# Six Ways Exabeam Helps You Detect Compromised Credentials

## An automated view into attacker behaviors

When an attacker has valid credentials, they are no longer an outsider; they are an insider. This guide explains why this threat is so difficult to detect and outlines six effective ways the New-Scale Security Operations Platform provides a modern solution.

A compromised credential is any authenticator—a user's password, an administrator's private key, or an AI agent's API token—that has been stolen by an adversary. Once inside, the attacker can operate with legitimate, trusted access, which is why the average cost of an insider threat incident has now soared to $17.4 million.

To find an attacker in disguise, you must look beyond static rules and focus on behavior. Here are six ways Exabeam accomplishes this.

### 1. Establish a Behavioral Baseline

The foundation of modern threat detection is understanding what is normal. The Exabeam platform ingests data from across your environment to create a unique behavioral baseline for every user and entity. It automatically learns what is normal for each one: What data do they typically access? What systems do they use? What hours do they work? Without this baseline, it is impossible to spot abnormal activity.

### 2. Detect Deviations in Real Time

Once a baseline is established, Exabeam user and entity behavior analytics (UEBA) can instantly spot deviations. When a user or entity's activity differs from its established pattern—such as accessing a sensitive project folder for the first time, logging in from a new country, or using a new device—Exabeam flags the activity as anomalous. This is the first signal that a credential may be compromised.

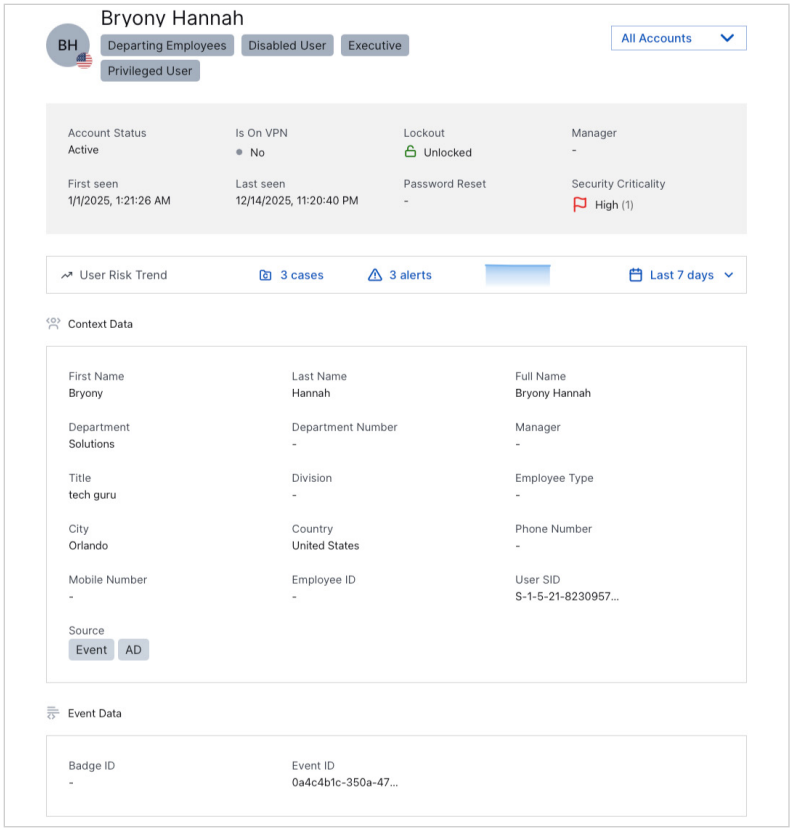


**Figure 1.** Exabeam builds a rich profile for every user, combining organizational context like their department and title with learned behaviors, such as the assets they normally use. This complete profile forms the baseline for detecting anomalies.

