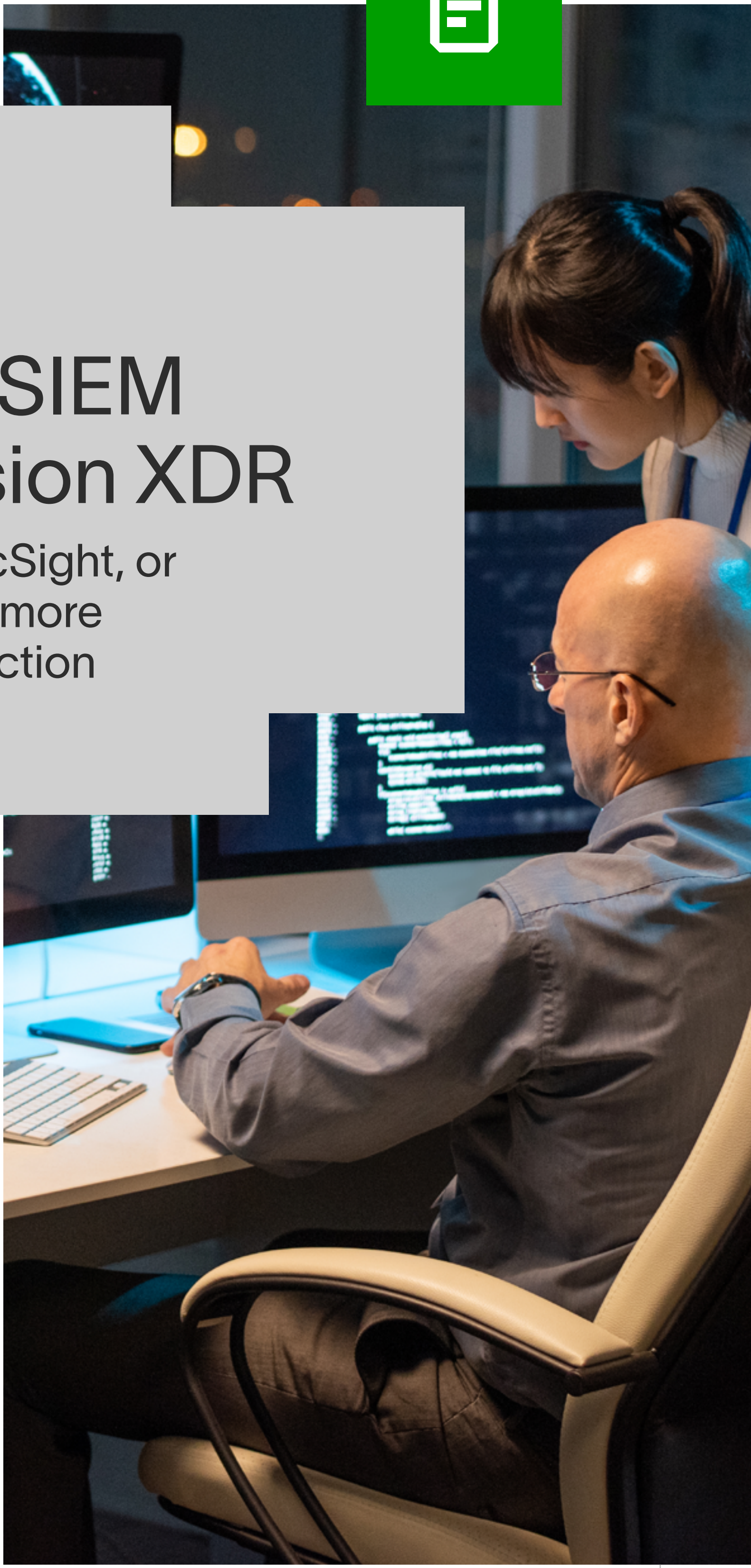
exabeam

Guide

Top 5 Benefits of Augmenting Your SIEM with Exabeam Fusion XDR

Transform a Splunk, QRadar, ArcSight, or data lake deployment for faster, more accurate, and easier threat detection and incident response



Managing your organization's security alerts is a full-time job — whether you monitor only Network Security Devices (NSD), Endpoint, Identity, or (ideally) all of the above. Traditional Security Information and Event Management (SIEM) products may be exactly what is required for log management and the requirements of compliance and governance, but they are seldom optimized for threat detection and incident response — and require extensive tuning to build events of interest.

