How Exabeam Solves Eight Compromised Insider Use Cases

A compromised insider is one of the most difficult security threats to detect and manage. This threat can be a trusted human user whose credentials have been stolen, or it can involve an adversary's unauthorized use of a tool like an AI agent or service account. Armed with valid credentials—from a user's password to an AI agent's API key—an attacker can operate as a trusted insider to perform reconnaissance within a network.

This guide explains how Exabeam identifies and mitigates eight common compromised insider use cases:

1. Compromised Credentials
2. Lateral Movement
3. Privilege Escalation
4. Privileged Activity
5. Evasion
6. Account Manipulation
7. Data Exfiltration
8. Compromised AI Agents

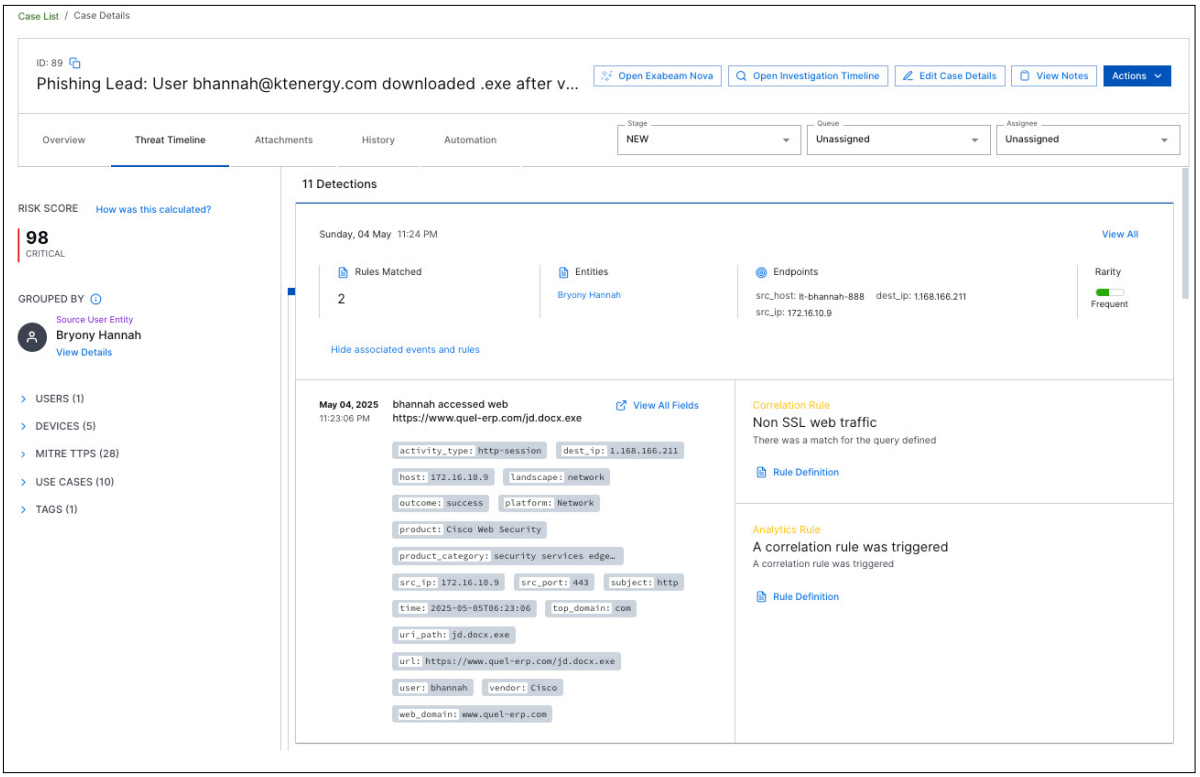

Figure 1.

Pinpointing the source of malware is critical. This automated timeline immediately links a phishing lead to a user downloading a malicious .exe file, giving analysts a clear starting point for incident response without needing to manually trace logs.

Defining the Risk

The risk from a compromised insider has two components. The first is protection: How secure are your accounts and assets? This involves the systematic security controls every enterprise should have. The other component is threat detection, investigation, and response (TDIR): How can you identify a compromised insider, what are they doing, and how can you respond before damage occurs? Relying solely on rules makes it impossible to distinguish between the legitimate actions of an authorized user and the malicious actions of an attacker using the same account.

