

v4.00



# Threat Hunting with Advanced Analytics

EDU-2170 : Module 5

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

1





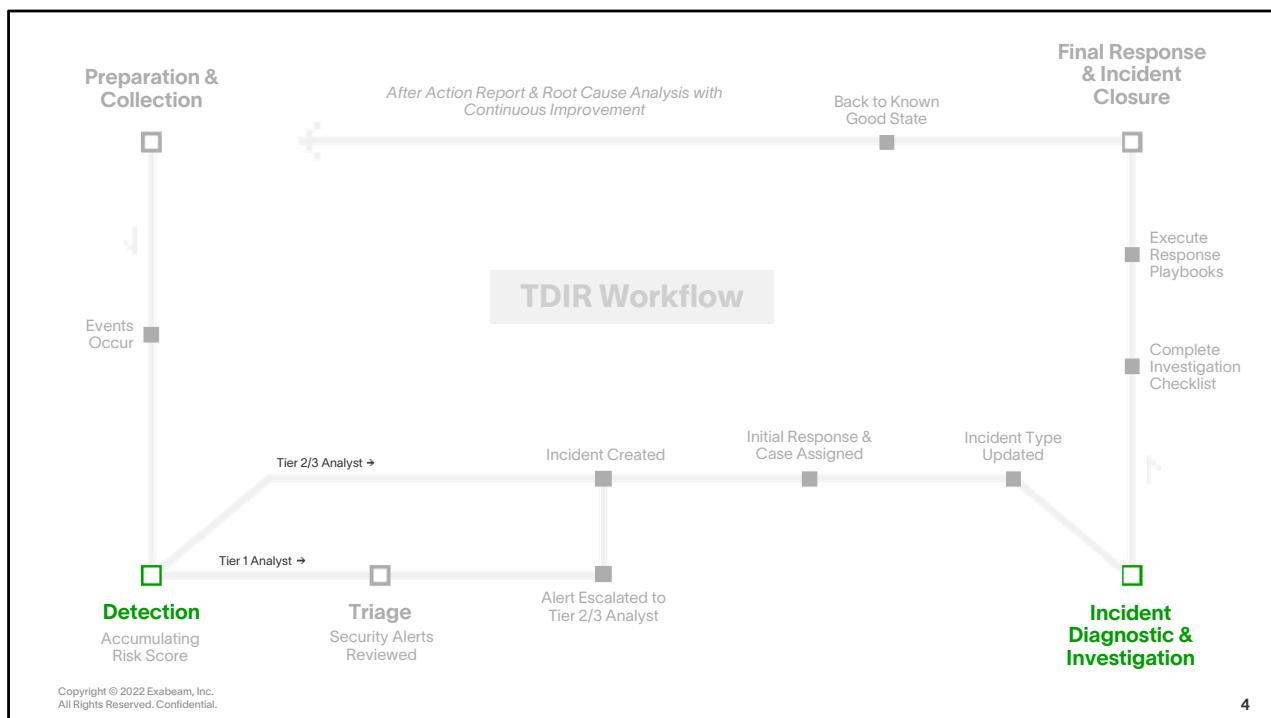
**What value is there in understanding tactics and techniques of malicious entities?**



## Lesson

At the end of this lesson, you will be able to:

- 1. Navigate the MITRE ATT&CK® Framework and extract information useful to threat hunting**
2. Use Threat Hunter to unearth hidden threats
3. Use Data Insights to identify trends and threats
4. Create and utilize watchlists to monitor risky users and entities



## Three Questions About MITRE ATT&CK®

Who is MITRE?

What is the meaning  
of ATT&CK?

What is the purpose  
of ATT&CK?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

5

### Student Notes

#### MITRE is an organization

ATT&CK is a free, open, globally accessible knowledge base of adversary behaviors, an encyclopedia of real-world observations of what adversaries have been seen to do

Techniques: 266 as of Aug 2019" (source: <https://medium.com/mitre-attack/automating-mapping-to-attack-tram-1bb1b44bda76>)

Coming in 2020 (source: <https://medium.com/mitre-attack/2020-attack-roadmap-4820d30b38ba>)

Sub-techniques will be added. Sub-techniques will help fix the unevenness across the knowledge base as some techniques are broad in definition and some specific

Examples:

Lateral movement: Remote Services will be broken out into Remote Desktop, SMB/Windows Admin Shares, Distributed Component Object Model, etc.

Credential Access: Brute Force will be broken out into Password Guessing, Password Cracking, Password Spraying, Credential Stuffing

Adversary behavior model for network infrastructure devices including routers, switches and firewalls Threat Report ATT&CK Mapper (TRAM) (beta released Dec 2019)

Provides a streamlined approach for analyzing reports and extracting ATT&CK techniques

Goal: reduce analyst fatigue, increase ATT&CK coverage, improve accuracy of threat intelligence mappings

Map ATT&CK to NIST 800.53 v4

Goal: better support efforts to identify controls that mitigate relevant threats and identify capability gap

#### More Information

<https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/the-philosophy-of-attck>

<https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer>

**Tactics**

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and

**Techniques**

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may perform shell escapes or exploit vulnerabilities in an application with the setuid or setgid bits to get code running in a different user's context. On Linux or macOS, when the setuid or setgid bits are set for an application, the application

**What** attackers are trying to achieve

**How** they accomplish those steps or goals

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

6

## Student Notes

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cyberattacks.

