exabeam

Solution Brief

Workforce Protection

Workforce protection identifies a user who is exhibiting signs of leaving an organization or communicating with a competitor

Employees may come and go. Make sure they do not harm the organization on the way out the door.

At-risk employees, aka "leavers," pose a significant threat to an organization as they may at any time decide to leave the organization with little to no advance notice. While most employees who decide to exit an organization will maintain their professional responsibilities through their final day, some will, unfortunately, use their last days with the organization to access, exfiltrate, or destroy critical business assets.

Today a person will likely have more than half a dozen employers during their careers, working on average four years per job. [1] These shorter tenures coupled with high employee turnover mean that employees no longer feel the same sense of loyalty toward an organization, increasing the threat of leavers.

Early identification and monitoring of users exhibiting signs of leaving an organization will help organizations mitigate the damage insiders who aim to cause monetary, reputation, or operational harm to the organization can inflict before exiting.

Today a person will likely have more than half a dozen employers during their careers, working on average four years per job.[1]

[1] US Department of Labor, Bureau of Labor Statistics, USDL-18-1500 (September 2020)

Exabeam and Workforce Protection

This workforce protection use case supports the detection, investigation, and response to an employee exhibiting signs of leaving an organization or communicating with a competitor via email, or searching for jobs, as well as sending files to a personal email address. Leveraging machine learning and user behavior analysis to baseline normal behavior for every user, device, and peer group, Exabeam automatically detects the abnormal behaviors that indicate an at-risk employee. Pre-packaged detection models do not require security engineers to create complex correlation rules. Exabeam helps security teams mitigate at-risk employees with automation coupled with purpose-built content across the full analyst workflow, from collection to response.

Key capabilities

Challenge 1: collection and detection
Traditional security tools do not detect behaviors indicative of at-risk employees as they largely focus on external threats making the risky assumption that their security controls protect them from a malicious insider.

Solution
Exabeam leverages machine learning and user behavior analysis to automatically detect abnormal behavior that could indicate an employee is at risk for leaving the organization and taking sensitive data. By learning and understanding the expected behavior for each user and their peer group, Exabeam can distinguish any abnormal behavior. Data Insights Models include additional details about anomalies.

The Exabeam solution models the large volume of events to identify unusual user behaviors such as a sudden user uptick in activity on job search sites, uploading data to job search sites, or sending sensitive data to their personal email addresses, alerting analysts in real-time.

Benefit
Analysts can quickly review instances of abnormal behavior, potentially preventing the at-risk employee from having the opportunity to complete their malicious actions.

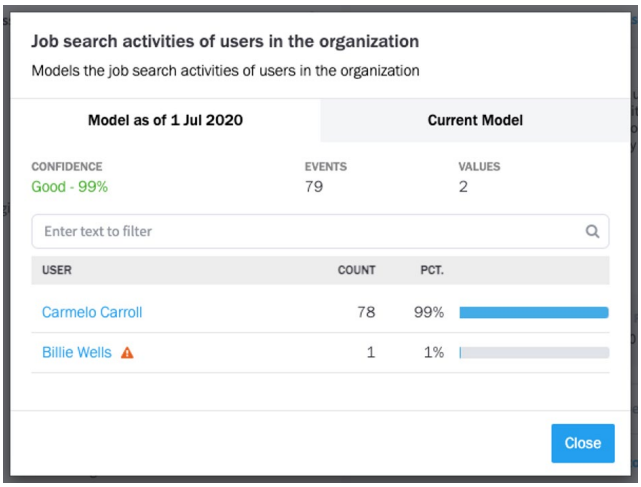

Figure 1 - This Data Insight Model Exabeam alerts on job search activity, comparing typical behavior for human resource employees compared to engineers.

