exabeam

Solution Brief

Data Leak

Data leak is when a malicious insider illicitly and deliberately transfers data outside of an organization.

Data leak

To support the operational efficiency of a business, data must move in and out of an enterprise. However, enabling access to data from outside the network perimeter introduces greater risk from malicious insiders. Easy accessibility to data provides an opportunity for malicious insiders with privileged access and knowledge of the organization's most valuable assets to exploit data. Instances of a data leak can closely resemble normal activity, making it more challenging for security teams to identify threats from insiders than threats that originate from outside the enterprise.

To detect data leak threats, many organizations rely on data loss prevention (DLP) tools, but detection from these tools depends primarily on static rules. Correlation rules, unfortunately can be either too broadly or narrowly defined, and result in noisy alerts with low fidelity or the risk of missing instances of a data leak. Additionally, malicious insiders may know the organization's security thresholds (for example how much outbound data transfer would trigger an alert), this can allow them to remain just under the threshold to avoid detection.

In 2019, Ponemon Institute estimated that the average cost of an insider data breach was $3.9m.

[1] DBIR Data Breach Investigations Report 2020

[2] IBM Cost of a Data Breach Report 2020

To reduce the risk of a data leak, organizations must be able to use behavior to understand the context and risk associated with incidents. Understanding context enables organizations to recognize malicious instances of a data leak.

Exabeam and data leak

Exabeam helps security and insider threat teams outsmart threats from insiders leaking data with the support of automation and use case content across the full analyst workflow, from detection to response. First, we prescribe useful data sources such as DLP tools, email, application and endpoints 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 insider begins to move within a network, abnormal activity is identified using pre-packaged detection rules and models. Anomalous activity is automatically associated with the MITRE tactics and techniques to help analysts easily understand the nature of the threat. This activity is flagged and added to the user or entity's risk score, alongside DLP alerts and our data leak alerts. Risk scores and watchlists prioritize the riskiest incidents, while Exabeam Smart Timelines automatically display the full attack chain, from the perspective of the user, to dramatically accelerate incident investigations. Transferring risk from previous sessions helps detect slowly-unfolding attacks that might occur over days or weeks in an attempt to avoid detection. Painting a full picture of user activity allows analysts to leverage user and asset contextual data in conjunction with the DLP alerts to determine if the insider is acting with malicious intent. A guided investigation checklist and automated response playbooks enable analysts to quickly and effectively remediate data breach incidents and reduce mean time to respond (MTTR).

Key capabilities

Challenge 1: collection and detection

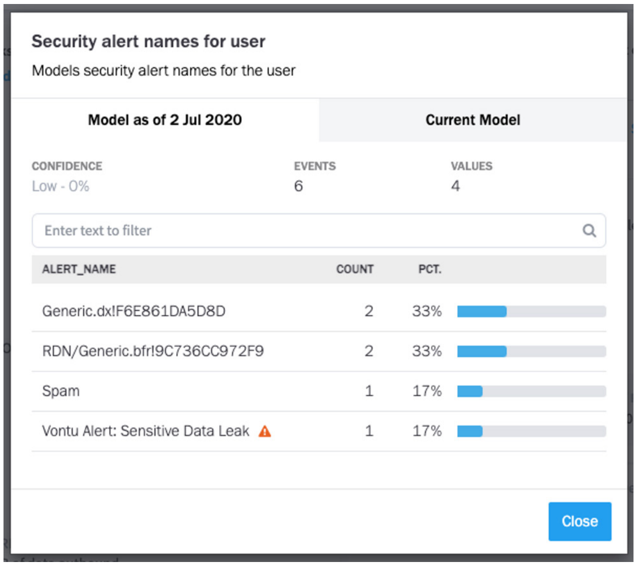
DLP tools that rely on static rules for detection require significant time and resources to maintain and tune. These tools often generate a high volume of alerts and false positives for analysts to sift through, complicating their ability to detect true data leak threats.

Solution

Exabeam takes a machine learning-based approach to identify data leak threats minimizing the burden of constantly tuning DLP policies. Instead of spending hours adding exceptions in a DLP tool to tune out false-positive alerts, remove your exclusions and send all of your DLP data to us. Exabeam will find the security alerts with the highest degree of anomalous activity based on deviations from a user or machine's baseline across all available data sources, prioritizing the riskiest instances of DLP for analysts to review. Additional details are provided in Data Insights Models (Figure 1).

Benefit

Increase your team's operational efficiency by using behavior analytics to increase DLP alert fidelity and prioritize response efforts.



