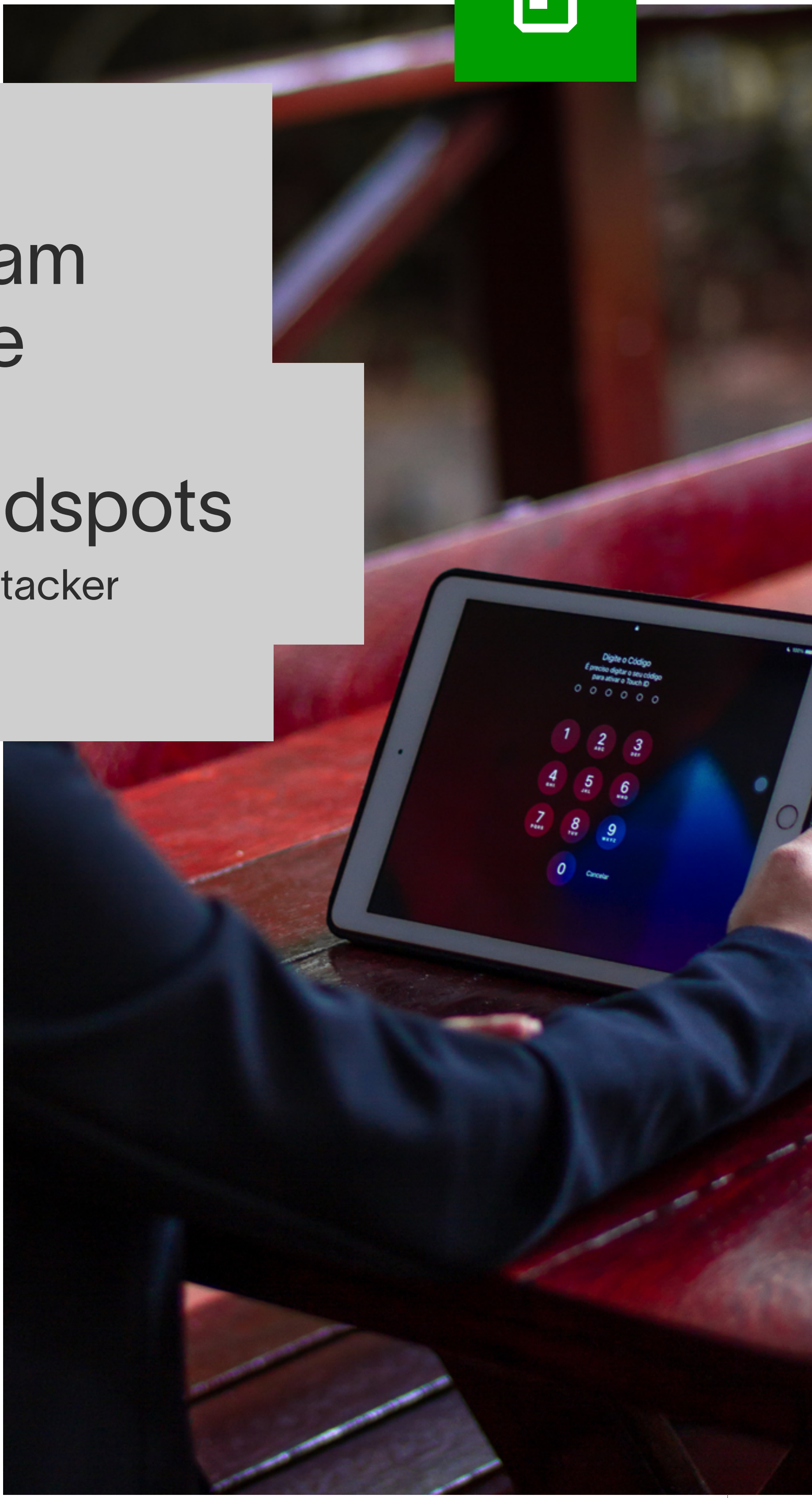
exabeam

Guide

5 Ways Exabeam Helps Eliminate Compromised Credential Blindspots

An automated view into attacker behaviors



Stolen credentials are a persistent problem that many organizations have yet to effectively solve.

Frequently, credential-stuffing attacks occur wherein a threat actor successfully steals credentials, logs in to the environment, and moves laterally to gain higher-level access. All activities have a singular focus: to access private data or high-value assets. The MITRE ATT&CK knowledge base provides information about tactics, techniques, and procedures (TTPs) used by threat actors that can help security teams build stronger security processes. This guide will show you five ways to leverage Exabeam's machine learning-powered solution to detect these activities through analytics, including mapping the activities to the MITRE ATT&CK framework.

