10 Reasons to Augment Your SIEM With Behavioral Analytics

Why Behavioral Analytics Is a Critical Upgrade for Your Security Framework

Today's cyberattacks are increasingly sophisticated, and your security teams are likely overwhelmed with alerts that lack context. According to the 2025 Verizon Data Breach Investigations Report (DBIR), 60% of all breaches involve a human element, from phishing to the use of stolen credentials. This makes it difficult for traditional, rules-based tools to distinguish legitimate activity from a genuine threat. You need a more effective solution.

Integrating behavioral analytics with your SIEM provides that solution. Exabeam New-Scale Analytics, built on a hyperscale, cloud-native architecture, ingests and analyzes data from hundreds of sources at petabyte scale. By applying AI and machine learning, it gives you a complete picture of adversary movement, providing your analysts with fewer, higher-fidelity alerts that pinpoint genuine threats.

Behavioral analytics is projected to grow at a compound annual growth rate (CAGR) of 33.4% from 2023 to 2030, reflecting its rapid adoption across industries. The technology establishes a baseline of normal behavior for every user and device in your environment. When an activity deviates from that baseline, like a login from a new location or unusual access to a sensitive file, it is assigned a risk score that rises with its severity. Once that score crosses a predefined threshold, the platform alerts your SOC analysts for immediate investigation.

With third-party involvement in breaches doubling in the last year, integrating behavioral analytics with your SIEM is essential for detecting modern threats that cross organizational boundaries.

1. Detect Compromised User Credentials

The 2025 DBIR confirms that the use of stolen credentials is still the most common initial access vector in breaches, accounting for 22% of incidents. Behavioral analytics addresses this gap by identifying anomalies in user behavior, such as suspicious logins from unusual locations or devices, that signal an account has been compromised.

2. Detect Privileged User Compromise

Your privileged accounts are prime targets for attackers. If compromised, they offer direct access to critical assets. Behavioral analytics monitors these high-value accounts, automatically identifying abnormal behavior—like unusual access patterns or privilege escalations—that signals a breach.

3. Monitor Your Executive Assets

Your executives' devices contain highly sensitive financial data, strategic plans, and competitive insights. Behavioral analytics strengthens your SIEM by automatically building behavior models for these assets. It continuously monitors for unusual access or usage, helping you protect these critical assets from misuse.

4. Detect Compromised Systems and Unmanaged Devices

The 2025 DBIR shows that 46% of corporate logins came from unmanaged, personal devices. Behavioral analytics gives you visibility into this activity by monitoring key vectors regardless of the device. It identifies unusual account activity, deviations from server baselines, and abnormal network traffic, enabling your team to respond to attacks faster.

5. Differentiate Normal Behavior From Malicious Behavior

Insider threats are a significant challenge because traditional tools often miss them. Behavioral analytics helps you identify risky activities that deviate from a user's normal behavior, such as logins at unusual times or abnormal data access. This allows your security teams to identify and mitigate insider threats more effectively.

6. Identify and Track Lateral Movement Across Your Environment

Attackers often move laterally through your network and into third-party environments. With third-party involvement in breaches doubling to 30% this year (2025 DBIR), visibility across platforms is critical. Behavioral analytics makes your SIEM more effective by connecting these disparate events, helping you detect lateral movement early.

7. Detect Instances of Data Exfiltration

To protect your sensitive information, you must detect data exfiltration. Behavioral analytics strengthens your SIEM by monitoring for unusual spikes in network traffic, suspicious email forwarding, and even the new risk of employees pasting sensitive data into Generative AI platforms, giving you a comprehensive view of data movement.

8. Provide Context to Failed Logins and Account Lockouts

Behavioral analytics automates the analysis of failed logins for your SIEM. It assesses patterns, such as frequency and location, and correlates them with other suspicious activities. This automation saves your security team significant time and helps them quickly assess risk.

9. Identify and Stop Service Account Misuse

Your service accounts often have elevated privileges and are a common blind spot. Behavioral analytics automatically identifies these accounts and establishes baselines for their normal activity. It monitors for deviations, alerting your teams to potential abuse or compromise that traditional tools would miss.

10. Automate Detection, Triage, and Investigations

The 2025 DBIR notes that the median time to remediate (MTTR) a leaked credential in a public repository is 94 days. Manual investigation is too slow. New-Scale Analytics automates the entire process, delivering complete incident timelines in seconds. It also provides prescriptive guidance for response, helping your SOC analysts focus on the most pressing threats and respond faster.

Upgrade Your SIEM with Behavioral Intelligence

A behavioral analytics solution is essential for detecting the advanced, complex threats that your traditional tools often miss. The Exabeam New-Scale Security Operations Platform is purpose-built to augment your existing SIEM or data lake. It delivers industry-leading threat detection, investigation, and response (TDIR) by integrating AI and automation into security workflows.

Exabeam automates the creation of incident timelines, providing your team with a clear, chronological view of events without manual searching. This automated insight helps your security teams investigate and respond to threats faster and more effectively. By ingesting your logs, alerts, and other telemetry, the New-Scale Platform transforms your SIEM into a powerful tool for detecting sophisticated attacks. With risk-based prioritization and machine learning, you can efficiently triage, investigate, and respond to threats.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →