CYBERSEER
THE VISION TO PROTECT

exabeam Microsoft

Cyberseer SOC & Exabeam & Microsoft EDR

Solution brief

Explore the potential of integrating Exabeam with Microsoft Defender for Endpoint, augmented by the expertise of Cyberseer's Managed Service. Learn how the holistic approach empowers organisations to stay ahead of evolving threats, from ransomware to insider risks, ensuring robust protection and swift response.

Approximate read time: 7 min

THE VISION TO PROTECT

Executive Summary & Key Benefits

- **Detect and investigate:**
  Identify advanced attacks and insider threats using endpoint telemetry and behaviour analytics.

- **Advanced Threat Detection:**
  Implement advanced threat detection with curated detection rules based on MITRE tactics, techniques, and procedures.

- **CrowdStrike Falcon Integration:**
  Utilise the full potential of Microsoft Defender for enhanced endpoint protection.

- **Predefined Response and Threat Hunting:**
  Enable advanced threat hunting and predefined responses to minimise dwell time and increase confidence in detections.

- **Centralised Visibility:**
  Achieve centralised visibility of your environment, including discoverable endpoints.

- **Actionable Intelligence:**
  Benefit from Forensic Analysts providing actionable intelligence, reducing incident investigation time to minutes.

- **Reduced Noise and 24/7 Threat Detection:**
  Eliminate unnecessary noise and ensure round-the-clock threat detection.

- **Smart Timelines:**
  Leverage smart timelines for a chronological view of user and asset activity across ingested log sources.

- **Unlimited Data Storage:**
  User-based licensing for efficient data storage.

- **Attack surface reduction:**
  Implement strategies for reducing the attack surface.

- **Combined Management Information:**
  Consolidate management information for streamlined operations.

- **Use Cases:**
  Detect advanced and insider threats, including lransomware, credential compromised insiders, accidental data loss and malicious insider.

Cyberseer has seamlessly integrated Microsoft Defender for Endpoint and Exabeam into its managed service offering to deliver managed detection and response across all endpoints and network devices in your environment. With continuous monitoring, alert triaging, and prioritising alerts, Cyberseer ensures critical threats receive your immediate attention.

The Challenge

Securing your environment is paramount, and the Security Operations Centre (SOC) is at the heart of this mission. However, the current landscape presents formidable challenges that the SOC teams must navigate:

1. **Alert Overload and Duplicate Alerts:**
   - Only 1 in 5 alerts is related to a unique security event.
   - Analysts spend an average of 30 minutes investigating each event, leading to time inefficiency.
   - The SOC struggles to distinguish critical incidents from the noise, hindering effective response.

2. **Enormous Volume of Alerts:**
   - The SOC team faces overwhelming alert volumes generated daily.
   - The SOC becomes less proactive, leading to slower detection of actual threats such as insider breaches, compromised accounts, and data exfiltration incidents.

3. **Emergence of Non-Malware-Based Attacks:**
   - According to the CrowdStrike 2023 Global Threat Report, 71% of observed attacks are non-malware-based, involving hands-on-keyboard activity, command line usage, or running shell scripts.
   - Addressing such attacks requires a blend of automation and human expertise in threat hunting, content review, and contextualisation.
   - This mix of art and science cannot be entirely solved by machine learning, demanding a comprehensive approach.

4. **Visibility Challenges:**
   - Security teams struggle to gain a holistic view of the environment due to the use of multiple security solutions.
   - The lack of integration among these best-in-class tools makes it challenging to correlate information for investigation and triage.
   - Achieving comprehensive visibility is crucial for quantifying business risk and enhancing overall security posture.

5. **The Endpoint Challenge:**
   - With the intensified focus on user endpoint devices as access points to corporate data, security implications become evident.
   - Poorly protected user endpoints connected to a corporate network become prime targets for malicious actors.
   - Addressing the endpoint challenge is essential to bolster overall security defences.

