



Lead Generation Campaign Playbook

Insider Threat

Help your customers shine a light on malicious insider threats with Exabeam.

This playbook provides the messaging and assets that Exabeam uses to promote our malicious insider use case package, as well as guidance for how to deploy this campaign and follow-up with responses. We invite our partners to leverage this content for educating clients on the risks of insider threat and how Exabeam helps shine a light on malicious insider threats. You are welcome to co-brand the assets with your company logo and information. Please contact channelmarketing@exabeam.com for any assistance.

Messaging

Malicious insiders hide in plain sight. Shine a light.

Exabeam allows security teams to detect malicious insiders that were previously difficult, or impossible, to find — with behavioral analytics that differentiates between normal and risky behavior, Exabeam sees the complete picture of a user's activity and quickly resolves incidents.

Target Personas

Primary Audience: Head of Insider Threat

- Director, Insider Threat Program
- Insider Threat Program Manager
- Head of Insider Trust Program
- VP, Insider Threat Monitoring
- Counter Insider Threat Office

Secondary Audience: Director of InfoSec / Security Leader

- Director of Information Security
- Director of IT security
- Director of cyber security

Campaign Assets

We have prepared the following assets for you to use with this campaign:

- Content hub landing page
- Promotion emails
- Social posts for LinkedIn and Twitter

Contact your Channel Account Manager or the Exabeam Channel Marketing team for the current Exabeam logo and any supporting images and graphics you wish to use for this campaign.

Campaign Guidance

Exabeam is using a content hub landing page at <https://pages.exabeam.com/ITC-Hub.html>. This is an Exabeam-hosted page. Please contact channelmarketing@exabeam.com when you are ready to launch the campaign so we can co-brand this page with your company's logo, and create custom tracking links so that we can track downloads of content from this page to your campaign.

We can do the same for the landing pages of the social media portion of this campaign. Contact the Channel Marketing team at Exabeam to create custom, trackable links for the assets promoted in the social posts provided below.

Exabeam recommends sending the emails to your target list on a weekly or bi-weekly basis. You should issue 1-2 posts per week for the social media campaign cadence.

Content Details

Content Hub landing page: <https://pages.exabeam.com/ITC-Hub.html>

Email messaging and examples:

Email #1 Headline/Subject: Automation can strengthen your insider threat program

Call to Action: Watch Now



2nd Headline: Actionable Tips to Get Ahead of Insider Threats

Body: According to the Verizon 2020 Data Breach Investigations Report, 30 percent of data breaches involved internal actors.

Detecting insider threats is difficult because the threat actor is using a trusted identity and has legitimate access to systems and data.

Watch our on-demand webinar to learn:

- Why insider threats often go undetected
- Key behavioral indicators that may identify an internal threat actor
- How automation can strengthen your insider threat program.



Automation can strengthen your insider threat program

WATCH NOW

Actionable Tips to Get Ahead of Insider Threats

According to the [Verizon 2020 Data Breach Investigations Report](#), 30 percent of data breaches involved internal actors.

Detecting insider threats is difficult because the threat actor is using a trusted identity and has legitimate access to systems and data.

Watch our on-demand webinar to learn:

- Why insider threats often go undetected
- Key behavioral indicators that may identify an internal threat actor
- How automation can strengthen your insider threat program

WATCH NOW

Contact us at: 1.844.392.2326 | [Request a Demo](#)

Email #2 Headline/Subject: Understanding Insider Threat Detection Tools

Call to Action: Read the Blog Now

2nd Headline: Three Tools that Help You Detect Insider Threats

Body: While an external attacker trying to gain access to the company network might raise redflags, an authorized contractor actively stealing information might not raise any suspicion at all. That's because the contractor has legitimate credentials and is already inside the firewall. Relying solely on standard security measures leaves your organization vulnerable to insider threats because you can't detect the attacker until after the incident has occurred.

Having tools and methods like employee monitoring, data loss prevention, and user and entity behavior analytics will help you detect insider threats that might otherwise go undetected.

