Enabling the High-Fidelity SOC with Behavioral Detection

The Data Science Secrets Behind Exabeam New-Scale Analytics

Sophisticated digital threats demand advanced detection and response. Traditional security information and event management (SIEM) and first-generation user and entity behavior analytics (UEBA) systems often overwhelm security operations centers (SOCs) with a high volume of low-fidelity alerts and false positives. This alert fatigue impacts morale and erodes trust in security systems. When analysts investigate dozens of false positives, they are more likely to dismiss a genuine threat, which slows threat detection, investigation, and response (TDIR) and increases organizational risk.

Exabeam is a long-recognized pioneer in AI and behavioral analytics. We introduced New-Scale Analytics as the next evolution of these core capabilities. It reinvents behavioral detection by replacing broad, static baselines with an adaptive, multi-dimensional model built for modern threats. By combining machine learning with use-case-specific baselining and business-driven risk prioritization, New-Scale Analytics reduces false positives, effectively surfaces high-fidelity threats, and provides the context needed to accelerate every stage of the TDIR lifecycle. The result is a more efficient, effective, and proactive SOC.

The Challenge of Noise in Modern Threat Detection

Cyberattacks are increasingly stealthy and evasive. Threat actors often use legitimate credentials, internal systems, and memory-resident malware to evade traditional signature-based defenses. While UEBA was a necessary evolution from static correlation rules, first-generation platforms introduced their own challenges.

The core issue is the one-size-fits-all problem: the use of a single, broad behavioral baseline that lacks context. For instance, applying a user's normal number of logins indiscriminately across different rules ignores that what is normal for endpoint activity may be highly abnormal for data exfiltration. This global averaging can flood analysts with noise, burying critical threat signals. Furthermore, these systems often rely on manually assigned, predefined scores that require constant human tuning and fail to reflect the true, combined risk of a sequence of events.

The SPOT Framework: A Process for Decisive Action

Your SOC operates in a high-pressure situation where rapid, accurate decisions are paramount. To succeed, you need a structured process to cut through the noise. The SPOT framework is a rapid decision-making process designed for these environments, aligning directly with an effective TDIR lifecycle. The acronym stands for **S**urvey, **P**rioritize, **O**ptimize, and **T**ake Action. New-Scale Analytics operationalizes this framework, giving your team a clear path from noise to action.

- **Survey:** This phase is about gathering a complete and accurate picture of your environment. Whether data is ingested directly or accessed via federated queries, the critical first step is analysis. New-Scale Analytics automates the most valuable part of this process by parsing and normalizing disparate logs into a common format, providing the visibility you need for high-fidelity analytics and detection.
- **Prioritize:** This phase involves identifying which events demand immediate attention. This is where most security tools fail. New-Scale Analytics addresses this through data-driven event scoring, grouping related events into coherent threat categories, and applying business knowledge to elevate the most critical risks to your organization.
- **Optimize:** This phase is about continuously improving your detection process. New-Scale Analytics embodies this principle with self-tuning, adaptive baselines and maturity thresholds, which automatically refine detection models and minimize false positives without constant human intervention.
- **Take Action:** The final phase is the response. With a clear, prioritized, and contextualized threat picture from New-Scale Analytics, your SOC team can respond faster and more decisively throughout the TDIR lifecycle.

SPOT Framework Documentation 2024 by Inbar Rose is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International.