1 Compromised Credentials

Definition

Credential compromise occurs when an attacker obtains a legitimate user's credentials—knowingly or unknowingly—to access corporate resources.

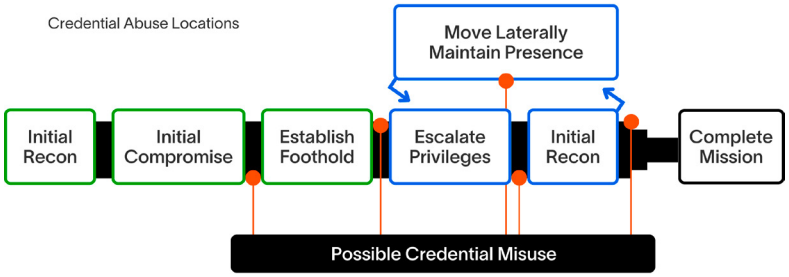

Figure 2.

Exabeam applies behavioral analytics to baseline user activity and automatically detects credential compromise when it sees anomalies like a first-time login from an unusual location.

Problem

Attackers use several methods to acquire legitimate credentials:

- **Phishing and spear-phishing**
  An attacker sends a message with a malicious link that tricks the user into entering their password. Spear-phishing targets high-value, privileged accounts.
- **Password spraying**
  An attacker attempts to authenticate with a known username and a list of common, unsafe passwords.
- **Credential stuffing**
  An attacker uses username and password combinations stolen from other data breaches.
- **Keyloggers**
  An attacker installs malicious software that logs keystrokes, including Bluetooth-based methods, to capture usernames and passwords.
- **Brute force**
  An attacker attempts to authenticate by iterating through a list of potential passwords, such as dictionary words or hashed values.
- **Social engineering**
  An attacker uses trickery, bribery, or coercion to persuade an individual to share their network credentials.

Solution

Exabeam mitigates threats from compromised credentials by applying industry-leading user and entity behavior analytics (UEBA). New-Scale Analytics provides UEBA capabilities that establish a behavioral baseline for every user and asset, then assigns risk scores to abnormal events and highlights deviations in a clear, actionable timeline. Exabeam combines risk scores from anomaly-based models and prebuilt correlation rules into a single session risk score. When the score crosses a defined threshold, it creates a notable session for analysts. The result is better coverage and less alert fatigue than relying on static correlation rules alone.

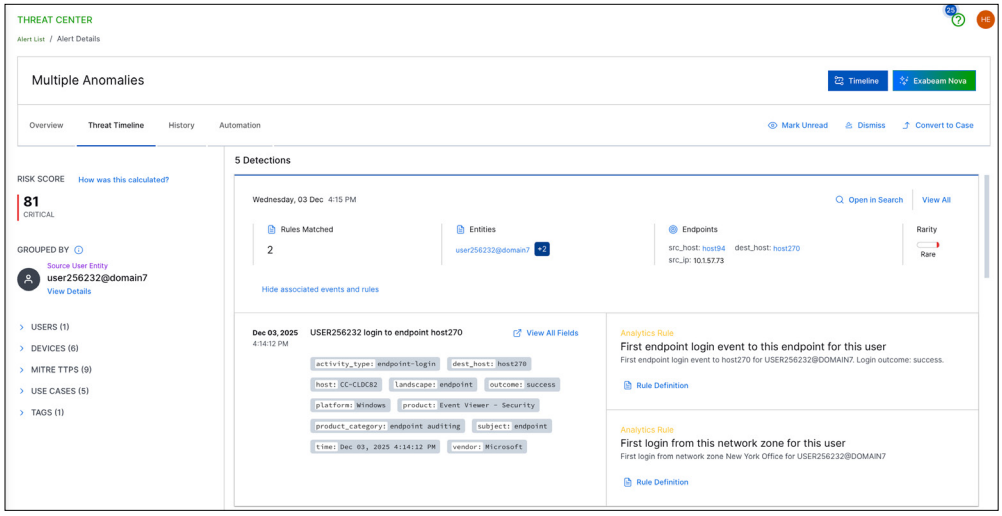

Figure 3.