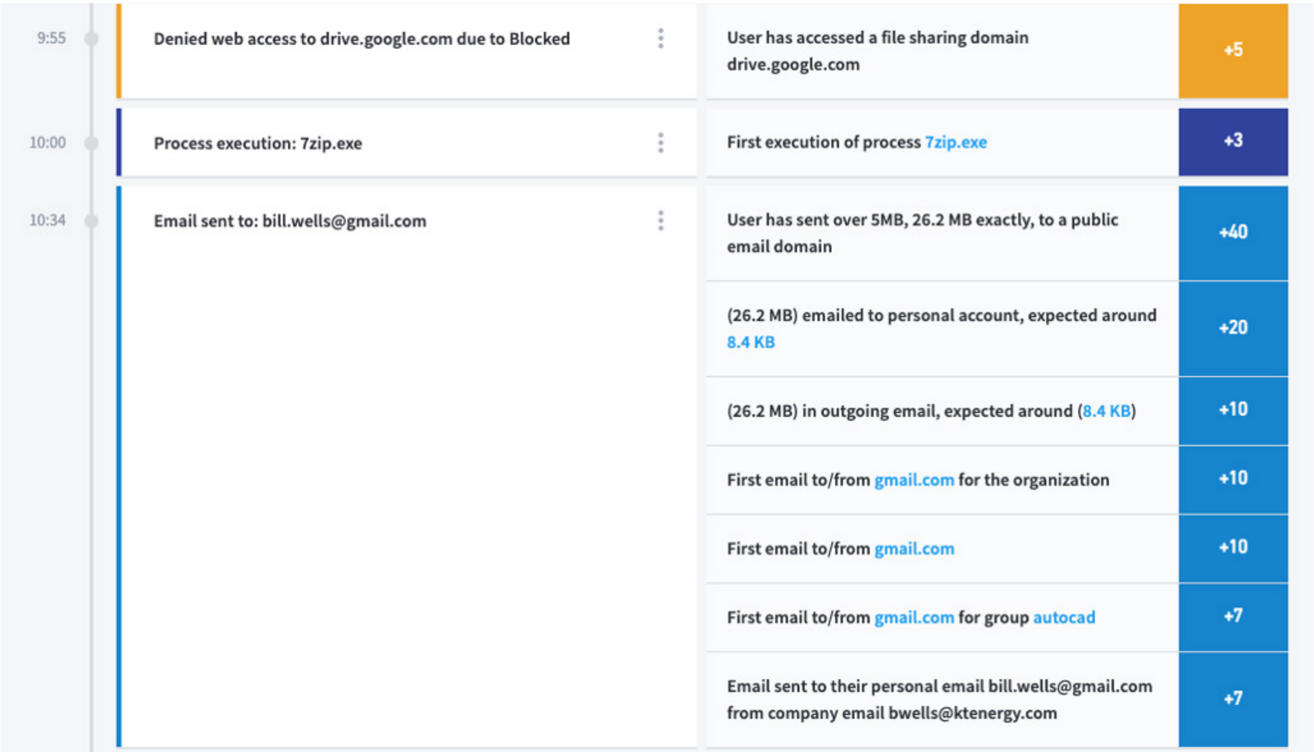
Security alert names for user

Models security alert names for the user

CONFIDENCE: Low - 0%
EVENTS: 6
VALUES: 4

ALERT_NAME	COUNT	PCT.
Generic.dx!F6E861DA5D8D	2	33%
RDN/Generic.bfr!9C736CC972F9	2	33%
Spam	1	17%
Vontu Alert: Sensitive Data Leak ⚠	1	17%

Figure 1 - This Data Insight Model shows the security alert names that have been attributed to the user. Exabeam alerts on anomalous alert notifications, in this case a sensitive Data Leak alert.



9:55	Denied web access to drive.google.com due to Blocked	User has accessed a file sharing domain drive.google.com	+5
10:00	Process execution: 7zip.exe	First execution of process 7zip.exe	+3
10:34	Email sent to: bill.wells@gmail.com	User has sent over 5MB, 26.2 MB exactly, to a public email domain	+40
		(26.2 MB) emailed to personal account, expected around 8.4 KB	+20
		(26.2 MB) in outgoing email, expected around (8.4 KB)	+10
		First email to/from gmail.com for the organization	+10
		First email to/from gmail.com	+10
		First email to/from gmail.com for group autocad	+7
		Email sent to their personal email bill.wells@gmail.com from company email bwells@ktenergy.com	+7

Figure 2 - This Smart Timeline event shows malicious insider Bill Wells sending an anomalously large amount of data to his personal email account.

Challenge 2: visibility and investigation

Security and insider threat teams lack a defined end-to-end solution and are unable to quickly and easily answer key investigation questions to ensure they do not risk a data leak attack.

Solution

Exabeam detects data leaks by analyzing all incoming DLP alerts. as well as other security relevant data—and quantifying the level of risk associated with them. Analysts are presented a list of users and assets that demonstrate a high level of risk. We recreate a timeline 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 (figure 2). Analysts can review the timelines to understand the activity that happened before and after the DLP alert was fired. Analysts can investigate further with behavior-based threat hunting to find other 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 data leak checklist to ensure their investigation is thorough and complete.

