exabeam

Data Sheet

Exabeam Fusion SIEM

Unify SIEM and XDR for a truly modern SecOps solution

Traditional SIEMs Aren't Built For Threat Detection, Investigation, & Response

Despite massive security investments, establishing an effective Threat Detection, Investigation, and response (TDIR) program remains a problem for today's SOCs. The doggedness of this problem can be traced back to several factors including the fact that purpose built security tools run in silos and traditional SIEMs — which were designed to centralize the data from these tools — have become overly complicated due to a focus on building features not outcomes. The result is security teams expend huge amounts of effort on customization to see basic value from their current SIEM.

Moreover, data centralization, powerful search capabilities, and audit and compliance reporting are basic necessities for security operations, however many SIEMs are inefficient at even these simple tasks. Deriving value from data often requires analysts to be skilled in highly complex proprietary query languages, creating a significant barrier to answers. When performing advanced queries, analysts often have to wait long periods of time to get results, which impacts their productivity.

Integrated SIEM and XDR — A Holistic Approach to TDIR and SecOps

Exabeam Fusion SIEM combines the best of both worlds — the unification of best in class detection and response delivered by Fusion XDR and the conventional capabilities of centralized data storage and compliance reporting, with built in rapid and intelligent search.

Fusion SIEM provides effective, outcome-focused TDIR that enables you to leverage and enhance the existing tools in your security stack, without forcing you to rip-and-replace them to centralize on a single vendor. It works out of the box using pre-built integrations with hundreds of 3rd party security tools and uses market-leading behavior analytics to combine weak signals from multiple products to find complex threats missed by other tools.

> Looking at the landscape of SIEM products out there, we were searching for underlying technology and architecture that lends itself to meeting the needs of a more agile security team."
>
> **Colin Anderson, CISO**
> **Levi's**

To help SOCs and security analysts standardize around the use of best practices, Fusion SIEM solutions include prescribed workflows and pre-packaged content that focus on specific threat types to achieve more successful TDIR outcomes. This enables SOCs to run their end-to-end TDIR workflows from a single control pane that performs automation of highly manual tasks involved with triage, investigation, and response. The result is boosted analyst productivity, reduced response times, and consistent, highly repeatable results.

