exabeam

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

Exabeam Security Operations 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. Prerequisites For Configuring Exabeam Threat Detection, Investigation & Response (TDIR) Use Case Packages 5
2. Configure Compromised Insiders Use Cases 6
    2.1. Configure The Compromised Credentials Use Case 6
        2.1.1. Collect 6
        2.1.2. Detect 7
        2.1.3. Investigate 8
        2.1.4. Respond 11
        2.1.5. Report 11
    2.2. Configure The Lateral Movement Use Case 11
        2.2.1. Collect 12
        2.2.2. Detect 12
        2.2.3. Investigate 13
        2.2.4. Respond 16
        2.2.5. Report 16
3. Configure External Threats Use Cases 18
4. Configure Malicious Insiders Use Cases 19

Prerequisites for Configuring Exabeam Threat Detection, Investigation & Response (TDIR) Use Case Packages

Before you configure any TDIR Use Case Package, ensure that you have the log sources you need.

Contact Exabeam Customer Success to help you onboard and validate the log sources needed to implement a given Exabeam use case. To contact Exabeam Customer Success, open a case in the Exabeam Community.

2. Configure Compromised Insiders Use Cases

Quickly get started with implementing *Compromised Insiders* use cases in your Exabeam environment.

Review everything you need to configure so you can investigate eight *Compromised Insiders* use cases:

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

2.1. Configure the Compromised Credentials Use Case

Quickly get started with implementing the *Compromised Credentials* use case in your environment. Ensure that you collect the right data, set up investigation tools, enable response mechanisms, and import relevant Data Lake reports.

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. When you investigate a use case, you might follow an end-to-end workflow that looks like:

- **Collect** – Ensure that you bring in the correct logs for the use case and that all fields populate.
- **Detect** – Use out-of-the-box rules and models to identify suspicious activity.
- **Investigate** – Ask important questions about the data from log sources, rules, and models.
- **Respond** – Isolate, neutralize, eliminate, and mitigate any threats you find.
- **Report** – Gather all the evidence in a report so you can share your investigation with others or use for compliance purposes.

Let's configure everything you need to successfully follow each stage of this end-to-end investigation workflow.

2.1.1. COLLECT

Collect the data needed to investigate the *Compromised Credentials* use case and ensure all context tables are populated correctly.

- Ensure that you contacted Exabeam Customer Success and they helped you onboard and validate the log sources needed to implement the *Compromised Credentials* use case.
- Ensure that you have specific out-of-the-box context tables:
  - web_malicious_categories
  - is_publicemail_domain

- workstations
- sourcecode_file_extensions
- user_is_executive
- user_is_privileged
- is_ip_threat
- user_employee_type
- user_is_executive
- is_dynamicdns_domain
- is_ranked_domain
- reputation_domains

- Create custom context tables for domain controllers, critical systems, and network zones.
- Ensure that users and assets have the correct labels based on the context tables. For example, if a user is in the user_is_privileged context table, navigate to the user's profile to verify they have the **privileged** label.

2.1.2. DETECT

Ensure you have all mechanisms in place, like rules, models, watchlists, and Threat Hunter™ searches, to successfully identify suspicious activity.

2.1.2.1. Rules and models

Validate out-of-the-box rules and models to ensure you accurately detect anomalous activity.

- Import the latest content packages on the Exabeam Community. These content packages contain the latest rules and models, which aren't available to install in Content Updates settings. You must download them from the Exabeam Community, then import them.
- Ensure that related rules and models are triggering correctly.

2.1.2.2. Threat Hunter searches

To quickly search for events that indicate someone's credentials have been compromised, create and save the suggested Threat Hunter search queries.

Threat Hunter search	Search criteria
Service accounts with interactive logons	• **Rule** – SL-UH-I, SL-UA-F-VPN • **User label** – service_account • **Date** – Last 7 days
User's first VPN connection	• **Rule** – AE-UA-F-VPN, AE-GA-F-VPN, AE-GA-F-VPN-new • **Activity type** – VPN • **Date** – Last 7 days
User, peer group, or organization's first activity from a geolocation	• **Rule** – APP-UAgC-F, WEB-OC-F, UA-GC-F, UA-GC-new, UA-OC-F, UA-UC-F, FA-OC-F, FA-GC-F, UA-OC-F, UA-GC-F • **Date** – Last 7 days

