Privilege Escalation

Detect, Investigate, and Respond to Privilege Escalation Attacks Faster With Exabeam

What Is Privilege Escalation?

Privilege escalation occurs when an attacker gains elevated permissions or unauthorized access to privileged accounts or systems. This can involve using valid credentials, switching to higher-access accounts, or exploiting vulnerabilities to increase permissions.

Why Privilege Escalation Matters

Privilege escalation is one of the most common tactics in cyberattacks, enabling adversaries to gain unauthorized access to high-value assets. According to the Verizon Data Breach Investigations Report, credential misuse and privilege abuse are major contributors to breaches. If undetected, attackers can exfiltrate data, disrupt operations, or install backdoors for persistent access.

How Exabeam Solves It

The New-Scale Security Operations Platform helps security teams detect, investigate, and respond to privilege escalation attacks quickly and accurately. Our approach combines behavioral analytics, risk-based prioritization, and automated workflows to reduce investigation time and improve outcomes.

Detection

Legacy tools often fail to catch privilege escalation when attackers use valid credentials, making these incidents hard to distinguish from normal user activity. Exabeam solves this by ingesting critical data sources, such as authentication logs, VPN access, and endpoint security, and applying behavioral analytics to detect anomalies like credential enumeration or first-time access to sensitive hosts.

Detection extends beyond user behavior. Agent Behavior Analytics (ABA) provides visibility into endpoint-level actions, such as AI usage by analyzing logs to identify risky interactions with AI tools that might signal misuse or attempts to access sensitive data during a privilege escalation attempt. Risk scoring and MITRE ATT&CK®-based detection rules ensure analysts can quickly identify and prioritize the highest-risk threats

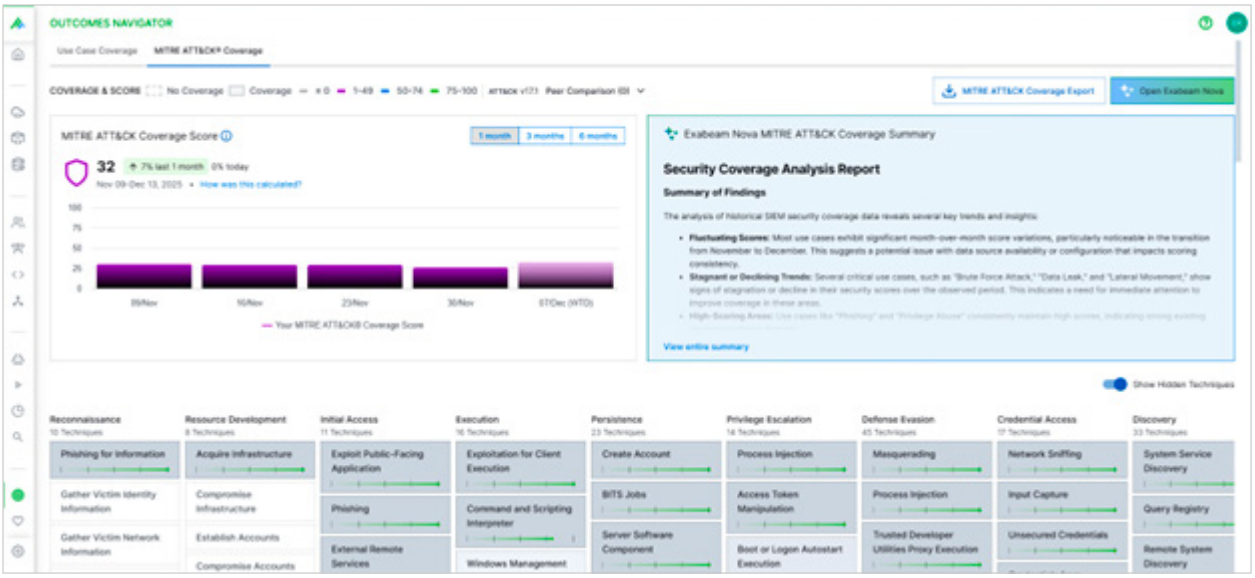

Figure 1. Outcomes Navigator highlights privilege escalation alerts with ATT&CK coverage.

Investigation

Visibility is key to stopping privilege escalation before it spreads. Exabeam provides complete context through Threat Timelines, which automatically assemble correlated events into a clear attack narrative. Analysts can drill into raw logs, pivot across related users and assets using Investigation Timelines, and follow the recommended Next Steps in the Exabeam Nova Investigation Summary to ensure their investigation is complete. This approach answers critical questions like "What does this user have access to?" and "Are they a privileged user?" without manual queries.

Response

Coordinating response across multiple tools can take hours, but Exabeam automates this process with standards-based playbooks that orchestrate actions across your security stack. Analysts can suspend accounts, enforce multifactor authentication (MFA), or reset credentials with a single click. These customizable workflows greatly reduce mean time to respond (MTTR) and improve operational efficiency, allowing teams to contain threats before they escalate further.

