exabeam

Get Started with Threat Detection, Investigation, and Response (TDIR) Use Case Packages

Exabeam SOC Platform - Cloud-Delivered Release Only

Publication date November 18, 2021

Exabeam
1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!

Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

Table of Contents

1. Threat Detection, Investigation, and Response (TDIR) Use Case Packages

A powerful, prescriptive, outcome-based approach to using your Exabeam product.

Threat Detection, Investigation, and Response (TDIR) Use Case Packages is an outcome-based framework for using your Exabeam product. It describes what threat you can detect, investigate, hunt, and respond to using a prescribed end-to-end workflow.

For example, if you use Exabeam to tackle a phishing threat, the *Phishing* use case defines specific rules and models to help detect anomalous email activity, a *Phishing* incident type to ensure you gather all necessary phishing-related evidence, specific tasks to investigate a phishing incident, and a *Phishing* turnkey playbook to quickly analyze and respond to the phishing threat.

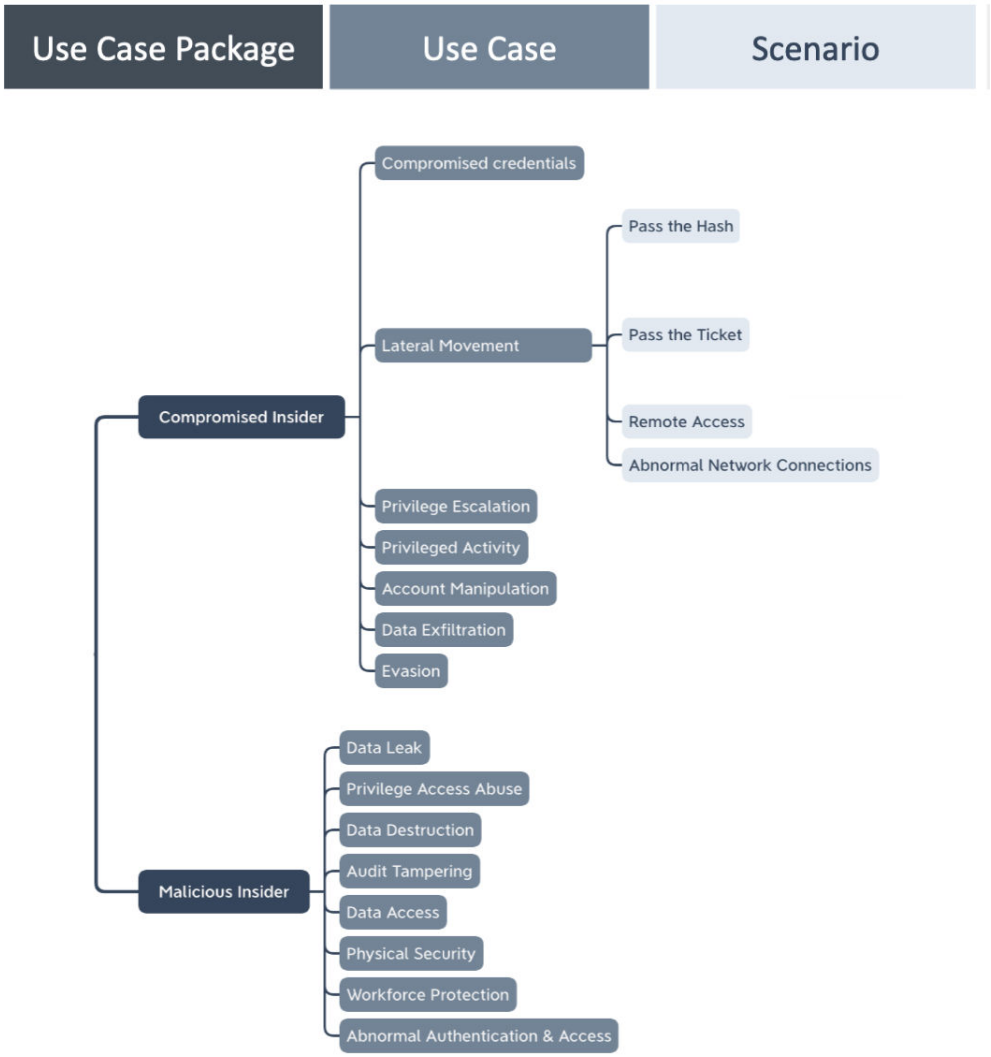
The TDIR Use Case Packages framework integrates expert knowledge and recommendations into every step of the process. You use standardized, repeatable workflows to address a given threat type, so you quickly define your security operations and ensure that you have consistent, effective, and measurable outcomes.

The TDIR Use Case Packages framework organizes threats in a hierarchy so you can break them down from a general type, like *Compromised Insiders*, to a specific scenario, like *pass the hash*. There are three use case packages: Compromised Insiders, Malicious Insiders, and External Threats. You can access certain use case packages based on your Exabeam license. To learn more, contact your technical account manager.

2. Threat Detection, Investigation, and Response (TDIR) Use Case Packages Hierarchy

Understand the overall structure of the TDIR Use Case Package framework: use case packages, use cases, and scenarios.

The TDIR Use Case Packages framework organizes threats in a hierarchy, from a broad category down to specific detection insights:



- **Use Case Package** – A collection of related use cases; for example, *Compromised Insiders*.
- **Use Case** – A specific problem a set of functionalities across Exabeam products are aligned to solve; for example, *Lateral Movement*.
- **Scenario** – A high-value detection insight within a use case; for example, *Pass the Hash*.

In most cases, you tackle a specific use case, but you may find it helpful to break down use cases into scenarios.