Threat Hunter search	Search criteria
First activity from a new user agent	• **Rule** – APP-UAg-F, APP-UAgC-F • **Date** – Last 7 dayss
Executive users who logged in from a new geolocation	• **Rule** – APP-UAgC-F, WEB-OC-F, UA-GC-F, UA-GC-new, UA-OC-F, UA-UC-F, FA-OC-F, FA-GC-F • **User label** – Executive • **Date** – Last 7 days
First process launched across your organization	• **Rule** – EPA-OP-F • **Date** – Last 7 days
First access to a domain identified as being generated from a domain generation algorithm (DGA)	• **Rule** – WEB-UD-DGA-F • **Date** – Last 7 days
VPN connections from multiple WAN IPs in the last 30 days	• **Rule** – VPN30 • **Date** – Last 30 days
Failed logins to an asset that a user has not previously accessed	• **Rule** – SEQ-UH-07 • **Date** – Last 7 days
Abnormal number of denied web activity events for a user	• **Rule** – WEB-UBlock, WEB-USequenceSize-Denied • **Date** – Last 7 days

2.1.2.3. Configure Settings to Search for Data Lake Logs in Advanced Analytics

If you have an on-premises deployment, ensure that you configure certain Advanced Analytics settings so you can search for Data Lake logs from a Smart Timelines™ event.

If you have a cloud-delivered product offering, ensure that you configure Data Lake as a log source.

2.1.3. INVESTIGATE

Ensure you have the tools you need, like tasks and incident types, to investigate the evidence you collect from log sources, rules, and models.

2.1.3.1. Case Manager Incident Type

In Case Manager, ensure that you have the out-of-the-box *Compromised Credentials* incident type, or create one if it isn't available out-of-the-box in your Exabeam product offering. Ensure the incident type has all corresponding incident fields.

2.1.3.2. Case Manager Tasks and Phases

In Case Manager, define a clear response plan to ensure everyone across your organization responds to a *Compromised Credentials* incident consistently. Under each phase, prescribe the relevant tasks for investigating, containing, and remediating a *Comprised Credentials* incident.

The out-of-the-box *Compromised Credentials* incident type comes with suggested phases and tasks. If you don't have the out-of-the-box *Compromised Credentials* incident type, create the following suggested phases and tasks for your custom *Compromised Credentials* incident type.

Phase: Detection & Analysis

1. **Task name** – Review normal activity for the user

Task instruction:

- Validate if the user recently changed roles or is involved in a new project.
- Validate if the user is on vacation or part of a separation event.

2. **Task name** – Identify the anomalous activity
   Task instruction:
   - Determine if the user accessed resources from unexpected locations. Look for anomalous geolocation activity.
   - Determine if the user accessed resources they don't normally access.
   - Determine if the user generated activity at times that are not normal for them (User agent/ browser/etc.)
   - Determine if the user accessed applications or functions within applications they don't normally access or use.
   - Determine how many systems were accessed.
   - Determine whether the user's peers emulate any similar activity.
   - Determine if the user has any additional anomalous activity; for example, accessed new applications, triggered security alerts, or exfiltrated data.
3. **Task name** – Validate logs were sent to the SIEM
   Task instruction – Validate that logs for the impacted users or systems were sent to the SIEM or system of record.
4. **Task name** – Assess impacted systems
   Task instruction – Determine if the potentially impacted systems are critical business or infrastructure systems.
5. **Task name** – Proactively monitor impacted users and systems
   Task instruction – Add the systems and users to a watchlist to proactively monitor them.

Phase: Containment

1. **Task name** – Communicate the incident to the SOC Manager
   Task instruction:
   - If needed, inform your SOC Manager of the incident and include the incident's expected start and end date.
   - Determine whether additional team members or teams, like HR, Legal, or Physical Security, must get involved.
2. **Task name** – Determine adequate response measures to contain the threat
   Task instruction:
   - If appropriate, disable the user account.
   - Quarantine affected systems.
   - Force multi-factor authentication (MFA) re-authentication or step-up authentication to the affected user accounts.

Phase: Eradication

1. **Task name** – Take measures to preserve logs for impacted systems and users
   Task instruction:
   - Retrieve and preserve all Data Lake logs associated with the user from the expected start to the present.
   - Upload the Data Lake logs to the incident.
   - To determine if there's possible nefarious intent, obtain a forensic image of the system or isolate the physical machine from the network.
2. **Task name** – Reset all affected credentials
   Task instruction – Reset all affected credentials in all systems.
3. **Task name** – Re-issue authentication tokens for affected users
4. **Task name** – Identify root cause
   Task instruction:
   - Determine whether a social engineering or phishing email was involved.
   - If a social engineering or phishing email was involved, determine how the team can increase user awareness for and better monitor similar occurrences.
5. **Task name** – Determine if there was a technical exploit
   Task instruction – If there was a technical exploit, ensure you put a patch or workaround in place.
6. **Task name** – Remediate
   Task instruction – Manually remove remnants; for example, files, registry keys, and autostart services OR re-image the impacted systems using the latest enterprise image and updated software patches.