Benefit

Exabeam's ease of use improves investigation quality and speed by enabling analysts to quickly answer key questions like "Are they a flagged user?" or "What data was leaked?" without performing advanced search queries.

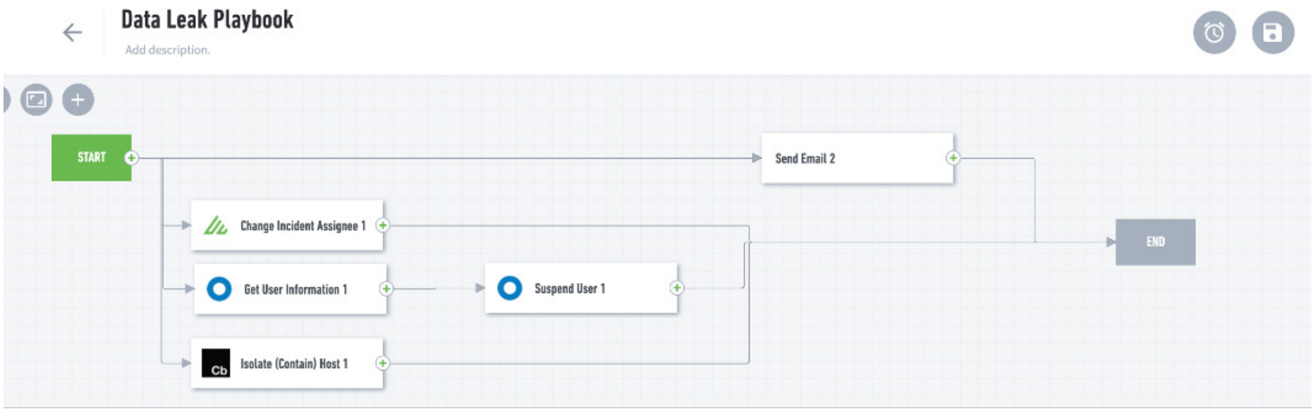


Figure 3 - This data leak playbook obtains context for a user, suspends them and their machine from the network, and sends an email notification of suspected data leak.

Challenge 3: response

Security and insider threat teams responding to data leak investigations spend hours or days coordinating response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to data leak incidents across your security stack (figure 3). Pre-built integrations with hundreds of popular security and IT products and customizable actions enable analysts to automate playbooks to respond to data leak incidents, such as contacting the user's manager or adding to a watchlist.

Benefit

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

Use case content

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

Key data sources

- Web security and monitoring
- Print activity
- Data loss prevention
- Email security and management
- File monitoring
- Database activity monitoring
- Endpoint security (EPP/EDR)

Key detection rule types

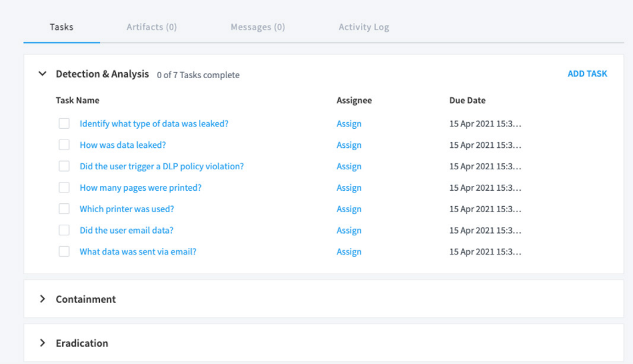
- Data leak
- Data leak via email
- Data leak via printer
- Data leak via a removable device
- Data leak via web

MITRE technique & tactic coverage

- TA0010: Exfiltration
- T1567: Exfiltration over web service
- T1052: Exfiltration over physical medium

Incident checklist

The workforce protection incident checklist prompts analysts to answer specific investigation questions and take containment actions.



Tasks | Artifacts (0) | Messages (0) | Activity Log

Detection & Analysis 0 of 7 Tasks complete ADD TASK

Task Name	Assignee	Due Date
□ Identify what type of data was leaked?	Assign	15 Apr 2021 15:3...
□ How was data leaked?	Assign	15 Apr 2021 15:3...
□ Did the user trigger a DLP policy violation?	Assign	15 Apr 2021 15:3...
□ How many pages were printed?	Assign	15 Apr 2021 15:3...
□ Which printer was used?	Assign	15 Apr 2021 15:3...
□ Did the user email data?	Assign	15 Apr 2021 15:3...
□ What data was sent via email?	Assign	15 Apr 2021 15:3...

Containment

Eradication

Figure 4 - The data leak 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
- Rotate credentials/reset/expire password
- Prompting for re-authentication via 2-factor/ multi-factor authentication
- Remove user from the group
- Suspend user

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.