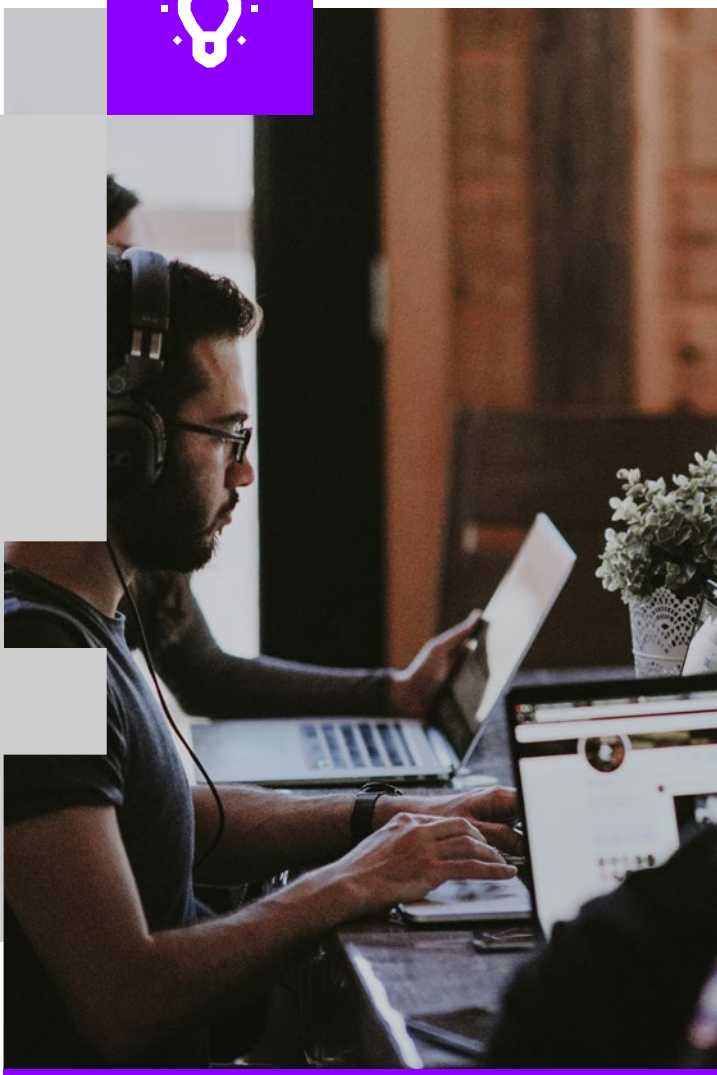
exabeam

Solution Brief

Exabeam Threat Detection Investigation and Response Use Case Packages

Achieve successful security outcomes with prescriptive, threat-centric solutions



Poorly Defined Processes Reduce SOC Effectiveness

Organizations are increasingly making significant investments in their security tools to stay one step ahead of increasingly sophisticated adversaries. However, many have not aligned their technologies with robust threat detection, investigation and response (TDIR) processes, which are often poorly defined or inconsistent. As a result, security operations centers (SOCs) find that different analysts develop different approaches to the same problem, creating gaps in detecting threats and subpar security posture.

Furthermore, the security tools used by SOCs, like traditional SIEMs, are often designed for complex functionality and robust customization, rather than delivering outcomes. This forces security teams to spend large amounts of time on implementation, customizing their tools to solve problems specific to their organization. As a result, security programs and projects suffer from long delays in time to value, without measurable increases in coverage against different threats.

> We were able to quickly turn on the 'out of the box' use cases and integrate with our systems and processes, improving our detect and response capabilities.
>
> **Jennifer Shields**
> Vice President of Information Technology, Procter & Gamble

USE CASE CONTENT

TDIR use case packages - an outcomes based approach to security

Exabeam TDIR Use Case Packages provide prescriptive, end-to-end workflows and prepackaged content that enable organizations to easily automate detection, investigation and response to compromised insiders, malicious insiders and external threats. Pre-packaged detection logic and investigation and response tools configured for each threat-centric use case are ready to deploy day one. With TDIR Use Case Packages, organizations can increase operational efficiency, accelerate time to value, and improve their security posture over time.

Follow Prescriptive Solutions For The Full Threat Lifecycle

Standardize TDIR workflows from start to finish with prescriptive use case packages. Exabeam guides security teams through each step of their workflows to address specific threat-centric use cases. For each type of threat, we recommend data and context sources needed to enable detection content that is mapped to MITRE techniques, provide a guided investigation and response checklist, and offer response actions for an analyst to take to effectively investigate and remediate an incident. With automated tools and analysis for the entire workflow, security teams can achieve greater consistency, faster time to resolution, and better utilization of resources.

Leverage Pre-Packaged Content For Common Threats

Stop spending endless cycles configuring and customizing your security tools. Security teams can take advantage of Exabeam's pre-packaged content including detection models and rules, pre-configured watchlists, prebuilt incident checklists and response playbook templates for over twenty threats. By avoiding lengthy implementations with pre-packaged content, organizations realize faster time to value and reduce total cost of ownership from their investment.

Onboard Modular TDIR Use Case Packages

The traditional approach to optimizing a SOC often involves automating each stage of the workflow—data collection, detection, triage, investigation, response—for all possible threat types at once. This approach is inefficient because it amounts to boiling the ocean of threats at each stage before moving forward to the next. Exabeam enables you to easily and successfully implement and operationalize one threat-centric use case from collection to response, then move on to successive use cases. As a result, organizations can improve their security posture by onboarding additional use cases over time, reducing the likelihood of a security breach.

Improve coverage for key threats

Exabeam TDIR Use Case Packages provide all the content and tooling SOCs need to address common and advanced threats including:

External Threats - Protect Against Prevalent Attack Vectors

Attack vectors like phishing or malware provide adversaries ample opportunities to breach a company's defenses. With the sheer volume of attacks on a daily basis, SOCs must be prepared to properly detect, investigate, and respond at a moment's notice.

Compromised Insiders - Identify Credential Based Attacks

By hiding under the cover of valid credentials, attackers can gain access to critical assets and sensitive information without raising suspicion. Worse still, security teams that build complex correlation rules and dashboards to find these bad actors are often overwhelmed with noisy false positive alerts.

Malicious Insiders - Detect Threats From The Inside

With the rise of remote workforces, collaboration tools and file sharing, employees hold unprecedented levels of access to valuable assets and information across an organization. However, this access is rife with abuse, particularly by disgruntled or departing employees.

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