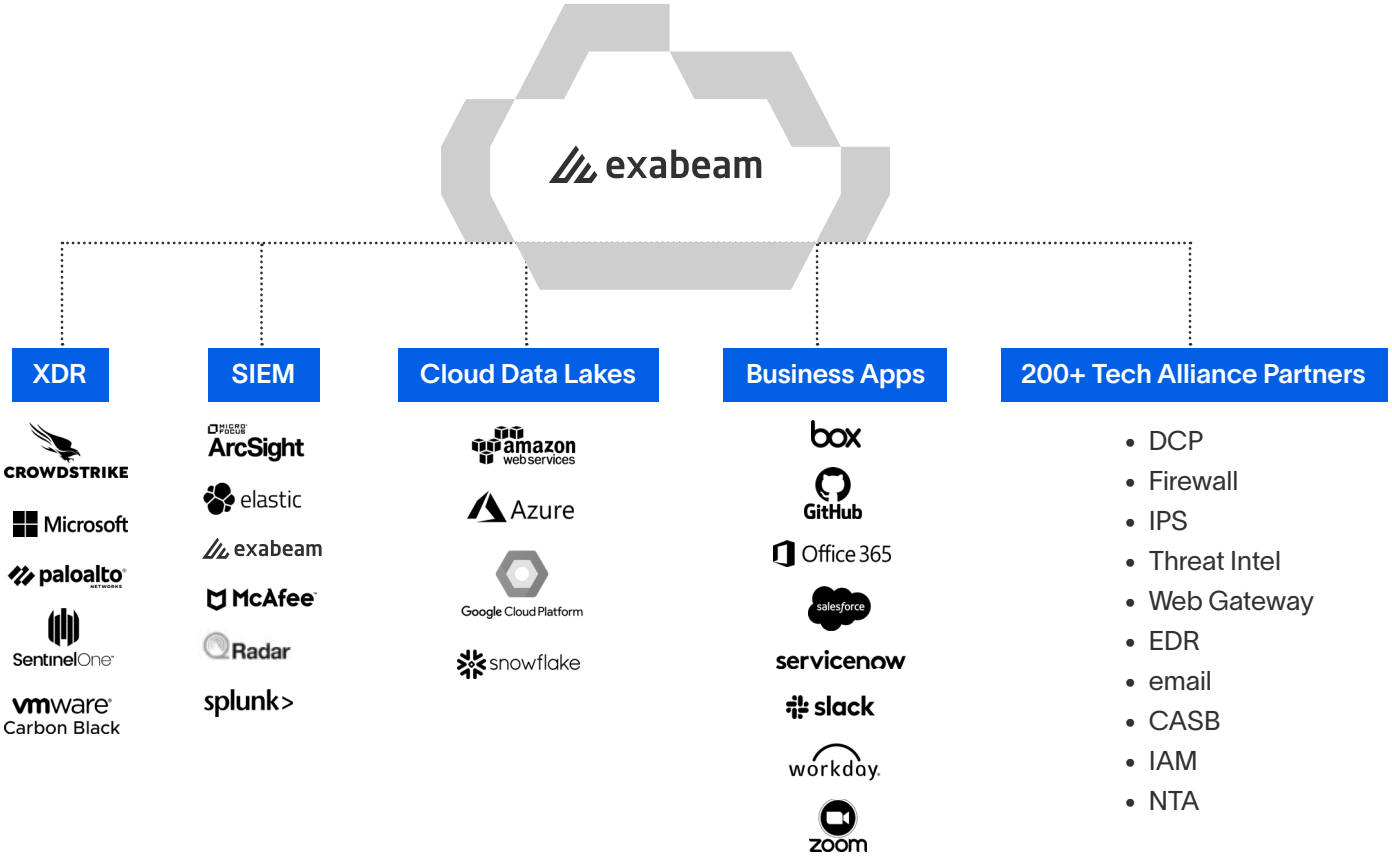
Collect, Store, and Search Data from Anywhere

From endpoint to cloud, and everything in between, your data is everywhere. Fusion SIEM provides highly scalable centralized storage and rapid intelligent search capabilities for inclusive visibility across your entire ecosystem. If more log storage, longer storage time, or additional processing power is needed Fusion SIEM easily scales to meet your needs.

Through rapid intelligent search and enhanced results, security analysts of all levels can quickly derive answers without limits — no overly complex query skills are needed, and there's no waiting around for hours for queries to complete. Experience faster investigations, higher productivity, and improved metrics.

Flexible Integration to Augment your Security Stack

Free yourself from vendor lock-in and rip-and-replace tech refresh cycles. Fusion SIEM enhances your existing security stack by layering on turn-key TDIR using hundreds of pre-built integrations that cover dozens of key technologies like endpoint, network, cloud and more. These integrations support the full TDIR lifecycle, from data ingestion and normalization, to threat detection and response automation. This approach enables Fusion SIEM to get more out of your existing security investments, and to tightly unify them into a single control plane for the SOC.



