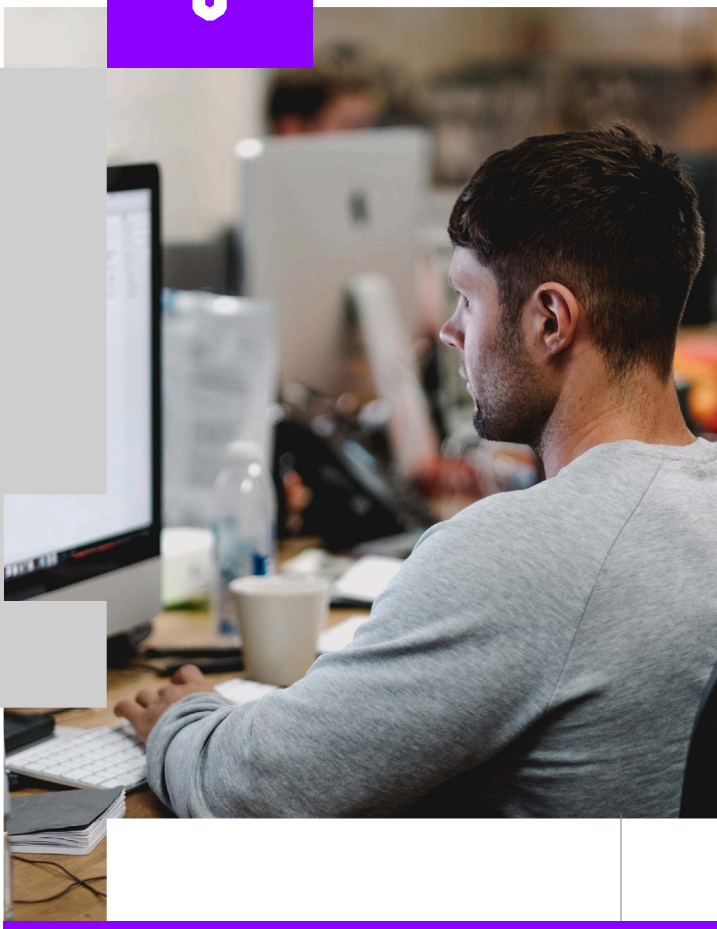
exabeam

Solution Brief

Audit Tampering

Audit tampering is when a user tampers with audit logs in an effort to destroy an incriminating audit trail and evade detection.



Threat detection and investigation falters when the trail runs cold

Organizations increasingly rely on audit logs as a detailed record of user and system activity. Many threat detection tools analyze these logs to track user behavior, identify anomalies indicative of user compromise, or support incident investigation. However, malicious insiders aware of organizational practices may circumvent detection by clearing or tampering with audit logs.

Without a reliable system of record, security and insider threat teams using traditional security tools are unable to identify or investigate these types of threats. Further, these tools lack the ability to leverage context to identify the intent behind user activity.

> ...Without protected and complete logging records [organizations] are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible[1].

[1] Center for Internet Security, Maintenance, Monitoring and Analysis of Audit Logs

Exabeam and audit tampering

Exabeam helps security and insider threat teams outsmart users engaging in audit tampering with the support of automation and use case content across the full analyst workflow, from detection to response. Exabeam automatically assembles all alerts, activity and contextual data and analyzes it from the point of view of the user to create a comprehensive, reliable record of user activity, if the underlying logs have been altered or deleted. Our behavior analytics develops a baseline of normal activity for every user and device and flags anomalous behavior indicating malicious behavior in a user's risk score. Timeline events parsed into plain, clear language allow security and insider threat teams to easily investigate activity details with minimal technical expertise and without repeatedly querying multiple systems. A guided investigation checklist and automated response playbooks enable analysts to quickly and effectively remediate incidents and reduce mean time to respond (MTTR).

Key capabilities

Challenge 1: collection and detection

Legacy security tools are unable to identify when users are abusing privileged access to logs or logs on critical assets when activity appears legitimate.