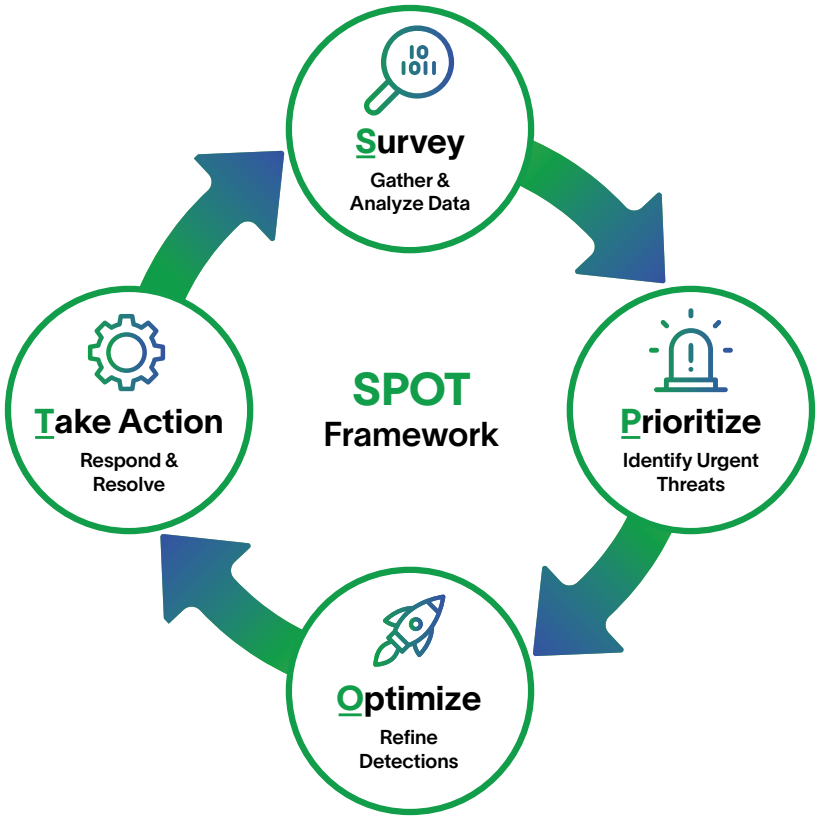

Figure 1. The SPOT framework is a four-stage process (Survey, Prioritize, Optimize, and Take Action) that is designed to guide rapid decision-making processes. The fast-paced, high-pressure environments of security operations centers serve as a perfect model for operationalizing SPOT. New-Scale Analytics was designed with these guiding principles to accelerate the TDIR lifecycle.

The New-Scale Analytics Approach: Precision Through Multi-Dimensional Baselines

New-Scale Analytics implements the SPOT framework to solve the false positive problem. It advances detection accuracy by applying contextual, adaptive models for specific use cases.

Multi-Dimensional Baselines Increase Precision

Each behavioral model in New-Scale Analytics builds its own tailored baseline. For example, a rule for Abnormal Logins builds a baseline of "unique endpoints per day," while a rule for Data Exfiltration builds a separate baseline of "volume of downloads per host." Baselines also adapt automatically for each specific entity (user, host) and activity type (logins, emails), ensuring comparisons are always contextual. This ensures your analysts see only the most relevant anomalies, reducing time wasted on insignificant alerts.

How it Works: Dynamic and Self-Learning

The New-Scale Analytics platform uses a long-term lookback period to learn what is normal for an entity's behavior. To do so, it maintains custom anomaly thresholds for each feature and rule, creating a precise and multi-dimensional pattern of typical behavior for every entity. Activity is measured over a rolling aggregation window and re-evaluated at set intervals. A maturity threshold ensures the baseline is stable before it is used for alerting, which prevents false positives that arise from insufficient data.