Phase: Recovery

1. **Task name** – Restore functional state of affected assets
   Task instruction:
   - After you re-image or clean the impacted systems, return the machines to users if it's safe to do so.
   - Ensure you restore the affected applications or network operations.
2. **Task name** – Notify affected users
   Task instruction – Notify affected users that they were involved in a security incident and their credentials were reset.
3. **Task name** – Implement relevant global security measures
   Task instruction – To prevent a similar incident from reoccurring, implement any additional security measures.

Phase: Post-Incident Activity

1. **Task name** – Update documentation
   Task instruction:
   - Ensure the incident contains documentation of all relevant events and actions taken.
   - Identify methods to improve the team's response to future incidents.

2. **Task name** – Hold post-mortem meeting
   Task instruction:
   - Hold a meeting with the team. Review the incident and lessons learned.
   - Document and track administrative and technical gaps identified during the incident.

2.1.3.3. Case Manager Incident Email

To collaborate on an incident with people across your organization, ensure that you configure incident email.

2.1.4. RESPOND

Enable response mechanisms you need to isolate, neutralize, eliminate, and mitigate any threats you find.

In Incident Responder, create triggers for all turnkey playbooks.

2.1.5. REPORT

To share your investigation with others or for compliance purposes, ensure you have the relevant out-of-the-box Data Lake reports:

- File Alert Activity
- Insecure Authentication Attempts
- IPS and IDS Alert Activity
- Object Access Summary
- Office 365 Summary
- Security Alert Summary - Impacted Hosts
- Security Alert Summary - Origin Hosts
- Security Alert Summary - Users
- Successful Application Logon Activity
- Successful Database Logon Activity
- User Account Lockout Activity
- Vendor Authentication Activity

2.2. Configure the Lateral Movement Use Case

Quickly get started with implementing the Lateral Movement use case in your environment. Ensure that you collect the right data, set up investigation tools, enable response mechanisms, and import relevant Data Lake reports.

The lateral movement use case describes when an attacker moves through a network and jumps between devices to search for sensitive data and other high-value assets. When you investigate a use case, you might follow an end-to-end workflow that looks like:

- **Collect** – Ensure that you bring in the correct logs for the use case and that all fields populate.
- **Detect** – Use out-of-the-box rules and models to identify suspicious activity.
- **Investigate** – Ask important questions about the data from log sources, rules, and models.
- **Respond** – Isolate, neutralize, eliminate, and mitigate any threats you find.
- **Report** – Gather all the evidence in a report so you can share your investigation with others or use for compliance purposes.

Let's configure everything you need to successfully follow each stage of this end-to-end investigation workflow.

2.2.1. COLLECT

Collect the data needed to investigate the *Lateral Movement* use case and ensure all context tables are populated correctly.

- Ensure that you contacted Exabeam Customer Success and they helped you onboard and validate the log sources needed to implement the *Compromised Credentials* use case.
- Ensure you have the *workstation* out-of-the-box context table.
- Create a custom context table for critical systems.
- Ensure that users and assets have the correct labels based on the context tables. For example, if a user is in the user_is_privileged context table, navigate to the user's profile to verify they have the **privileged** label.

2.2.2. DETECT

Ensure you have all mechanisms in place, like rules, models, watchlists, and Threat Hunter™ searches, to successfully identify suspicious activity.

2.2.2.1. Rules and models

Validate out-of-the-box rules and models to ensure you accurately detect anomalous activity.

- Import the latest content packages on the Exabeam Community. These content packages contain the latest rules and models, which aren't available to install in Content Updates settings. You must download them from the Exabeam Community, then import them.
- Ensure that related rules and models are triggering correctly.

2.2.2.2. Threat Hunter searches

To quickly search for events that may indicate someone is moving through your network and searching for valuable data, create and save the suggested Threat Hunter search queries.