By stitching together events from multiple sources, the Exabeam timeline provides a clear narrative of a phishing attack. Analysts can instantly see how an initial suspicious link led directly to a malware infection on the user's workstation, saving critical investigation time.

2 Lateral Movement

Definition

Lateral movement occurs when an attacker compromises an asset and then moves internally ("east-to-west") to other devices on the network. This is often the next step after a credential compromise. While not always necessary, compromising additional assets helps attackers reach systems that allow them to achieve their objectives.

Problem

Common methods for lateral movement include:

- **Port scans**
  Attackers use tools like Nmap to find vulnerable ports to expand their footprint or find other accounts to compromise.
- **Remote desktop access**
  With valid credentials, an attacker can gain full access to a computer's graphical user interface and move freely.
- **Windows attacks**
  Attackers abuse protocols like Windows Server Message Block (SMB) with commands such as PsExec and scheduled tasks to move across the network.
- **Pass-the-Hash (PtH)**
  An attacker steals a user's hashed password from a compromised machine and uses it to authenticate to other network resources. This allows the attacker to move laterally without ever needing to know the user's actual plaintext password.
- **Pass-the-Ticket (PtT)**
  An attacker steals a valid, previously issued Kerberos ticket and uses it on a new device to access resources as a legitimate user.
- **Golden ticket**
  A more sophisticated attack where an adversary compromises a domain controller to steal the Kerberos Ticket Granting Ticket (TGT) service account hash. They use this to forge an authentication ticket that grants them administrative access to any user or resource in the entire domain.

Solution

Exabeam products, including New-Scale SIEM, LogRhythm SIEM, New-Scale Analytics, and LogRhythm Intelligence, include prebuilt rules to highlight lateral movement activity. These rules provide risk scores for prioritization, watchlists for high-risk users, and lists of compromised assets. This improves analyst efficiency, enabling investigations that take minutes instead of hours and reducing the risk of lateral movement on your network.

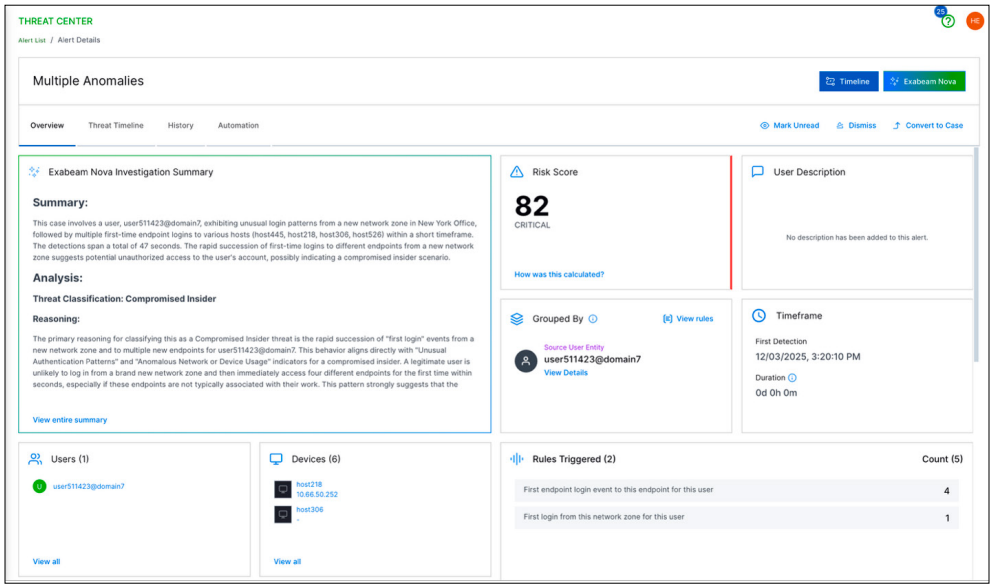

Figure 4.

The Exabeam Nova Investigation Summary provides a plain-language narrative of an attack. Here, it automatically identifies lateral movement by highlighting the rapid succession of "first login" events to multiple new endpoints, explaining that this is a strong indicator of a compromised insider moving through the network.