Solution

Exabeam ingests and analyzes key data sources to detect unusual activity such as accessing an audit log for the first time or disabling event tracing. Exabeam behavioral models put anomalous activity like modifying, clearing or otherwise obfuscating event logging into the context of historic behavior for an individual or their peers. With user labels such as "Suspected Leavers," Exabeam allows analysts to quickly identify when an insider is behaving maliciously before an incident occurs.

Benefit

Strengthen security posture against malicious insiders by using behavior analytics to attribute anomalous audit tampering activity back to a user.

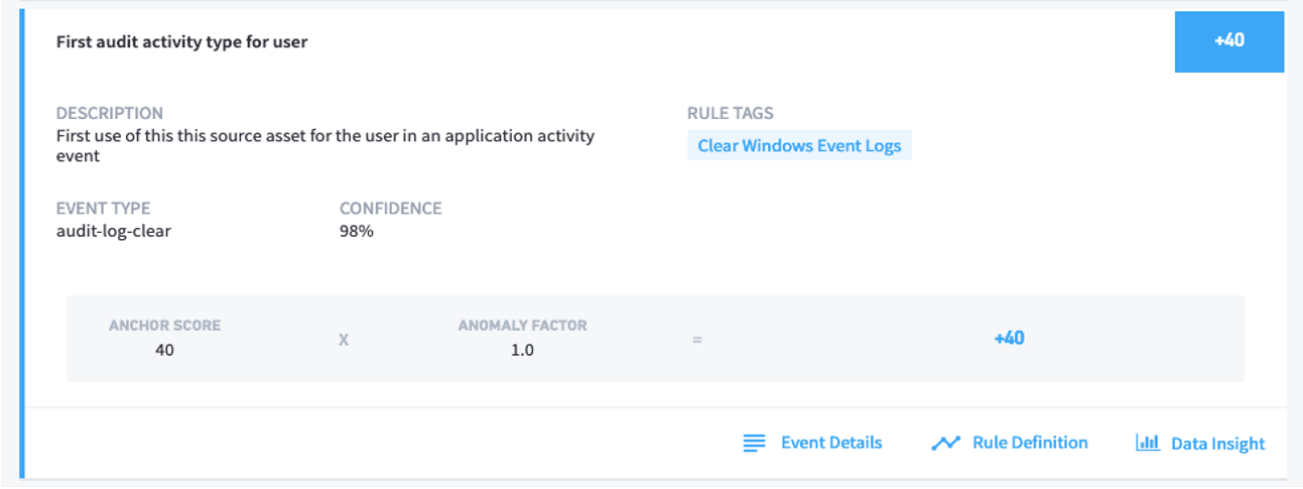


Figure 1 - Anomalous activity, such as a user's first time performing audit activity, specifically, clearing Windows Event logs, adds to a user's risk score to indicate malicious behavior.

Challenge 2: visibility and investigation

Security and insider threat teams are unable to rely on audit logs for their investigations when malicious insiders have manipulated or deleted incriminating evidence.

Solution

Exabeam provides a reliable source of truth for analysts for their investigations. Our Smart Timelines automatically capture and assemble all activity data, including clearing audit logs or running processes for obfuscation. Patented host-IP-user-mapping attributes this activity back to a user, presented as clear, readable events, all without an analyst needing to write a single query.

Analysts can investigate further with Exabeam Threat Hunter to find all audit tampering, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our audit tampering checklist to ensure their investigation is thorough and complete.

Benefit

Exabeam enables reliable and streamlined investigations, regardless if underlying evidence has been tampered with or destroyed. With Exabeam, even non-technical analysts can answer key questions like "What activity did a user perform before clearing the log?"