Read our blog post, [Understanding Insider Threat Detection Tools](#), to ensure that you are investing in areas that defend against insider threats.

Understanding Insider Threat Detection Tools

[READ THE BLOG NOW](#)

Three Tools that Help You Detect Insider Threats

While an external attacker trying to gain access to the company network might raise redflags, an authorized contractor actively stealing information might not raise any suspicion at all. That's because the contractor has legitimate credentials and is already inside the firewall. Relying solely on standard security measures leaves your organization vulnerable to insider threats because you can't detect the attacker until after the incident has occurred.

Having tools and methods like employee monitoring, data loss prevention, and user and entity behavior analytics will help you detect insider threats that might otherwise go undetected.

Read our blog post, [Understanding Insider Threat Detection Tools](#), to ensure that you are investing in areas that defend against insider threats.

[READ THE BLOG NOW](#)

Contact us at: 1.844.392.2326 | [Request a Demo](#)





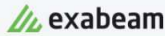
Email #3 Headline and Subject: Preventing Insider Threats with User and Entity Behavior Analytics

Call to Action: Read the White Paper Now

2nd Headline: Identify Suspicious Behavior Early

Body: Inappropriate data access and theft by current employees, contractors, or suppliers put your organization at risk. Early detection is difficult because the signals that point to a malicious insider may live in multiple places and piecing them together may require a level of expertise that few systems and no humans have.

Our white paper, Preventing Insider Threats with UEBA, explains how security teams can identify early patterns of risky behavior to prevent loss of sensitive data by using user and entity behavior analytics (UEBA) to identify insider threats.



Preventing Insider Threats with User and Entity Behavior Analytics

READ THE WHITE PAPER NOW

Identify Suspicious Behavior Early

Inappropriate data access and theft by current employees, contractors, or suppliers put your organization at risk. Early detection is difficult because the signals that point to a malicious insider may live in multiple places and piecing them together may require a level of expertise that few systems and no humans have.

Our white paper, [Preventing Insider Threats with UEBA](#), explains how security teams can identify early patterns of risky behavior to prevent loss of sensitive data by using user and entity behavior analytics (UEBA) to identify insider threats.

READ THE WHITE PAPER NOW

Contact us at: 1.844.392.2326 | [Request a Demo](#)

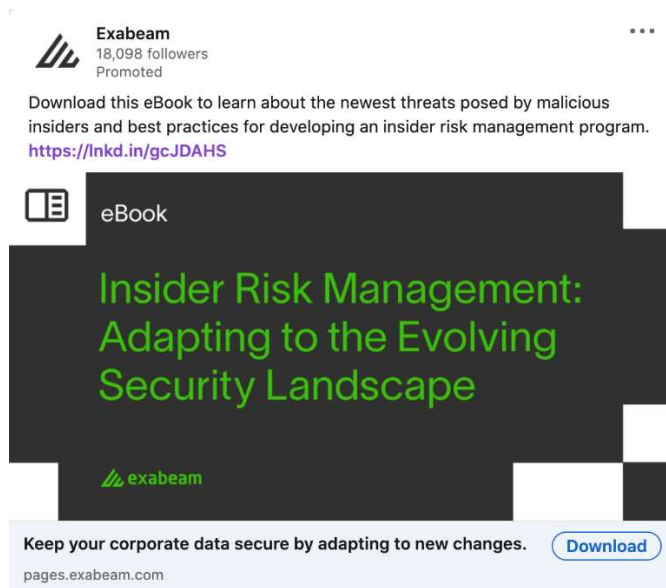
Social media messaging and examples

Asset: Ebook: Insider Risk Management

Text: Intro text (600 limit) Insider Risk Management: Adapting to the Evolving Security Landscape

Headline (200 limit): Download this eBook to learn about the newest threats posed by malicious insiders and best practices for developing an insider risk management program.

