exabeam

Solution Brief

Data Exfiltration

Data exfiltration occurs when an external attacker illicitly and deliberately transfers data outside of an organization

Data exfiltration can cost an organization financially

Data exfiltration is a common tactic of cybercriminals which account for 70% of breaches, with organized crime accounting for 55% of breaches.[1] Adversaries target specific organizations and sectors with the intent of gaining access to sensitive corporate or customer data. Once they have transferred the data out of the organization, the attacker may leverage the extracted data to exploit the organization for financial gain or sell the data to the highest bidder. This results in huge financial and reputational costs to the organization, with Ponemon Institute reporting that malicious attacks cause the majority of breaches and cost breached organizations an average of $4.27 million.[2]

While many organizations use data loss prevention (DLP) tools to address data exfiltration threats, their detection primarily relies on static rules. When rules are defined broadly to capture any instance of potential data exfiltration, analysts receive a high volume of DLP alerts that more often than not, are false positives. The deluge of noise DLP alerts generate can force an analyst to ignore true threats, dismissing them as a false positive.

> Using an analytics approach—such as that employed by Exabeam—is like having a dedicated DLP analyst with unlimited capacity for reviewing events.
>
> **MUFG Union Bank**
> Managing Director

[1] DBIR Data Breach Investigations Report 2020

[2] IBM Cost of a Data Breach Report 2020

Overwhelmed by DLP alerts, security teams may pivot to defining rules more narrowly resulting in false negatives and data loss. To reduce the risk of data exfiltration, and in turn minimize the financial impact, organizations must be able to use behavior to understand the context and risk associated with each DLP alert. Understanding context enables organizations to prioritize investigating the riskiest instances of DLP.

Exabeam and data exfiltration

Exabeam helps security teams outsmart adversaries using data exfiltration with the support of automation and use case content across the full analyst workflow, from detection to response. First, we prescribe data sources from DLP tools and others 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 tactics and techniques associated with data exfiltration. This activity is flagged and added to the user or entity's risk score, alongside DLP alerts and our data exfiltration alerts with authentication, access, and contextual data sources. Risk scores and watchlists prioritize the riskiest incidents of data exfiltration, while Exabeam Smart Timelines automatically display the full attack chain to dramatically accelerate incident investigations. 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 user has been compromised by an external bad actor. 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 exfiltration threats.

Solution

Exabeam takes a machine learning-based approach to identify data exfiltration minimizing the burden of constantly tuning DLP policies. Instead of spending hours adding exceptions in a DLP tool to tune out false-positive alerts, Exabeam will learn what is normal activity and automatically tune out these alerts over time prioritizing the riskiest instances of DLP for analysts to review. Additional details are provided in Data Insights Models (figure 1).

Benefit

Increase operational efficiency by using behavior analytics to increase DLP alert fidelity.

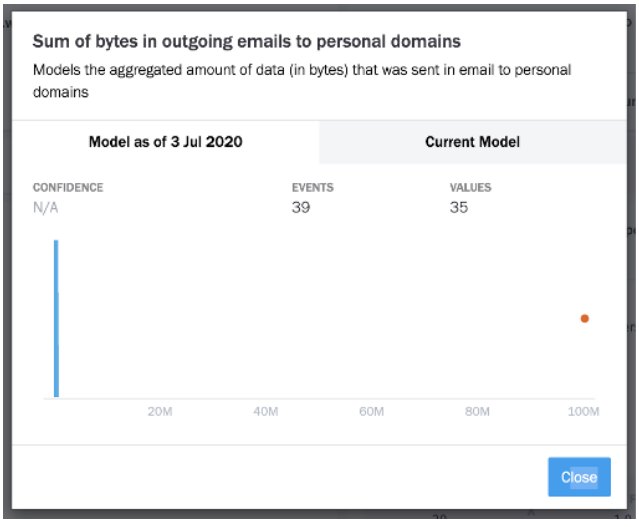

Figure 1 – This Data Insight Model shows the amount of data sent by a user to a personal domain. Exabeam alerts on anomalous amount of data sent, in this case close to 100 Megabytes.

