Audit Tampering

Detect, investigate, and respond to audit log manipulation with complete visibility.

Audit tampering occurs when a user alters or deletes audit logs to hide activity. When logs are incomplete or manipulated, security teams lose the ability to confirm what occurred, assess intent, or determine incident scope. Actions like clearing Windows Event logs, disabling event tracing, or changing configurations can obscure key signals. Traditional tools can't reliably detect this behavior or rebuild what happened afterward.

The New-Scale Security Operations Platform creates a dependable, user-centric activity record as events occur. Even if underlying logs are modified or removed in the future, the timeline still reflects the activity captured at the time.

How Exabeam Stops Audit Tampering

Exabeam helps security operations teams identify and respond to audit log manipulation by providing full-workflow coverage across threat detection, investigation, and response (TDIR). The New-Scale Platform automatically assembles alerts, activity, and context into a complete user-centric record in real time. Because the platform correlates signals as they stream in, analysts retain an accurate picture of what happened. Traditional tools that reconstruct timelines only from stored log files may lose critical detail when logs are changed or deleted.

Behavioral analytics and dynamic risk scoring reveal suspicious actions like unexpected log access, event tracing changes, or attempts to clear audit logs. The addition of Agent Behavior Analytics (ABA) extends this visibility to both human users and agentic processes that can modify audit configurations.

Threat Timelines present activity in clear, readable language, removing the need for complex queries. Threat Center brings detections and related events together so analysts can quickly review what happened and why it is significant. Investigation checklists and automated response playbooks guide teams through next steps, helping them reduce time spent coordinating actions across tools and move more quickly through containment.

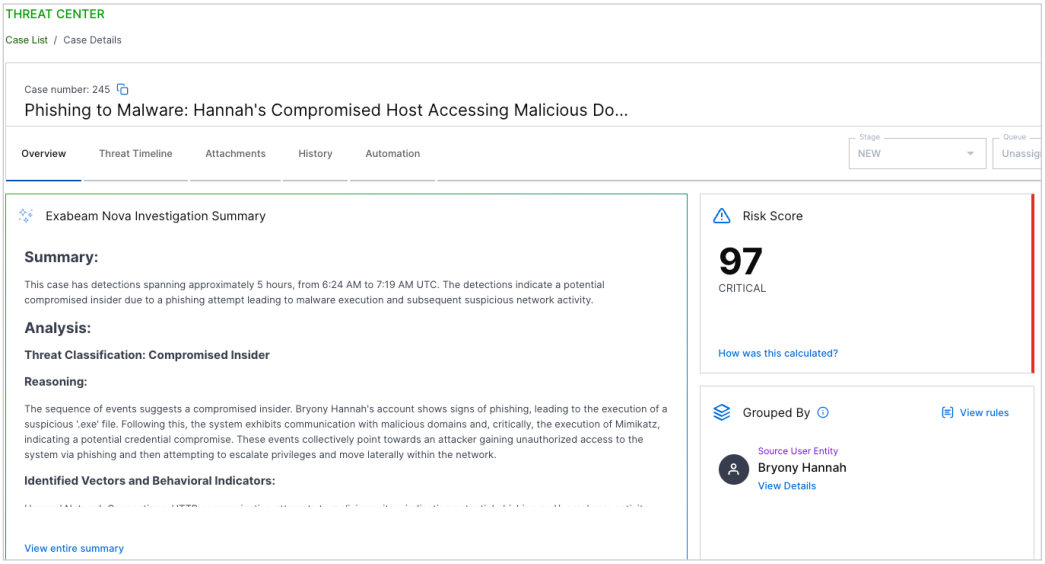

Figure 1.

Threat Center highlights suspicious activity and risk signals associated with potential misuse, giving analysts a clear starting point for investigating audit-related anomalies.

Detect Abnormal Activity Tied to Audit Log Manipulation

Challenge

Privileged users can clear or modify logs in ways that appear routine, leaving teams unable to detect early signs of malicious behavior.

