exabeam

Solution Brief

Privilege Escalation

Detect, Investigate and Respond to Privilege Escalation Incidents

Privilege escalation refers to an attack where the attacker gains higher-level permissions or unauthorized access to privileged user accounts or assets. The attacker might use an enumeration tool to find a valid account to compromise, switch to an account with greater access privileges or increase permissions on a compromised user or system to elevate their access.

Security teams struggle to detect attacks using privilege escalation

Privilege escalation is the fourth most common tactic used in reported data breaches[1]. However, many legacy security systems that rely on static correlation rules are unable to detect when an attacker escalates privileges. Additionally, a privileged user's work patterns may not occur in regular, predictable patterns, making it difficult to detect privilege escalation with legacy tools.

If undetected, a privilege escalation can give an adversary access to high value assets with impunity. The result of a privilege escalation attack can be devastating to an organization, as these attacks gain access to networks, typically with the aim of exfiltrating data, disrupting business activity, or installing backdoors to enable continued access to internal systems.

APT10, or Red Apollo, is a Chinese cyber espionage group that leverages privilege escalation to deliver malware and steal intellectual property. APT10 has been linked to Cloud Hopper, considered one of the largest-ever corporate espionage efforts.

Source: Operation Cloud Hopper

EXABEAM AND PRIVILEGE ESCALATION

Exabeam helps security teams outsmart adversaries using privilege escalation with the support of automation and use case content, like behavioral models, rules and checklists, across the entire analyst workflow, from detection to response. First, we prescribe data sources to collect and analyze. User and entity behavior analytics (UEBA) is then used to develop a baseline of normal activity for every user and device in an organization. As an adversary begins to move within a network, abnormal activity is identified using out of the box detection rules and models, including 11 MITRE techniques associated with privilege escalation. This anomalous activity is flagged and added to the user or entity's risk score.

The use of 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).

Analysts can also create watchlists to track privileged users at a glance. If an analyst identifies an attack using privilege escalation, they can escalate the incident for review or kick-off an incident response workflow to take additional action like prompting a user to re-authenticate via two-factor authentication.

Key Capabilities

Challenge 1: Collection and Detection

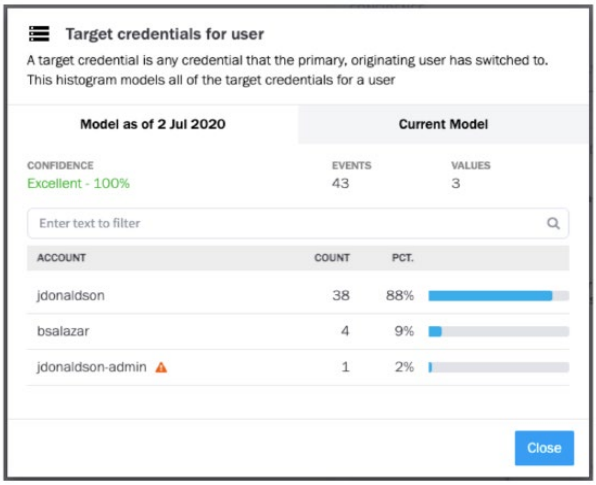
Legacy security tools cannot distinguish privilege escalation by adversaries using valid credentials from normal user activity

Solution

Exabeam ingests and analyzes key data sources to detect risky access and techniques like credential enumeration, bloodhound execution and more. Exabeam also uses behavioral detection models that put anomalous activity like first time access to hosts and assets, or permission changes in the context of the historic behavior of that user, their peers and their organization to clearly distinguish adversary behavior from normal activity. Data Insights Models provide additional details by summarizing a user's activity through histograms.

Benefit

Strengthen your security posture by detecting privilege escalation, including techniques described in the MITRE ATT&CK framework like OS credential dumping and valid accounts.



This Data Insight Model shows the list of credentials a user has switched to. Exabeam alerts on anomalous access to a new account, in this case access to account jdonaldson-admin

Challenge 2: Visibility and Investigation

Security teams are unable to answer key investigation questions and ensure they do not risk missing parts of an attack involving a privilege escalation.

Solution

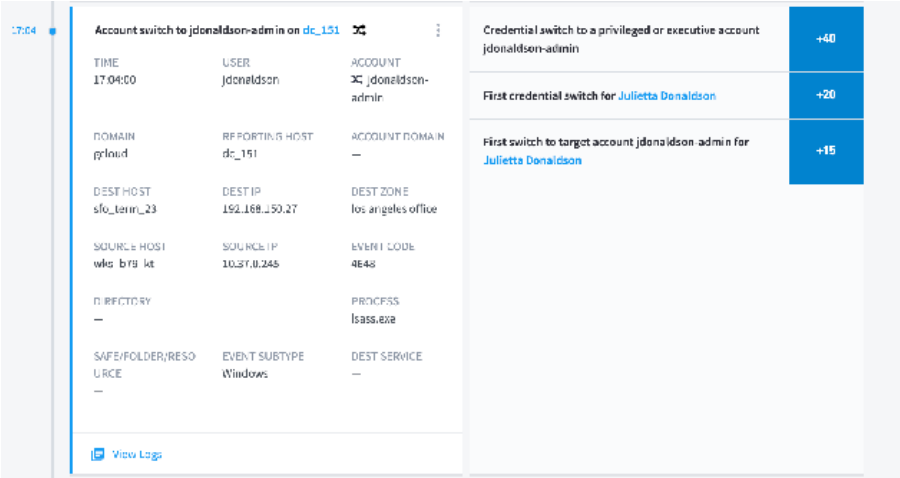
Exabeam provides complete visibility into privilege escalation attacks by providing a list of compromised users and assets. We create Smart Timelines for each user and asset using patented host-IP-user mapping to automatically assemble activity data into clear, readable events, all without an analyst needing to write a single query. Analysts can investigate further with Exabeam Threat Hunter to find other

compromised users or assets, or drill into the timeline events to review the raw logs. At each step of the way, analysts can reference our privilege escalation checklist to ensure their investigation is thorough and complete.

