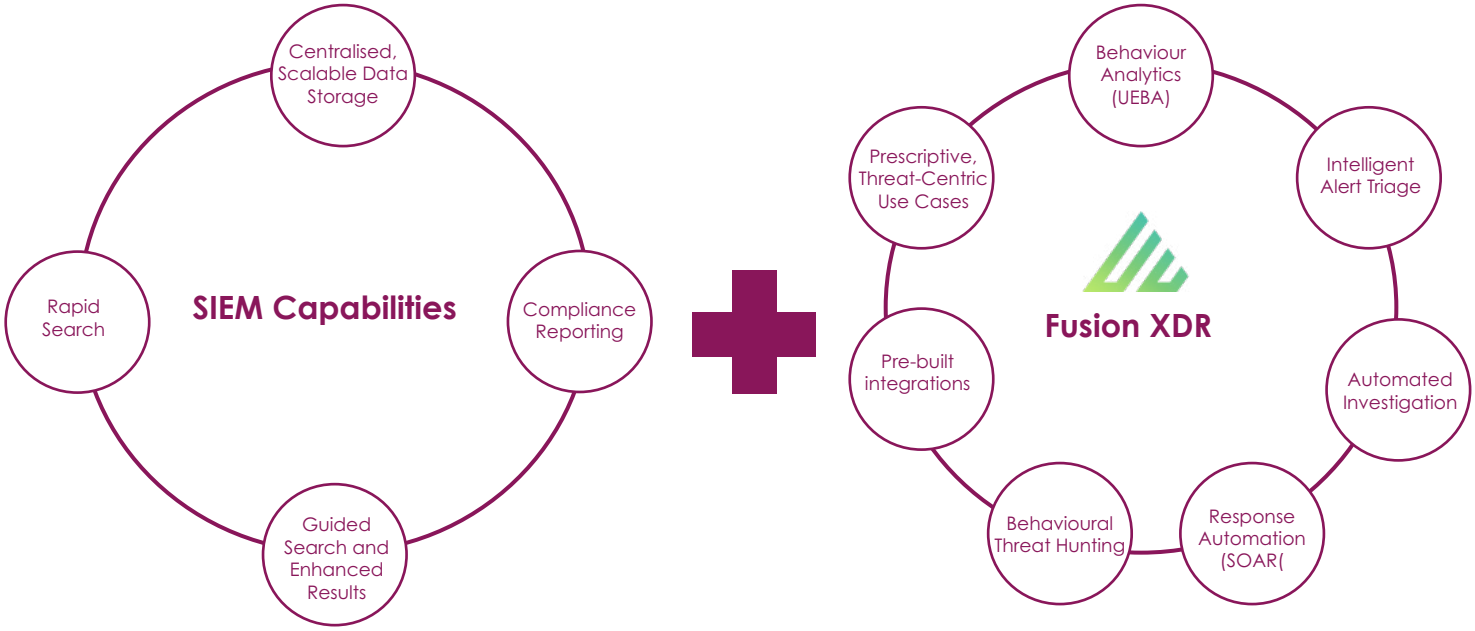
Credentials exploited by **someone outside the organisation** for the purpose of data theft and/or sabotage.

