exabeam

Solution Brief

Privileged Activity

Detect and respond to unusual behavior by privileged accounts, critical assets, and privileged processes

A top target for bad actors

Privileged accounts pose one of the largest security risks for organizations. According to a Ponemon report, 14% of incidents involved the abuse of privileged users' access, costing organizations, on average, $2.79 million annually[1]. Compared to standard users, privileged accounts like admin or executive accounts have extensive control over access to sensitive data and IT systems, such as domain controllers or Active Directory.

Having unrestricted access to critical IT systems and other valuable assets makes privileged accounts a top target for attackers. If an attacker can compromise a privileged account, the attacker gains access that could be used to disrupt corporate operations, or exfiltrate large amounts of sensitive data.

> Bad guys are going after privileged users. Privileged users have access to your sensitive data, and they have access to the keys to your kingdom. And that's what you really want to protect.
>
> **David Madhi**
> Gartner Security Risk Management Summit, 2020

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

Exabeam and privileged activity

Exabeam helps security teams outsmart adversaries compromising privileged accounts with the support of automation and pre-packaged use case content across the full analyst workflow, from detection to response. First, we prescribe the data sources to collect and analyze which provide the greatest visibility over privileged activity. Our user and entity behavior analytics (UEBA) then develops a baseline of normal activity for every privileged account and asset in an organization. As an adversary begins to move within a network, abnormal activity is identified using pre-packaged detection rules and models, including MITRE techniques associated with privileged activity. This activity is flagged and added to the user or entity's risk score. Risk scores and watchlists help security teams focus on the riskiest incidents, while Exabeam Smart Timelines automatically display the full attack chain to dramatically accelerate incident investigations. 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 assets, traditional security tools struggle to detect attacks involving privileged activity.

Solution

Exabeam ingests context from directory services platforms and other systems to identify and classify privileged accounts such as domain controllers, admins, and executives. Through behavioral modeling of users and assets, Exabeam automatically baselines normal activity, assigns a risk score to suspicious events, and intelligently prioritizes them for further evaluation. Identifying privileged accounts, such as an executive or IT admin, allows the system to model privileged users and assets and add additional risk to anomalous behaviors associated with them.

Privileged accounts are also associated with assets, providing the context needed to identify whether the asset is a laptop or server, and if it belongs to an executive. Understanding context enables analysts to identify privileged activity, like a non-executive user accessing an executive asset or a user who has been given mailbox permissions for an executive user. Since privileged users pose a great risk to an organization, Exabeam enables analysts to discern whether the privileged account or asset is behaving suspiciously and detect privileged activity.

Benefit

Strengthen your security posture with the ability to detect adversary activity on privileged accounts or assets.

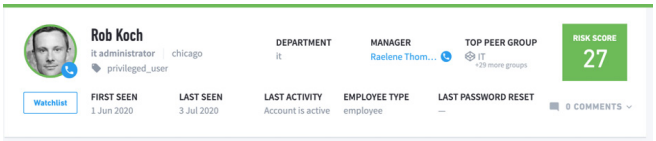

Figure 1 – Exabeam provides context within a user or asset profile. From the user's profile, an analyst can quickly understand if the asset or user has privileged access, in this case, Rob Koch has been tagged as a privileged user.

Challenge 2: Visibility and Investigation

Security teams do not have visibility into privileged activity, or the ability to continuously monitor privileged users for privileged activity.

Solution

Exabeam gives complete visibility into privileged activity attacks by aggregating security alerts and events together into a user or entity timeline. Timelines leverage patented host-IP-user mapping to automatically assemble a user or entity's activity, anomalous and normal, into clear, readable events, all without an analyst needing to write a single query (figure 2). Analysts can access the timelines from a curated watchlist that centralizes privileged users and assets for continuous monitoring. For further investigation, Exabeam provides a behavior-based threat hunting tool capable of honing in on the abnormal activity associated with privilege activity threats, for example, an analyst can search for non-executive users accessing executive assets or disabled users showing activity. Each step of the way, analysts can reference our privileged activity checklist to ensure their investigation is thorough and complete.

