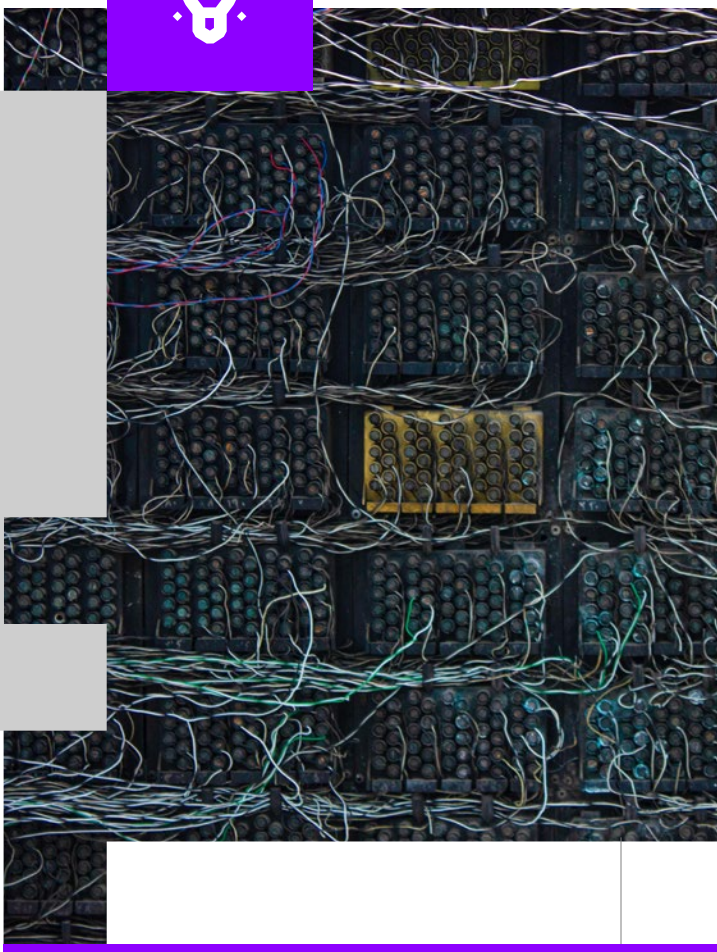
exabeam

Solution Brief

Data Access Abuse

Data access abuse is when a user abnormally accesses sensitive corporate data or resources. This activity serves as a leading indicator of data leakage.



Security and insider threat teams struggle to detect users accessing sensitive data

With the proliferation of various applications to collaborate across the business, employees have gained unprecedented access to sensitive data housed in file shares, content management systems, databases and more. According to industry research, in a study of several hundred organizations 17% of all sensitive files were accessible to every employee[1]. Testing access to and staging sensitive data is often the first step malicious insiders take before a data leak, which can mean huge financial and reputational costs to the organization.

Traditional security tools are unable to distinguish employees accessing sensitive data for normal business purposes apart from data access abuse such as snooping on customer information, sensitive information like medical records, and more. Further, these tools lack the ability to leverage context to identify the intent behind user activity.

A 2019 research study showed on average, every employee in an organization was found to have access to 17 million files and 1.21 million folders.[2]

[1] 2019 Varonis Data Risk Report
[2] 2019 Varonis Data Risk Report

Exabeam and data access abuse

Exabeam helps security and insider threat teams outsmart users abusing their access to data with the support of automation and use case content across the full analyst workflow, from detection to response. Instead of forcing analysts to connect the dots across data silos, Exabeam automatically assembles 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. Machine-created timelines allow security and insider threat teams to easily investigate event 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 cannot distinguish data access abuse by malicious insiders from legitimate access.

Solution

Exabeam ingests and analyzes key data sources to detect unusual access and activity such as sudden interest in an application, file, or database a user has not previously accessed. Exabeam behavioral models put anomalous activity like access to new or abnormal files or file sharing into the context of historic behavior, while dynamic peer grouping further shows when a user's activity deviates from their peers, clearly identifying a change in user intent from normal activity.

With context tags such as "Suspected Leavers" or "Intellectual Property", Exabeam allows analysts to quickly identify when an insider is behaving maliciously before an incident occurs.

Benefit

Strengthen security posture against malicious insiders by using behavior analytics to attribute activity back to a user and automatically identify data access abuse.

