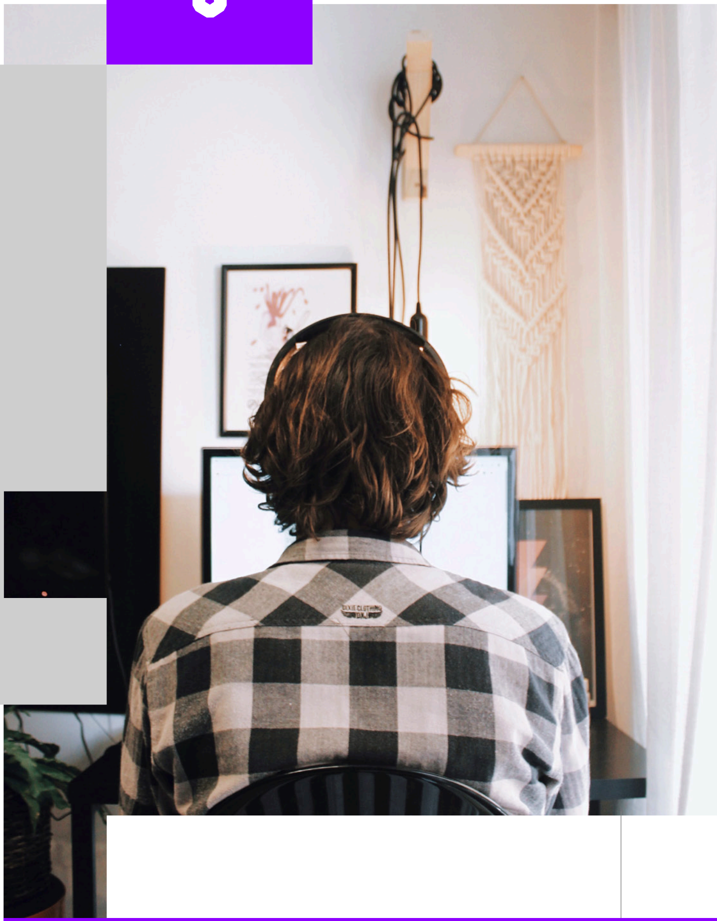
exabeam

Solution Brief

Destruction of Data

Destruction of data is when a user destroys data in an effort to evade detection or sabotage a corporation.



Disgruntled employees can deal damage

Organizations with recent restructurings, terminations, or other major events can often leave employees disgruntled. With access to sensitive data and critical systems, these employees can wreak havoc by disrupting or halting business operations. According to one incident reported by Verizon, an unhappy IT administrator abused service accounts to schedule mass delete commands prior to important deadlines, such as tax season and prior to holiday bonuses[1].

Because file deletion is generally considered normal, permissible activity, security and insider threat teams are often unable to detect these types of threats. By the time teams are aware of an incident, the damage is already done.

> Disgruntled employees aren't just angry. They're potentially dangerous, even if they don't resort to physical violence. Some may turn to cybercrime, including stealing information, destroying property, systems, or data, and disrupting business operations[1].

[1] Verizon Insider Threat Report, 2020

Exabeam and destruction of data

Exabeam helps security and insider threat teams outsmart users destroying data with the support of automation and use case content across the full analyst workflow, from detection to response. Exabeam automatically assembles all 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. Timeline events parsed into plain, clear language allow security and insider threat teams to easily investigate activity 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