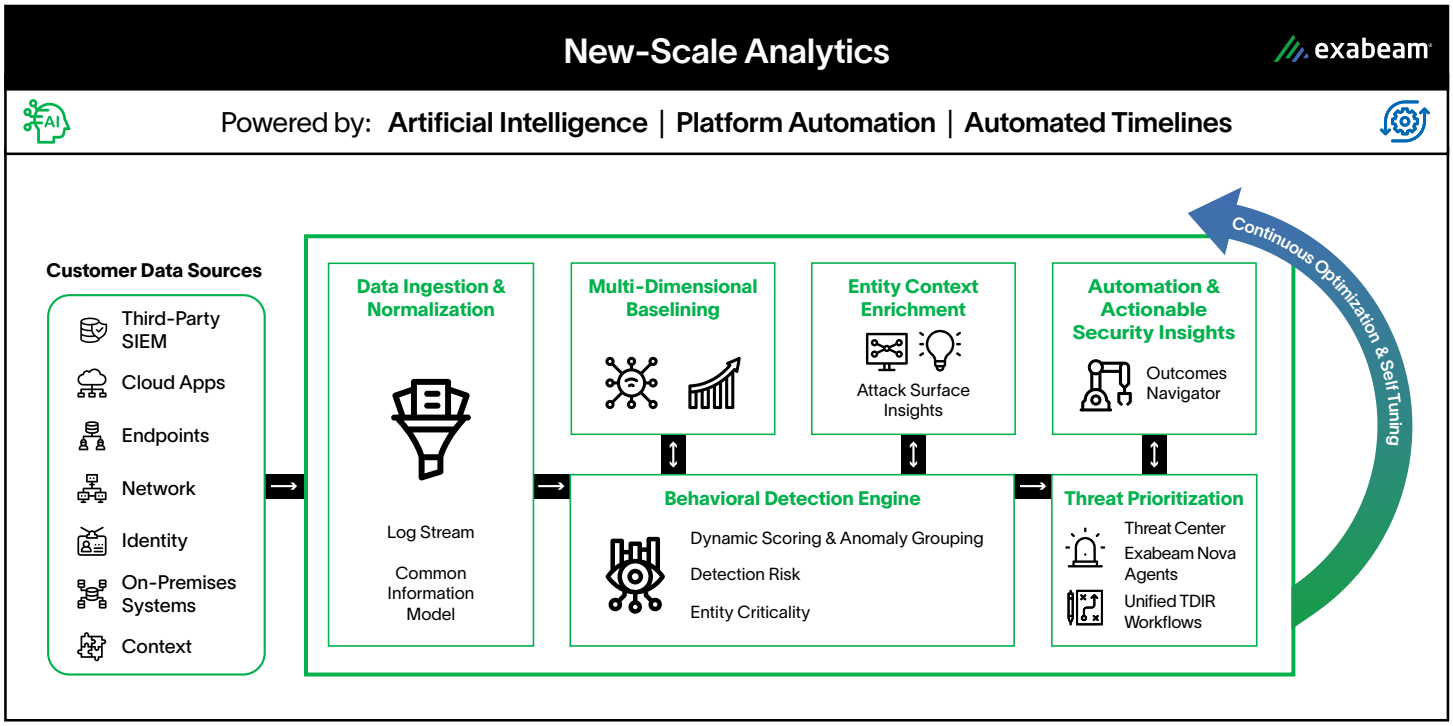

Figure 2. New-Scale Analytics processes normalized data using both multidimensional baselining and dynamic rarity analysis. An advanced behavioral detection engine then enriches these findings with business factors to deliver prioritized threats and actionable insights, all within a self-tuning system.

From Individual Events to Prioritized Threats

New-Scale Analytics transforms statistical findings into actionable security insights through a five-step process that builds a complete threat narrative.

1. **Event-level scoring (dynamic rarity):** The process begins with a dynamic, machine-learning-driven approach to scoring. The platform continuously measures the statistical rarity of an event by referencing both local (specific to the entity) and global (across the organization) rarity factors. This approach automatically deemphasizes common, low-risk events and reduces noise, freeing your team from the constant manual tuning required by other solutions.
2. **Anomaly grouping:** Anomalous events that have triggered rules are automatically grouped per entity. The individual scores are then summed up to form a single, unbounded threat score for the entire group, eliminating the need for your team to manually connect the dots.
3. **Enrich with entity context (Attack Surface Insights):** A New-Scale Platform-wide feature, Attack Surface Insights provides event-driven entity context. Rather than relying solely on identity systems like Active Directory (AD), it builds a comprehensive asset and user inventory from observations made directly through platform telemetry. This allows it to identify and profile devices that may not exist in your AD, such as networking equipment or non-domain-joined devices. While directories inform the process, the actual logs are the source of activity, creating a far more accurate and complete entity profile for enrichment. This accuracy becomes a catalyst for prioritization, ensuring the most critical risks rise to the top.
4. **Threat score normalization:** An unbounded threat score is difficult for your analysts to interpret. To solve this, New-Scale Analytics normalizes the score to a bounded range between 0 and 100. This step provides a clear, consistent baseline score for every threat and makes it easy for you to set a score threshold for automated case creation.
5. **Threat prioritization (Business Factors Adjustment):** Using the full threat story and rich entity context, the system prioritizes the threat. It adjusts the score based on key business factors, like the number of high-scoring detections and the involvement of high-criticality entities. This single, meaningful score transforms anomalies into a clear business-risk signal, enabling your analysts to focus on threats that are not just unusual, but genuinely critical.