Solution

Exabeam detects unusual behavior through user and entity behavior analytics (UEBA), which compares activity against a user's history and peer groups, and Agent Behavior Analytics (ABA) to identify anomalous process execution, configuration changes, or attempts to disable logging.

Examples of signals include:

- First-time interaction with audit logs
- Attempts to change or disable event tracing
- Scripted log clearing
- Suspicious system utility execution
- First time access to storage systems

Customer Outcome

Teams identify suspicious activity earlier, reduce missed indicators, and focus attention on users whose patterns meaningfully diverge from normal operations.

Reconstruct a Reliable Story of What Happened

Challenge

Once logs are missing or modified, manual reconstruction is slow and incomplete.

Solution

Exabeam automatically builds a clear activity timeline using:

- **Automated timelines** that correlate data from multiple systems
- **Patented host-IP-user mapping** to connect activity to a specific user
- **Exabeam Nova Investigation Agent and Analyst Assistant Agent** to summarize events, highlight anomalies, and recommend next steps
- **Threat Center**, which provides a unified investigation workspace and automatically groups related detections, events, and risk signals

Together, these capabilities give analysts a full narrative even when evidence is incomplete. Analysts can search across raw logs, associated events, and related behaviors without writing complex queries.

Customer Outcome

Analysts reduce time spent piecing together activity and can quickly understand what happened before, during, and after the tampering event.

