Abnormal Authentication
Using out-of-the-ordinary authentication actions to identify a malicious insider

This use case identifies users that are performing authentication or access activities outside of their typical behavior patterns.

Every employee now and then will log in to their corporate account at an unusual time. Whether it is an employee logging in late in the evening to finish up an important assignment or someone logging in from their vacation home, there are legitimate reasons an employee may access the corporate environment at odd hours from unusual locations. However, there are scenarios where an abnormal authentication, coupled with other actions, can indicate the presence of a malicious insider.

Considering the volume of authentications that occur daily it is simply impossible for any human to identify when abnormal equals malicious. Further, traditional security controls that exclusively use fixed rules to detect threats will never be able to discover when an employee’s abnormal authentication is a warning sign of an active threat. Considering there are users in every company with significant privileges, such as admins, when abnormal authentication occurs the ramifications for the company can be huge.

Exabeam helps security and insider threat teams outsmart users engaging in abnormal authentication and access 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 to create a comprehensive, reliable record of user activity, even if the underlying logs have been altered or deleted. 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).

While the average employee may have 10 to 15 different systems with different log-on credentials, that number skyrockets for admin employees.”

CSO Online
Key capabilities

Challenge 1: Collection and detection
Traditional security solutions are unable to detect when a user that is authenticating in an abnormal way is actually a malicious insider.

Solution
Exabeam ingests and analyzes key data sources to detect unusual activity such as attempting to logon from a different country for the first time. Exabeam behavioral models put anomalous activity such as login location, time, and means into historic behavior for an individual or their peers. With user labels such as “Suspected Leavers,” 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 identify abnormal user authentication and access.

Challenge 2: Visibility and investigation
Abnormal authentication and access largely go unnoticed by security teams due to the sheer volume of data associated with user authentications.

Solution
Our Smart Timelines automatically capture and assemble all activity data, including logon to a critical system and excessive distance traveled between logins, to name a few. Patented host-IP-user mapping attributes this activity back to a user, presented 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 abnormal authentication, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our abnormal authentication checklist to ensure their investigation is thorough and complete.

Benefit
Exabeam enables comprehensive and streamlined abnormal authentication investigations. With Exabeam, even non-technical analysts can answer key questions like “How many times did the user fail to login to the app?”

Figure 1: This data insight model shows two suspicious login records from Russia and Ukraine, not typical for this user.

Figure 2: This Smart Timeline event shows malicious insider Barbara Salazar performing an anomalous access attempt for the first time from Ukraine, indicating suspicious behavior.
Challenge 3: Response
Security and insider threat teams responding to abnormal authentication incidents spend a significant amount of time coordinating responses across multiple security tools.

Solution
Exabeam playbooks orchestrate the response to abnormal authentication and access incidents across your security stack. Pre-built integrations and customizable actions enable analysts to automate playbooks to respond to abnormal authentication, such as suspending a user or requiring two-factor authentication.

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

Figure 3: SOAR playbook showing steps for responding to abnormal authentication
Use case content

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

Key data sources
- Operating system logs (e.g. UNIX/LINUX/OSX/Windows)
- VPN activity
- Physical access logs
- Web activity

Key detection rule types
- Data access

MITRE Technique Coverage
- T1078 Valid Accounts
- T1133 External Remote Services

Incident checklist

Response actions
- Contact User/Manager/HR Department via email
- Add User to a watchlist
- Rotate account credentials
- Expire password
- Reset password
- Remove user from a group
- Send 2FA push
- Suspend user

Figure 1: This data insight model shows two suspicious login records from Russia and Ukraine, not typical for this 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 Operations 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.

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