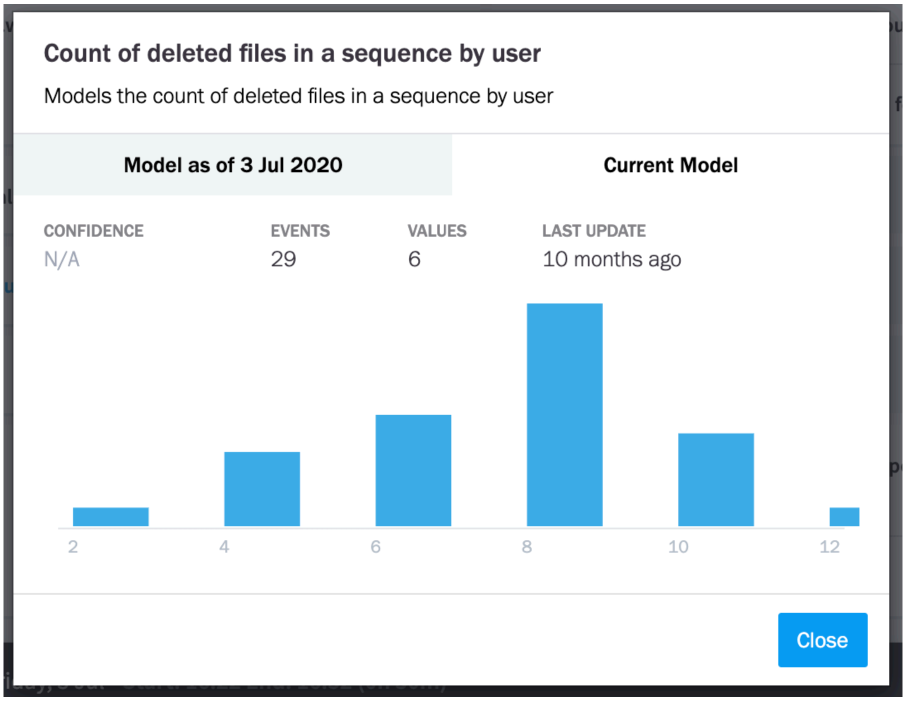
Legacy security tools are unable to identify when users are destroying data with malicious intent as compared to normal, permissible activity.

Solution

Exabeam ingests and analyzes key data sources to detect unusual activity such as deleting an abnormal number of files. Exabeam behavioral models put anomalous activity like file deletion into the context of historic behavior for an individual or their peers. Further, with context labels such as "Critical System," Exabeam allows analysts to quickly identify when an insider is deleting important data.

Benefit

Strengthen security posture against malicious insiders by using behavior analytics to identify anomalous file deletion activity.



Count of deleted files in a sequence by user

Models the count of deleted files in a sequence by user

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
N/A	29	6	10 months ago

Figure 1 - This Data Insight Model shows the typical number of files a user deletes in sequence. Exabeam alerts on an anomalous number of file deletions, such as the 12 shown above.

Challenge 2: visibility and investigation

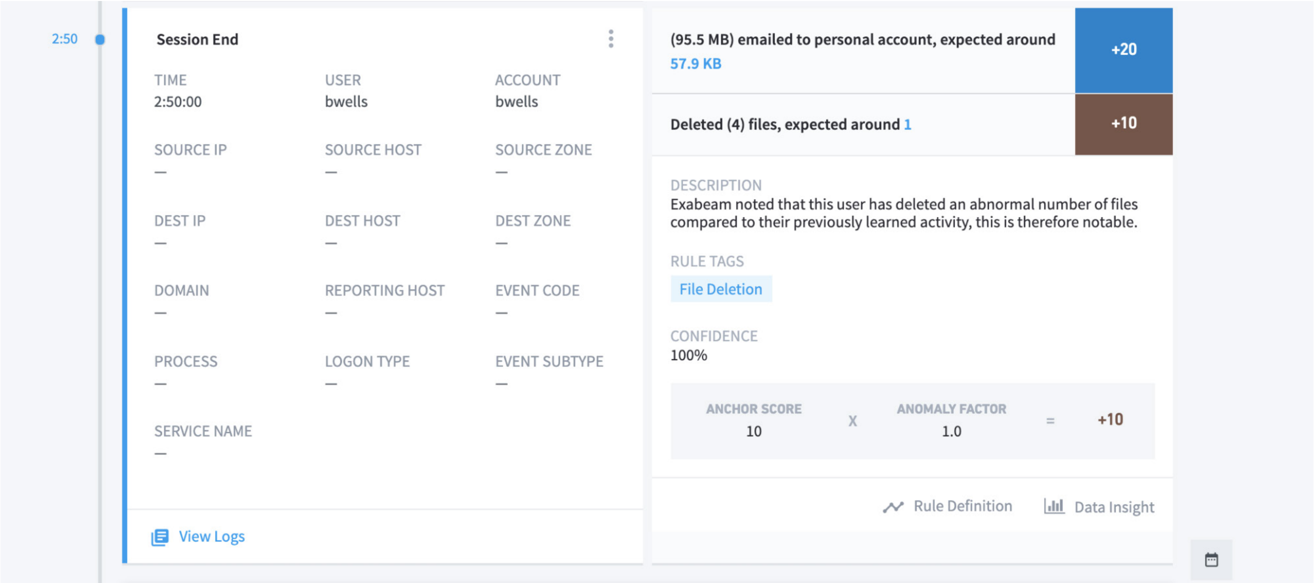
Security and insider threat teams are unable to answer key investigation questions to ensure they do not risk missing parts of a malicious insider destroying data.