Landing Page URL: <https://pages.exabeam.com/plp-2020-Gartner-Market-Guide-for-Insider-Risk-Management-Solutions.html>



Asset: Blog to PDF: Insider Threat Programs: 8 Tips to Build a Winning Program

Text: Insider Threat Programs: 8 Tips to Build a Winning Program

Download this guide for eight essential tips to building your insider threat program, including how to determine critical assets, how to perform background checks, and how to build insider threat use cases.

Landing Page URL: https://pages.exabeam.com/plp_Insider_Threat_Programs.html




Asset: Blog to PDF - Understanding Insider Threat Detection Tools


Text: Understanding Insider Threat Detection Tools

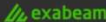
Download this guide to learn about three tools and methods that can help you detect insider threats, including employee monitoring, data loss prevention, and user and entity behavior analytics.

Landing Page URL: https://pages.exabeam.com/plp_understanding_insider_threat_detection_tools.html

**Exabeam**
18,098 followers
Promoted

Download this guide to learn about three tools and methods that can help you detect insider threats, including employee monitoring, data loss prevention, and user and entity behavior analytics. https://lnkd.in/gzn_m8q

Guide

**Understanding Insider Threat Detection Tools**


Insider threats are much harder to detect and prevent compared to threats from outside the organization. [Download](#)

Asset: Webinar - Detecting Insider Threats: Actionable Tips


Text: Detecting Insider Threats: Actionable Tips to Get Ahead of Insiders

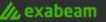
Watch this on-demand webinar to learn key behavioral indicators that help identify internal threat actors, tools that can be used to automate insider threat detection, and how automation can help organizations improve their insider threat programs.

Landing Page URL: <https://www.exabeam.com/library/detecting-insider-threats-actionable-tips-to-get-ahead-of-insiders/>

**Exabeam**
18,098 followers
Promoted

Watch this on-demand webinar to learn key behavioral indicators that help identify internal threat actors, tools that can be used to automate insider threat detection, and how automation can help organizations improve their insider threat programs. <https://lnkd.in/gwVs7u6>

On-Demand Webinar

**Detecting Insider Threats: Actionable Tips**

Detecting Insider Threats: Actionable Tips to Get Ahead of Insiders [Register](#)

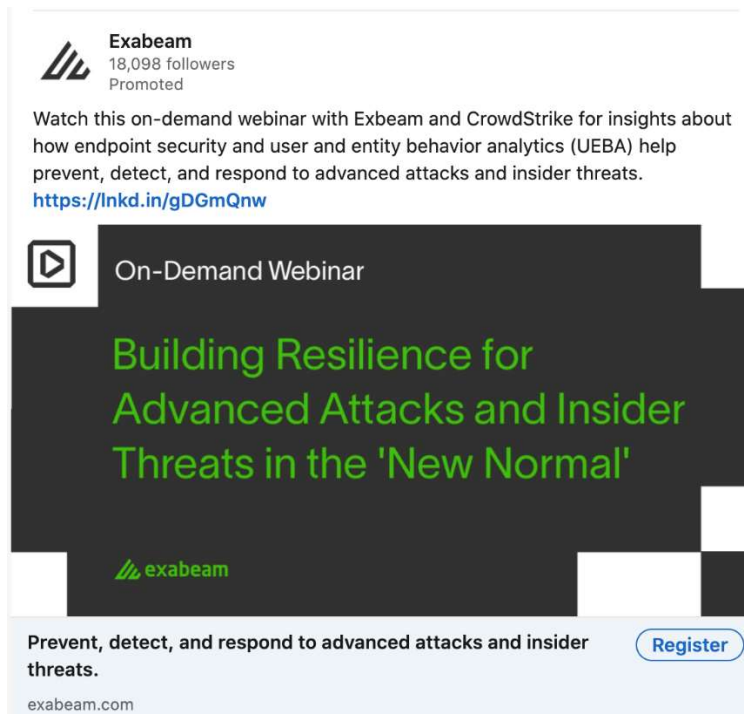
exabeam.com

Asset: Webinar with CrowdStrike - Building Resilience for Advanced Attacks and Insider Threats in the 'New Normal'

Text: Build Resilience for Advanced Attacks and Insider Threat

Watch this on-demand webinar with Exbeam and CrowdStrike for insights about how endpoint security and user and entity behavior analytics (UEBA) help prevent, detect, and respond to advanced attacks and insider threats.