Looking Ahead:

The challenges faced by the SOC are further compounded by the evolving threat landscape. New security concerns emerge, and attackers increasingly leverage AI, ensuring the alert volume continues to grow. The SOC is left inundated, reactive, and at risk of missing critical threats amidst the noise.

The Solution: Cyberseer SOC, Exabeam & Microsoft Defender

Exabeam is a cloud-native platform offering rapid data ingestion, powerful behavioural analytics, and automation for swift threat response.

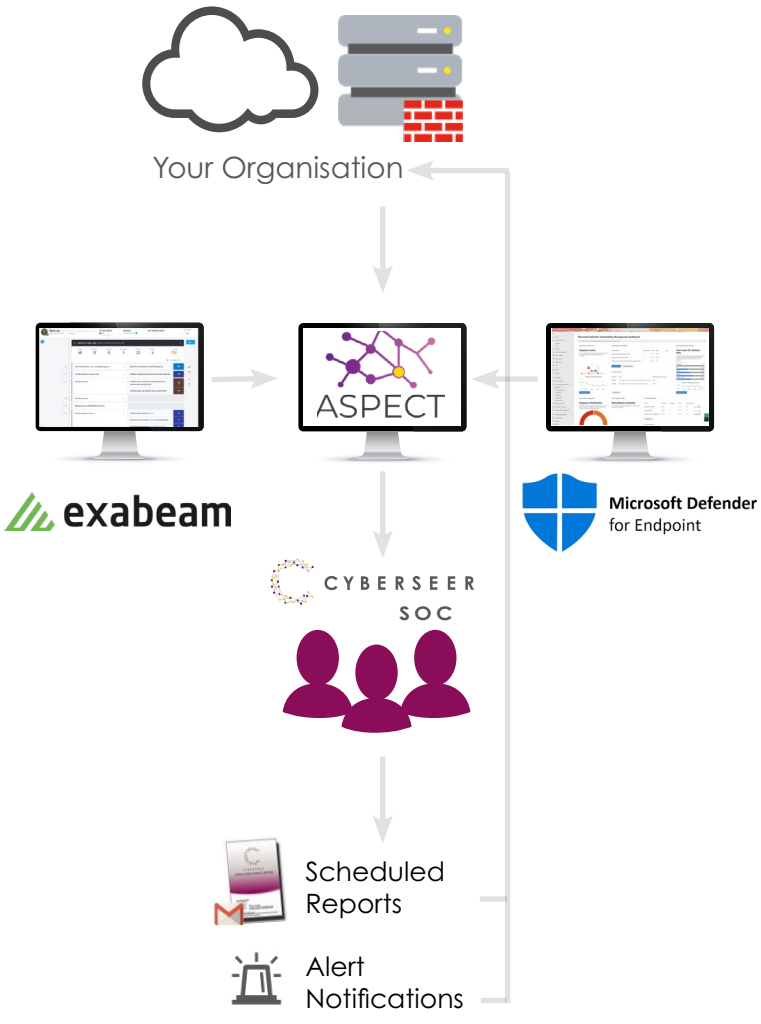
Microsoft Defender for Endpoint is a leading cloud-native enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Its features include endpoint visibility and AI-powered cyber threat protection to help stop threats across Windows, macOS, Linux, Android, iOS and IoT devices.

Integration Benefits:
By integrating Defender with Exabeam, security teams can leverage user baselines for anomaly detection and:

- Combine endpoint detection and response (EDR) with user and entity behaviour analytics (UEBA) for behavioural baselining and enhanced detection.
- Augment alert-based investigations with risk-prioritised user analysis.
- Use Smart Timelines for automatic analysis during and after an attack.

ASPECT Platform:
The fully integrated SaaS offering from Microsoft Defender for Endpoint and Exabeam delivered through Cyberseer's ASPECT platform provides a comprehensive and powerful solution for managed detection and response. By efficiently pulling and enriching alerts from Exabeam and Defender for Endpoint, we reduce response times and minimise threat dwell time, enabling a quick and effective response to critical threats in a robust yet efficient way.