3 Privilege Escalation

Definition

Privilege escalation is a technique attackers use to gain higher-level permissions or unauthorized access. An attacker might switch to an account with greater access or increase permissions on a compromised user or system.

Problem

Attackers use several methods to escalate privileges:

- **Horizontal escalation**
  An attacker uses compromised credentials to move between devices, searching for a system or privileged account to take over, often targeting domain administrator or service accounts.
- **Discovery**
  Abnormal account switching can indicate horizontal or vertical escalation, as can unusual password retrieval activity.
- **Credential dumping**
  An attacker dumps a Windows Security Accounts Manager (SAM) database to obtain user hashes, then uses those hashes in pass-the-hash attacks to gain privileges.
- **Vertical escalation**
  An attacker bypasses account controls to increase permissions, often using post-exploitation tools to modify group policies, exploit weak service permissions, or bypass user account control settings.
- **Weak security**
  An attacker finds and modifies configuration files or executable binaries with weak permissions to escalate privileges.

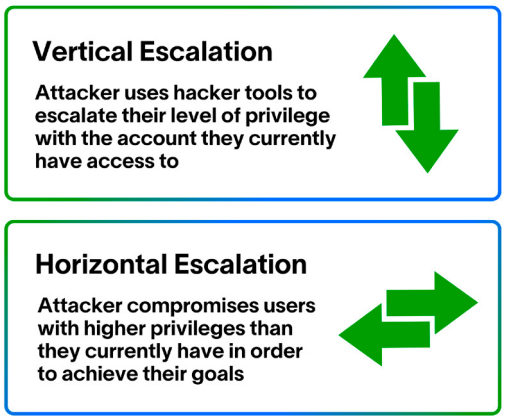

Figure 5.

Whether an attacker is moving between accounts (horizontal escalation) or gaining higher permissions (vertical escalation), Exabeam UEBA detects this abnormal behavior by comparing it against a user's established baseline of normal activity.

Solution

Exabeam highlights privilege escalation when an account or entity displays abnormal behavior. The New-Scale Security Operations Platform, New-Scale Analytics, and LogRhythm SIEM with LogRhythm Intelligence apply a baseline of what systems a user typically accesses. A compromised account used to escalate privileges triggers prebuilt rules based on the user's behavioral models, alerting analysts to the threat.

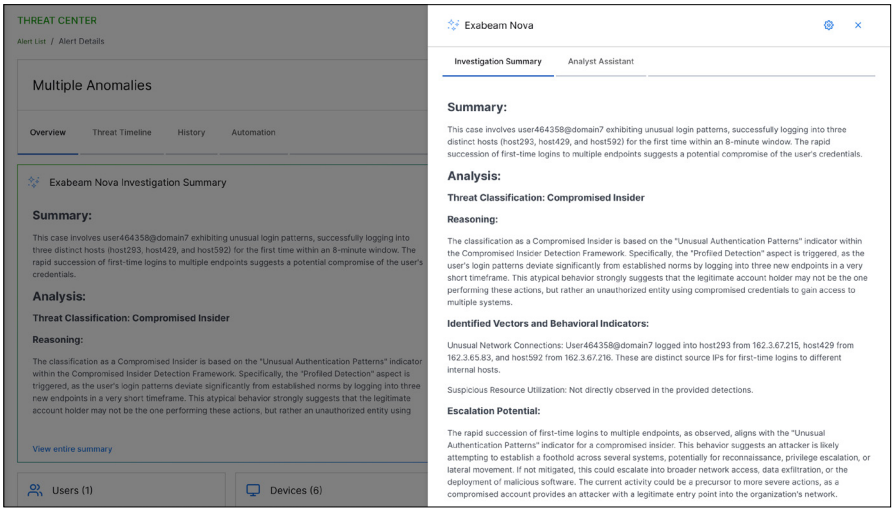

Figure 6.

The Exabeam Nova Investigation Summary explains not just what happened, but what could happen next. While the initial threat detected was an attacker moving between multiple hosts, the Escalation Potential analysis correctly warns that this behavior is often a direct precursor to privilege escalation, as the attacker will likely now attempt to find and elevate privileges on these newly accessed machines.