Threat Hunter search	Search criteria
A user or asset exhibiting MITRE Lateral Movement or Remote Services Tactics, Techniques, and Procedures (TTPs)	• **Rule tags** – Remote Services, External Remote Services, Exploitation of Remote Services, Lateral Movement, Pass the Hash, Pass the Ticket • **Date** – Last 7 days
A user or asset exhibiting MITRE Proxy TTP	• **Rule tags** – Connection Proxy, Multi-hop Proxy, Standard Application Layer Protocol • **Date** – Last 7 days
A user who failed to log in to a system they have never successfully logged into	• **Rule** – SEQ-UH-07 • **Date** – Last 7 days
A user who triggered a third-party security alert and accessed systems for the first time	• **Activity type** – Security Alerts • **Rule** – A-AL-DhU-F, AL-HLocU-F, LL-UH-F, RA-F-F-CS, RA-GH-F-new, RA-UH-F, RL-GH-F-new • **Date** – Last 7 days
A user who accessed more hosts than is normal for the entire organization	• **Rule** – AL-OHcount, RA-OHcount • **Date** – Last 7 days
Abnormal communication between hosts	• **Rule** – A-RLA-AA-A, F-RLA-AA-F • **Date** – Last 7 days
A user who connected to a known malicious or host	• **Rule** – A-NET-TI-H-Inbound, A-NET-TI-H-Outbound, A-NET-TI-IP-Inbound, A-NET-TI-IP-Outbound, A-NETF-TI-H-Outbound, A-NETF-TI-IP-Outbound • **Date** – Last 7 days
A new user who has accessed a critical host	• **Rule** – RA-UH-CS-NC, NEW-USER-F, RA-F-A-CS, RA-F-F-CS • **Date** – Last 7 days

Configure Settings to Search for Data Lake Logs in Advanced Analytics

If you have an on-premises deployment, ensure that you configure certain Advanced Analytics settings so you can search for Data Lake logs from a Smart Timelines™ event.

If you have a cloud-delivered product offering, ensure that you configure Data Lake as a log source.

2.2.3. INVESTIGATE

Ensure you have the tools you need, like tasks and incident types, to investigate the evidence you collect from log sources, rules, and models.

2.2.3.1. Case Manager Incident Type

In Case Manager, ensure that you have the out-of-the-box *Compromised Credentials* incident type, or create one if it isn't available out-of-the-box in your Exabeam version. Ensure the incident type has all corresponding incident fields.

2.2.3.2. Case Manager Tasks and Phases

In Case Manager, define a clear response plan to ensure everyone across your organization responds to a *Lateral Movement* incident consistently. Under each phase, prescribe the relevant tasks for investigating, containing, and remediating a *Lateral Movement* incident.

The out-of-the-box *Lateral Movement* incident type comes with suggested phases and tasks. If you don't have the out-of-the-box *Lateral Movement* incident type, create the following suggested phases and tasks for your custom *Lateral Movement* incident type.

Phase: Detection & Analysis

1. **Task name** – Review normal activity for the user
   Task instruction:
   - Validate if the user recently changed roles or is involved in a new project.
   - Validate if the user is on vacation or part of a separation event.

2. **Task name** – Identify the anomalous activity
   Task instruction:
   - Determine if the user accessed resources from unexpected locations. Look for anomalous geolocation activity.
   - Determine if the user accessed resources they don't normally access.
   - Determine if the user generated activity at times that are not normal for them (User agent/ browser/etc.)
   - Determine if the user accessed applications or functions within applications they don't normally access or use.
   - Determine how many systems were accessed.
   - Determine whether the user's peers emulate any similar activity.
   - Determine if the user has any additional anomalous activity; for example, accessed new applications, triggered security alerts, or exfiltrated data.

3. **Task name** – Validate logs were sent to the SIEM
   Task instruction – Validate that logs for the impacted users or systems were sent to the SIEM or system of record.
4. **Task name** – Assess impacted systems
   Task instruction – Determine if the potentially impacted systems are critical business or infrastructure systems.
5. **Task name** – Proactively monitor impacted users and systems
   Task instruction – Add the systems and users to a watchlist to proactively monitor them.

Phase: Containment

1. **Task name** – Communicate the incident to the SOC Manager
   Task instruction:
   - If needed, inform your SOC Manager of the incident and include the incident's expected start and end date.
   - Determine whether additional team members or teams, like HR, Legal, or Physical Security, must get involved.

2. **Task name** – Determine adequate response measures to contain the threat
   Task instruction:
   - If appropriate, disable the user account.

- Quarantine affected systems.
- Force multi-factor authentication (MFA) re-authentication or step-up authentication to the affected user accounts.

