exabeam

Solution Brief

Privilege Abuse

Detect and respond to unusual behavior by privileged accounts as well as privileged activity by non-privileged users

Key to the kingdom

Privileged accounts such as admins or executives often have access to sensitive information or critical assets, making them rife for abuse. Insiders may use these privileges to enact regulatory, operational, financial, and reputational harm to an organization.

Legacy security tools struggle to integrate contextual data to identify activity associated with privileged accounts and assets. This means malicious behavior such as account manipulation or abusing service or executive accounts may go undetected.

Exabeam and Privilege Abuse

Exabeam helps security and insider threat teams outsmart users abusing their access to privileged accounts or assets with the support of automation and use case content across the full analyst workflow, from detection to response. Instead of forcing analysts to connect the dots across data silos, Exabeam automatically assembles alerts, activity and contextual data and analyzes it from the point of view of the user, reducing the likelihood of missing a threat from the inside. 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.

> The explosion of cloud services has driven proliferation of privileged accounts and credentials to a state that, for most organizations, is unmanageable without processes and tools.
>
> **Gartner Magic Quadrant for Privileged Access Management, 2020**

[1]2020 Global Cost of Insider Threats; Ponemon Institute

Machine-created timelines allow security and insider threat teams to easily investigate event 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
Without the ability to automatically identify privileged accounts and critical assets, traditional security tools struggle to detect malicious insiders abusing access.

Solution
Exabeam ingests context from directory services platforms and other systems to identify and classify privileged accounts such as service accounts or executives as well as critical assets that hold sensitive information. Identifying privileged accounts allows the system to model privileged users and assets and add additional risk to anomalous behaviors associated with them. In addition, with user context Exabeam can identify when a non-privileged user commits malicious activity such as granting themselves greater access privilege or admin permissions, account creation or deletion, or accesses executive resources like a mailbox or critical assets.

Benefit
Strengthen your security posture with the ability to detect abnormal malicious activity by privileged accounts or assets.

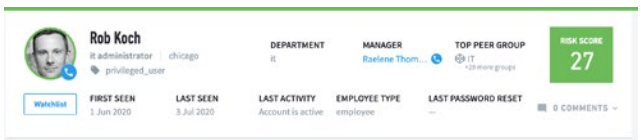

Figure 1 - Exabeam provides context within a user or asset profile to help an analyst quickly identify privileged users, such as IT administrator Rob Koch.

Challenge 2: visibility and investigation
Security teams lack visibility and continuous monitoring capabilities for privileged accounts or assets.

Solution
Exabeam leverages context to create watchlists and continuously monitor privileged users and assets for changes in their risk score that may indicate suspicious activity. From a watchlist, an analyst can gain further visibility into privilege abuse by navigating to a user or entity timeline. Timelines leverage patented host-IP-user mapping to automatically aggregate security alerts, events and a user or entity's activity, anomalous and normal, and assemble them into clear, readable events, all without an analyst needing to write a single query. For further investigation, Exabeam provides a behavior-based threat hunting tool capable of honing in on the abnormal activity associated with privilege abuse, such as non-executive users accessing executive assets. At each step of the way, analysts can reference our privilege abuse checklist to ensure their investigation is thorough and complete.

Benefit
Quickly and easily identify privilege abuse across your entire security stack and improve investigation quality and speed by enabling analysts to quickly answer key questions like "Did a new or non-privileged user access an executive asset?"

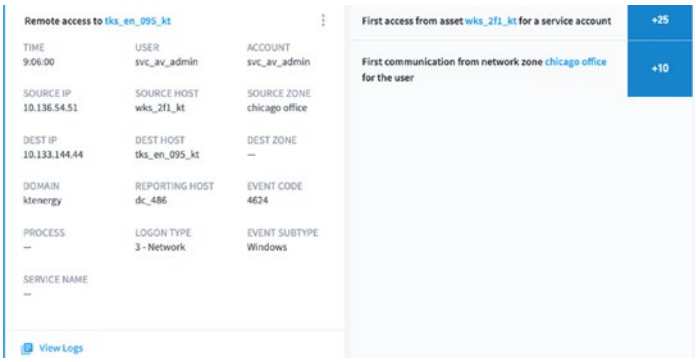

Figure 2 - This Smart Timeline event shows anomalous access from asset wks_2f1_kt by a privileged service account.