Malicious Insiders

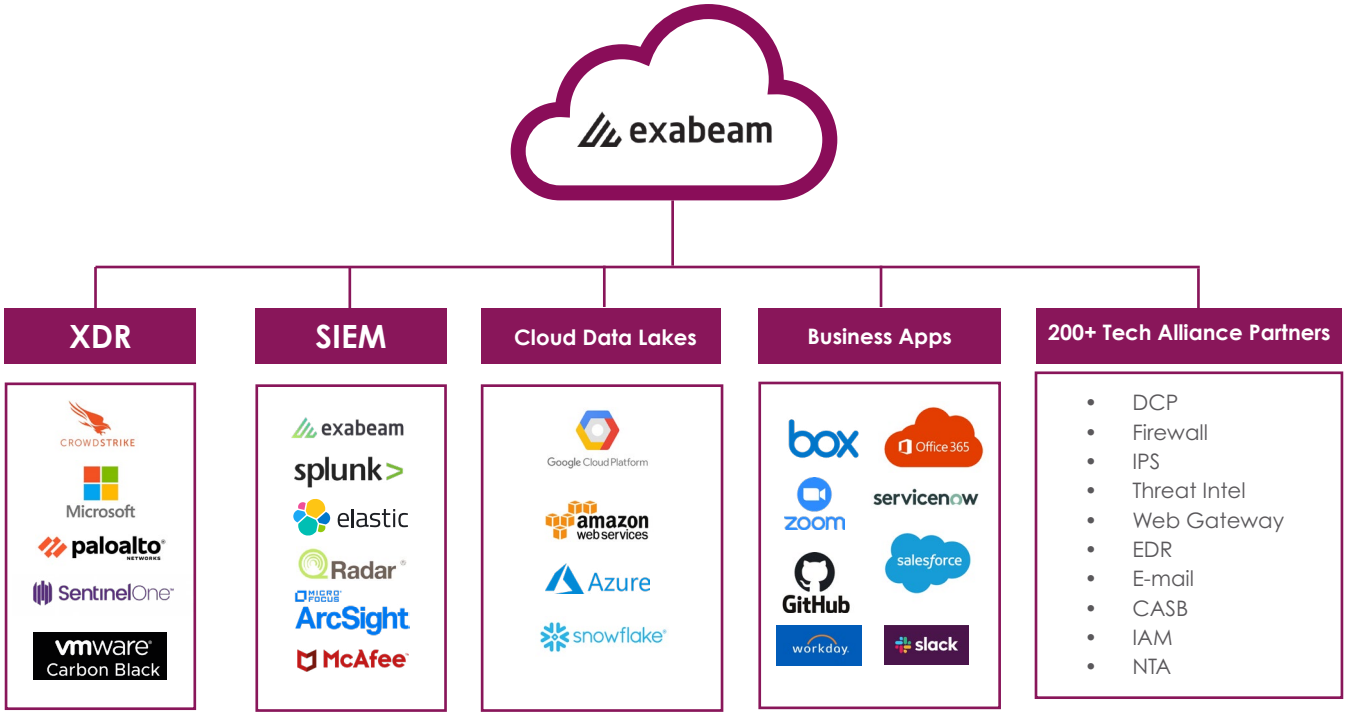
Intentional sabotage or data theft by an **employee, contractor or partner** for either personal reasons or financial gain.

CREATING A TRULY MODERN SECURITY OPS: THE TECHNICAL SOLUTION

Exabeam's leading technology, Fusion XDR and Fusion SIEM, can be used to either augment or replace your existing SIEM solution respectively, providing advanced threat detection and investigation across endpoint, network, public cloud and SaaS productivity applications.



Using AI-driven Advanced Analytics, Exabeam Fusion XDR uses machinebuilt timelines to automatically gather evidence and build a cohesive story. This provides actionable intelligence across your data centres, hybrid cloud, multi-cloud and SaaS environments. Exabeam threat-centric use cases deliver prescriptive, pre-packaged content for collection, detection, triage, investigation and response to threats.



Pre-built connectors tightly integrate hundreds of popular security IT tools

COLLECT alerts from your existing SIEM or utilise Exabeam Fusion SIEM with Site Collector and Cloud Connector to collect logs from both on premise log sources and over 40 cloud services.

DETECT using Exabeam Fusion XDR with Advanced Analytics and Entity Analytics. This uses behavioral modelling and machine learning to successfully detect threats, removing the complexity of creating and maintaining statically defined correlation rules which would otherwise miss or create a high volume of false positives. Exabeam Smart Timeline uses AI to automatically gather all events that came from a single user, this even includes lateral movement due to privilege escalations that would normally be missed if just tracking on user ID or an IP address.

RESPOND with Fusion XDR which automates the manual, time consuming steps of performing triage, investigation, and incident response. Machine-built timelines automatically gather evidence and assemble it into a cohesive story that can be used to perform an initial investigation.

Guided checklists prescribe the appropriate steps for resolving specific threat types and premade actions and response playbooks that integrate with hundreds of popular security and IT products help automate the resolution of those steps. This approach boosts analyst productivity and reduces incident responses times.

RAPID RESPONSE TO INCIDENT MANAGEMENT

With ASPECT – our Automated Security Platform for Enriching Cyber Threats. Our advanced, proprietary platform was developed to process, prioritise and escalate the output of core service monitoring technologies. ASPECT facilitates automated, contextual, enrichment of observed activity and prioritises escalation to the SOC 24x7. By automating these processes, we eliminate the need for a 'follow the sun' methodology, and instead provide a more efficient on-call model. All

Cyberseer SOC analysts are Tier 3 team members located within the UK who are trained to comprehensively threat hunt, triage and investigate prioritised activity generated by any of our core technologies.

Our forensic analysts work as an extension of your security team and build up a good understanding of your environment and organisation. This style of working relationship is key as it provides further context for the analysts to understand the impact of a threat. We can act quickly and you're not wasting time bringing us up to speed. Cyberseer analysts perform an initial triage process to classify an incident, before alerting you using pre-defined communications channels and escalation contacts. The analyst will walk you through their current understanding of the incident and classification that has been assigned, and then fully support you with their response efforts and investigate the activity further.

Cyberseer provides all customers with three types of reports:

1. Priority incident reports detailing escalated priority threats

2. Weekly reports detailing all threat tickets raised during the week.

3. Monthly trend reports detailing the number of incidents, threat classifications, breaches by attack phase, total threats and risk scores.