Use Case Content

Collection

- Predefined data sources
- 500+ integrations
- Cloud connectors

Detection

- Behavior based threat detection
- Watchlists
- MITRE mapping

Triage

- Alert prioritization
- Context gathering and enrichment
- Auto case creation

Investigation

- Prebuilt incident timelines for all entities
- Automated Q&A

Response

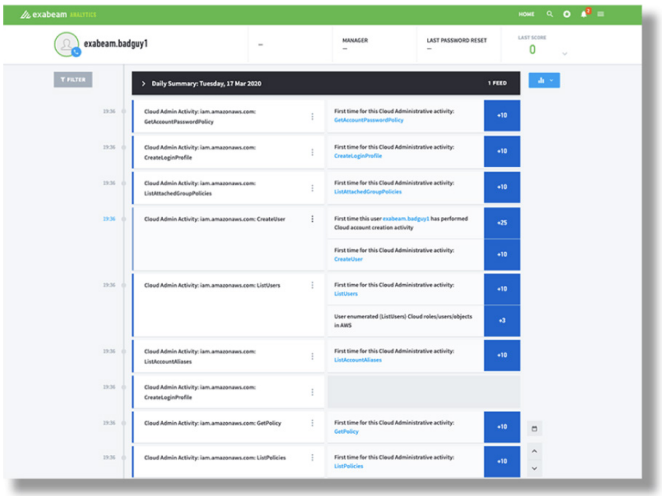
- Turnkey playbooks
- Custom incident types
- Incident checklists

Prescriptive TDIR Use Cases

It has become too complicated to create an effective TDIR program using legacy SIEMs and a smattering of purpose built security products. To compound the issue, there are no standard ways to run security. Every SOC is unique; with its own mix of tools, level of staffing and maturity, and processes. Fusion SIEM solves this by leveraging prescriptive threat-centered use cases packages that provide repeatable workflows and prepackaged content that spans the entire TDIR lifecycle. These use cases provide a standardized way to easily achieve effective, repeatable security outcomes for specific threat types. They include all of the content necessary to operationalize that use case, including: prescribed data sources, parsers, detection rules and models, investigation and response checklists, and automated playbooks.

Detect Threats Missed by Other Tools

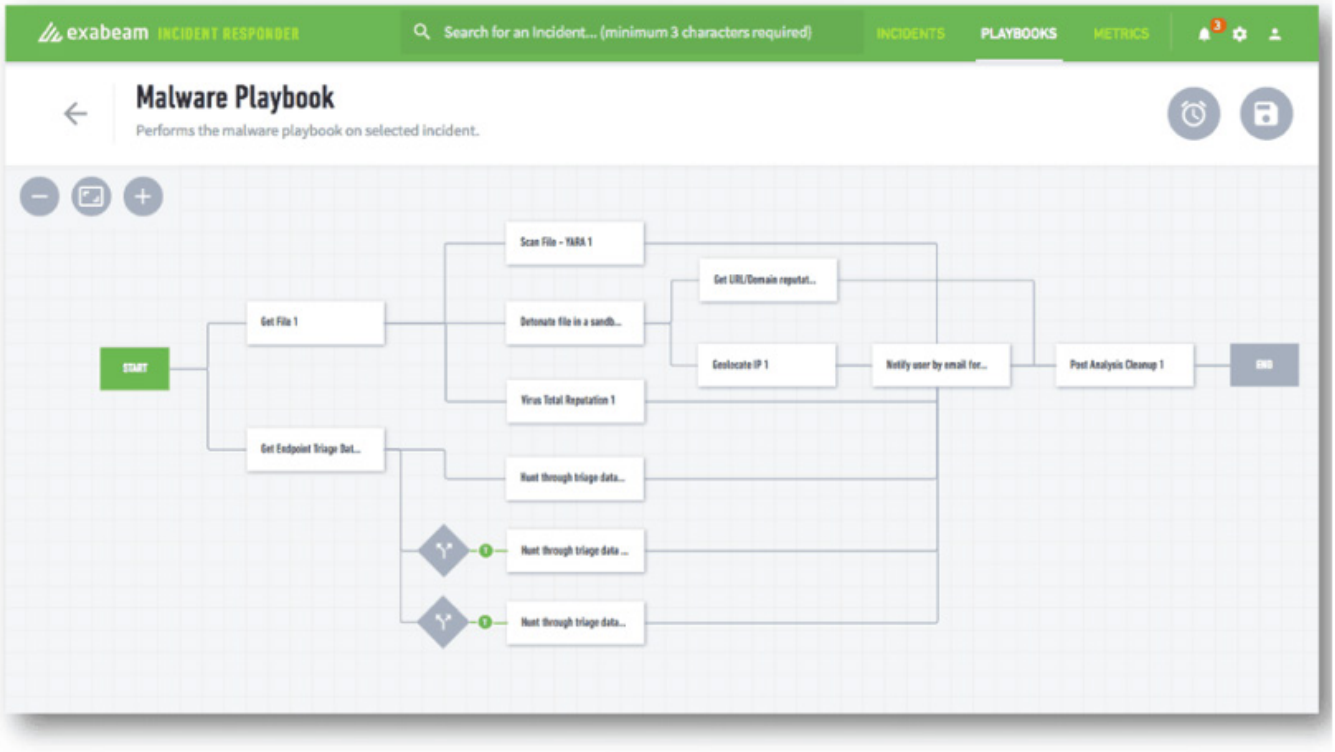
Security teams have an average of 19 TDIR solutions — many of which are point solutions that serve a specific purpose. Despite having impressive arsenals at their disposal, common threats like phishing and malware are regularly missed. Why? Security tools operate in silos and lack visibility or context on what's happening in other tools. Fusion SIEM breaks down these silos by combining weak signals from many products into high fidelity threat indicators using behavior analytics. This approach easily detects complex, unknown, and insider threats to find attacks missed by purpose built tools themselves or other analytics tools your organization has deployed.