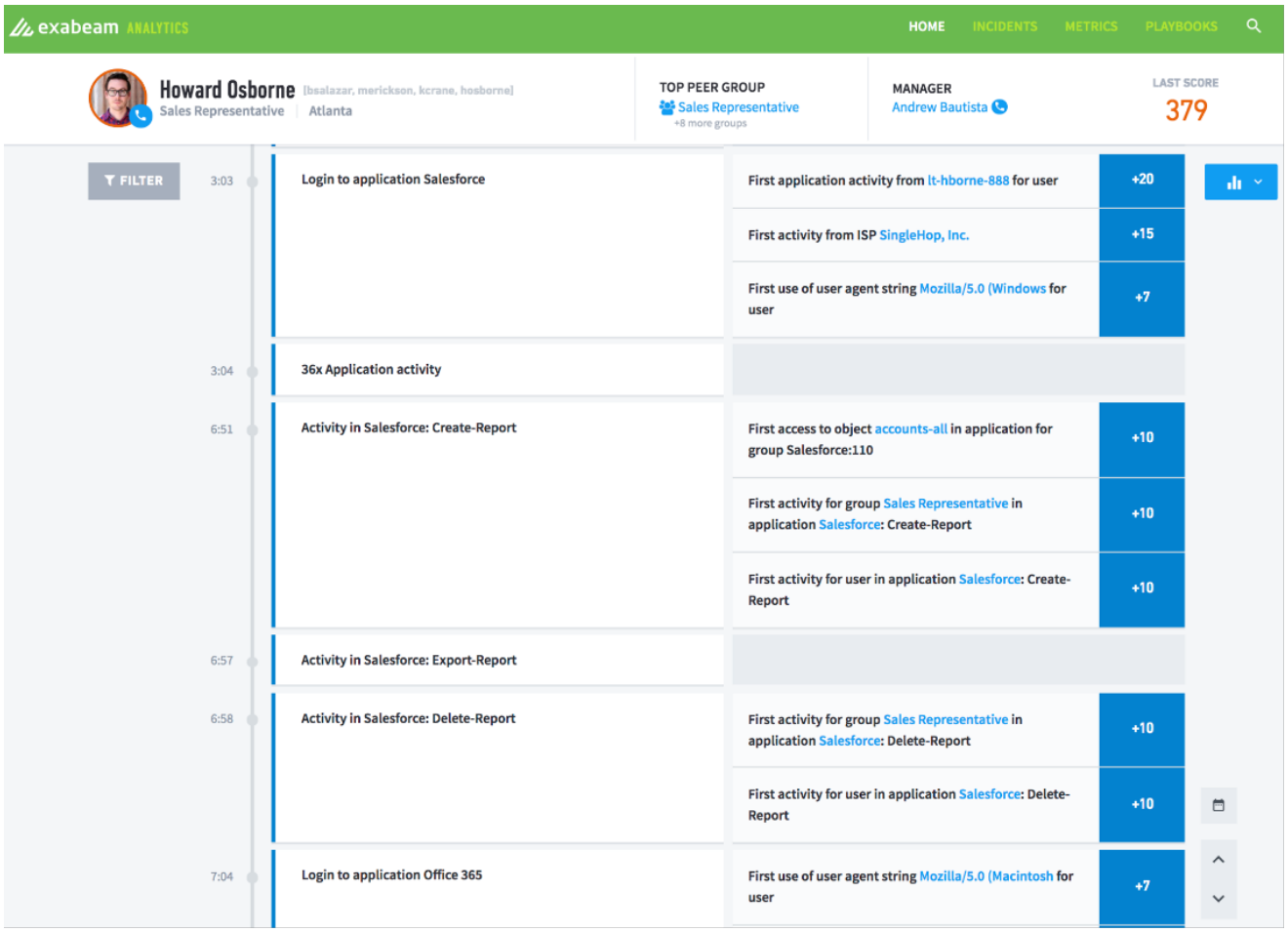


Figure 2 - Smart Timelines automatically correlate activity across multiple tools and assemble events attributed back to a user, drastically reducing the time needed to collect and analyze evidence.