With Cyberseer you get complete comfort with a rock-solid SLA. We provide a rapid response to incident management – real-time monitoring, coupled with process-led incident teams, reduces the time between incident awareness and remediation.

ABOUT CYBERSEER

If you're looking for a path forward to modernise security operations and boost efficiency, we can help you determine if an XDR strategy is right for you.

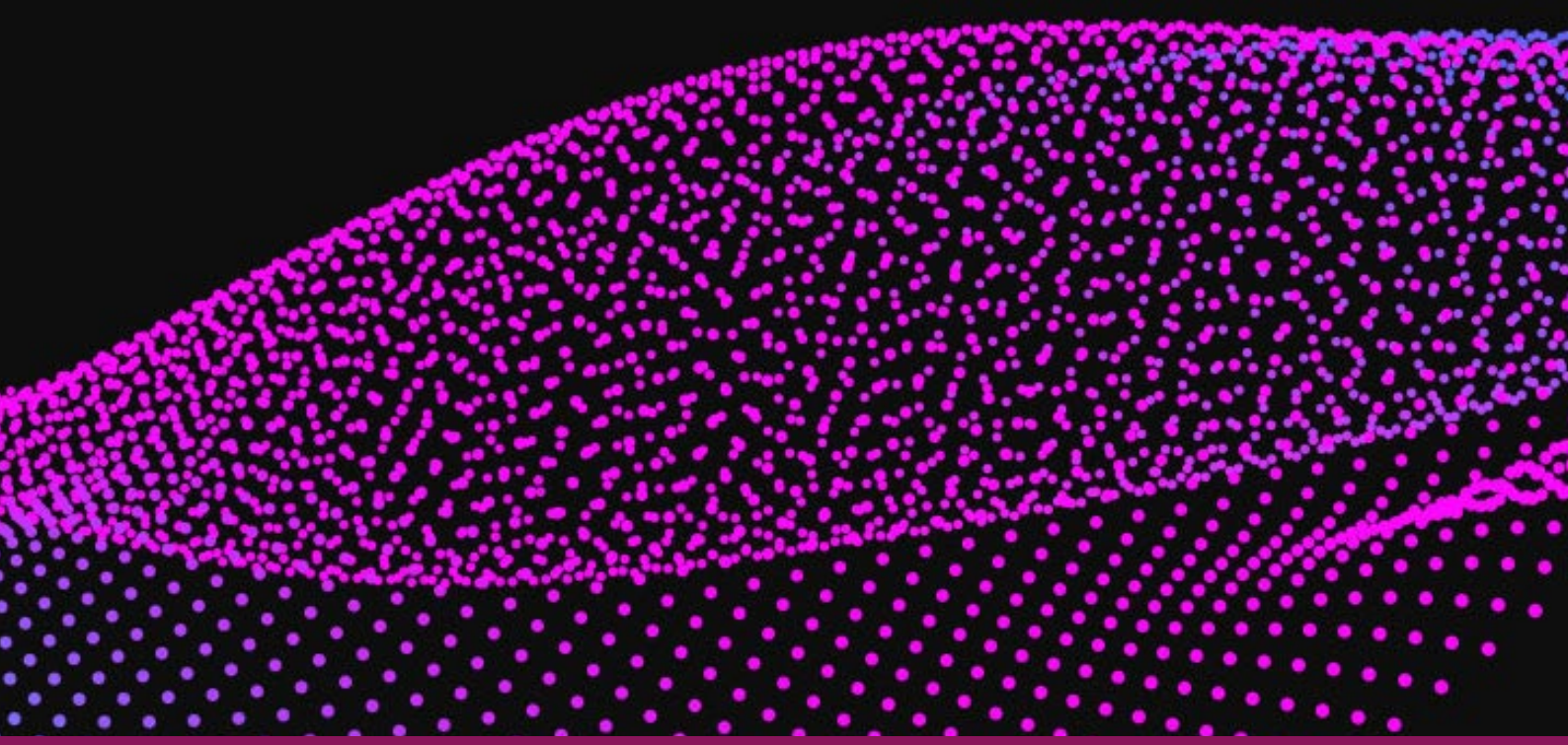
Keeping your business safe is your number one priority. It's ours too. Fusing advanced detection technologies with deep forensic expertise, we help you join all the dots to rapidly distil threats. Our innovative solutions give you the confidence and proactive control you need – whatever comes your way.

We're here to help you keep your people and your reputation safe. It's what we do for companies around the world every day.

With Cyberseer, you're no longer on your own.

Reference:

1. Gartner Report: Innovation Insight for Extended Detection and Response.



CYBERSEER

CONTACT US - +44 (0)203 823 9030

If you would like to find out about how the Cyberseer team can make difference within your organisation with regards to advanced threat detection, contact us today:

info@cyberseer.net | www.cyberseer.net