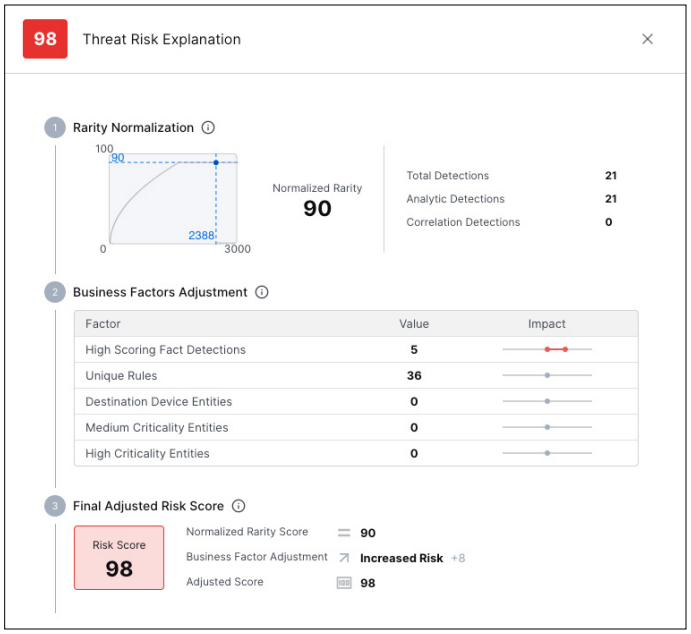

Figure 3. New-Scale Analytics translates statistical rarity into a clear business-risk signal. In this example, a normalized rarity score of 90 is elevated to a final risk score of 98 based on critical business context—in this case, the presence of five high-scoring fact detections. This final score enables your analysts to prioritize threats that pose a genuine risk to the organization.

Reducing False Positives and Detecting Overlooked Threats

An advanced analytics platform is measured as much by what it deemphasizes as by what it detects. Reducing false positives is critical for your SOC's efficiency. Here are four common scenarios where traditional analytics generate noise and how New-Scale Analytics provides a high-fidelity, actionable signal instead.

Scenario 1: The Traveling Executive—Distinguishing Business from Breach

- **The false positive:** A CFO logs into your corporate VPN from a hotel Wi-Fi hotspot. A legacy UEBA system sees the new IP address and triggers a high-priority alert. Your SOC spends time verifying the activity, only to confirm it was legitimate.
- **The New-Scale Analytics approach:** The system analyzes a vector of features, going beyond simple geolocation. While a new IP may be rare, the combination of other features (the user's device, their normal working hours) is not considered rare for that executive's profile. The resulting risk score is lower, preventing a false positive without manual intervention.

Scenario 2: The Developer's Code Download—Understanding Role-Specific Behavior

- **The false positive:** A developer downloads a large, 500 MB source code repository. A system using a one-size-fits-all baseline sees this large data transfer, compares it to the user's average, and flags it as potential data exfiltration.
- **The New-Scale Analytics approach:** New-Scale Analytics establishes a local rarity score for each developer's activity, which in turn informs a global rarity score for the developer peer group. For this developer, a 500 MB download is normal. By understanding this behavior is common within the context of the developer's role, the system correctly identifies it as legitimate work, avoiding an unnecessary alert for your team.

Scenario 3: The Multi-Vendor Environment—Unifying Detections

- **The overlooked detection:** Your SOC uses an EDR from CrowdStrike, cloud infrastructure on AWS, and identity services from Okta. An attacker compromises an Okta account and uses the compromised credential to access a sensitive S3 bucket. Each tool sees only a piece of the puzzle, forcing your analysts to manually stitch disparate alerts.
- **The New-Scale Analytics approach:** Our behavioral analytics are vendor agnostic. New-Scale Analytics correlates the anomalous Okta login with the unusual S3 access, automatically grouping these events into a single, high-priority threat timeline and presenting a complete attack narrative that no one tool could build on its own.

Scenario 4: The Unique Threat—Creating Custom Analytics in Minutes

- **The missing detection:** Your security team learns about a new tactic, technique, or procedure (TTP) where attackers abuse a vulnerability in a legitimate, internal financial application. Your existing security tools have no pre-built rules for this.
- **The New-Scale Analytics approach:** Our detection-building features make creating powerful, custom analytics simple. You can build a new detection model for a behavior in minutes. Your SOC can immediately hunt for this unique threat across your environment without waiting for a vendor update or paying a consultant to write a new rule.

The Business Value of High-Fidelity Detections

With New-Scale Analytics, your security operations team can move from reactive firefighting to proactive, business-aligned defense. By reducing noise and aligning detections with business context, your analysts gain time back, leaders gain more certainty, and your organization lowers the risk of costly breaches.

- **Faster response and lower mean time to respond (MTTR):** High-fidelity detections direct your analysts' attention to the most critical threats. Customers report up to 80% faster triage and investigations compared to traditional SIEM workflows.
- **Improved SOC and engineering efficiency:** Self-tuning baselines and automated threat timelines minimize manual rule adjustments and correlation. Organizations see a 70% reduction in log onboarding time and lower engineering overhead, freeing staff for higher-value initiatives.
- **Reduced breach likelihood:** By identifying unknown threats and credential misuse before adversaries achieve their objectives, you materially reduce risk. For example, Exabeam flagged a compromised service account at an energy company hours before their EDR tool, preventing lateral movement.

New-Scale Analytics provides a new approach to behavioral detection that delivers measurable outcomes. We help you modernize operations, strengthen defenses, and maximize your return on investment.

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 →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2026 Exabeam, LLC. All rights reserved.