exabeam

Solution Brief

Financial Services

A Behavior-Based Approach to Detecting Insider Threats and Compromised Credentials

Mitigate Cyber Security Risks, Improve Customer Experience and Overcome the Cyber Security Skills Gap

Faced with the rising expectations of customers and employees, the financial service sector is navigating a cultural shift, one which is driving new partnerships and innovations in customer and employee experience. For your security team, each innovation, each partnership, introduces more risk that they must account for. Yet they are already engaged in an uphill battle. The skills shortage combined with overly complex, manual processes are prohibiting them from quickly and accurately gathering the data points needed to identify and respond to malicious threats across the ecosystem.

Exabeam helps banks and financial service firms address today's cyber security challenges. Exabeam detects advanced threats including insider threats and compromised credentials to help you mitigate your cyber security risks, improve customer experience and retention and overcome the cyber security skills shortage by improving operational efficiency through automation.

> Exabeam is processing much faster and much more than any amount of staff could.
>
> **MUFG Bank**

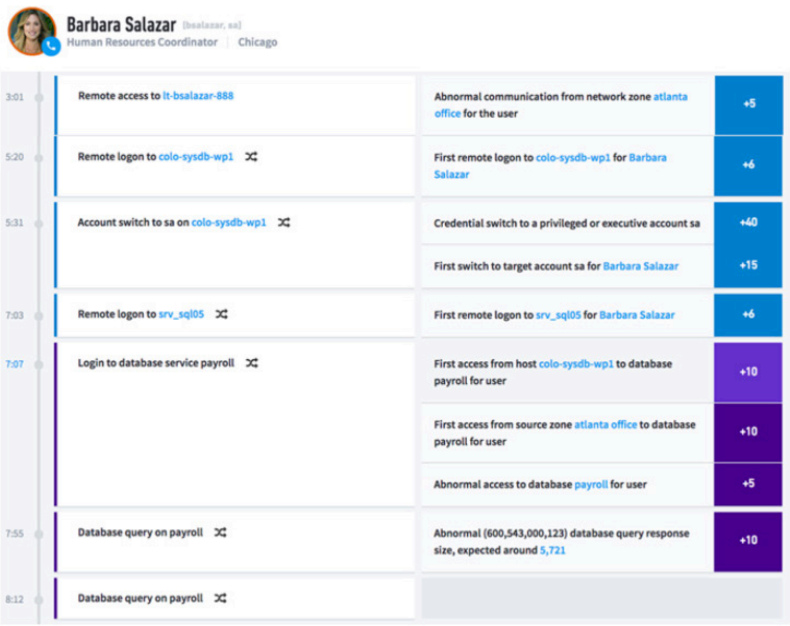
Mitigating Cyber Security Risk

A lack of visibility into insider activity and lateral movement of adversaries leaves banks and financial service firms vulnerable to attack, either from financially motivated insiders or external sources which can impact your reputation and bottom line.

Exabeam solutions are designed to accurately detect high risk, anomalous activity on your network, in SWIFT transactions and across your cloud instances through behavioral analytics. By analyzing user behavior, your security team is directed, in near real time, to instances of a potentially malicious employee activity, or indicators of compromise where an attacker, using stolen credentials is already within your network.

Security analysts view this analysis as an investigation attack chain or 'smart timeline' as shown in figure 1.

Exabeam Smart Timelines provide all the information your analysts need to perform rapid investigations and response. They include every action a user took, including SWIFT-related events, during a specific session, so your team can see what preceded the security alert and what the employee did next from the time they logged on to the time they logged off. Each action is represented in the timeline with a risk score and includes surrounding context such as if the alert maps to the MITRE ATT&CK framework.



Barbara Salazar [bsalazar, sa]
Human Resources Coordinator | Chicago

3:01	Remote access to lt-bsalazar-888	Abnormal communication from network zone atlanta office for the user	+5
5:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+6
5:31	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa	+40
		First switch to target account sa for Barbara Salazar	+15
7:03	Remote logon to srv_sql05	First remote logon to srv_sql05 for Barbara Salazar	+6
7:07	Login to database service payroll	First access from host colo-sysdb-wp1 to database payroll for user	+10
		First access from source zone atlanta office to database payroll for user	+10
		Abnormal access to database payroll for user	+5
7:55	Database query on payroll	Abnormal (600,543,000,123) database query response size, expected around 5,721	+10
8:12	Database query on payroll		

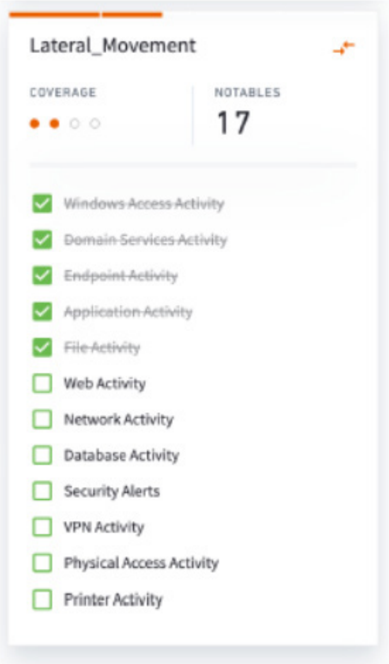
Figure 1 – Exabeam Smart Timelines. Each action taken by the user is attributed with a risk score, denoting how risky an individual's activity is to the organization.

Supporting Customer Experience and Retention

Ensuring that your systems and applications remain online is critical and to achieve that, visibility of threats is key.

With Exabeam you can be assured that rules, alerts, and searches are performed against a complete dataset, regardless of modern network evolution. Exabeam Cloud Connectors allow you to collect logs from over 45 cloud services such as AWS, Google, Microsoft 365, Salesforce and Zoom and ensure that you can centralize all of your activity data from your cloud instances with the rest of your IT and security infrastructure.

No relevant event is missed and automated Smart Timelines eliminate manual processes, enabling even your most junior team members to pinpoint anomalous behavior.



Lateral_Movement

COVERAGE ●●○○

NOTABLES 17

- ☑ ~~Windows Access Activity~~
- ☑ ~~Domain Services Activity~~
- ☑ ~~Endpoint Activity~~
- ☑ ~~Application Activity~~
- ☑ ~~File Activity~~
- □ Web Activity
- □ Network Activity
- □ Database Activity
- □ Security Alerts
- □ VPN Activity
- □ Physical Access Activity
- □ Printer Activity

Figure 2 – Exabeam provides guidance on which logs are needed to ensure you have coverage where it matters most.

Addressing the Skills Shortage

SIEM solutions are renowned for being resource intensive, requiring skilled analysts to run manual investigations that consume huge amounts of time and are prone to human error. Your ability to source, train and retain proficient talent to run such solutions is expensive and hard to fulfill in a market that already suffers from a significant skills gap.

Exabeam's modular solutions improve analyst productivity through natural language querying, context enhanced parsing and data presentation, providing security analysts the ability to quickly create new rules without the need for copious amounts of training.

Exabeam enables you to improve the operational efficiency of your team with automation throughout your workflow.

- Automated detection eliminates the need to maintain correlation rules; automated triage identifies notable users and assigns a risk score to each action taken;
- Automated triage identifies notable users and assigns a risk score to each action taken;
- Automated investigations, visualized through Smart Timelines, help analysts accurately detect insider threats faster;
- Automated response rounds out the workflow with pre-configured playbooks.

By automating the end-to-end workflow, Exabeam cuts the time spent on security tasks by 51% and further supports your compliance requirements by removing the potential for human error borne out of historically manual processes.

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.