- Tactics – the *why* of an attack, e.g., Privilege Escalation, Defense Evasion
- Techniques – the *how* of an attack, e.g., Access Token Manipulation, Clear Command History
- Common Knowledge – the documented use of tactics and techniques by adversaries
- Matrices – the visual organization of Tactics and Techniques for Enterprise, Mobile et al
- Groups – sets of related intrusion activity that are tracked by a common name in the security community, e.g., APT3 (Gothic Panda from China)

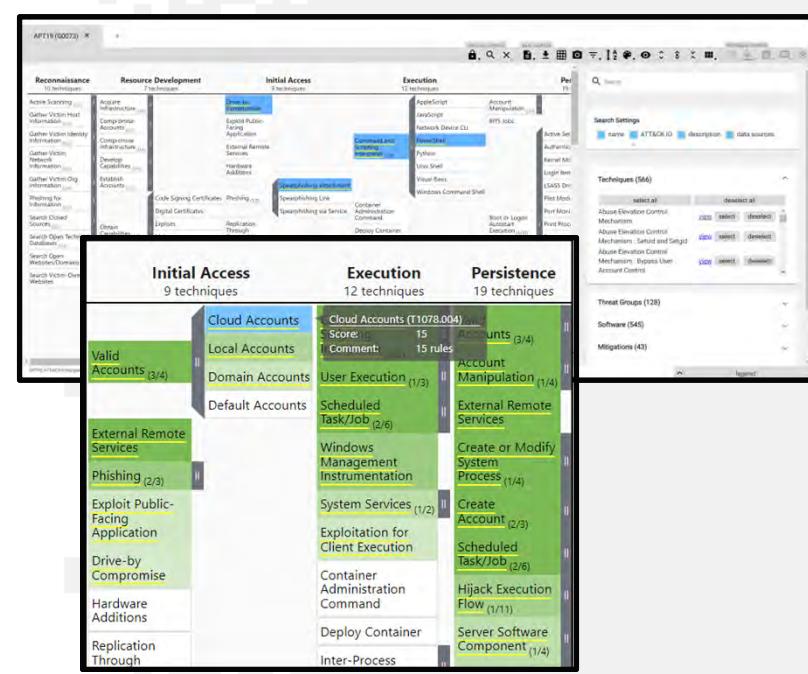
## More Information

[https://www.exabeam.com/wp-content/uploads/2020/01/Exabeam\\_Whitepaper\\_MitreAttack.pdf](https://www.exabeam.com/wp-content/uploads/2020/01/Exabeam_Whitepaper_MitreAttack.pdf)  
<https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer/>

# Demo



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



## Exabeam detection requires having the right logs

The diagram illustrates the connection between MITRE ATT&CK data and Exabeam log sources. It features two main sections:

- ATT&CK® identifier:** A screenshot of the MITRE ATT&CK interface for T1003.001, showing details like "Tactic: Credential Access" and "Platforms: Windows". A green arrow points from this section to the "Log Sources" section.
- Log Sources:** A screenshot of the Exabeam interface showing a table of log sources. One row is highlighted, showing "Domain: Enterprise", "ID: T1148", "Name: Abuse Elevation Control Mechanisms", and "Severity: Severe". Another green arrow points from the "ATT&CK® identifier" section to this table.

**Source: MITRE**

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

8

### Student Notes

MITRE articles often indicate the needed log sources for detection and prevention.

## Seeing ATT&CK® in the Smart Timeline when searching

The screenshot shows the Exabeam Advanced Analytics interface with a Smart Timeline for Julietta Donaldson. The timeline displays three events:

- 16:04 Remote logon (info\_term\_22)
- 16:04 Account switch (jdonaldson-admin on dc\_151)
- 16:13 Created zeroctf's account (cal-ad-003)

Annotations with green lines point from these events to their corresponding MITRE TTP labels and techniques:

- Tactic: Lateral Movement  
Technique: Remote Desktop Protocol
- Tactic: Privilege Escalation  
Technique: Valid Accounts
- Tactic: Persistence  
Technique: Account Creation

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

9

## Student Notes

MITRE TTPs appear in the Smart Timeline multiple ways.