4 Privileged Activity

Definition

Privileged activity refers to actions performed by entities with elevated permissions. Attackers who compromise these entities can gain broad access to sensitive systems and data.

Problem

Because privileged entities are authorized to make significant changes, it is difficult to distinguish between legitimate administrative tasks and malicious actions. An attacker's goal is to compromise these entities to gain control of the environment. The primary targets include:

- **Privileged users**
  Attackers specifically target the credentials of users who have elevated access to sensitive information, such as system administrators and executives. A compromise of one of these accounts can serve as a skeleton key to the kingdom.
- **Privileged accounts**
  Service accounts, which are used by applications to interact with the operating system, are a prime target. Because they are often shared, not tied to a single human user, and may not have regular password resets, their credentials are valuable for an attacker seeking persistent, under-the-radar access
- **Privileged assets**
  These are the critical systems that house sensitive data, such as customer information, intellectual property, or financial records. Domain Controllers are a particularly high-value privileged asset, as they control user authentication for an entire domain. However, they are notoriously difficult to monitor with legacy tools due to the high volume of log data they generate.

Solution

New-Scale Fusion and New-Scale Analytics establish a baseline of normal behavior for every user and key asset in your environment. The platform models the specific applications, servers, and data each privileged user typically accesses, and at what times. For privileged service accounts, Exabeam provides deep monitoring to give security teams a clear view of all activity. When a compromised user account is used to access a new critical server, perform an unusual type of privileged action, or access data outside its normal scope, Exabeam flags the behavior and escalates its risk score. This allows security teams to focus on genuine threats without blocking legitimate administrative work.

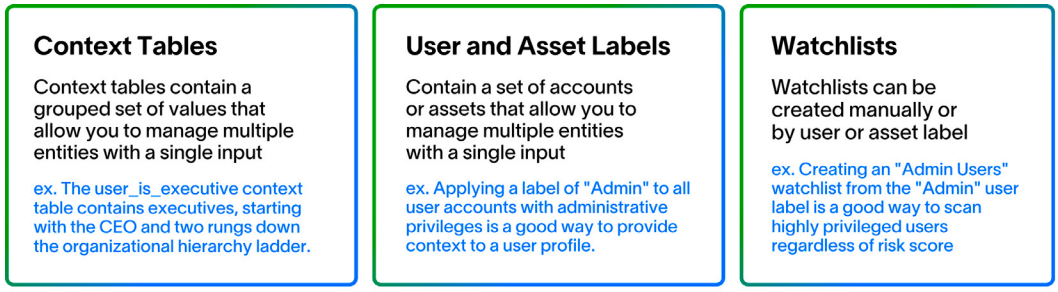

Figure 7.

Exabeam uses features like labels, dynamic watchlists, and context tables to enrich privileged accounts and assets. This allows security teams to apply higher risk scoring to any activity from these critical entities, ensuring immediate prioritization.

5 Evasion

Definition

Evasion techniques are actions an attacker takes to avoid detection by security tools. By covering their tracks, attackers can remain in a network for extended periods to find and exfiltrate valuable data.

Problem

According to the IBM Cost of a Data Breach Report 2025, the average time to identify and contain a data breach is now 282 days. This figure highlights the persistent challenge of detection and the effectiveness of adversarial tradecraft. Evasion techniques are designed to extend this timeline, making it harder for security teams to detect and respond. Common methods include:

- **Disabling security tools and logs:** Using scripts and commands (for example, via PowerShell) to disable security software, manipulate critical processes like Sysmon, and erase evidence by clearing audit logs or command histories
- **Obfuscating commands and traffic:** Hiding malicious activity by passing encoded commands (such as Base64) or anonymizing their location and traffic with networks like Tor
- **Using attacker toolkits:** Repurposing legitimate IT tools or deploying specialized malware to manipulate trusted processes and bypass standard security controls
- **File and timestamp manipulation:** Deleting files that contain evidence of an intrusion or altering file timestamps ("timestomping") to make malicious files appear to be part of the benign operating system

Solution

Exabeam detects evasion techniques by correlating activity from multiple data sources. While an attacker might successfully clear logs on one machine, Exabeam can still identify the intrusion by analyzing corresponding network traffic, authentication logs from a domain controller, or alerts from other security tools. The platform includes prebuilt rules to detect specific evasion tactics, such as a user attempting to stop a security service or a suspicious clearing of audit logs. By stitching these events together in an automated timeline, Exabeam exposes the full attack sequence.

