exabeam

Data Sheet

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.

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.

> 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, VP of Information Technology**
> **Procter & Gamble**

Use Case Content

Collection

- Predefined data sources
- 500+ integrations
- Cloud connectors

Detection

- Behavior based threat detection
- Watchlists
- MITRE mapping

Triage

- Alert prioritization
- Context gathering and enrichment
- Auto case creation

Investigation

- Prebuilt incident timelines for all entities
- Automated Q&A

Response

- Turnkey playbooks
- Custom incident types
- Incident checklists

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. With Automated Incident Diagnosis, Exabeam analyzes abnormal behavior to automatically diagnose the type of threat associated with an incident and classifies it by use case. Based on the use case identified, we prescribe tailored investigation and remediation steps in checklists and playbooks, and further enrich the case with key context and evidence, allowing analysts to achieve more efficient investigations, greater consistency and faster time to resolution. For each use case, we also recommend data and context sources needed to enable detection content.

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.

External Threats

- Malware
- Phishing
- Ransomware
- Brute Force Attack
- Cryptomining

Compromised Insiders

- Compromised Credentials
- Lateral Movement
- Privilege Escalation
- Privileged Activity
- Account Manipulation
- Data Exfiltration
- Evasion

Malicious Insiders

- Data Leak
- Privilege Abuse
- Data Access Abuse
- Audit Tampering
- Destruction of Data
- Physical Security
- Workforce Protection
- Abnormal Access and Authentication

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools — including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond.

For more information, visit exabeam.com

exabeam