Abnormal Authentication

Detect, identify, and respond to risky authentication behavior before it becomes a breach

Authentication anomalies—logins at unusual times, from unexpected locations, or using atypical methods—are often early indicators of insider threats or compromised accounts. While occasional anomalies can be legitimate, patterns of abnormal activity demand attention. The challenge is scale: Organizations process thousands of authentication events daily, making manual detection impossible. Complicating matters further, lost or stolen credentials are still valid credentials, which makes it difficult for traditional rule-based detection engines to recognize when an authentication attempt is actually malicious. Because rule sets evaluate events only in the moment, without understanding the user's historical behavior, they can't reliably distinguish harmless deviations from true threats.

The New-Scale Security Operations Platform addresses this problem by applying behavioral analytics, automation, and prescriptive workflows to accelerate threat detection, investigation, and response (TDIR). Unlike correlation rules, which evaluate activity only at a single point in time, New-Scale Analytics uses user and entity behavior analytics (UEBA) to build a behavioral history for every user and device, which allows the platform to automatically create timelines of activity and detect meaningful deviations in authentication behavior. With this context, analysts can detect risky logins faster, investigate with a clear picture of what's changed, and respond decisively, reducing risk and minimizing disruption.

From Detection to Response: How It Works

Detection starts by establishing a baseline of normal behavior for every user and device. When a login occurs from an unfamiliar country or at an unusual time, the system flags it for review. Risk scoring adds context by correlating anomalies with peer behavior, helping analysts prioritize the most critical threats.

Investigation is streamlined through automated timelines that assemble authentication events, contextual data, and alerts into clear, chronological views. Analysts can drill down into suspicious patterns without writing complex queries, and guided checklists ensure investigations are thorough and consistent.

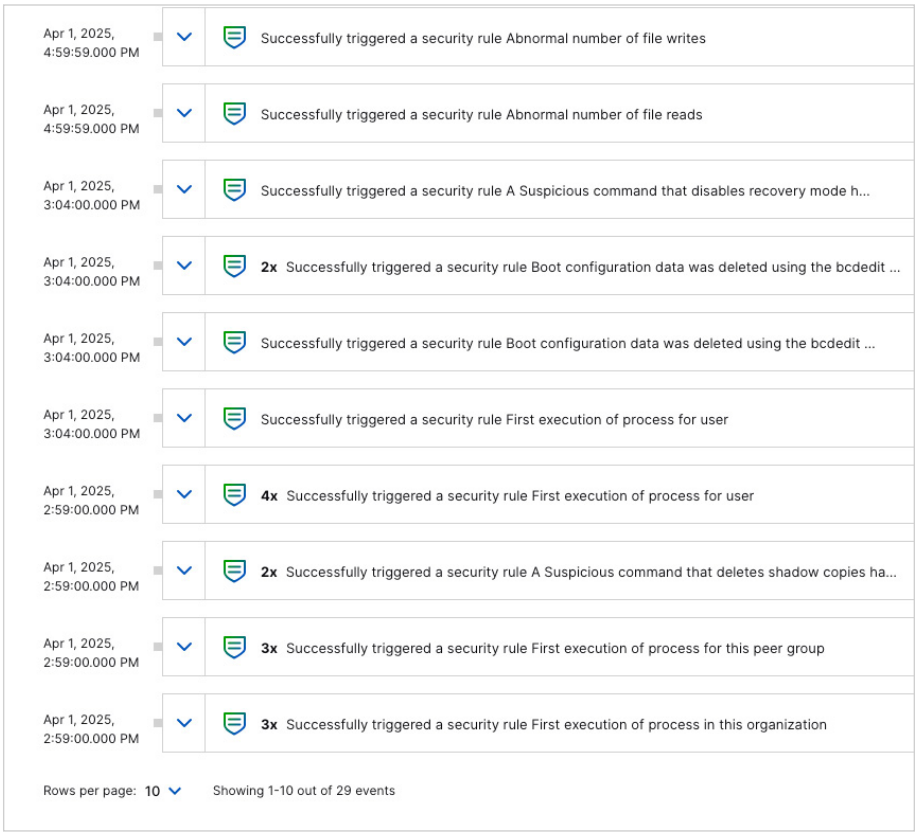

Figure 1. Investigation Timeline displaying abnormal authentication-related events and security rule triggers for streamlined analysis.

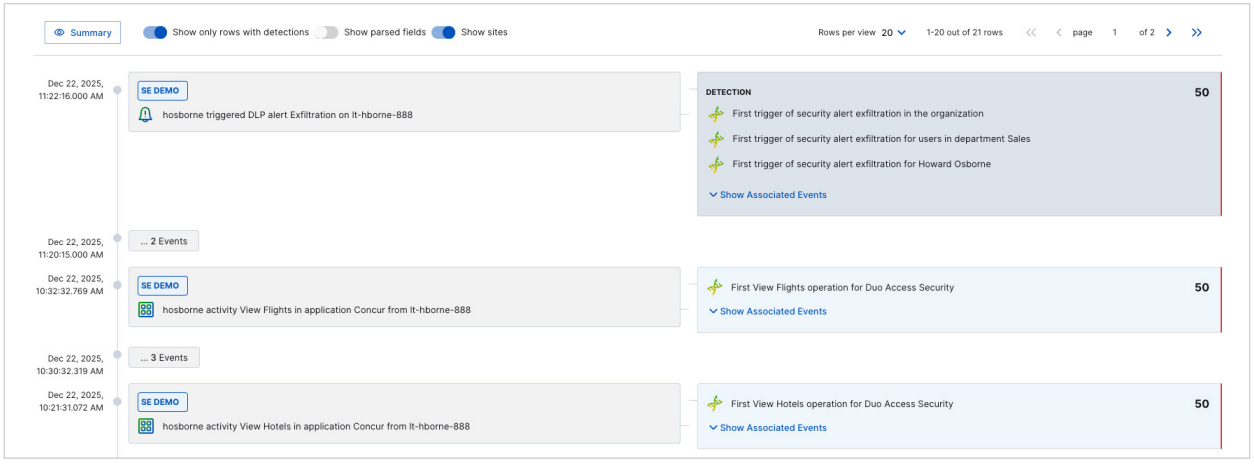

Figure 2. Threat Timeline consolidating detections and correlated events for a user exhibiting suspicious authentication behavior.