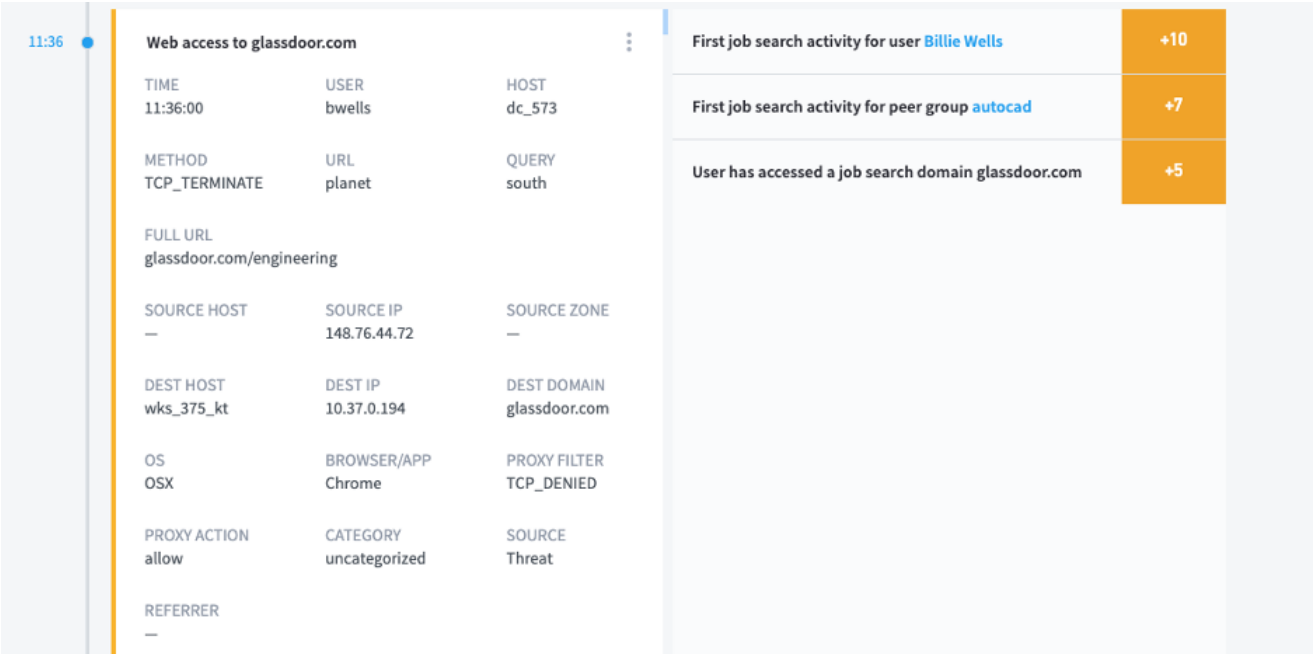

Figure 2 - This Smart Timeline event shows an instance of an at-risk employee, aka a leaver, indicating the user's job search activity.

Challenge 2: visibility and investigation

Security teams lack visibility and continuous monitoring capabilities for privileged accounts or assets.

Solution

Exabeam accelerates the investigation process by automatically creating Smart Timelines that automatically assemble and present a user's session of activities, including the lists of accounts and systems accessed, thereby eliminating tedious manual evidence gathering. Analysts can also create watchlists of suspected leavers, making it easy to monitor their behavior closely.

Benefit

Improve investigation quality and speed. Investigate at-risk users in minutes, not hours, without needing to write a single query.

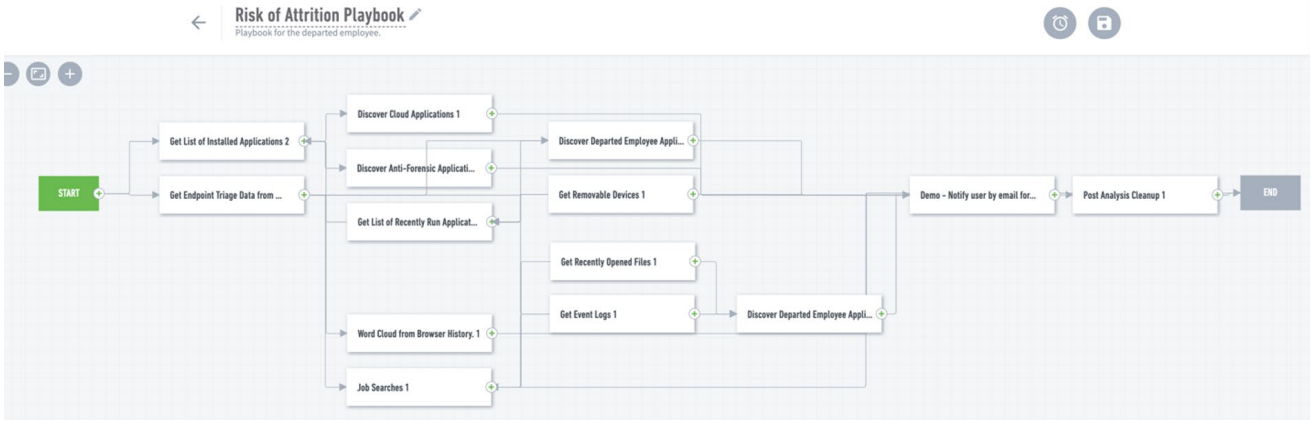

Figure 3 - This playbook analyzes recent employee activity, such as application usage, browser history, and job search activity as well as potential data exfiltration activity.

Challenge 3: response

Processes and procedures related to incident response are often not tailored to the specific threat and essentially entail manual processes.

Solution

Exabeam provides pre-defined checklists including recommended remediation steps and response playbooks for incident response teams.

Benefit

Resolve at-risk employee investigations faster.

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

- Authentication and access management
- Applications activity
- DLP alerts
- Operating system logs (e.g., UNIX/LINUX/OSX/Windows)

Key detection rule types

- Abnormal web user activity (job search)
- Abnormal office entry/exit activity
- Abnormal email activity (competition, personal email)
- Abnormal file access activity

Response actions

- Contact User/Manager/HR Department via email
- Add user to a watchlist
- Get application and file activity
- Identify removable devices (e.g. USB)
- Analyze browser history
- Identify job search activity

Incident checklist

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

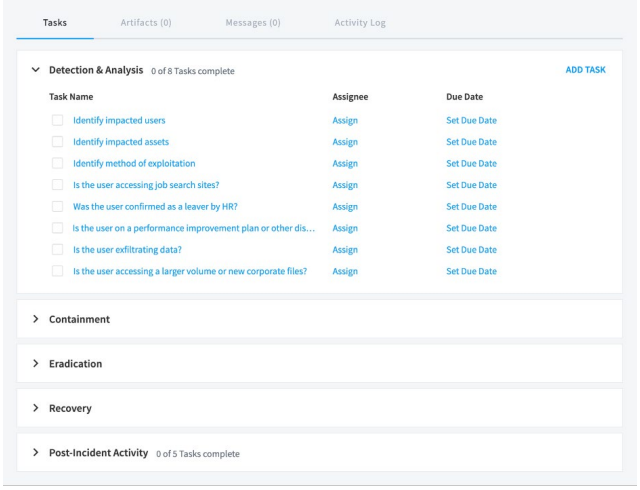

Figure 4 - The workforce protection checklist prompts analysts to answer specific investigation questions and take containment actions.

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