Enter Exabeam Fusion XDR. When combined with a SIEM solution such as Splunk, QRadar, or a data lake, you add threat analysis, entity (user, endpoint, server, etc.) behavior analysis, risk scoring, correlation, and built-in incident response and case handling. All of this is possible without having to rip and replace your SIEM.

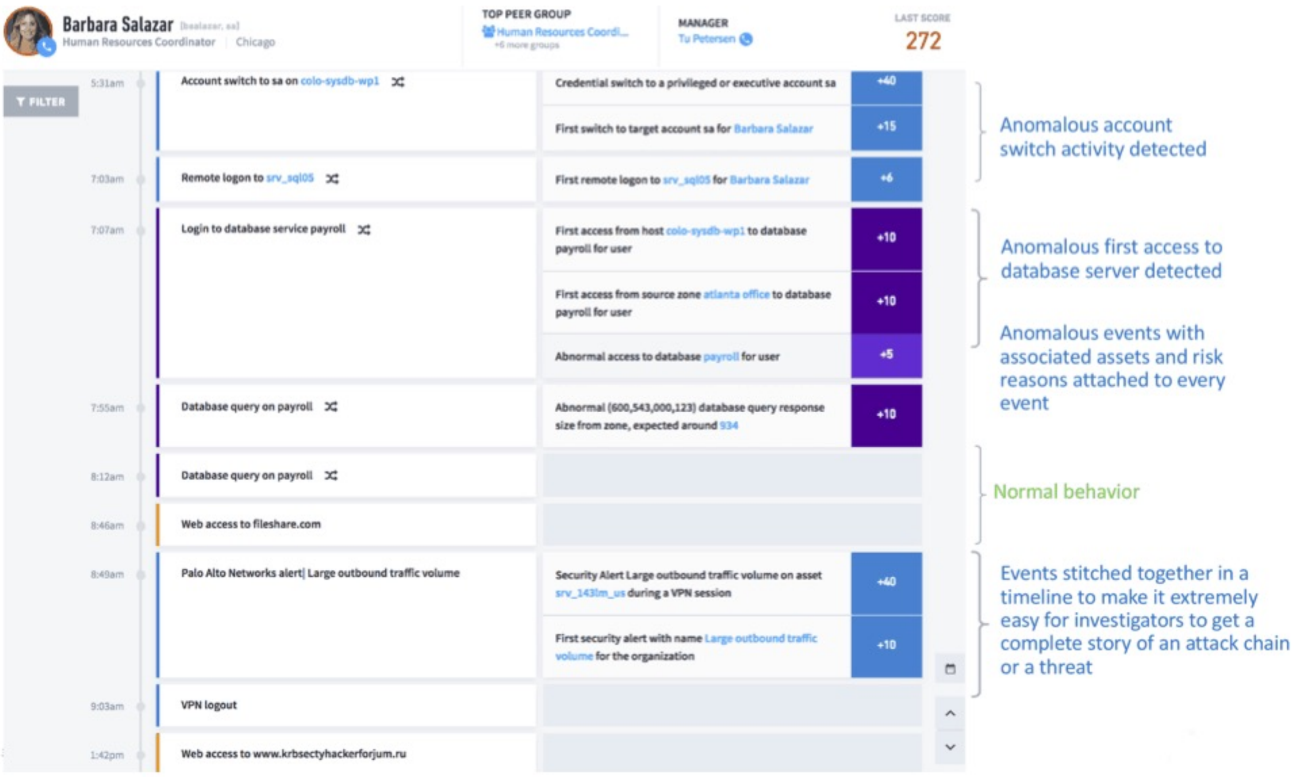
Instead of letting your legacy SIEM leave you vulnerable, Exabeam Fusion XDR allows you to add powerful machine learning and automation to help detect and respond to hard-to-find threats such as ransomware, rogue insiders, or attacks involving compromised credentials and lateral movement. Fusion XDR will help your team quickly become outcomes-focused with use case packages and reporting, and an easy interface for building more specific to your needs.