1. Model your users and assets

During initial deployment, Exabeam will use your data sources (e.g., syslogs) to start modeling users and assets. Once you have your data onboarded, Exabeam will monitor all behavior, assigning risk values to certain actions. As these actions continue, the user and/or asset risk score will rise until it surpasses your threshold. At that time the user/asset will be flagged as “notable” and will appear on your Exabeam dashboard.

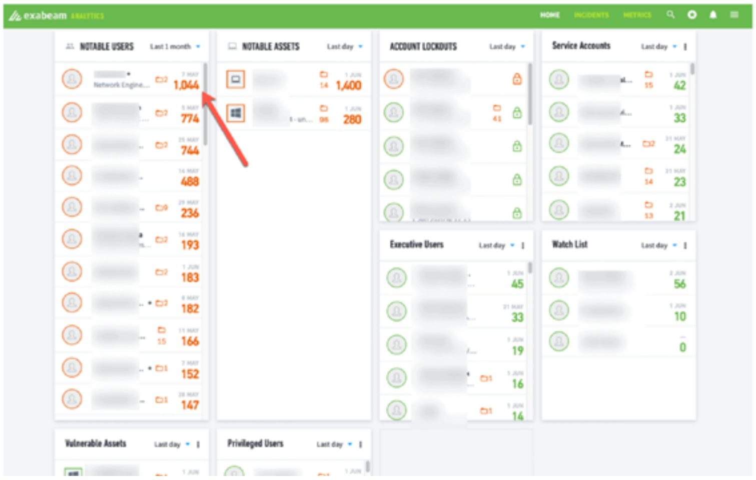


Figure 01 Exabeam Analytics shows an unusual amount of activity for a user.

2. Get insights into normal vs. abnormal user activity

Trend timelines can give you a clear indication that the user’s behavior is abnormal. Using dynamic KPIs, you can also see the user’s normal level of behavior for the days prior to this event being triggered, further confirming that the user does not normally generate this level of risk, use this many accounts, or access this many assets.

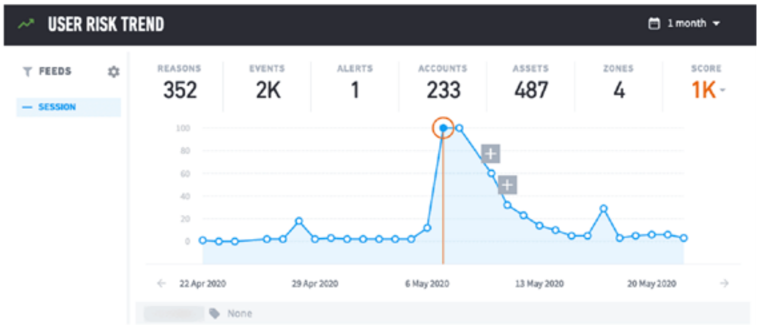


Figure 02 Viewing this activity on the Trend Timeline shows the spike in contrast to normal activity for the user.

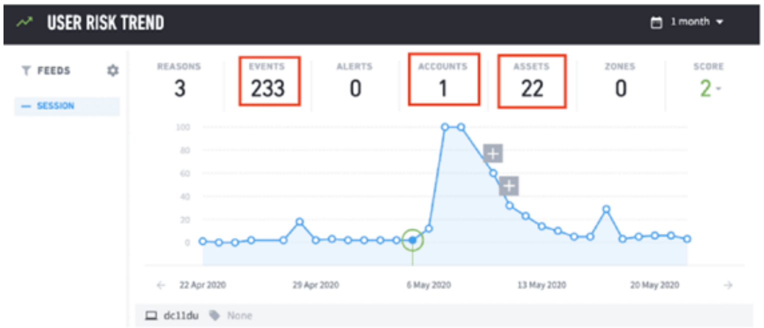
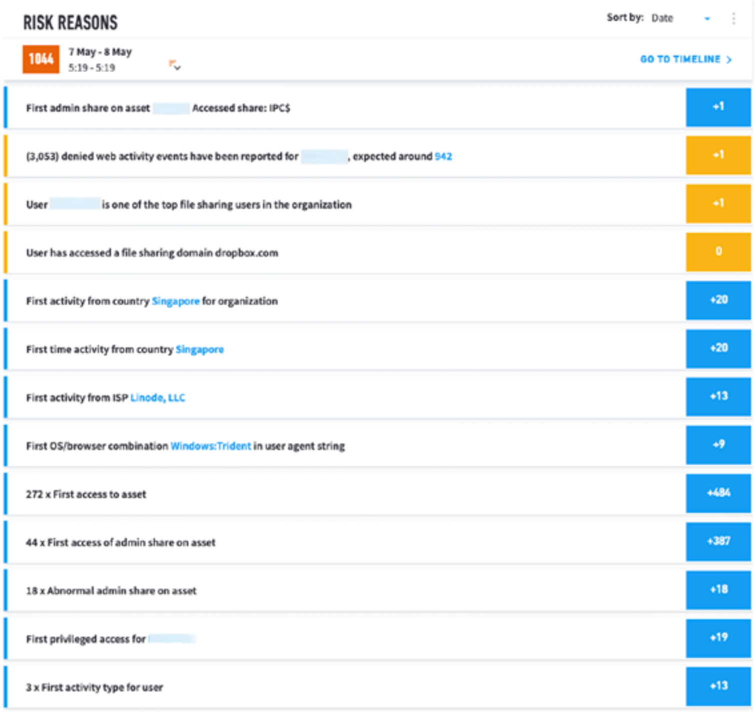