ASPECT from Cyberseer is at the core of the Cyberseer SOC. It is a proprietary, 24x7, distributed platform that integrates with Exabeam and Defender for Endpoint via API to pull alerts for enrichment, prioritisation, and escalation to our Forensic Analysts. The automation of these repetitive and time-consuming processes, along with



the enrichment of alerts with internal and external contextual threat data, enables us to do more with less by efficiently and effectively identifying and routing priority threats to Analysts. This combination of Exabeam, Defender and ASPECT means Cyberseer analysts are responding to priority issues ASAP, reducing the time to respond and minimising threat dwell time.

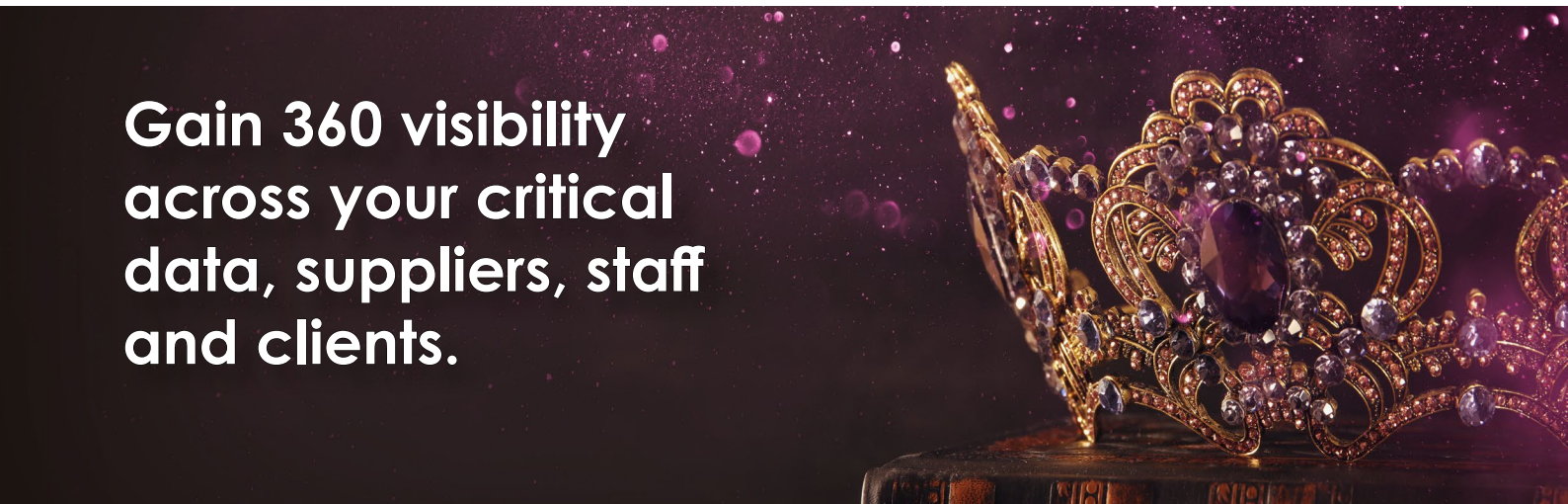
Analyst Expertise:
All Cyberseer SOC Analysts are trained to comprehensively threat hunt, triage, and investigate prioritised activity, serving as an extension of your security team. This working relationship is key as it provides further context for the Analysts to understand the impact of a threat in your environment. When you are contacted out-of-hours, Analysts are already familiar with your environment, reducing overall response time.

Cyberseer Analysts perform an initial triage process to classify an incident, before alerting the customer using pre-defined communication channels and escalation contacts. The Analyst walks the customer through their current understanding of the incident and classification that has been assigned, supporting the customer with their response efforts and further investigating the activity.

Reporting:
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.

Delivery at scale.
Cyberseer's service, delivered through ASPECT is specifically designed for businesses with stretched security resources in terms of time, costs, or requisite skillset. Fusing advanced automation technologies with hands-on forensic expertise, Cyberseer helps you gain 360-visibility across your critical data, suppliers, staff, and clients and find those important signals in large data sets. The result: Rapid identification of priority alerts, reduced time-to-detection, and your team getting back to what they do best - all within the per-user per-year subscription fee.