Benefit

Quickly and easily identify leading indicators of compromise across your entire security stack and improve investigation quality and speed by enabling analysts to quickly answer key questions like "Is there activity from a disabled user" or "Did a new or non-privileged user access an executive asset?"

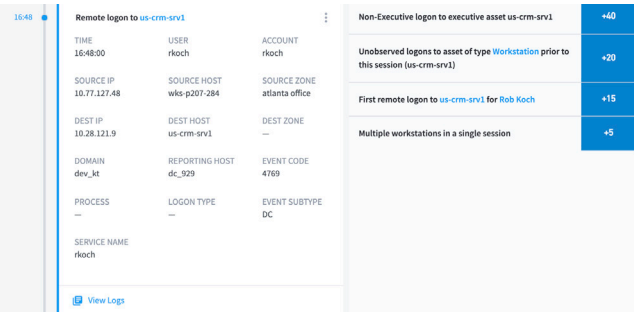

Figure 2 – This Smart Timeline event shows compromised insider Rob Koch performing an anomalous remote login to the executive asset us-crm-srv1.

Challenge 3: Response

Security teams responding to privileged activity investigations spend hours or days coordinating a response across multiple security tools.

Solution

Exabeam orchestrates response to privileged activity incidents across your security stack (figure 3) 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 privileged activity 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.

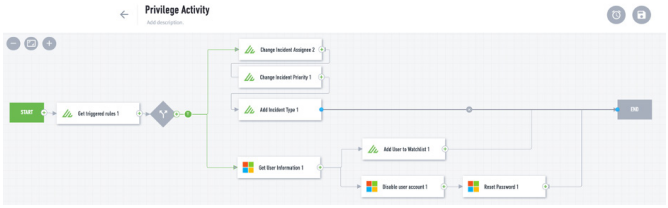

Figure 3 – This privileged activity playbook characterizes and escalates the incident, adds the compromised user to a watchlist while disabling their account, and resets their password.

Use case content

To provide coverage for privileged activity, 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
- File monitoring
- Remote logon activity
- DLP alerts
- Web activity

Key Detection Rule Types

- Abnormal activity on domain controllers
- Executive account activity
- Privileged account activity
- Disabled account activity
- Privileged asset activity
- Privileged process execution

MITRE Technique & Tactic Coverage

- T1078: Valid Accounts
- T1059: Command and Scripting Interpreter
- T1204: User Execution
- T1003: OS Credential Dumping

Incident Checklist

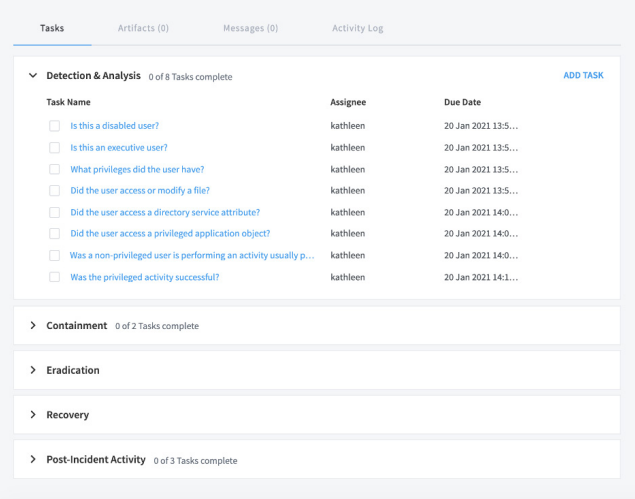

Figure 4 – The privileged activity incident checklist prompts analysts to answer specific investigation questions and take containment actions.

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
- Prompting for re-authentication via 2-factor/multi-factor authentication
- Remove user from group
- Clear user session
- Get asset/user/process info
- Kill process

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit **exabeam.com**.

exabeam

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