Figure 03 Looking back at the user’s behavior over recent days, it’s easy to see that there is no level of risk compared to the new alerts.

3. Know when the risk score hits the acceptable threshold

Once you've established that the user's behavior is indeed out of the ordinary, it's important to find out why. By drilling into the user details, you will see a summary of the reasons why the user was flagged as notable. You'll see risk scores assigned to specific behaviors, for example, 20 points for accessing the VPN from a different country than usual, and 22 additional points for connecting from an ISP that's never been observed from them before, along with connecting from a user-agent string that's never before been associated with them. At this stage, the user has a risk score of 62 points.

Looking at the timeline, you're able to see the sequence of events. In this example, an hour later the user began accessing assets that they've never been observed accessing before — each one flagging 10 points of risk. Once at 93 points, the user's risk score crossed the global threshold to become notable, triggering an analyst to investigate the user.



RISK REASONS

1044 7 May - 8 May 5:19 - 5:19

First admin share on asset [redacted] Accessed share: IPC$	+1
(3,053) denied web activity events have been reported for [redacted], expected around 942	+1
User [redacted] is one of the top file sharing users in the organization	+1
User has accessed a file sharing domain dropbox.com	0
First activity from country Singapore for organization	+20
First time activity from country Singapore	+20
First activity from ISP Linode, LLC	+13
First OS/browser combination Windows:Trident in user agent string	+9
272 x First access to asset	+484
44 x First access of admin share on asset	+387
18 x Abnormal admin share on asset	+18
First privileged access for [redacted]	+19
3 x First activity type for user	+13

Figure 04 Looking more closely, you're able to see each behavior that adds up to a high risk score.

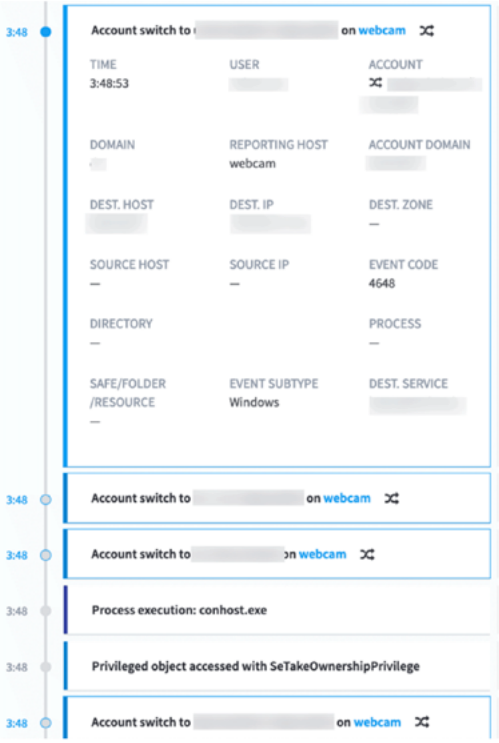
4. Stitch each behavior into the timeline

When a notable user is finally able to find credentials to switch to and laterally move off the initial host. Exabeam can stitch this into the timeline as an account switch activity, displaying the original username and the username and host to which they moved.

In our example, this user dumped and attempted to use hundreds of credentials from Mimikatz — a credential dumper capable of obtaining plain text account logins and passwords — before laterally moving off the initially compromised host to another asset in the environment.

Exabeam can identify this specific asset, once again due to behavioral changes on that asset. If using along with an EDR tool, the Mimikatz usage alerts from the EDR tool are also stitched into the Exabeam Assets Timeline, further accelerating the overall risk score.

Exabeam Timelines plus modeling can trigger a notable user and asset just from behavior-driven aspects, while also stitching together events to provide a clear view of what took place during an attack.