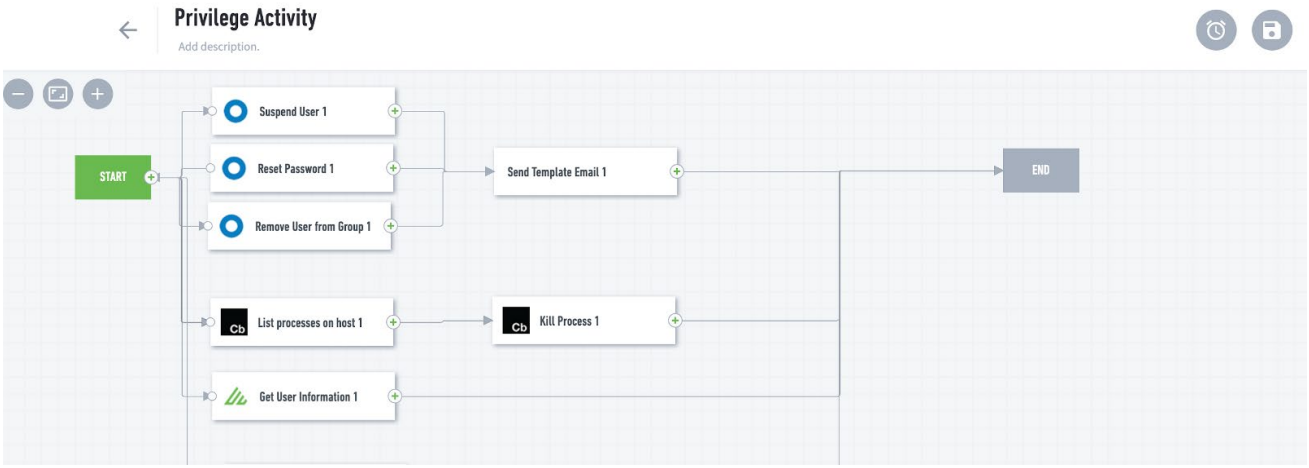

Figure 3 - This privilege abuse playbook characterizes and escalates the incident, adds the compromised user to a watchlist while disabling their account, and resets their password.

Challenge 3: response
Security teams responding to privilege abuse investigations spend hours or days coordinating response across multiple security tools.

Solution
Exabeam orchestrates response to privilege abuse incidents across your security stack using response actions and playbooks. Pre-packaged integrations with hundreds of popular security and IT products and customizable actions enable security teams to automate playbooks to respond to privilege abuse incidents, such as suspending a user or resetting a password.

Benefit
Improve operational efficiency and decrease MTTR with security orchestration automation and response (SOAR) powered playbooks.

Use case content

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

Key data sources
- Asset logon and access
- Authentication and access management
- VPN and zero trust network access
- Application activity
- Privileged access management and activity
- Remote logon activity

Key detection rule types
- Account manipulation
- Executive account abuse
- Service account abuse

MITRE technique coverage
- T1078: Valid Accounts
- T1098: Account Manipulation
- TA0009: Privilege Abuse

Incident checklist

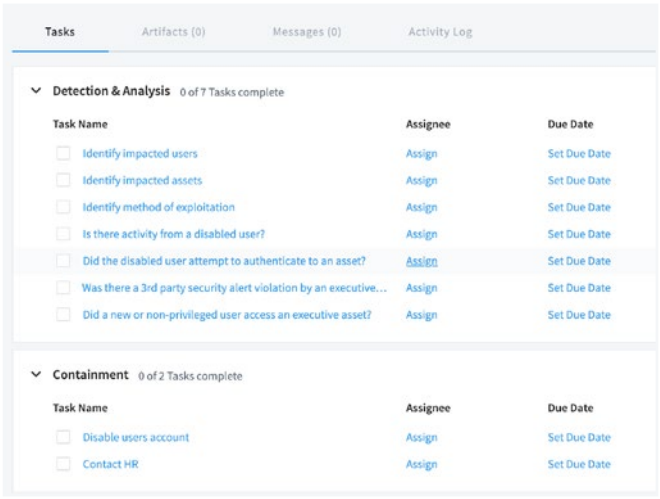

Figure 4 - The privilege abuse incident checklist prompts analysts to answer specific investigation questions and take containment actions.

Response actions

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

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**.

exabeam

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