Benefit

Improve investigation quality and speed by enabling analysts to quickly answer key questions like

"What does this user have access to?" Or, "Are they a privileged user?"



Challenge 3: Response

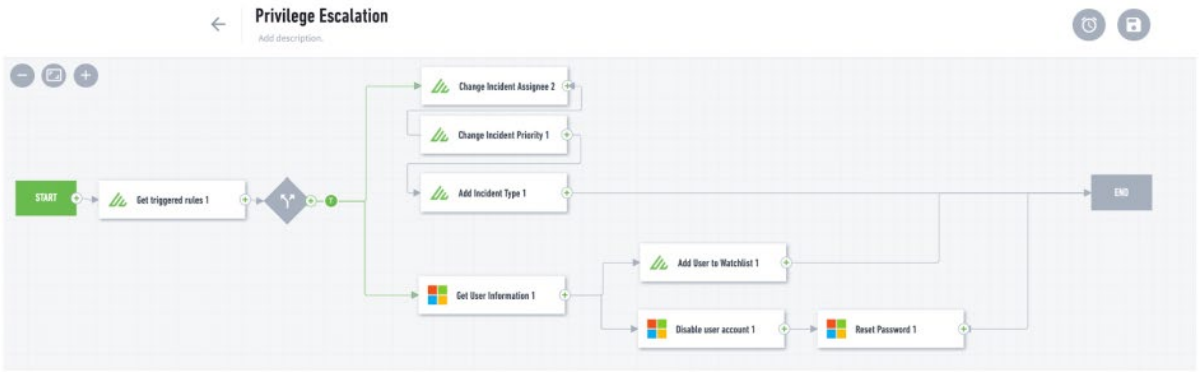
Security teams responding to privilege escalation investigations often spend hours or days coordinating a response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to privilege escalation incidents across your security stack. Out of the box integrations and customizable actions enable security teams to automate playbooks to quickly respond to privilege escalation investigations, such as sending a two-factor authentication push or suspending a user.

Benefit

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



This privilege escalation playbook characterizes and escalates the incident, adds the compromised user to a watchlist while it disables their account, and resets their password.

Use Case Content

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

Key Data Sources

- Authentication and Access Management
- Remote Access
- VPN/Zero Trust Network Access
- Endpoint Security (EPP/EDR)
- Privileged Access Management (PAM)

Key Detection Rule Types

- Credential switch to privileged or executive account
- Execution of credential enumeration tools on an asset
- Detection of artifacts used by MITRE APT groups
- Exploiting vulnerabilities which provide greater account access or escalation of privileges
- Users executing applications/processes to bypass user access controls
- Credential switching to privileged or executive accounts

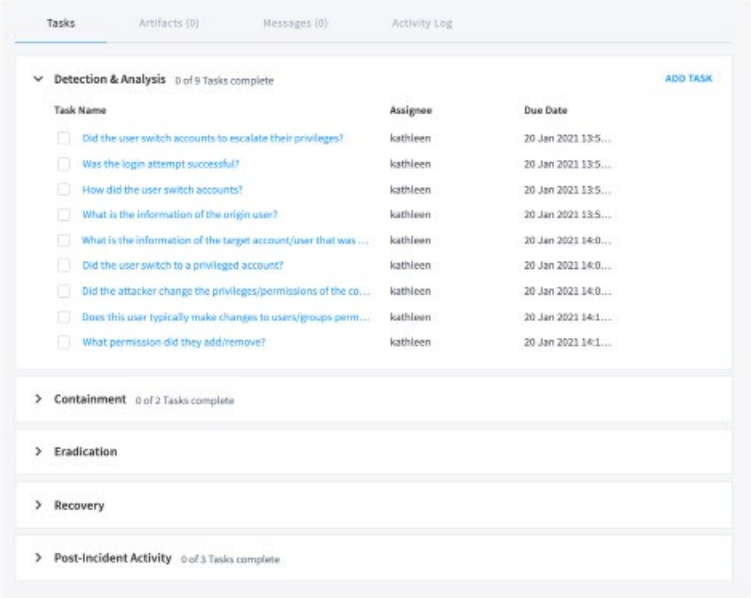
MITRE Technique Coverage

- TA0004: Privilege Escalation
- T1003: OS Credential Dumping
- T1033: System Owner/User Discovery
- T1053: Scheduled Task/Job
- T1055: Process Injection
- T1057: Process Discovery
- T1068: Exploitation for Privilege Escalation
- T1078: Valid Accounts
- T1087: Account Discovery
- T1134: Access Token Manipulation
- T1548: Abuse Elevation Control Mechanism

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/reset password
- Prompt for re-authentication via 2-factor/multi-factor authentication
- Isolate systems
- Clear user session
- Gather additional asset or user contextual information
- Kill process or get process information

INCIDENT CHECKLIST



The Privilege Escalation incident checklist prompts analysts to answer specific investigation questions and take containment actions.

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 www.exabeam.com.

exabeam

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