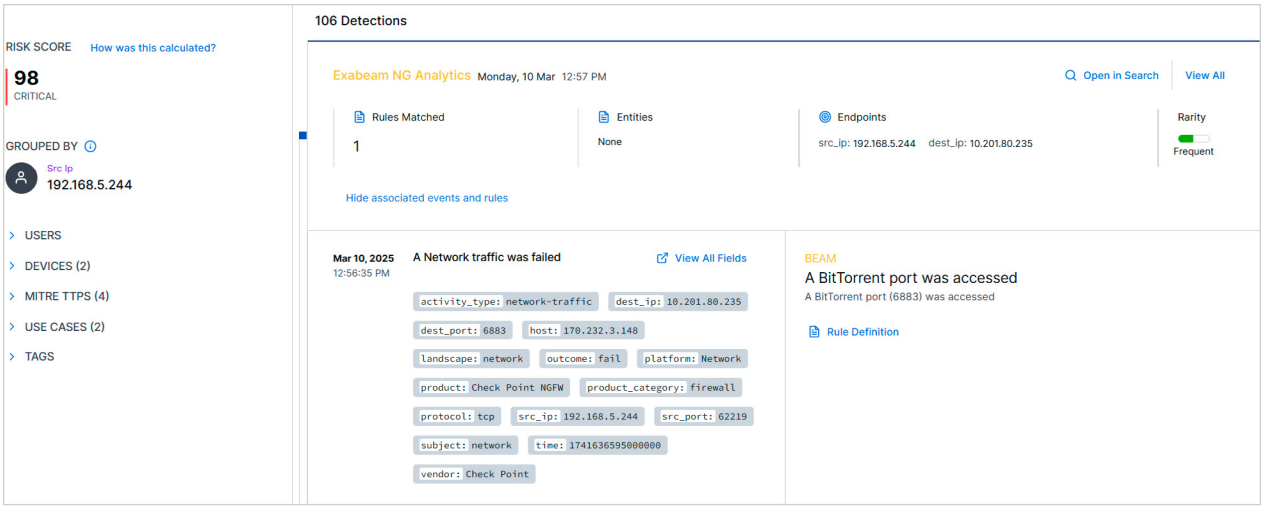


**Figure 2.** The Threat Timeline instantly flags specific deviations from a user's behavioral baseline. In this example, it has detected that "A BitTorrent port was accessed"—a high-risk activity that is clearly abnormal for a typical corporate user and requires immediate investigation.

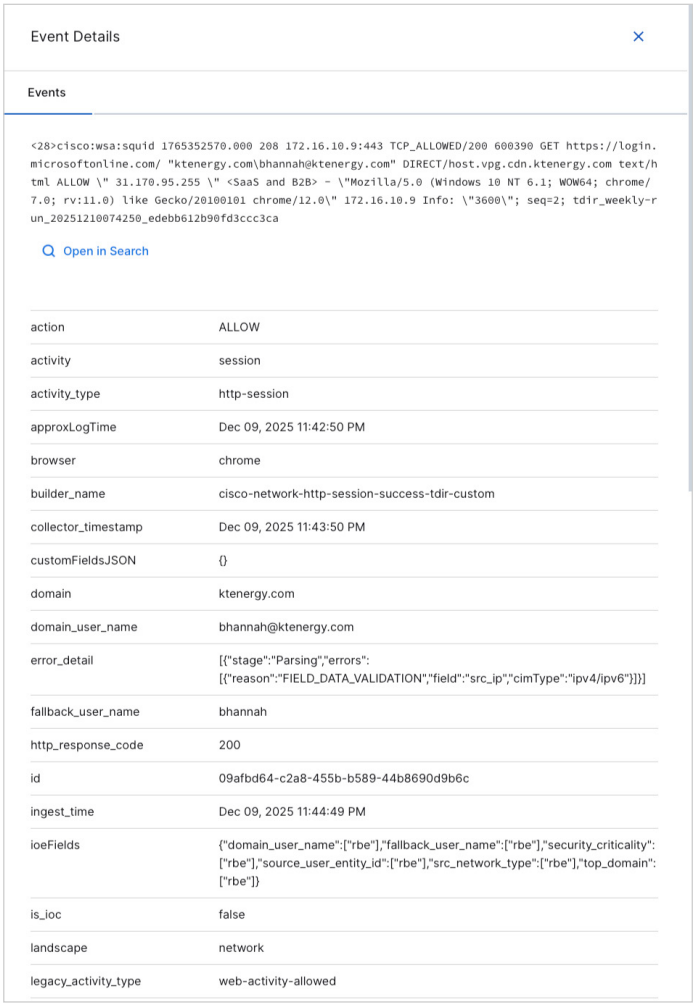


**Figure 3.** Context turns data into answers. This view shows how Exabeam helps analysts move beyond raw logs by automatically adding business context to help them instantly grasp the business impact of an event.

## 3. Enrich Events With Context

An anomaly alone is not enough. To be useful, it needs context. Exabeam automatically enriches security events with critical context, such as the user's role and department, the asset's location and owner, and whether the activity involves a critical system. This helps an analyst quickly understand the potential business impact of an alert.

## 4. Automate Incident Timelines

Instead of generating thousands of isolated alerts, Exabeam automatically stitches all related activity—both normal and abnormal—into a timeline for each potential incident. This allows an analyst to see the full story of an attack immediately, from the initial compromise to lateral movement and data exfiltration, distinguishing a real threat from a false positive in minutes.