Join Solution Benefits

- **Improved Detection:**
  The integration of Exabeam and Microsoft Defender enables behaviour analytics to be leveraged to protect endpoints by creating a baseline for normal user and endpoint activity.

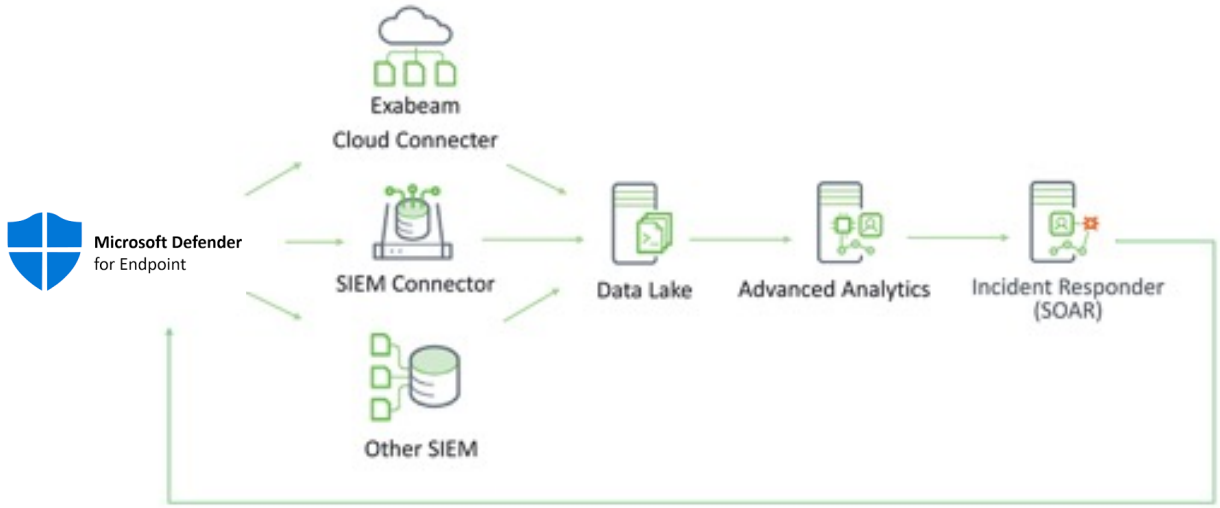
- **Threat Intelligence Enrichment:**
  Enhanced context of security events with the integration of threat intelligence feeds, aiding identification and understanding of potential threats.

- **24/7 Priority Threat Detection & Consistent Workflows:**
  Automated 24 x 7 alert escalation enforces standardised workflows, reducing human error.

- **Enhanced Team Productivity:**
  Prioritise attention on critical threats, reducing alert fatigue and improving team focus.

- **Reduce Time-to-Detection:**
  Efficiently identify and prioritise threats with machine-built incident timelines, reducing response times..

- **Assess the Risk:**
  Exabeam collects data from the Microsoft Defender platform to monitor user activity and will automatically flag and assign risk scores to anomalous endpoints and network activity, such as a file entering the network from a user's laptop.



About Exabeam

Exabeam helps 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 Smart Timelines, sequences of users and device behaviour created using machine learning, further reduce the time and specialisation required to detect attacker tactics, techniques, and procedures.

exabeam

About CrowdStrike

Microsoft Defender for Endpoint (MDE) combines anomaly-based detection, deterministic countermeasures, and automated response in a single modern interface to cover all tactics of MITRE ATT&CK framework. MDE empowers your enterprise to rapidly stop attacks, scale your security resources and evolve your defences by delivering best-in-class endpoint security across Windows, macOS, Linux, Android, iOS and network devices.

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.

For more information about our Managed Security Service or our advanced technologies please contact us.

CYBERSEER

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

ADDISON LEE axi MARKERSTUDY INSURANCE COMPANY LIMITED MIZUHO Knight Frank