CYBERSEER
THE VISION TO PROTECT

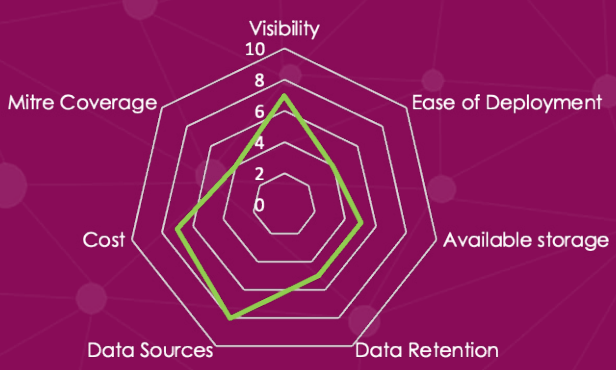
exabeam

Cyberseer SOC & Exabeam

Solution brief

Discover how organisations that deploy Exabeam Security Management Platform with ASPECT from Cyberseer benefit from a market leading solution and highly trained analysts, so you are only alerted to immediate actionable threats.

At a glance:



Approximate read time: 7 min

THE VISION TO PROTECT

Executive Summary & Key Benefits

- Actionable intelligence from Tier 3 analysts
- Reduced dwell time
- Eliminate the noise
- 24x7 threat detection
- Smart timelines
- Intelligence across all environments
- Unlimited data storage with user-based licensing
- Reduced incident investigation time to minutes

Securing an organisations IT infrastructure is a complicated task. Organisations often rely on multiple vendors to help secure these environments against complex and unknown attacks. The majority of vendors provide solutions focussed on prevention capabilities. These solutions attempt to prevent both known and zero-day attacks by using threat intelligence feeds and sandboxed environments. 90% of attacks use e-mail and the web as an attack vector. A typical organisation will at a minimum deploy a Next-Generation firewall and an e-mail gateway. The Next-Generation firewall will reduce the available attack surface whilst attempting to prevent malware from entering your infrastructure. E-mail gateways focus on detecting and preventing phishing e-mails, as well as the detection of malicious links and files.

With many best of breed point solutions on the market today, it is essential that we have visibility and detection across all of these solutions. It is, therefore, necessary to have a layered approach to security. A siloed prevention only approach will lack the cohesion to stop a complicated attack and lack the capability to detect compromised user and insider threats. This is where we can add a true detection layer to complement other layers of security.

This overarching detection layer up until now has relied heavily on SIEM and correlation rules to provide a view of the organisation. Using existing legacy SIEM's has resulted in partial visibility due to the expense of SIEM storage costs. Valuable telemetry from data sources was never logged as a result. Also, during maintenance windows, event logging on devices has in some cases been inadvertently switched off or misconfigured. This only comes to light when there is a real necessity to have the data.

Security Operation Centres using SIEM reliant on correlation rules found the volume of noise generated from the security systems to be too great, generating many false positives. Correlation rules not being predefined for a particular threat meant not all alerts were investigated, whilst others missed entirely.

Cyberseer has partnered with Exabeam to automate the detection of complex and unknown attacks through enrichment and machine learning with UEBA. Through integration with Exabeam and ASPECT, you are only made aware of critical threats when they arise. All triage and prioritisation are done through our team of expert analysts. There will be no more false positives or dead-end trails that consume your SOC team for hours at a time.