Amplifying your SIEM with the addition of Exabeam Fusion XDR has many benefits — here are the top 5 quick wins.

1. Improved threat detection

Exabeam brings your threat detection to the next level, using behavioral analytics to find lateral movement and persistence faster and more accurately than signature-based detection alone. Rather than drowning in alerts, Fusion XDR uses machine learning to pattern both user and machine behavior and deliver you a picture of normal. This picture allows you to track any changes or anomalies as they occur. Over time, Exabeam creates behavior models that can detect anomalies and alert security investigators, often long before they pose a threat to your organization.

Fusion XDR enhances your Splunk instance, helping prioritize alerts and offer risk scores for entities, helping your analysts efficiently monitor and protect your network. Alerts are chronologically ordered in smart timelines to make threats easy to spot so that investigators can quickly act on any issues. The tool also includes point-and-click threat hunting so analysts can proactively search for incoming threats. This analysis includes prescribing data sources that would help solve the problem, providing detection, mapping to MITRE, automating investigation, as well as defining the steps needed to contain, investigate, remediate, and recover from specific threats.



Barbara Salazar [bsalazar, sa]
Human Resources Coordinator | Chicago
TOP PEER GROUP: Human Resources Coordi... +6 more groups
MANAGER: Tu Petersen
LAST SCORE: 272

5:31am Account switch to sa on colo-sysdb-wp1
- Credential switch to a privileged or executive account sa +40
- First switch to target account sa for Barbara Salazar +15

7:03am Remote logon to srv_sql05
- First remote logon to srv_sql05 for Barbara Salazar +6

7:07am Login to database service payroll
- First access from host colo-sysdb-wp1 to database payroll for user +10
- First access from source zone atlanta office to database payroll for user +10
- Abnormal access to database payroll for user +5

7:55am Database query on payroll
- Abnormal (600,543,000,123) database query response size from zone, expected around 934 +10

8:12am Database query on payroll

8:46am Web access to fileshare.com

8:49am Palo Alto Networks alert| Large outbound traffic volume
- Security Alert Large outbound traffic volume on asset srv_143lm_us during a VPN session +40
- First security alert with name Large outbound traffic volume for the organization +10

9:03am VPN logout

1:42pm Web access to www.krbsectyhackerforjum.ru

Anomalous account switch activity detected

Anomalous first access to database server detected

Anomalous events with associated assets and risk reasons attached to every event

Normal behavior

Events stitched together in a timeline to make it extremely easy for investigators to get a complete story of an attack chain or a threat

Figure 01 A sample Smart Timeline that shows a complete entity behavior story to pinpoint anomalies and respond to security incidents faster.

2. Faster, more accurate incident response

Detection is only one step in the incident response process. Once a threat has been detected by Fusion XDR and a risk score exceeds a threshold, it immediately gathers data and context from across your security stack and organizes it together in the form of a machine-built Smart Timeline. The timeline lets your analysts then use automation to take action on the threat through visually investigating, validating, and suggesting the next correct action.

Say your business suffers a phishing attack: your analysts will get an alert, along with a Smart Timeline that they can review. They'll not only see the attack itself, but the events leading up to and following it. You'll be able to see the links that were in the email and research the reputation of the domain. At the same time, the user account's network access can be restricted to prevent further damage, or two-factor authentication enforced if credential hijacking is suspected. The Fusion XDR existing and customizable use cases help you adopt a best practice consistency for handling threats without needing to build or customize your tools and SIEM. This content reduces the effort to build and maintain an effective threat detection and incident response (TDIR) process, thus freeing analysts' time to take on other tasks.

