exabeam

Solution Brief

Account Manipulation

Account manipulation refers to persistence techniques an attacker uses to maintain access to a network, such as creating a new account or manipulating an existing user and/or group.

Security teams struggle to detect attacks using account manipulation

After initially compromising an account, adversaries use account manipulation techniques in order to establish persistence on the network, move around covertly, and grant themselves access to critical corporate resources. To achieve their objective, adversaries may increase the privileges of a group, create temporary users or shield their identity behind default system accounts.

Because IT or security admins may perform similar account management functions as part of their normal job responsibilities, legacy security tools cannot usually differentiate legitimate activity from adversary behavior. Attackers take advantage of this gap in detection to remain on the network undetected to achieve their end goals of intellectual property theft, data exfiltration, or other damage.

> APT3 and Account Manipulation – APT3 is a China based threat group that has been known to use account manipulation to add created accounts to local admin groups to maintain elevated access.[1]

[1] https://attack.mitre.org/groups/G0022/

Exabeam and account manipulation

Exabeam helps security teams outsmart adversaries using account manipulation with the support of automation and use case content across the full analyst workflow, from detection to response. First, we recommend what types of data sources to collect and analyze. Our user and entity behavior analytics (UEBA) then develops 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 the MITRE techniques associated with account manipulation. 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 capabilties

Challenge 1: Collection and Detection

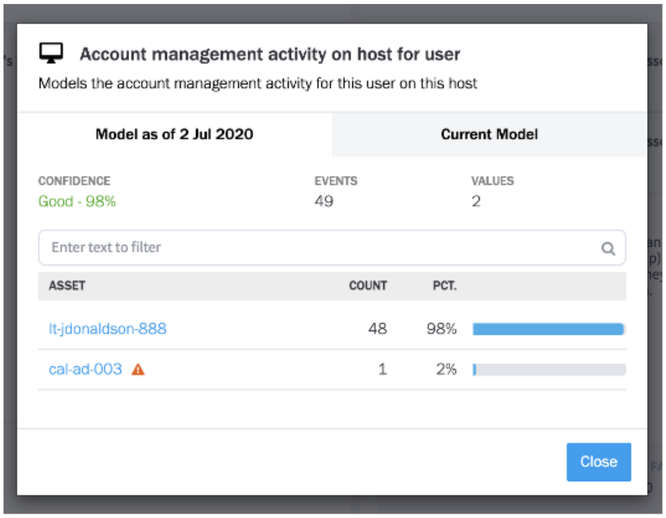
Legacy security tools cannot distinguish between legitimate users performing account management from adversaries using account manipulation techniques.

Solution

Exabeam ingests and analyzes key data sources to detect risky account management techniques like abnormal directory services activity, account creation or deletion, or modifying group membership or other permissions. By further leveraging user context, Exabeam automatically builds a user profile including details like title and department to identify whether account management activity is legitimate for users like administrators, or anomalous and potentially indicative of user compromise. Additional details are displayed in Data Insight models.

Benefit

Strengthen security posture by using behavior analytics and user context to automatically differentiate between normal account management activities and anomalous account manipulation associated with user compromise.



Account management activity on host for user

Models the account management activity for this user on this host

Model as of 2 Jul 2020 | Current Model

CONFIDENCE	EVENTS	VALUES
Good - 98%	49	2

Enter text to filter

ASSET	COUNT	PCT.
lt-jdonaldson-888	48	98%
cal-ad-003 ⚠	1	2%

Figure 1 – This Data Insight Model shows the account management activity on different assets for a user. Exabeam alerts on anomalous activity on a new asset, cal-ad-003.

Challenge 2: Visibility and Investigation

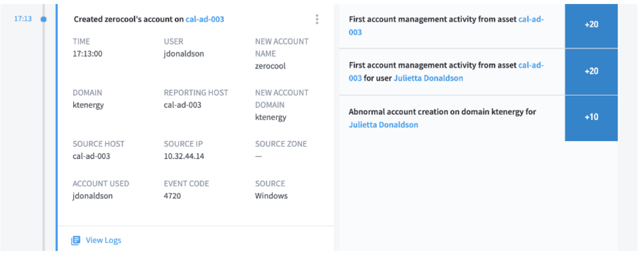
Security teams are unable to answer key investigation questions that ensure they do not risk missing parts of an attack involving account manipulation.

Solution

Exabeam gives complete visibility into attacks involving account manipulation 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 by threat hunting to find other compromised users or assets, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our account manipulation checklist to ensure their investigation is thorough and complete.

Benefit

Improve investigation quality and speed by enabling analysts to view all activity associated with newly performed accounts for full visibility into the attack chain. This enables analysts to quickly answer key questions like "Was a new account created?" or "What does the newly created account have access to?"