The Challenge

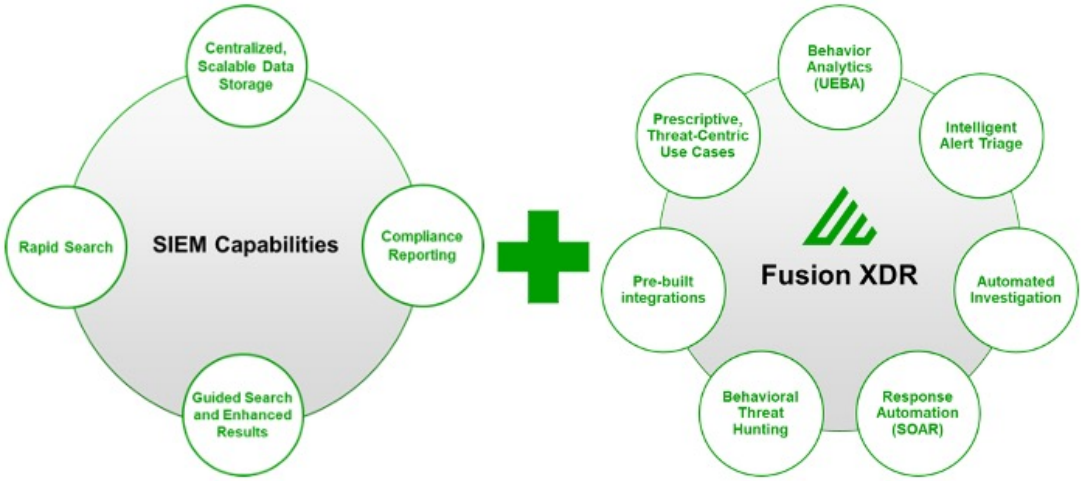
Today's businesses are undergoing monumental changes. Digital transformation projects and the move to the cloud are all having an overwhelming impact on security. The fast pace of development means that security teams are constantly working to try and secure these everchanging environments and as a result they often lag behind.

The SOC is the key to securing your environment but with the average large enterprise deploying security products from over 70 different vendors means that many generate duplicate alerts and only about 1 in 5 alerts is related to a unique security event. With Analysts spending 30 mins on average to investigate each event this leaves the SOC struggling to pinpoint the critical incidents versus the noise. The enormous number of alerts generated per day means that the SOC team are continually overwhelmed by the sheer volume.

With new technologies being added to address new emerging security concerns combined with number of attackers increasingly making use of AI, the alert volume is only going to get larger. The SOC team are left flooded with alerts and reactive with many undetected insider threats, compromised accounts and exfiltration.

The Solution

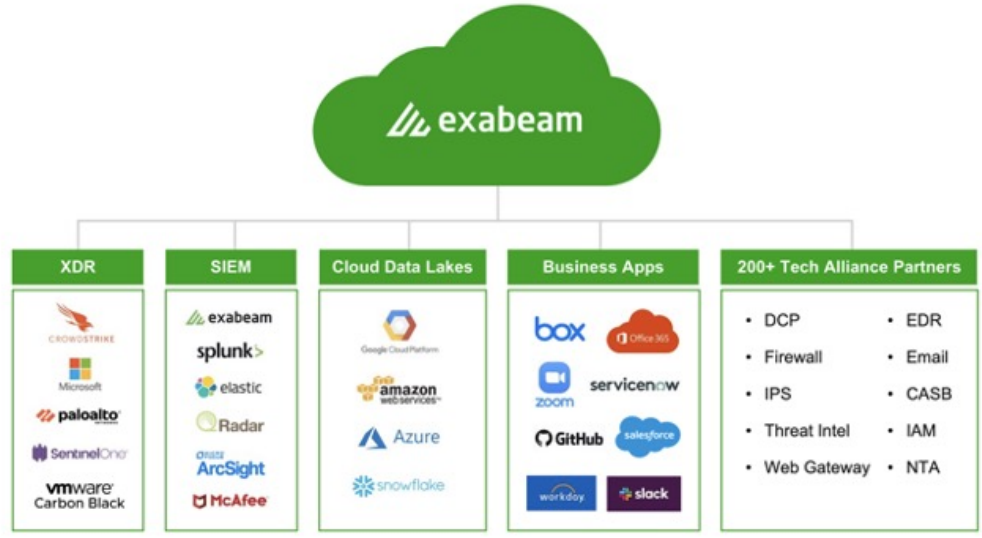
Organisations that deploy Exabeam Fusion with ASPECT from Cyberseer benefit from a market-leading solution and highly trained analysts, where you are only alerted to immediate actionable threats. This both reduces the cost and increases the efficiency of your SOC by removing the noise generated by the sheer volume of alerts and focusing on what matters – responding to an incident quickly.



Fusion SIEM, Unify SIEM and XDR for a truly modern SecOps Solution

Exabeam 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 uses machine-built timelines to automatically gather evidence and build a cohesive story. This provides actionable intelligence across your data centers, 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.