[1] IBM. "Cost of a Data Breach Report 2025." IBM.com, 30 Jul. 2025, https://www.ibm.com/reports/data-breach.

6 Account Manipulation

Definition

Account manipulation involves modifying existing accounts or creating new ones to maintain access or escalate privileges.

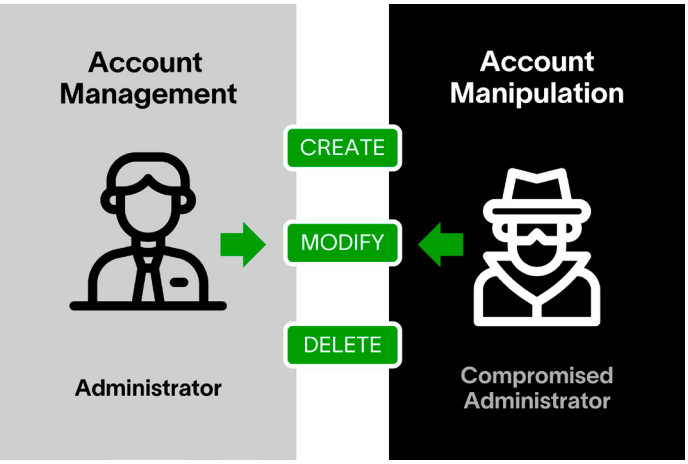

Figure 8.

Automated timelines stitch together all user activities, making it easy for an analyst to see when a legitimate process like account creation is being abused by an attacker.

Problem

Once inside a network, an attacker can manipulate accounts to establish persistence. Common tactics include:

- Adding a compromised user account to a privileged group, such as Domain Admins or Enterprise Admins
- Creating a new local administrator account on a compromised machine
- Modifying group membership and permissions to grant a low-level account new privileges
- Assigning excessive roles or permissions to a compromised user in a cloud environment

Because these actions involve making changes to directory services and other systems in a way that can mimic the work of a legitimate administrator, they often go undetected. Without a behavioral baseline of who normally performs these actions, an attacker can create accounts and assign permissions without raising any alarms.

Solution

Exabeam automatically detects and alerts on suspicious account manipulation. The platform baselines all account creation and modification activities, understanding which users (like IT or HR personnel) normally perform these actions. When a non-administrative user suddenly creates a new admin account or adds a user to a sensitive group, Exabeam flags the activity as abnormal. This allows security teams to quickly identify and investigate unauthorized attempts to establish persistence or escalate privileges that would otherwise appear legitimate.

7 Data Exfiltration

Definition

Data exfiltration is the unauthorized transfer of data from a network. This is often the final stage of an attack, where the adversary steals the sensitive information they were targeting.

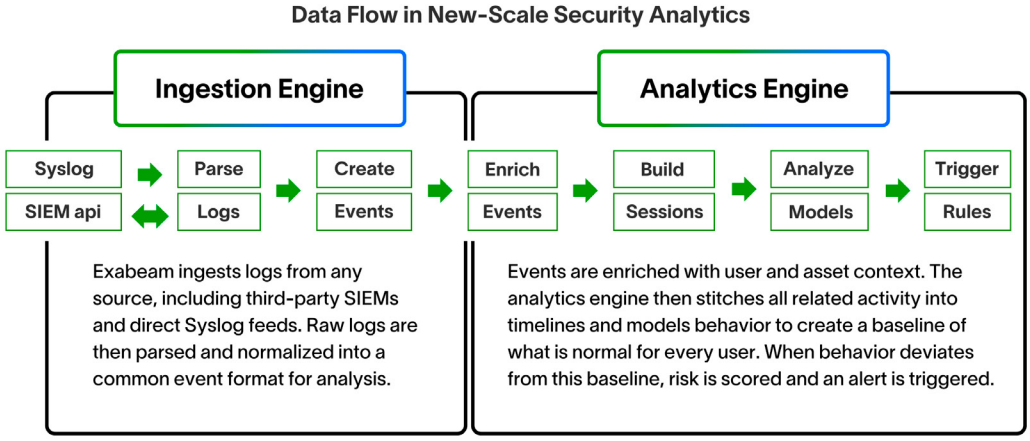

Figure 9.