3. Extending security to the cloud

Businesses are increasingly relying on cloud-based solutions to conduct daily activities. Yet in many environments, Splunk is limited to local network activity. Exabeam can extend your protection using cloud connectors to many of the standard cloud business applications. This allows your Splunk instance to gather logs from dozens of additional cloud services, including Google, Microsoft 365, Salesforce, and Amazon Web Services.

Not only do these cloud connectors gather information from cloud services, but they also adapt to any API changes which means you're always getting up-to-date protection against external threats. With the cloud connector tool, behavior analytics is hard at work, detecting any issues with the cloud services being accessed through your network each day.

As a cloud-delivered solution, Exabeam Fusion XDR can amplify any on-premises or Cloud SIEM, providing a fast path to more advanced threat detection and response.

Phishing Attack in Exabeam Fusion XDR

You get an alert accompanied by a Smart Timeline to review. You will see the attack and all the events both leading up to and following it. You can see the links in the email and research the reputation of the domain. Using automation, the user account's network access can be restricted, or two-factor authentication enforced if credential hijacking is suspected.

4. Improved case management

Every analyst may have a different approach to investigating an issue and communicating with higher-level analysts, engineering, and IT. To work an incident or alert quickly and efficiently, security analysts need the right information at their fingertips. Homegrown ticketing systems and ITSM tools are not built to hold security data nor are they embedded within analyst workflows. Exabeam Fusion XDR includes a built-in case manager so analysts can gather data from detection tools, track the status of investigations, and coordinate response actions from a single system of record. With incident notes and bi-directional communication via email or ITSM integrations, analysts can seamlessly access and update incident information for faster, more efficient investigation and response.

SOCs can further customize the layout, fields, and values for their environment and quickly access this information from the entire XDR platform, improving visibility and enhancing analyst productivity. Further, SOC management can get performance reports demonstrating improved response times, lower mean time to detect and respond, and other ROI efficiencies showing the effectiveness of their SOC team and toolsets.

Fusion XDR can augment your existing SIEM solutions to create better, more advanced threat protection for your business, its users, and its customers. For more in-depth information watch the full video here or read the datasheet.

5. Empowerment: Splunk Ninjas, QRadar, and ArcSight Admins

During the early years of SIEM, solutions like ArcSight, Splunk, and QRadar defined the market. Their rise was built on powerful capabilities, such as search (Splunk), correlation (QRadar), and alert consolidation (ArcSight). A key ingredient to the success of these early leaders was a passionate following of expert users/ninjas/analysts able to do the impossible and extend these solutions to solve new challenges.

As the SIEM market and the data footprint has evolved, these "search," "correlation," and "regex" gurus are mired in alerts, chasing down false positives, and investigating dead ends. Augmenting these solutions with XDR allows you to "get your experts back."

By amplifying your SIEM with Exabeam Fusion XDR behavioral analytics and automation, your power users can respond to anomalies rather than spending time looking for them. The Exabeam model creation capability offers these power users the ability to develop advanced machine learning models in minutes that will save them countless hours in search and correlation building. Exabeam Fusion XDR gives your experts a new secret weapon!

About Fusion XDR

Exabeam Fusion XDR, a cloud-delivered solution, takes an outcome-based approach and offers prescriptive workflows and pre-packaged, threat-specific content to efficiently solve threat detection, and incident response (TDIR). Pre-built integrations with hundreds of 3rd party security tools — including Splunk and QRadar — and our market-leading behavior analytics combine weak signals from multiple products with an understanding of normal operating behavior to find complex threats missed by other tools. Prescribed workflows and pre-packaged content focused on specific threat types enable SOC teams to achieve more successful TDIR outcomes. Automation of triage, investigation, and response activities from a single, centralized control plane turbocharges analyst productivity and reduces response times.

Contact us for a demo to see how you can augment your Splunk, QRadar, or legacy SIEM implementation with Exabeam.
Visit exabeam.com/demo.

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com

exabeam