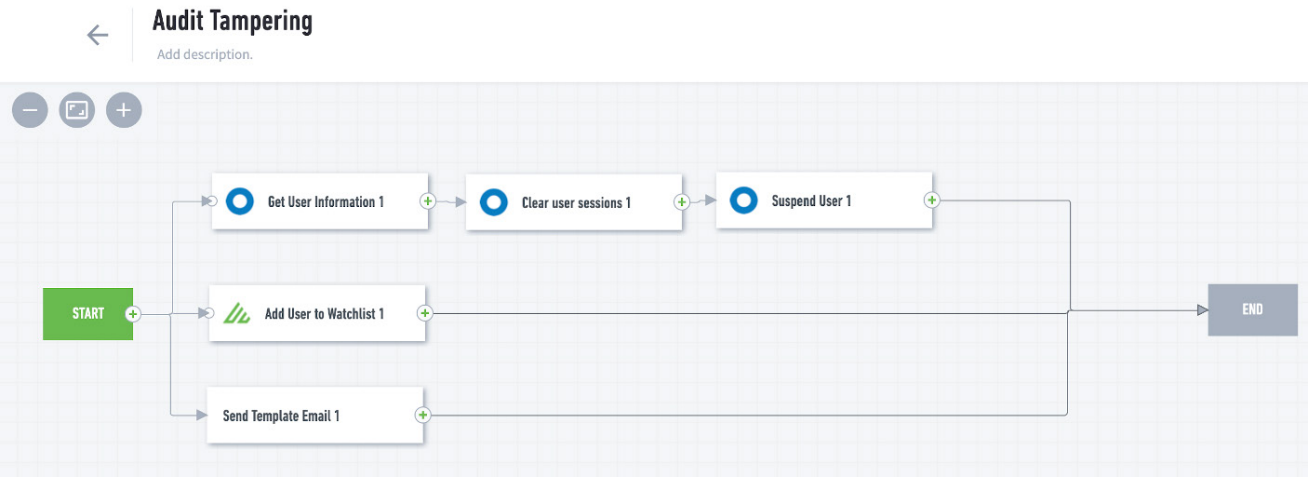


Figure 3 - This audit tampering abuse playbook obtains contextual information about the malicious insider, clears their session, suspends the user, and adds them to a watchlist before sending an email notification.

Challenge 3: response

Security and insider threat teams responding to audit tampering incidents spend hours or days coordinating response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to audit tampering incidents across your security stack. Pre-built integrations and customizable actions enable analysts to automate playbooks to respond to audit tampering, such as suspending a user or resetting a password.

Benefit

Enhance analyst productivity and decrease MTTR with security orchestration automation and response (SOAR) powered playbooks.

Use case content

To provide coverage for audit tampering abuse, Exabeam identified key data sources and has built content for collection, detection, investigation and response.

Key data sources

- Endpoint security (EPP/EDR)
- File access and activity
- Operating system logs (e.g. UNIX/Linux/ OSX/Windows)
- Process execution and activity

Key detection rule types

- Audit log tampering

MITRE technique coverage

- T1070: Indicator removal on host
- T1562: Impair defenses
- T1213: Data from information repositories

Incident checklist

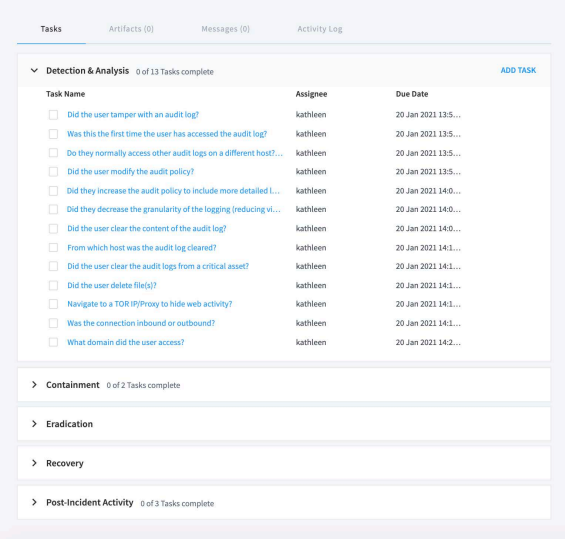


Figure 4 - The audit tampering incident checklist prompts analysts to answer specific investigation questions and take containment actions.

Response actions

- Contact user/manager/HR department via email
- Add user to a watchlist
- Block, suspend, or impose restrictions on users involved in the incident
- Rotate credentials/reset password
- Prompting for re-authentication via 2-factor/ multi-factor authentication

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Management Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users, and malicious adversaries, minimize false positives and make security success the norm. For more information, visit **www.exabeam.com**.

To learn more about how Exabeam can help you visit exabeam.com today.

exabeam