



Data Sheet

Exabeam Fusion XDR

Efficiently detect, investigate,
and respond to threats without
disrupting your existing
security stack

Traditional approaches to threat detection, investigation, & response fail

Despite massive security investments, establishing an effective Threat Detection, Investigation, and response (TDIR) program remains a problem for today's SOC's. The doggedness of this problem can be traced back to several factors including the fact that purpose built security tools run in silos and 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 SIEM.

Another trend compounding the situation is that SOC teams often lack standard procedures and know-how for how to deal with specific threats resulting in an inability to efficiently or effectively operationalize their tooling for threat detection, investigation, and response. Meanwhile, security stacks have grown in size and complexity and there is no single control plane for the SOC. Instead thinly-stretched SOC teams run manual, disjointed workflows across multiple tools. This leads to slow, inconsistent, and incomplete incident response.



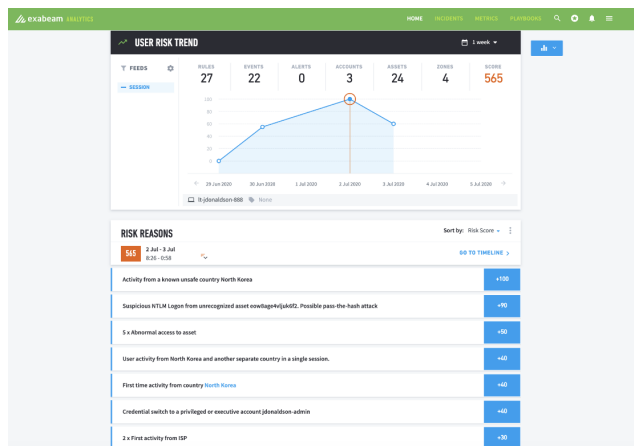
Extended detection and response (XDR) describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components.

Peter Firstbrook & Craig Lawson
Gartner Analysts
Innovation Insight for Extended Detection
and Response, April 2021

XDR - a smarter approach to TDIR

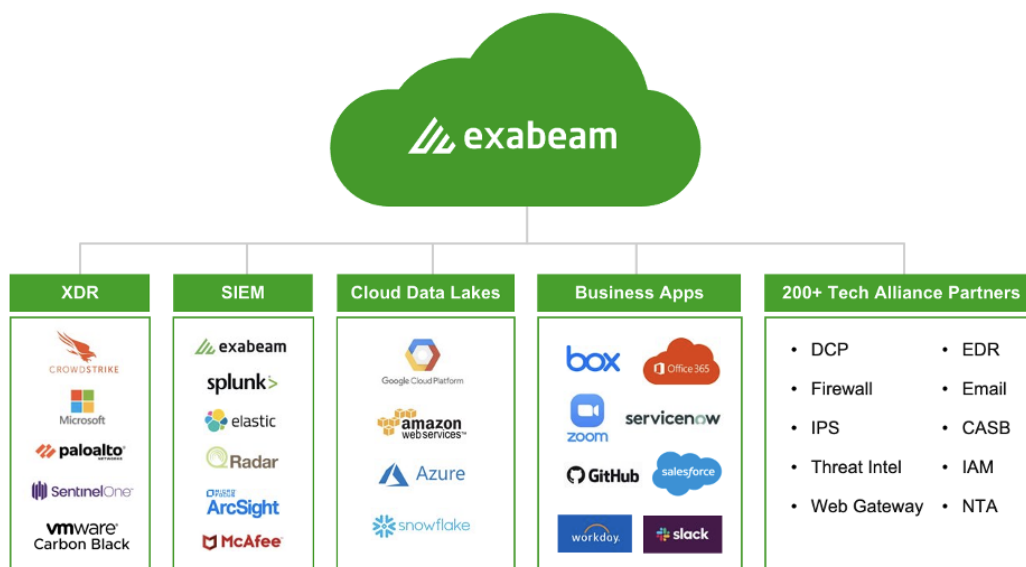
Exabeam Fusion XDR is an effective, outcome-focused TDIR that enables you to leverage and enhance the existing tools in your security stack, without forcing you to rip-and-replace them to centralize on a single vendor. It works out of the box using pre-built integrations with hundreds of 3rd party security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

To help SOC's and security analysts standardize around the use of best practices, Fusion XDR solutions include prescribed workflows and pre-packaged content that focus on specific threat types to achieve more successful TDIR outcomes. With Fusion XDR, SOC's are able to run their end-to-end TDIR workflows from a single control pane that performs automation of highly manual tasks like alert triage, incident investigation, and incident response. This boosts analyst productivity, reduces response times, and ensures consistent, highly repeatable results.



Flexible Integration to Augment your Security Stack

Free yourself from vendor lock-in and rip-and-replace tech refresh cycles. Fusion XDR 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 XDR get more out of your existing security investments, and to tightly unify them into a single control plane for the SOC.



USE CASE CONTENT



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 XDR solves this by leveraging prescriptive threat-centred 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 XDR 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.

The screenshot displays the Exabeam Fusion XDR interface for a user named 'exabeam.badguy1'. It shows a timeline of cloud administrative activities for Tuesday, 17 Mar 2020. The timeline includes events such as 'First time for this Cloud Administrative activity: GetAccountPasswordPolicy', 'First time for this Cloud Administrative activity: CreateGroupProfile', 'First time for this Cloud Administrative activity: LoadAttachedGroupPolicies', 'First time this user exabeam.badguy1 has performed Cloud account creation activity', 'First time for this Cloud Administrative activity: CreateUser', 'First time for this Cloud Administrative activity: LoginUsers', 'User enumerated (ListUsers) Cloud roles/users/objects in AWS', 'First time for this Cloud Administrative activity: ListGroupPolicies', 'First time for this Cloud Administrative activity: CreatePolicy', and 'First time for this Cloud Administrative activity: ListPolicies'. Each event is accompanied by a score, such as +15, +10, +25, +10, +15, +1, +15, +10, and +10.

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. 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.

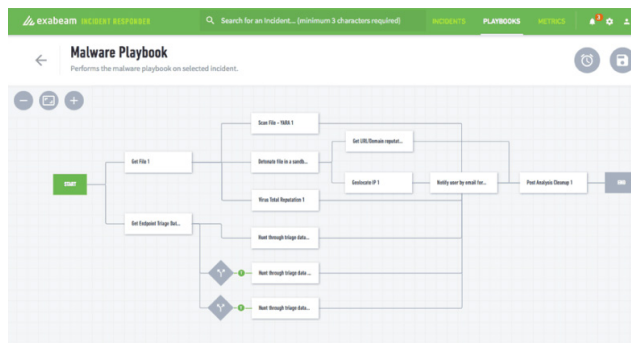
Fusion XDR automates the manual, time consuming steps of performing triage, investigation, and incident response. Machine-built timelines automatically gather evidence and assemble it into a cohesive story that can be used to perform an initial investigation.

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 response times.

Key features

Exabeam Fusion XDR provides 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:

- **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 SOC's to see quick time to value and achieve successful TDIR outcomes.



- **Patented Lateral Movement Tracking** - automatically detects lateral movement and follows attacks no matter where they spread to make sure your security team sees everything.
- **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** - SaaS 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.