Solution

Exabeam gives complete visibility into malicious insiders destroying data. Our Smart Timelines automatically capture and assemble all activity data, including events leading up to and after file deletions. Patented host-IP-user mapping attributes this activity back to a user and presents it as clear, readable events, all without an analyst needing to write a single query. Analysts can investigate further with Exabeam Threat Hunter to find all file deletion activity, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our destruction of data checklist to ensure their investigation is thorough and complete.

Benefit

Exabeam improves investigation quality and speed, even if underlying evidence has been destroyed. With Exabeam, even non-technical analysts can answer key questions like "What file was deleted?" or "What types of files did the user delete?"



2:50

Session End

TIME 2:50:00	USER bwells	ACCOUNT bwells
SOURCE IP —	SOURCE HOST —	SOURCE ZONE —
DEST IP —	DEST HOST —	DEST ZONE —
DOMAIN —	REPORTING HOST —	EVENT CODE —
PROCESS —	LOGON TYPE —	EVENT SUBTYPE —
SERVICE NAME —		

View Logs

(95.5 MB) emailed to personal account, expected around 57.9 KB +20

Deleted (4) files, expected around 1 +10

DESCRIPTION
Exabeam noted that this user has deleted an abnormal number of files compared to their previously learned activity, this is therefore notable.

RULE TAGS
File Deletion

CONFIDENCE
100%

ANCHOR SCORE		ANOMALY FACTOR		
10	X	1.0	=	+10

Rule Definition Data Insight

Figure 2 - This Smart Timeline event shows malicious insider Billie Wells deleting an abnormally high number of files, compared to the expected number of 1.