3:48 Account switch to [redacted] on webcam

TIME 3:48:53	USER [redacted]	ACCOUNT [redacted]
DOMAIN [redacted]	REPORTING HOST webcam	ACCOUNT DOMAIN [redacted]
DEST. HOST [redacted]	DEST. IP [redacted]	DEST. ZONE —
SOURCE HOST —	SOURCE IP —	EVENT CODE 4648
DIRECTORY —		PROCESS —
SAFE/FOLDER /RESOURCE —	EVENT SUBTYPE Windows	DEST. SERVICE [redacted]

3:48 Account switch to [redacted] on webcam

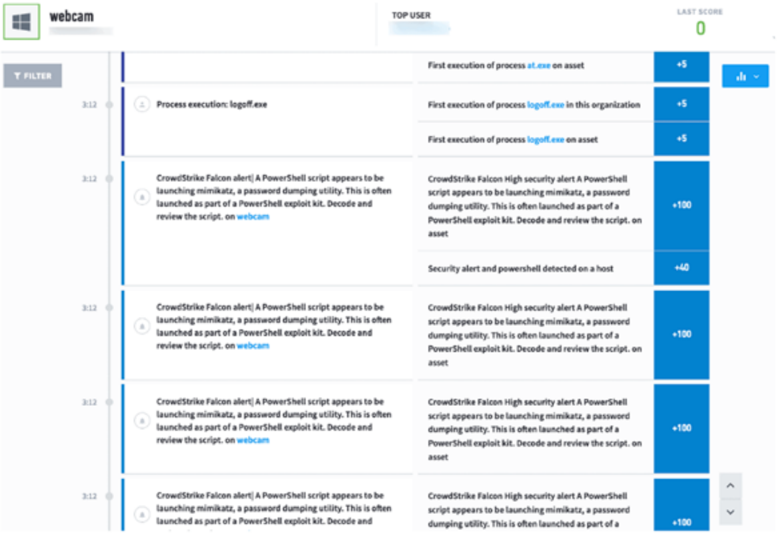
3:48 Account switch to [redacted] on webcam

3:48 Process execution: conhost.exe

3:48 Privileged object accessed with SeTakeOwnershipPrivilege

3:48 Account switch to [redacted] on webcam

Figure 05 The user finds credentials to switch to and laterally moves off the initial host.



webcam [redacted]

TOP USER [redacted]

LAST SCORE 0

First execution of process at.exe on asset +5

3:12 Process execution: logoff.exe

First execution of process logoff.exe in this organization +5

First execution of process logoff.exe on asset +5

3:12 CrowdStrike Falcon alert| A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on webcam

CrowdStrike Falcon High security alert A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on asset +100

Security alert and powershell detected on a host +40

3:12 CrowdStrike Falcon alert| A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on webcam

CrowdStrike Falcon High security alert A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on asset +100

3:12 CrowdStrike Falcon alert| A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on webcam

CrowdStrike Falcon High security alert A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. on asset +100

3:12 CrowdStrike Falcon alert| A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and

CrowdStrike Falcon High security alert A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a +100

Figure 06 Alerts from the customer's EDR tool show notifications of Mimikatz tools being used.

5. Use the MITRE ATT&CK framework to your advantage

The MITRE ATT&CK framework has been embraced by many security teams as a way to streamline threat identification, investigation, and response. By standardizing processes around this publically available framework, security teams can deliver more consistent, dependable security no matter what changes in resources might occur. Exabeam provides MITRE ATT&CK framework mapping across all use cases defined in the product, making it easy for security analysts to take decisive actions, mitigating threats as quickly as possible.

Conclusion

Compromised credentials will continue to be a leading method by which attackers carry out their attacks. The good news is that with Exabeam you have a powerful, automated solution designed to help you identify when a user's behavior is operating outside their normal patterns, indicating a potential attack is underway. With the field-proven capabilities and approach outlined in this guide your team has a fighting chance to identify these attacks early and mitigate the threat before it can cause significant damage to your organization.

Exabeam Fusion

As the leading Next-gen SIEM and XDR, Exabeam Fusion provides a cloud-delivered solution for threat detection and response. Exabeam Fusion combines behavioral analytics and automation with threat-centric, use case packages focused on delivering outcomes. Exabeam Fusion is modular; we can augment your legacy data lake or SIEM deployment with XDR, or replace your SIEM entirely. It's your call.

Exabeam Fusion provides the following benefits:

- Industry-leading behavioral analytics to detect threats other tools miss
- Advanced third party alert triage capabilities — 83% of analysts report the ability to triage twice as many alerts as a legacy SIEM
- Faster threat detection and response, as much as 50% faster
- Built-in automation with predefined workflows and checklists to improve analyst productivity
- Metrics to show whole analyst team improvement in Mean Time to Detect, supporting your SLAs

To learn more about how Exabeam Fusion can help, **request a demo today**.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is 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. Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives and best protect their organizations.

For more information, visit exabeam.com.

exabeam™