Phase: Eradication

1. **Task name** – Take measures to preserve logs for impacted systems and users
   Task instruction:
   - Retrieve and preserve all Data Lake logs associated with the user from the expected start to the present.
   - Upload the Data Lake logs to the incident.
   - To determine if there's possible nefarious intent, obtain a forensic image of the system or isolate the physical machine from the network.
2. **Task name** – Reset all affected credentials
   Task instruction – Reset all affected credentials in all systems.
3. **Task name** – Re-issue authentication tokens for affected users
4. **Task name** – Identify root cause
   Task instruction:
   - Determine whether a social engineering or phishing email was involved.
   - If a social engineering or phishing email was involved, determine how the team can increase user awareness for and better monitor similar occurrences.
5. **Task name** – Determine if there was a technical exploit
   Task instruction – If there was a technical exploit, ensure you put a patch or workaround in place.
6. **Task name** – Remediate
   Task instruction – Manually remove remnants; for example, files, registry keys, and autostart services OR re-image the impacted systems using the latest enterprise image and updated software patches.

Phase: Recovery

1. **Task name** – Restore functional state of affected assets
   Task instruction:
   - After you re-image or clean the impacted systems, return the machines to users if it's safe to do so.
   - Ensure you restore the affected applications or network operations.
2. **Task name** – Notify affected users
   Task instruction – Notify affected users that they were involved in a security incident and their credentials were reset.
3. **Task name** – Implement relevant global security measures
   Task instruction – To prevent a similar incident from reoccurring, implement any additional security measures.

Phase: Post-Incident Activity

1. **Task name** – Update documentation
   Task instruction:
   - Ensure the incident contains documentation of all relevant events and actions taken.
   - Identify methods to improve the team's response to future incidents.

2. **Task name** – Hold post-mortem meeting
   Task instruction:
   - Hold a meeting with the team. Review the incident and lessons learned.
   - Document and track administrative and technical gaps identified during the incident.

2.2.3.3. Case Manager Incident Email

To collaborate on an incident with people across your organization, ensure that you configure incident email.

2.2.4. RESPOND

Enable response mechanisms you need to isolate, neutralize, eliminate, and mitigate any threats you find.

In Incident Responder, create triggers for all turnkey playbooks.

2.2.5. REPORT

To share your investigation with others or for compliance purposes, ensure you have the relevant out-of-the-box Data Lake reports:

- Authenticated User Accounts on Hosts
- Cisco Firepower Summary
- Failed Host Logon Attempts by Users
- Failed VPN Login Attempts and Remote Session Timeouts
- Firewall ActivityFirewall and Router Configurations
- Firewall and Router Device Interfaces
- Microsoft Windows Overview
- Netflow Traffic Summary
- Network Applications by Volume of Traffic
- Network Device Login - Authenticated Users
- Ports by Volume of TrafficProtocols by Network Traffic
- Remote Session Overview
- System Critical and Error Activity Summary

- Top Allowed and Denied Destinations - Inbound
- Top Allowed and Denied Destinations - Outbound
- Top Allowed and Denied Sources - Inbound
- Top Conversations by Volume of Traffic
- Top Destinations by Volume of Traffic
- Top Sources by Volume of Traffic
- User Account Lockout Activity

3. Configure External Threats Use Cases

Quickly get started with implementing *External Threats* use cases in your Exabeam environment.

Review everything you need to configure so you can investigate five *External Threats* use cases:

- Configure the Phishing Use Case DOCUMENTATION COMING SOON
- Configure the Malware Use Case DOCUMENTATION COMING SOON
- Configure the Ransomware Use Case DOCUMENTATION COMING SOON
- Configure the Brute Force Attack Use Case DOCUMENTATION COMING SOON

4. Configure Malicious Insiders Use Cases

Quickly get started with implementing *Malicious Insiders* use cases in your Exabeam environment.

Review everything you need to configure so you can investigate eight *Malicious Insiders* use cases:

- Configure the Data Leak Use Case DOCUMENTATION COMING SOON
- Configure the Privilege Access Abuse Use Case DOCUMENTATION COMING SOON
- Configure the Data Access Abuse Use Case DOCUMENTATION COMING SOON
- Configure the Audit Tampering Use Case DOCUMENTATION COMING SOON
- Configure the Destruction of Data Use Case DOCUMENTATION COMING SOON
- Configure the Physical Security Use Case DOCUMENTATION COMING SOON
- Configure the Workforce Protection Use Case DOCUMENTATION COMING SOON
- Configure the Abnormal Authentication and Access Use Case DOCUMENTATION COMING SOON