2.1. Use Case Packages

A use case package is a collection of related use cases.

In the Threat Detection, Investigation, and Response (TDIR) Use Packages hierarchy, use case packages are a top-level classification that organizes and groups use cases into three general types:

- Compromised Insiders
- Malicious Insiders
- External Threats

For example, the *Compromised Insiders* use case package contains the *Compromised Credentials*, *Lateral Movement*, *Privilege Escalation*, *Privileged Activity*, *Account Manipulation*, and other use cases.

2.2. Use Cases

A use case is a specific problem Exabeam products are aligned to solve.

A use case represents a threat you can detect, investigate, hunt, and respond to using a set of functionalities across Exabeam products. These functionalities ensure that you deliver measurable outcomes using repeatable procedures.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Packages hierarchy, all use cases are categorized under a use case package: *Compromised Insiders*, *Malicious Insiders*, or *External Threats*. For example, the *Lateral Movement* use case is categorized under the *Compromised Insiders* use case package. Some use cases further break down into scenarios.

2.3. Scenarios

A scenario is a high-value detection insight within a use case.

A scenario typically describes an Indicator of Compromise (IOC) or a method an attacker uses to create the threat the use case describes.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Packages hierarchy, each scenario falls under a specific use case. For example, the *Lateral Movement* use case contains the *Abnormal Network Connection*, *Abnormal Remote Access*, *Pass the Hash*, and *Pass the Ticket* scenarios.

Not all use cases contain scenarios; for example, the *External Threats* use cases don't have scenarios.

3. Compromised Insiders Use Case Package

The *Compromised Insiders* use case package categorizes all use cases related to compromised insiders.

The *Compromised Insiders* use case package is a top-level classification that groups all use cases in which someone outside your organization exploits credentials to steal data or sabotage your operations.

Compromised Insiders use cases include:

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

3.1. Compromised Credentials Use Case

Learn about the *Compromised Credentials* use case and what Exabeam functionalities are aligned to solve it.

The *Compromised Credentials* use case describes when an attacker disguises as a valid user with legitimate access and uses stolen credentials to access your system.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Packages hierarchy, the *Compromised Credentials* use case is categorized under the *Compromised Insiders* use case package. It contains specific scenarios, including:

- Abnormal Application Access
- Abnormal Authentication and Access
- Abnormal Database Access
- Abnormal File Access
- Abnormal VPN Access
- Abnormal Web Access
- Compromised Asset
- Compromised Service Account
- Credential Theft

In Case Manager, use the out-of-the-box *Compromised Credentials* incident type to standardize incident fields, phases, and tasks for compromised credentials incidents.

View more information what compromised credentials are and how it happens on the Exabeam Community.

3.1.1. ABNORMAL APPLICATION ACCESS SCENARIO

Learn about the *Compromised Credentials* *Abnormal Application Access* scenario.

The *Abnormal Application Access* scenario describes when an attacker compromises valid credentials and accesses an application. You can often identify this scenario when someone's application access and interaction patterns change.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Packages hierarchy, the *Abnormal Application Access* scenario falls under the *Compromised Credentials* use case.

4. External Threats Use Case Package

The *External Threats* use case package categorizes all uses cases related to external threats.

The *External Threats* use case package is a top-level classification that groups all use cases in which an adversary deceives users, accesses valid credentials, or exploits corporate assets.

External Threats use cases include:

- Malware
- Phishing DOCUMENTATION COMING SOON
- Ransomware DOCUMENTATION COMING SOON
- Brute Force Attack DOCUMENTATION COMING SOON
- Cryptomining DOCUMENTATION COMING SOON

4.1. Malware Use Case

Learn about the *Malware* use case and what Exabeam functionalities are aligned to solve it.

The *Malware* use case describes when an attacker develops malicious programs or code to access your system without authorization or damage your data or system.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Package hierarchy, the *Malware* use case falls under the *External Threats* use case package. It doesn't contain any scenarios.

In Case Manager, use the out-of-the-box *Malware* incident type to standardize incident fields, phases, and tasks for malware incidents.

In Incident Responder , use the *Malware* turnkey playbook to analyze suspicious files and detonate potential malware.

View more information about what malware is and how it happens on the Exabeam Community.

5. Malicious Insiders Use Case Package

The *Malicious Insiders* use case package categorizes all use cases related to malicious insiders.

The *Malicious Insiders* use case package is a top-level classification that groups all use cases in which someone in your organization intentionally sabotages or steals data for personal reasons or financial gain.

Malicious Insiders use cases include:

- Data Leak
- Privileged Abuse DOCUMENTATION COMING SOON
- Data Access Abuse DOCUMENTATION COMING SOON
- Audit Tampering DOCUMENTATION COMING SOON
- Destruction of Data DOCUMENTATION COMING SOON
- Physical Security DOCUMENTATION COMING SOON
- Workforce Protection DOCUMENTATION COMING SOON
- Abnormal Authentication and Access DOCUMENTATION COMING SOON

5.1. Data Leak Use Case

Learn about the *Data Leak* use case and what Exabeam functionalities are aligned to solve it.

The *Data Leak* use case describes when an employee, partner, or contractor illicitly transfers data outside your organization.

In the Threat Detection, Investigation, and Response (TDIR) Use Case Package hierarchy, the *Data Leak* use case falls under the *Malicious Insiders* use case package. It contains specific scenarios, including:

- Data Leak
- Data Leak via Email
- Data Leak via Printer
- Data Leak via Removable Device
- Data Leak via Web

In Case Manager, use the out-of-the-box *Data Leak* incident type to standardize incident fields, phases, and tasks for data leak incidents.