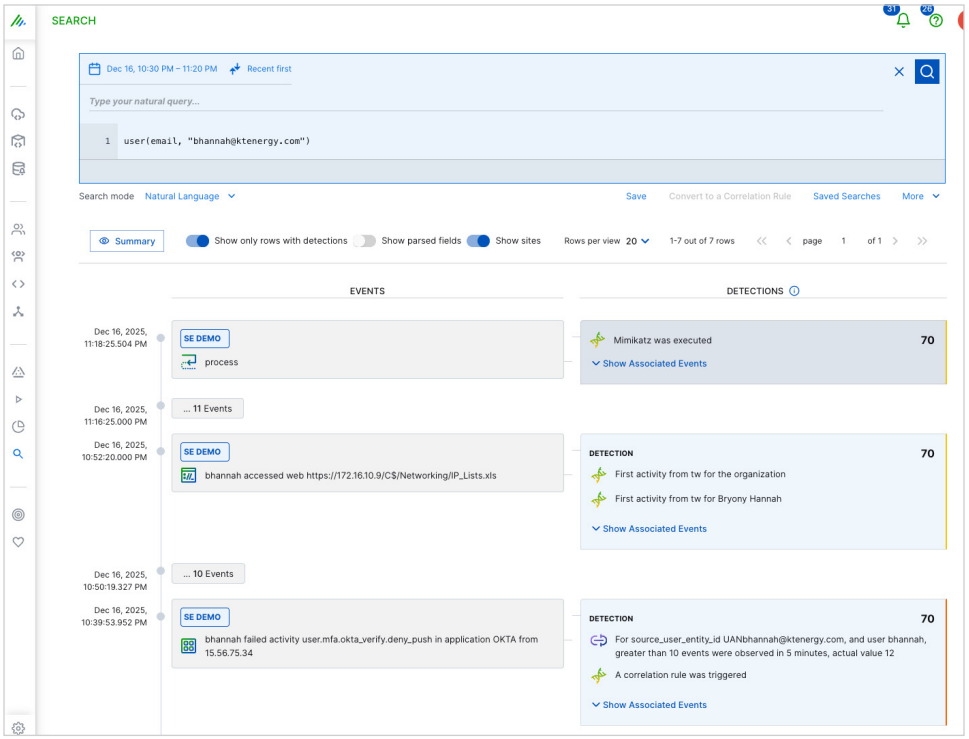


**Figure 4.** To save analysts from manually connecting alerts, the Threat Timeline automatically stitches together all related user activities into a single, chronological story. This view shows the complete narrative of a potential incident, allowing an analyst to understand the entire attack chain at a glance.

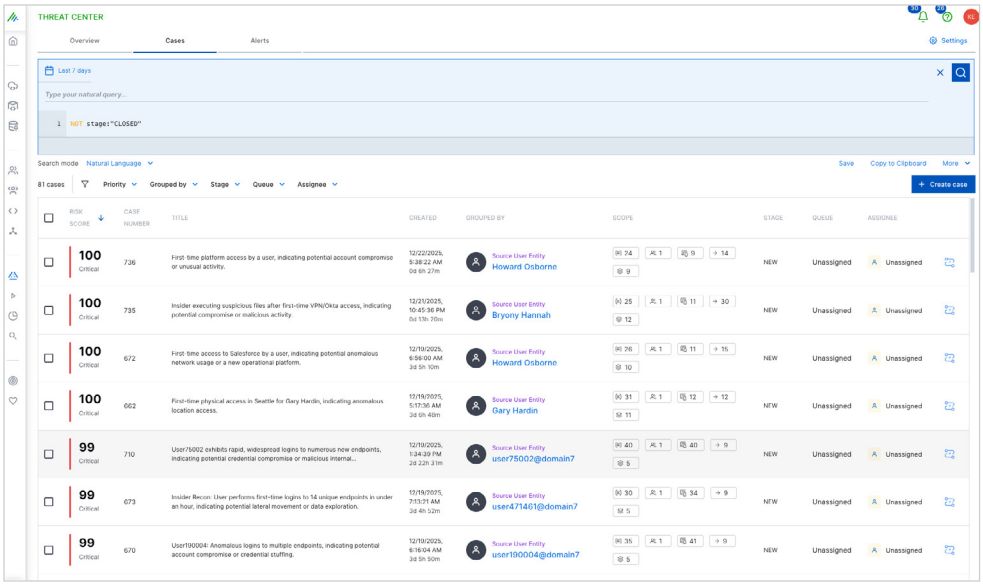


**Figure 5.** The Threat Center case view acts as the analyst's prioritized work queue. By aggregating risk scores from all anomalous activity, it presents a clear list of the most significant threats, ensuring the highest-risk incidents are addressed first.

## 5. Prioritize Threats With Risk Scoring

To distinguish between minor deviations and a genuine attack, Exabeam assigns a dynamic risk score to every anomalous event. A login from a new device might add five points, while access to a critical server might add 50. As these scores accumulate, the riskiest incidents automatically rise to the top of a prioritized queue, enabling your security team to focus its resources on the most credible threats.

## 6. Extend Detection to Your Digital Workforce

The definition of an "insider" has expanded. As your organization builds and deploys custom AI agents, you create a new class of digital insider. These agents operate with trusted API keys and service account tokens to perform their functions.

An adversary can compromise these digital insiders by:

- Stealing API keys to impersonate an AI agent and access sensitive systems.
- Using attacks like prompt injection to manipulate the agent, tricking it into bypassing safety controls or leaking confidential information.

The New-Scale Platform applies the same behavioral analytics to this new digital workforce. It monitors behavior for each AI agent—learning which APIs it calls and its typical data throughput—and detects any risky deviations. This extends threat detection to your entire workforce, both human and digital.

## Secure Your Entire Workforce

Defending against an attacker with valid credentials requires a shift in mindset from watching the perimeter to understanding behavior within it. By implementing these six methods with the automated, analytics-driven approach of the New-Scale Platform, your security operations team can finally see the threats that legacy tools miss and protect your organization from the inside out.

## 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 →**