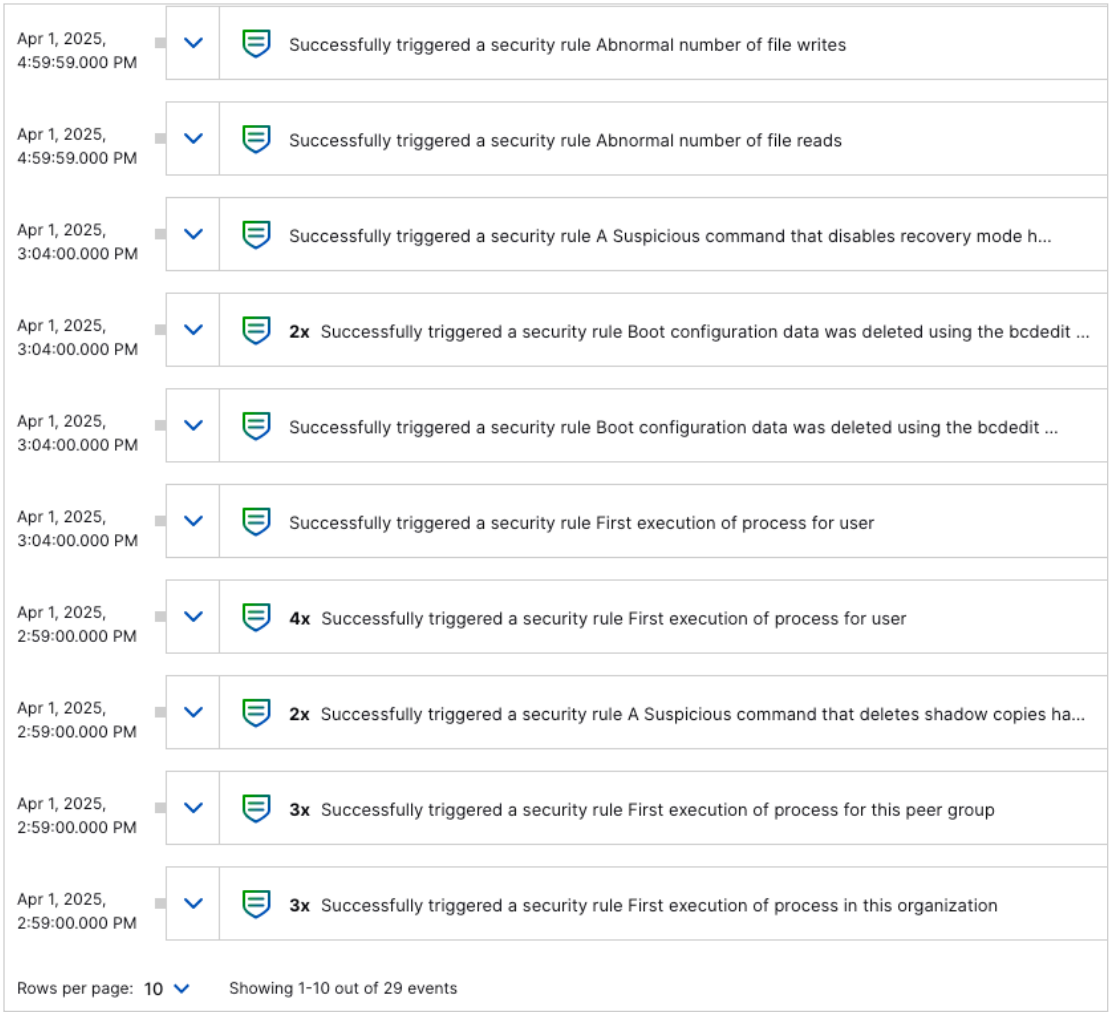

Figure 2.

The Investigation Timeline displays event-level activity around audit log manipulation, helping analysts review what happened before, during, and after suspicious changes.

Respond at Speed Across Tools and Teams

Challenge

Coordinating containment across tools slows response and leaves windows of risk.

Solution

With the New-Scale Platform:

- Automated playbooks handle suspension, password resets, watchlist updates, and notifications.
- Analysts can route critical steps through security orchestration, automation, and response (SOAR), ensuring consistent actions across the environment.
- Outcomes Navigator helps leadership understand the organization's coverage of audit tampering and similar use cases, including gaps and recommended improvements.

Customer Outcome

Faster containment and reduced manual effort help close windows where insiders might escalate or repeat harmful activity.

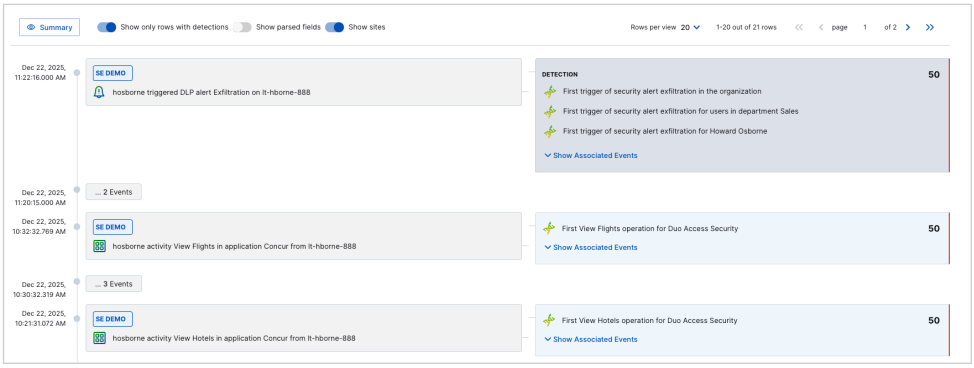

Figure 3.

The Threat Timeline groups related detections and activity into a clear sequence, helping analysts understand the broader story behind audit log manipulation.

Use Case Content

Key Data Sources

- Operating system logs (UNIX, Linux, macOS, Windows)
- Endpoint activity
- File access
- Process execution

Detection Rules

- Audit log tampering
- Event tracing disabled
- Logging configuration changed

MITRE ATT&CK Technique Coverage for Audit Tampering

Technique ID	Technique Name
T1070	Indicator Removal on Host
T1562	Impair Defenses
T1213	Data From Information Repositories

Incident Response Checklist

- → **Contact user or manager**
- → **Add user or asset to a watchlist**
- → **Block, suspend, or restrict users**
- → **Rotate credentials/reset password**
- → **Require MFA reauthentication**

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam™

Learn more at
www.exabeam.com →