Augment SIEM With New-Scale Analytics

Modernize Threat Detection Without Ripping and Replacing Your SIEM

Security teams are under pressure. Alert fatigue, analyst burnout, and identity-based attacks have exposed the limits of traditional SIEM platforms. Most SIEMs detect known threats using static rules. But today's adversaries use stolen credentials and escalate privileges slowly—blending in as routine behavior.

To catch these threats, your security operations team needs more than log aggregation and correlation rules. It needs behavior-based context. This white paper explains how Exabeam New-Scale Analytics can augment your existing SIEM—without replacing infrastructure—to detect threats that rules alone miss.

Whether your team uses a legacy SIEM or a modern cloud-based platform, New-Scale Analytics enhances threat detection, improves SOC productivity, and extends the value of your current investments.

The Challenge: Identity-Based Threats Are Evading Detection

Organizations face mounting pressure from both external attackers and internal actors. Meanwhile, many SOCs are overwhelmed:

- 62% of alerts are ignored due to high volumes and low fidelity.
- 84% of security professionals report burnout, with more than half leaving their roles because of it.
- Credential theft attacks surged 703% in late 2024, driven by phishing kits and compromised insiders.

Once an attacker has valid credentials, they don't need to break in—they log in. Most SIEMs lack the behavioral insight needed to flag this activity. They monitor events, not patterns. As a result, actions like odd-hour access, privilege changes, or data downloads often appear benign in isolation.

Insider threats add to the challenge. These users operate with legitimate access, making their behavior difficult to distinguish from routine activity. Rule-based systems often miss the gradual build-up to malicious acts.

The Resource Gap in Security Operations

SOCs are stretched thin. With more than four million cybersecurity jobs unfilled and 67% of organizations reporting moderate to critical skills gaps, security teams are forced to do more with less.

At the same time, the complexity of hybrid infrastructure—fragmented tools and log sources make it harder to spot subtle anomalies. Traditional SIEM and extended detection and response (XDR) tools often rely on static rules that don't scale well or adapt to new tactics.

What's needed now is real-time context. Behavioral analytics fills this gap by learning normal activity patterns and identifying when something is off—even if it doesn't match a known attack signature.

SIEMs Miss the Story Between the Lines

Static correlation rules detect known threats well, but today's attacks don't always look like attacks. A contractor printing sensitive files or an engineer escalating privileges might not trigger alerts. But these behaviors, over time, may point to compromise or misuse.

Most SIEMs treat each event—like a login or file access—as isolated. They lack the ability to connect these actions into a behavioral sequence or timeline. As a result, analysts are left to manually sift through logs, trying to assemble the full picture.

This fragmented approach delays response and allows threats to persist. The challenge isn't always sophistication. It's that these threats appear normal. What links them is identity.

Why Behavioral Analytics Matters

Behavioral analytics changes the equation by providing context. Instead of relying on signatures or static rules, it learns what's normal for each user and device, then flags deviations.

- A login from an unusual location
- Off-hours access to critical systems
- Unexpected spikes in file transfers

Individually, these actions may not seem suspicious. But together—and in context—they can reveal a serious threat. Behavioral analytics uses machine learning (ML) to evaluate risk based on patterns, not just events. New-Scale Analytics also organizes activity into automated timelines, reducing manual correlation. Analysts get a complete view of what happened—without switching or writing complex queries.

Use Cases That Require Machine-Learned Detection

Compromised Credentials

In 2024, more than 3.2 billion credentials were exposed. Most SIEMs see a successful login, not a threat. Behavioral analytics monitors post-login activity to surface anomalies—such as access to unfamiliar systems or lateral movement—associated with compromised identities.

Privilege Escalation Over Time

Attackers often move slowly, escalating privileges bit by bit. Behavioral analytics correlates these changes and flags access patterns that deviate from a user's baseline.

Malicious Insiders

Insiders rarely trigger alerts in one step. They operate cautiously, testing limits. Behavioral analytics flags unexpected behavior—like changing audit settings or downloading atypical file volumes—based on each user's normal activity.

Audit Evasion

Behavior like disabling logs or clearing trails is high risk, especially when done by users who don't typically perform such actions. Behavioral analytics highlights these deviations.

Data Exfiltration

Transfers that are larger than usual, sent to new destinations, or happen at odd times may indicate exfiltration. Behavioral analytics detects these signals in context.

Reducing Alert Fatigue

Instead of flooding analysts with isolated alerts, behavioral analytics highlights real threats, grouping events and assigning risk scores.

Integrating New-Scale Analytics with Your SIEM

New-Scale Analytics connects directly to your SIEM via Syslog, API, or prebuilt cloud collectors. It ingests only the log types needed for behavioral analysis, such as authentication events, file access, VPN use, and directory changes.

Once integrated, it builds behavior models, applies risk scoring, and visualizes threat activity in automated timelines. Analysts can continue working in their existing tools, now with enhanced detections and clearer context.

There's no need for a rip-and-replace migration. New-Scale Analytics fits alongside your current environment, improving detection accuracy, reducing false positives, and enabling faster triage.

Augment, Don't Replace

Today's threats are subtle, persistent, and identity driven. Most SIEMs aren't built to detect what looks normal on the surface but hides malicious intent underneath.

With New-Scale Analytics, you can:

- Detect threats that static tools miss.
- Reduce false positives and analyst fatigue.
- Accelerate investigations with automated timelines.
- Improve SOC productivity without expanding your team.

You don't have to replace your SIEM to modernize your SOC.

See what your SIEM is missing. Schedule a demo to experience New-Scale Analytics in action.

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 →