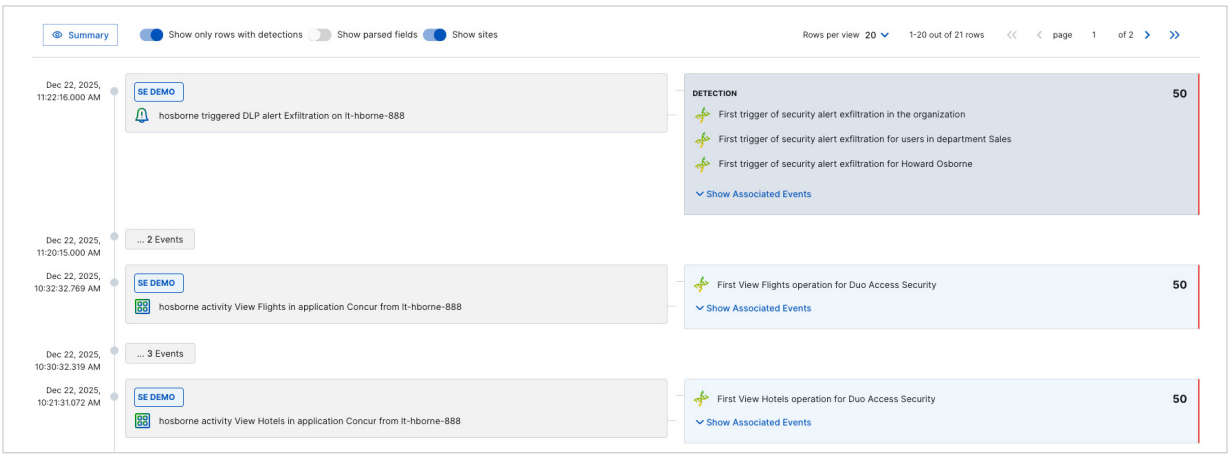

Figure 2. Threat Timelines provide a complete view of correlated events, accelerating investigations and reducing manual efforts.

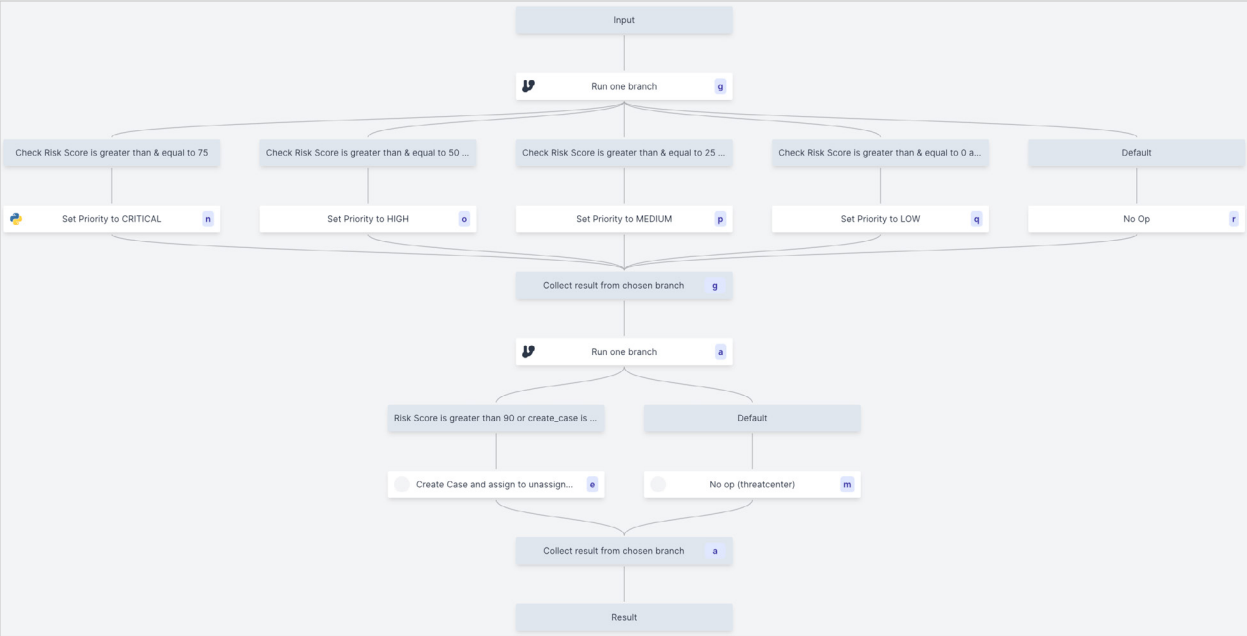

Figure 3. Exabeam playbooks automate containment and remediation for privilege escalation incidents.

Customer Outcomes

- Reduce MTTR by up to 60%.
- Detect privilege escalation in minutes, not hours.
- Improve analyst efficiency with automation and guided workflows.

Use Case Content

Key Data Sources

- Authentication and Access Management
- Remote Access
- VPN/Zero Trust Network Access
- Endpoint Security (EPP/EDR)
- Privileged Access Management (PAM)
- Agent Behavior Analytics
- Agent Activity Logs

Behavioral Detections

- Credential switching to privileged or executive account
- Execution of credential enumeration tools
- Detection of artifacts used by MITRE APT groups
- Exploiting vulnerabilities for privilege escalation
- Processes bypassing user access controls

MITRE ATT&CK Technique Coverage for Privilege Escalation

Technique ID	Technique Name
TA004	Privilege Escalation
T1003	OS Credential Dumping
T1033	System Owner/User Discovery
T1053	Scheduled Task/Job
T1055	Process Injection
T1057	Process Discovery
T1068	Exploitation for Privilege Escalation
T1078	Valid Accounts
T1087	Account Discovery
T1134	Access Token Manipulation
T1548	Abuse Elevation Control Mechanism

Table 1. Exabeam provides prebuilt detection for 1 1 ATT&CK techniques tied to privilege escalation.

Incident Response Checklist

- ✓ Contact user or manager
- ✓ Add user or asset to a watchlist
- ✓ Block or suspend accounts
- ✓ Rotate credentials/reset password
- ✓ Prompt for MFA reauthentication
- ✓ Isolate systems
- ✓ Clear user session
- ✓ Gather additional context
- ✓ Kill malicious processes

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.