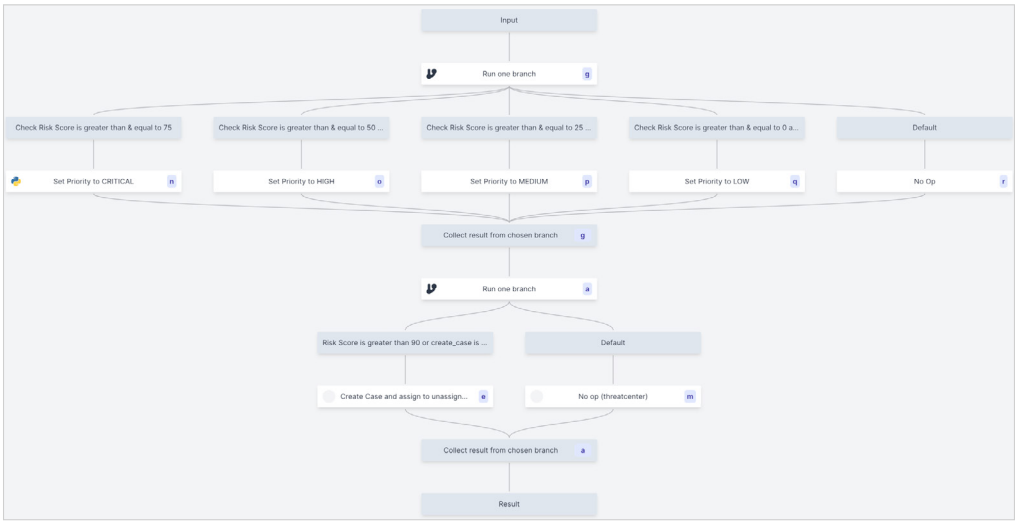

Figure 3. Automated playbook workflow for abnormal authentication response, dynamically adjusting priorities and creating cases based on risk scores.

Response is equally efficient. Automated playbooks coordinate actions across the security stack—suspending accounts, enforcing multifactor authentication (MFA), or rotating credentials—without manual effort. Prebuilt integrations with identity, endpoint, and SIEM tools reduce mean time to respond (MTTR) and improve analyst productivity

Extending Protection to AI Agents

As organizations adopt AI-driven workflows, the attack surface expands. Agent Behavior Analytics (ABA) applies the same behavioral modeling to AI agents. AI Usage Security applies governance policies to prevent unauthorized access and data exposure. These capabilities strengthen abnormal authentication detection without overshadowing the core mission: protecting identities and stopping breaches.

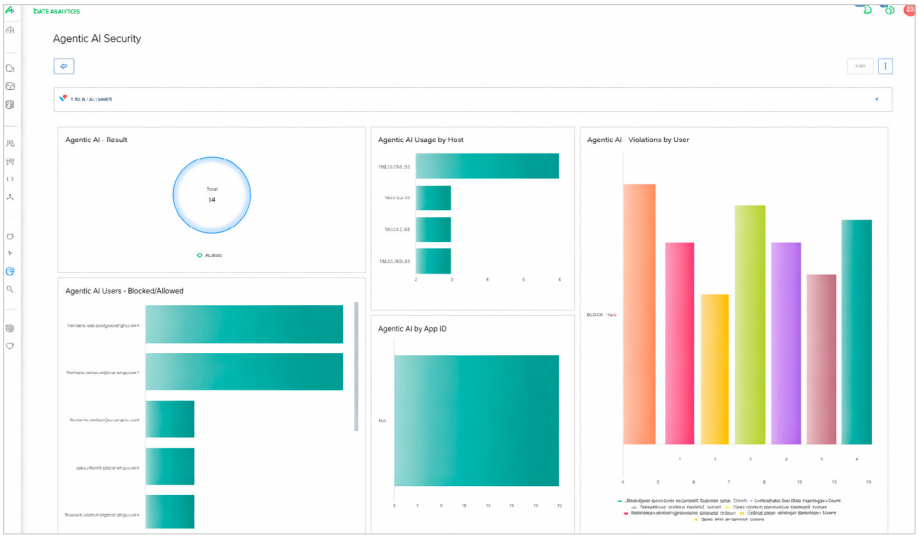

Figure 4. Agentic AI dashboard showing violations by user, blocked actions, and usage patterns for AI agents.

Use Case Content

Key Data Sources

- Operating system logs (UNIX, Linux, macOS, Windows)
- VPN activity
- Physical access logs
- Web activity
- AI agent activity logs

Behavioral Detections

- Abnormal login location or time
- Excessive distance between logins
- First-time foreign access
- Unauthorized API calls by AI agents

MITRE ATT&CK Technique Coverage for Privilege Escalation

Technique ID	Technique Name
T1078	Valid Accounts
T1133	External Remote Services

Incident Response Checklist

- ✓ Contact user or manager
- ✓ Add user or asset to a watchlist
- ✓ Rotate credentials/reset password
- ✓ Expire password
- ✓ Remove user from a group
- ✓ Send MFA push
- ✓ Suspend user

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 →