The Exabeam two-stage analytics architecture is key to detecting sophisticated threats. By separating data ingestion from behavioral analysis, the platform builds a reliable baseline for every user, making it possible to automatically spot deviations that indicate a threat, such as data exfiltration.

Problem

Data can be exfiltrated through numerous channels, making it a significant challenge to monitor and prevent. Methods include:

- **Cloud storage:** Uploading data to personal accounts on services like Google Drive, Dropbox, or OneDrive
- **Email:** Sending sensitive files to external email addresses
- **Large file transfers:** Using protocols like FTP or SFTP to move large volumes of data out of the network
- **Low-and-slow:** Siphoning small amounts of data over a long period to avoid triggering volume-based alerts
- **Physical media:** Copying data to a USB drive or other external storage device

Solution

Exabeam detects data exfiltration by monitoring for unusual data movement and access patterns. The platform's behavioral analytics can identify when a user accesses a sensitive database for the first time and then uploads a large amount of data to an external website. It can also detect when data is touched in a sequence that matches a known exfiltration pattern. By baselining normal data access and transfer behavior for each user, Exabeam can distinguish between routine work and a high-risk data theft event.

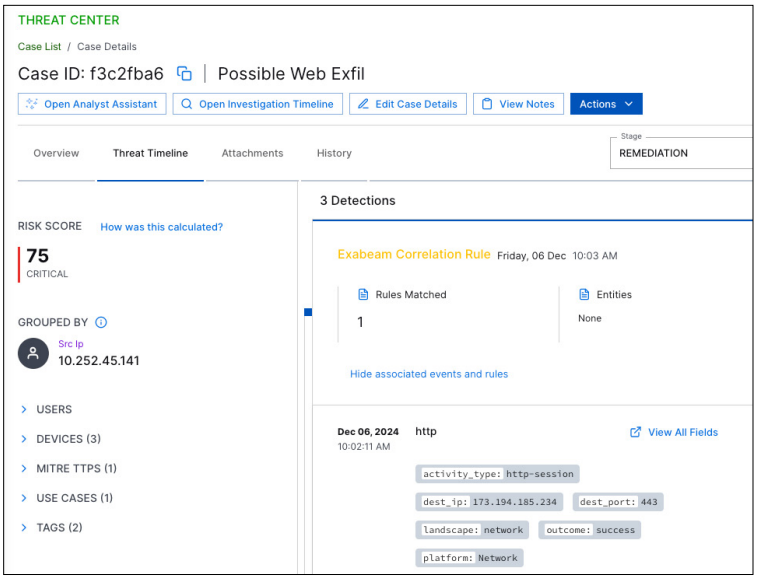

Figure 10.

Exabeam detects potential data exfiltration by analyzing network traffic. This automated Threat Timeline highlights a high-risk case, triggered by a rule analyzing http-session activity to a suspicious external IP address.

8 Compromised AI Agents

Definition

A compromised AI agent refers to the unauthorized use or manipulation of non-human entities like AI-powered applications, service accounts, or API keys. As organizations increasingly adopt AI, these non-human entities are becoming a prime target for attackers.

Problem

AI agents and other non-human entities often have broad permissions to access and process data, yet their activity is not always scrutinized as closely as that of human users. An attacker can:

- Steal API keys or tokens to impersonate an AI agent and access sensitive systems.
- Use attacks like prompt injection to manipulate an AI model's inputs, tricking it into bypassing safety controls, generating malicious outputs, or leaking confidential information.
- Poison the data used to train an AI model, corrupting its behavior for future use.

Solution

Exabeam addresses this emerging threat by applying its deep visibility and analytics capabilities to non-human entities.