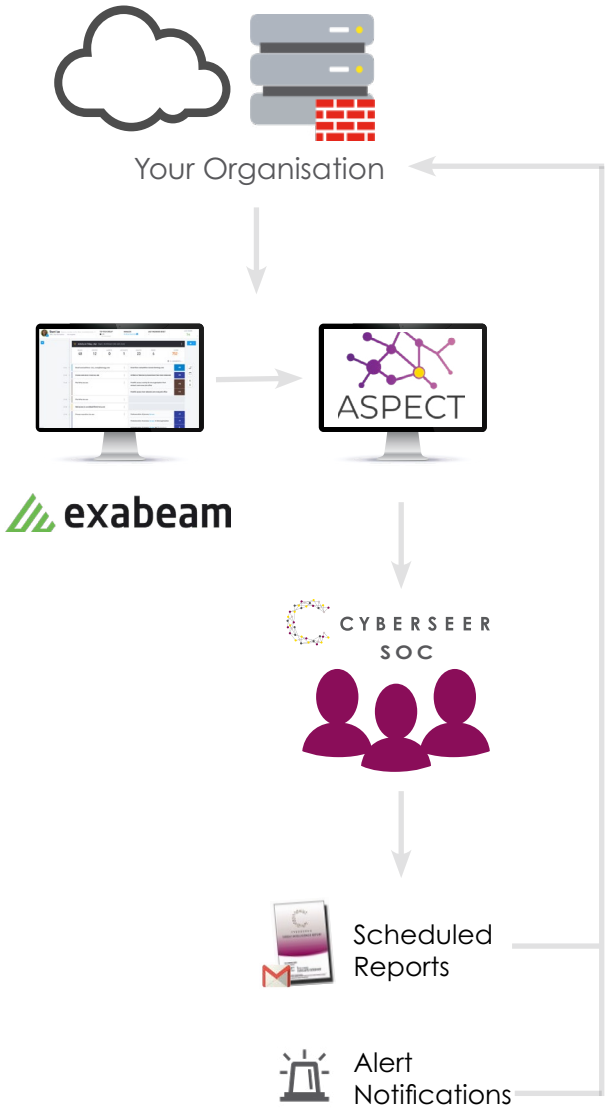


Pre-built connectors tightly integrate hundreds of popular security IT tools.

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 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 ASPECT. Cyberseer's advanced, proprietary platform which underpins our 24x7 service is known as ASPECT - Automated Security Platform for Enriching Cyber Threats - and 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. The automation of these processes enables us to do more with less whilst maintaining a high degree of efficiency, allowing us to eliminate the need for a 'follow the sun' methodology in favour of the much more beneficial on-call model. All Cyberseer SOC analysts are Tier 3 people located within the UK who are trained to comprehensively threat hunt, triage and investigate prioritised activity generated by any of our core technologies.



Cyberseer 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 in your environment. Also, when you are contacted out-of-hours you will not need to bring the analyst up-to-speed on your environment which further reduces your overall response time.

Cyberseer analysts perform an initial triage process to classify an incident, before alerting the customer using pre-defined communications channels and escalation contacts. The analyst will walk the customer through their current understanding of the incident and classification that has been assigned, and then support the customer 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.

Benefits

- Reduction in alert fatigue - only priority alerts are immediately escalated.
- Expert extension to SoC Staff, 24x7x365.
- Store all your event data, licensed per user not EPS or GBD.
- Identify anomalous activity through notable users.
- Show value in weekly and monthly reports highlighting threats and areas of concern.
- Cost savings by reducing the number of Tier 1, Tier 2 analysts.
- Identify threats in near real-time across everything, investigate in minutes not days.
- Automatically triaging of events - threats accurately prioritised and acted upon.
- Detection using behaviour and context, not rules.
- Identify compromised accounts, anomalies, data exfiltration and lateral movement. Threat hunting and indicators of compromise.
- Automatically identify notable users indicating unusual or anomalous behaviour.

About Exabeam

Exabeam help security teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 per cent less time.

Security organisations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioural analytics to detect attacks, and automate incident response, both on-premises or in the cloud.

exabeam

About Cyberseer

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 24x7. It's what we do for companies around the world every day. With Cyberseer, you're no longer on your own.

CONTACT US +44 (0)203 823 9030
info@cyberseer.net

William Hill · Addison Lee · Markerstudy Insurance Company Limited · Slaughter and May · Mizuho · Knight Frank