17:13

Created zerocool's account on cal-ad-003

TIME 17:13:00
USER jdonaldson
NEW ACCOUNT NAME zerocool
DOMAIN ktenergy
REPORTING HOST cal-ad-003
NEW ACCOUNT DOMAIN ktenergy
SOURCE HOST cal-ad-003
SOURCE IP 10.32.44.14
SOURCE ZONE —
ACCOUNT USED jdonaldson
EVENT CODE 4720
SOURCE Windows

View Logs

First account management activity from asset cal-ad-003 +20

First account management activity from asset cal-ad-003 for user Julietta Donaldson +20

Abnormal account creation on domain ktenergy for Julietta Donaldson +10

Figure 2 – This Smart Timeline event shows compromised insider Julietta Donaldson performing abnormal account management by creating a new account, zerocool, on asset cal-ad-003.

Challenge 3: Response

Security teams responding to account manipulation incidents spend hours or days coordinating a response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to account manipulation incidents across your security stack (image 3). Out of the box integrations with hundreds of popular security and IT products and customizable actions enable security teams to automate playbooks to respond to account manipulation incidents, such as suspending a user or resetting a password.

Benefit

Improve operational efficiency and decrease MTTR with automated response playbooks.

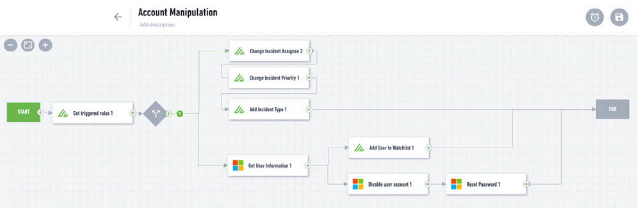


Figure 3 – This account manipulation playbook obtains context for an incident and prioritizes it for triage. It also adds the compromised user to a watchlist while disabling their account, and resets their password.

Use case content

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

Key Data Sources

- Authentication and access management
- Application activity
- Privileged access management
- Operating system logs (e.g. UNIX/LINUX/OSX/Windows)

Key Detection Rule Types

- Abnormal directory services activity
- Account creation activity
- Account deletion activity
- Membership and permission modifications
- System account activity
- Abnormal account management activity

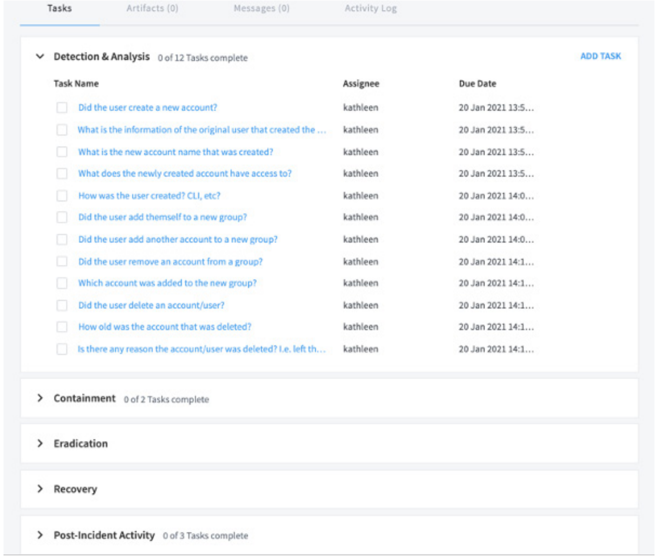
MITRE Techniques

- T1098: Account manipulation
- T1136: Create account
- T1151: Account access removal
- T1207: Rogue domain controller

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
- Prompting for re-authentication via 2-factor/multi-factor authentication

Incident Checklist



Detection & Analysis 0 of 12 Tasks complete

	Task Name	Assignee	Due Date
□	Did the user create a new account?	kathleen	20 Jan 2021 13:5...
□	What is the information of the original user that created the ...	kathleen	20 Jan 2021 13:5...
□	What is the new account name that was created?	kathleen	20 Jan 2021 13:5...
□	What does the newly created account have access to?	kathleen	20 Jan 2021 13:5...
□	How was the user created? CLI, etc?	kathleen	20 Jan 2021 14:0...
□	Did the user add themself to a new group?	kathleen	20 Jan 2021 14:0...
□	Did the user add another account to a new group?	kathleen	20 Jan 2021 14:0...
□	Did the user remove an account from a group?	kathleen	20 Jan 2021 14:1...
□	Which account was added to the new group?	kathleen	20 Jan 2021 14:1...
□	Did the user delete an account/user?	kathleen	20 Jan 2021 14:1...
□	How old was the account that was deleted?	kathleen	20 Jan 2021 14:1...
□	Is there any reason the account/user was deleted? I.e. left th...	kathleen	20 Jan 2021 14:1...

Containment 0 of 2 Tasks complete

Eradication

Recovery

Post-Incident Activity 0 of 3 Tasks complete

Figure 4 – The account manipulation 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 **exabeam.com.**

exabeam

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