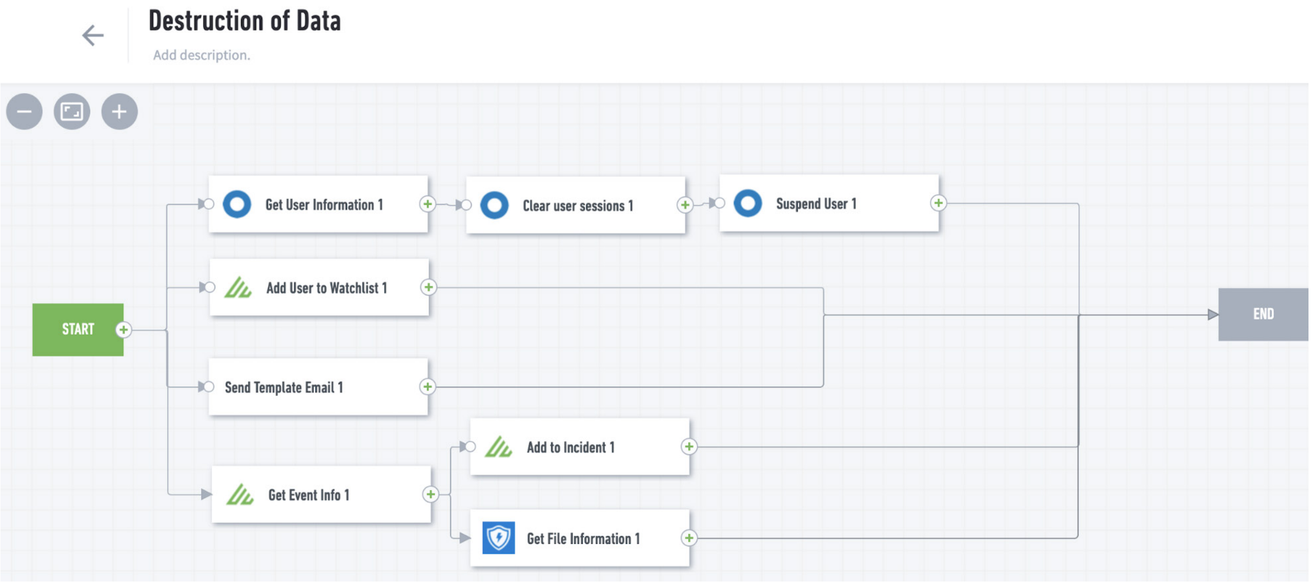


Figure 3 - This destruction of data playbook obtains contextual information about the malicious insider, adds them to a watchlist, and disables their account.

Challenge 3: response

Security and insider threat teams responding to destruction of data incidents spend hours or days coordinating response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to destruction of data incidents across your security stack. Pre-built integrations and customizable actions enable analysts to automate playbooks to respond to audit tampering, such as suspending a user or resetting a password.

Benefit

Enhance analyst productivity and decrease MTTR with security orchestration automation and response (SOAR) powered playbooks.

Use case content

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

Key data sources

- File access and activity
- Process execution and activity

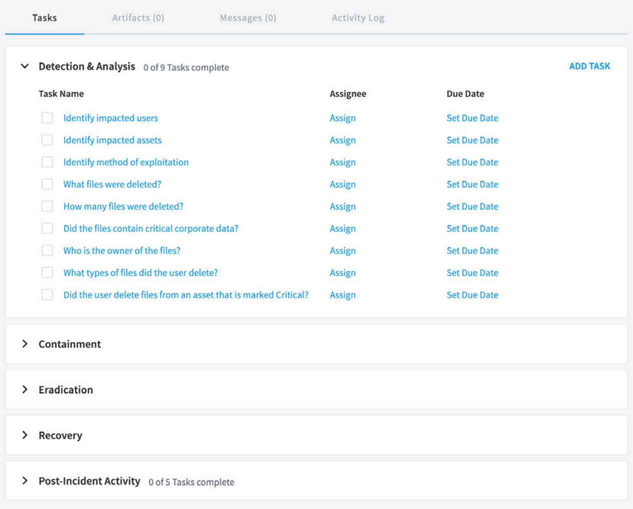
Key detection rule types

- Data deletion

MITRE technique coverage

- T1485: Data Destruction

Incident checklist



Detection & Analysis 0 of 9 Tasks complete

	Task Name	Assignee	Due Date
□	Identify impacted users	Assign	Set Due Date
□	Identify impacted assets	Assign	Set Due Date
□	Identify method of exploitation	Assign	Set Due Date
□	What files were deleted?	Assign	Set Due Date
□	How many files were deleted?	Assign	Set Due Date
□	Did the files contain critical corporate data?	Assign	Set Due Date
□	Who is the owner of the files?	Assign	Set Due Date
□	What types of files did the user delete?	Assign	Set Due Date
□	Did the user delete files from an asset that is marked Critical?	Assign	Set Due Date

Containment

Eradication

Recovery

Post-Incident Activity 0 of 5 Tasks complete

Figure 4 - The destruction of data incident checklist prompts analysts to answer specific investigation questions and take containment actions.

Response actions

- Contact user/manager/HR department via email
- Add user 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

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.