Challenge 2: Visibility and Investigation

Security teams are unable to answer key investigation questions and ensure they do not miss a malicious data exfiltration attack.

Solution

Exabeam detects data breaches by analyzing all incoming DLP alerts and quantifying the level of risk associated with them. Analysts are presented a list of compromised 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 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 data exfiltration checklist to ensure their investigation is thorough and complete.

Benefit

Improve investigation quality and speed by enabling analysts to quickly answer key questions like "How was this user compromised?" or "Was data exfiltrated?"

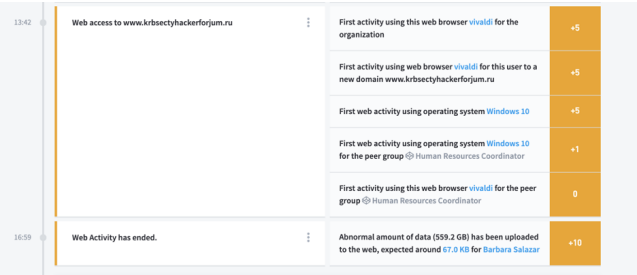

Figure 2 – This Smart Timeline event shows compromised insider Barbara Salazar uploading an anomalously large amount of data to the web.

Challenge 3: Response

Security teams responding to data exfiltration investigations spend hours or days coordinating a response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to data exfiltration incidents across your security stack (figure 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 data exfiltration incidents, such as contacting the user's manager or adding to a watchlist.

Benefit

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

Figure 3 – This data exfiltration playbook characterizes and escalates the incident, adds the compromised user to a watchlist while creating an external ticket, and sends a two-factor authentication push.

Use case content

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

Key Data Sources

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

Key Detection Rule Types

- Data exfiltration
- Data exfiltration via DNS
- Data exfiltration via email
- Data exfiltration via web upload
- Data exfiltration via email data

MITRE Technique & Tactic Coverage

- TA0010: Exfiltration
- T1567: Exfiltration over web service
- T1114: Email collection
- T11048: Exfiltration over alternative protocol

Incident checklist

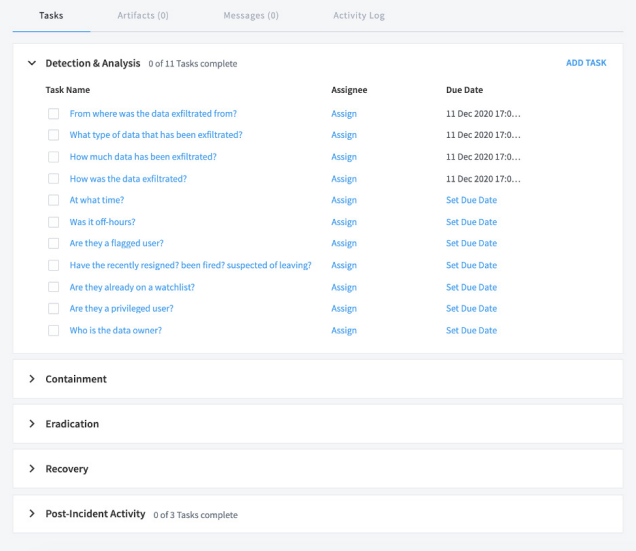

Figure 4 – The data exfiltration incident checklist prompts analysts to answer specific investigation questions and take containment actions.

Response Actions

- Contact user/manager/HR department via email
- Add user or asset to a watchlist
- Block, suspend, or impose restrictions on users involved in the incident
- Rotate credentials/reset/expire password
- Prompting for re-authentication via 2-factor/multi-factor authentication
- Isolate systems
- Remove user from group
- Clear user session
- Get user or asset info

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.