Automated Investigation & Response

SOC teams are expected to manage an increasing volume and complexity of threats using limited staff and manual processes. This often leads to slow response times, as well as missed incidents. Differences in analyst domain experience and skill can lead to inconsistent and potentially incomplete incident response. For instance, when tasked with analyzing abnormal activity, analysts may not be able to correctly identify the type of threat, let alone know how to address it. Additionally, performing investigation and response typically requires analysts to switch between dozens of different security tools for incident response which can be slow and error prone.

Fusion SIEM 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. Automated Incident Diagnosis analyzes abnormal behavior to automatically diagnose the type of threat associated with an incident and classifies it by use case to guide investigations with tailored checklists that prescribe the appropriate steps for resolving specific threat types. 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.



Key Features

Exabeam Fusion SIEM provides centralized log storage, rapid intelligent search, compliance reporting, turn key threat detection, investigation, and response capabilities as well as prescriptive workflows and pre-packaged threat-specific content that can be layered onto any security tech stack. Key features include:

- **Centralized, Highly Scalable Data Storage**
  Inclusive visibility across your entire ecosystem ensuring no event or activity is missed.
- **Guided Search and Enhanced Results**
  Search fields are auto populated as you type, and enhanced view highlights key pieces of information for quick review.
- **Rapid Search**
  Full indexing at the point of log ingestion means queries return results faster. Analyst productivity and efficiency is significantly improved as they aren't left waiting for information indicative of a potential data breach or attack.
- **Audit and Compliance Reporting**
  Hundreds of out-of-the-box compliance reports and dashboards eliminate the need for unwieldy spreadsheets when the auditors visit.
- **Flexible Integration**
  Pre-built connectors tightly integrate over 500 popular security and IT tools for threat detection, investigation, and response.
- **Behavior-Based Detection**
  Market leading behavior analytics (UEBA) finds advanced threats like credential-based attacks, insider threats, and ransomware that are missed by other tools.
- **Prescriptive, Threat-Centric Use Cases**
  Prescriptive, end-to-end workflows and security content enable SOCs to see quick time to value and achieve successful TDIR outcomes.
- **Automated Incident Diagnosis**
  Behavior analytics analyzes abnormal user activity to automatically classify incidents by threat-centric use cases.
- **Automated Investigation**
  Machine-built Smart Timelines automatically gather evidence and assemble it into cohesive incident timelines that boost productivity and ensure nothing slips through the cracks.
- **Response and Remediation**
  Guided checklists and automated response actions and playbooks reduce response times and enable consistent, repeatable workflows
- **Cloud-Based Deployment**
  Cloud based delivery removes the operational overhead of implementing and maintaining another security program so your analysts can focus on security.

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools — including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond.

For more information, visit exabeam.com

exabeam