Landing Page URL: <https://www.exabeam.com/library/building-resilience-for-advanced-attacks-and-insider-threats-in-the-new-normal/>



The image is a screenshot of a LinkedIn post from the company Exbeam. At the top left is the Exbeam logo, followed by the text 'Exbeam', '18,098 followers', and 'Promoted'. Below this is a short description of the webinar: 'Watch this on-demand webinar with Exbeam and CrowdStrike for insights about how endpoint security and user and entity behavior analytics (UEBA) help prevent, detect, and respond to advanced attacks and insider threats.' A link is provided: 'https://lnkd.in/gDGmQnw'. The main part of the post is a video player thumbnail. It has a play button icon in the top left corner and the text 'On-Demand Webinar' in the top right. The center of the thumbnail features the title 'Building Resilience for Advanced Attacks and Insider Threats in the 'New Normal'' in green text on a dark background. The Exbeam logo is in the bottom left of the thumbnail. Below the thumbnail, there is a light blue banner with the text 'Prevent, detect, and respond to advanced attacks and insider threats.' on the left and a 'Register' button on the right. The URL 'exabeam.com' is at the bottom left of the banner.

Exbeam
18,098 followers
Promoted

Watch this on-demand webinar with Exbeam and CrowdStrike for insights about how endpoint security and user and entity behavior analytics (UEBA) help prevent, detect, and respond to advanced attacks and insider threats.
<https://lnkd.in/gDGmQnw>

On-Demand Webinar

Building Resilience for
Advanced Attacks and Insider
Threats in the 'New Normal'

exabeam

Prevent, detect, and respond to advanced attacks and insider threats.

Register

exabeam.com

Sales Outreach

Here are some questions and talking points for your sales teams to use when following-up with leads and prospects who respond to the campaign.

Conversation Starters:

1. What problem caused you to contact us about Exbeam?
2. What are the biggest gaps in your security posture or programs?
3. Are there problems with your investigation or response processes today?
4. Was your inquiry driven by the security team, or another department like compliance, legal, or HR?
5. Do you have any of the following business initiatives:
 - a. Log Management/SIEM
 - b. Security initiatives like Insider Threat or DLP
 - c. Automation (in prog)

Listen for:

- Alert overload across multiple tools
- Unhappiness with current SIEM (performance, pricing, etc)
- Lack of visibility into data and threats
- Inability to address or find all threats
- Continued breaches even with security tools
- SOC staffing issues?

Types of Insider Threat

- **Compromised Insider:** Victim of an external actor who has gained access to their device and/or user credentials via phishing, malware, or other common threats
- **Malicious/deliberate insider:** An employee/contractor who knowingly looks to steal information or disrupt operations
- **Negligent Insider:** An employee who does not follow proper IT procedure

Exabeam can prevent Insider Threats with:

- User and Entity Behavior Analytics (UEBA) based detection for complex modern threats, including credential-based attacks, insider threats, and ransomware
- Pre-constructed Smart Timelines to automate triage and investigation, and makes proactive analysis faster and easier.
- Single pane of glass for detection, investigation, and response for complex modern threats, including credential-based attacks, insider threats, and ransomware. Helps avoid Swivel Chair IR.
- Intelligent security alert prioritization to ensure analysts can easily find the alerts which require the most attention.
- Threat Hunt using behavior modeling, including MITRE ATT&CK technique mapping

Launch Your Campaign

To get started, please contact your Exabeam Channel Account Manager or reach out to channelmarketing@exabeam.com. Happy prospecting!