1. **Provide deep visibility into agent activity:** By ingesting data from platforms where agents are built and run (such as Google Cloud), Exabeam provides a centralized platform to monitor and correlate all AI agent activity. What APIs does it call? How often does it run? All of this activity is collected and organized for clear analysis.
2. **Enable rapid investigation:** This centralized visibility gives security teams a powerful forensic tool. Analysts can proactively hunt for suspicious patterns in agent behavior or use the rich data to instantly investigate activity that has been flagged by other systems. This closes a critical visibility gap that exists in most security programs.
3. **Respond with context:** With a complete, correlated timeline of an agent's actions, security teams can respond decisively. If a compromise is suspected, analysts have the clear evidence needed to quickly disable the suspicious agent or API key, containing the threat before significant damage can occur. This extends threat management to your entire workforce—both human and digital.

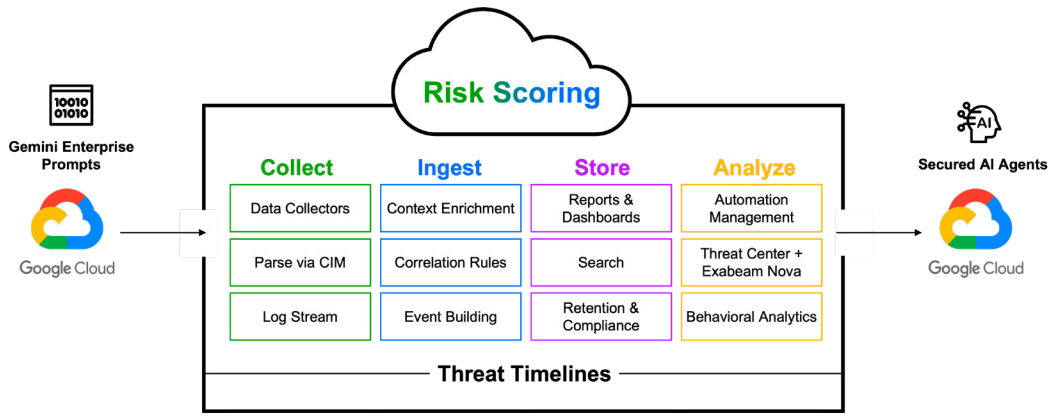

Figure 10.

To monitor AI agents, Exabeam integrates directly with Google Cloud. As this diagram illustrates, alerts and prompts are collected and processed by the New-Scale Platform, which correlates this activity to provide a comprehensive security layer for your AI workforce.

Conclusion

Relying solely on correlation rules makes it impossible to swiftly and accurately detect a compromised insider. Manually collating security logs is time-consuming and requires an advanced approach to distinguish between legitimate user activity and an attack. The New-Scale Platform and LogRhythm SIEM with LogRhythm Intelligence provide these advanced analytics to detect threats often missed by other tools. By providing automated timelines for investigation, Exabeam improves the productivity of security teams and reduces response times from days to minutes.

Learn more about how Exabeam behavioral analytics can help.

Powering the Modern SOC With the New-Scale Security Operations Platform

The New-Scale Platform is engineered for the demands of modern security operations, integrating cloud-scale security log management, industry-leading behavioral analytics, and an automated investigation experience. Its purpose-built, cloud-native architecture delivers the speed and scale required to detect complex threats across today's hybrid environments.

The platform helps security operations teams achieve excellence by focusing response on risk-based priorities, automating triage and investigation, and applying behavioral analytics across billions of events. This empowers teams to work more effectively while controlling budgets with predictable, cloud-based economics.

Whether you're looking to replace a legacy SIEM or complement an existing SIEM or data lake with market-leading UEBA, the New-Scale Platform helps your security operations succeed. The platform capabilities are delivered through our New-Scale Fusion packages, which are composed of the following offerings:

- **New-Scale SIEM:** Cloud-native SIEM
- **New-Scale Analytics:** Hybrid analytics and automation for your existing SIEM or data lake
- **LogRhythm SIEM:** Self-hosted SIEM
- **LogRhythm Intelligence:** Hybrid New-Scale Analytics delivered within LogRhythm SIEM

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 →