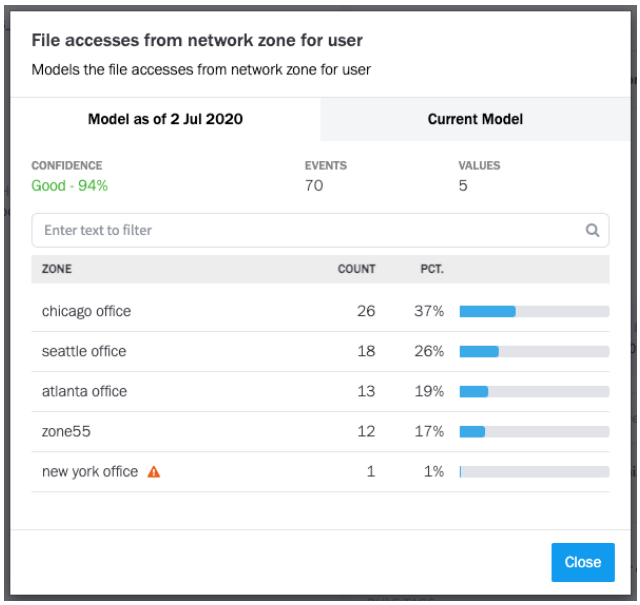


Figure 1 - This Data Insight Model shows the typical network zones that a user accesses their files from. Exabeam alerts on anomalous access, such as from the New York office.

Challenge 2: visibility and investigation

Analysts are overwhelmed with false positive alerts for data access, and struggle to complete comprehensive investigations for the events that pose the greatest risk.

Solution

Exabeam helps analysts focus their investigations on malicious insiders performing true data access abuse by quantifying the level of risk associated with all data access events. 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 with Exabeam Threat Hunter to find all activity associated with suspected leavers or access attempts for key intellectual property, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our data access abuse checklist to ensure their investigation is thorough and complete.

Benefit

Exabeam's ease of use allows analysts to streamline investigations, even for non-technical users. With Exabeam, analysts can answer key questions like "Has a user been flagged for recent resignation or firing" or "What data has the user recently accessed?"

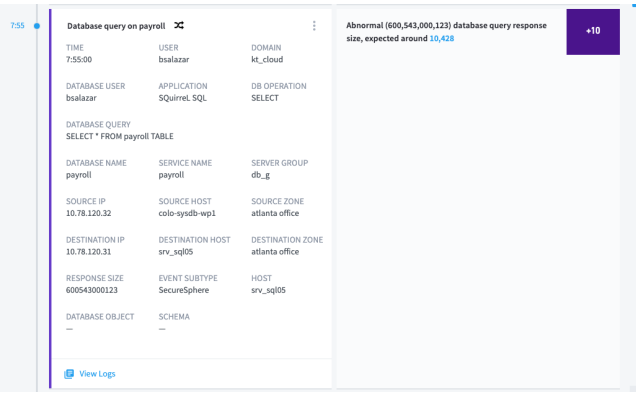


Figure 2 - This Smart Timeline event shows malicious insider Barbara Salazar performing a database query to access an unusually large amount of data.

Challenge 3: response

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

Solution

Exabeam playbooks orchestrate response to data access abuse incidents across your security stack. Pre-built integrations and customizable actions enable analysts to automate playbooks to respond to data access abuse incidents, 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.

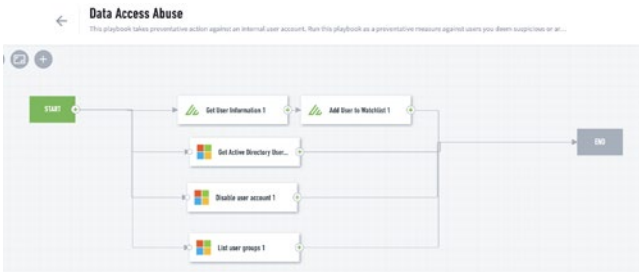


Figure 3 - This data access abuse playbook obtains contextual information about the malicious insider, adds them to a watchlist and disables their account.

Use case content

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

Key data sources

- Application activity
- Authentication and access management
- File access and activity
- Database access and activity

Key detection rule types

- Database activity monitoring
- Access to application data
- Access to file data

MITRE technique coverage

- TA0009: Collection
- T1005: Data from a local system
- T1213: Data from information repositories

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

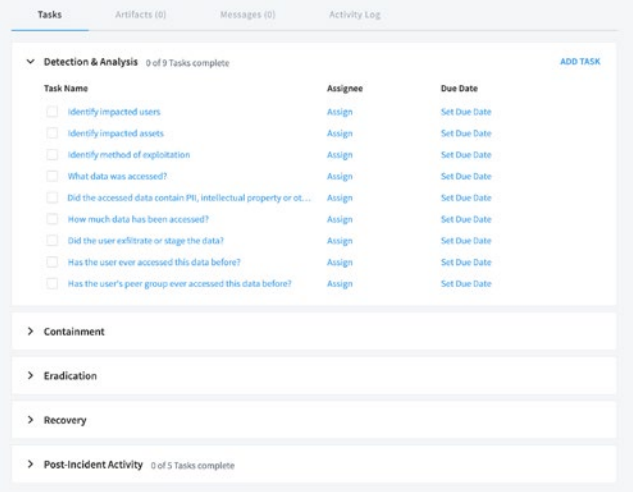


Figure 4 - The data access abuse incident checklist prompts analysts to answer specific investigation questions and take containment actions.

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**.

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

exabeam