Seeing ATT&CK® in the Smart Timeline in event details

**Tactic: Execution  
Technique: User Execution**

**Tactic: Defense Evasion  
Technique: File Deletion**

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

10

Web access to dlknknlnkkaa.zoomer.cn			First time a user is accessing an internet IP address in this country China +5	
TIME 11:20:00	USER fweber	HOST bc_srv_1	DESCRIPTION First time a user is accessing an internet IP address in this country RULE TAGS <b>User Execution</b>	
METHOD GET	URL /dl/	QUERY t=barbarian.jar	CONFIDENCE 94%	
FULL URL dlknknlnkkaa.zoomer.cn				

Process execution: vssadmin.exe			A Suspicious command that deletes shadow copies has been executed for process vssadmin.exe +20	
TIME 11:32:00	USER fweber	HOST -	DESCRIPTION Exabeam detected a suspicious command that was issued to delete shadow copies on the system, this activity is common for malware/ransomware to hide its tracks and therefore this event is notable RULE TAGS <b>File Deletion</b>	
SENSOR ID kt_ampe_srv_1	DIRECTORY c:\windows\system	PROCESS vssadmin.exe 32		
COMMAND LINE delete shadows /force:			IMPHASH e23dd973e1444684 eb36365def1fc74	

### Student Notes

Event details in the Smart Timeline may be tagged with MITRE TTP labels.

Example 1: Tactic: Execution; Technique: User Execution

Example 2: Tactic: Defense Evasion; Technique: File Deletion

## Mapping Exabeam Model to ATT&CK® Techniques

MITRE ATT&CK®  
Technique T1075:  
Pass the Hash

**Detection**  
Audit all logon and credential use events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity. NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious.

Exabeam  
Identifies abnormal  
behaviors associated  
with account creation

Remote access to sfo_term_23			Suspicious NTLM Logon from 175.45.176.5 to unrecognized asset sfo_term_23. Possible pass-the-hash attack	+90
TIME 15:43:00	USER jdonaldson	ACCOUNT jdonaldson		
SOURCE IP 175.45.176.5	SOURCE HOST eowbagge4uijuuk6f2	SOURCE ZONE —		
DEST IP 10.28.121.95	DEST HOST sfo_term_23	DEST ZONE —		
DOMAIN ktenerry	REPORTING HOST dc_723	EVENT CODE 4769		
PROCESS —	LOGON TYPE —	EVENT SUBTYPE DC		
SERVICE NAME jdonaldson				

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

11

## Student Notes

Additional details of a TTP can be viewed from the MITRE website.



## Lesson

At the end of this lesson, you will be able to:

1. Navigate the MITRE ATT&CK® Framework and extract information useful to threat hunting
- 2. Use Threat Hunter to unearth hidden threats**
3. Use Data Insights to identify trends and threats
4. Create and utilize watchlists to monitor risky users and entities

## Discussion

Do you have a  
**proactive threat  
hunting program**, and  
how does it work?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



13

### Student Notes

Threat hunting activities include:

- **Hunting for insider threats or outside attackers** – Cyber threat hunters can detect threats posed by insiders, like an employee, or outsiders, like a criminal organization.
- **Proactively hunting for known adversaries** – A known attacker is one who is listed in threat intelligence services, or whose code pattern is on the deny list of known malicious programs.
- **Searching for hidden threats to prevent the attack from happening** – Threat hunters analyze the computing environment by using constant monitoring. Using behavioral analysis, they can detect anomalies which could indicate a threat.
- **Executing the incident response plan** – When they detect a threat, hunters gather as much information as possible before executing the incident response plan to neutralize it. This is used to update the response plan and prevent similar attacks.

### Source

<https://www.exabeam.com/security-operations-center/threat-hunting/>

What is Basic Search in Advanced Analytics?

The image displays three separate search results from the Advanced Analytics interface:

- Find User by Name or Username**: A search for "Lee" returns results for users like Sherri Lee and Aileen Chen, along with an asset named "it-slee-008".
- Find Asset by Hostname / IP**: A search for "10.32.44.19" returns results for assets, including one named "atl-addc-002".
- Find Alerts by Alert ID**: A search for "512740" returns results for security alerts, including one named "en\_tks\_10".

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

14

## Student Notes

The basic search in the Advanced Analytics interface allows analysts to find entities quickly, see their current risk score, and follow links to their profile pages.

Be careful not to concentrate only on risk that is considered notable. Elevated risk scores can indicate trends or quieter lurking threats.

## Demo

### Exploring Basic Search in Advanced Analytics

The screenshot shows a search interface with a search bar at the top containing the query "abnormal". Below the search bar, there are several sections: "USERS", "ASSETS", "SEQUENCE", "ASSETS ASSOCIATED WITH IP", and "INCIDENTS". Under each section, it says "No search results found.". In the "INCIDENTS" section, there are two entries:

- hosborne: Abnormal access and upload activity**  
SOC-3 / 2022-03-15 17:32:18 -0500 MEDIUM
- jdonaldson-03: Notable AA Session**  
SOC-26 / 2022-03-30 14:53:54 -0500 MEDIUM



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

**Proactive Hunting**

The screenshot displays the Exabeam Threat Hunter interface. On the left, a sidebar titled "Threat Hunter" contains filters for "ADVANCED ANALYSIS" such as Dates, User Name, Account, User Names, Assets, Network Zones, Peer Groups, Account Names, Event Types, and Rule Tags. A "Sessions List" section shows results for User Session, File Activity, and Account. It lists sessions for Julietta Donalds, Billie Wells, and Barbara Salazar, each with a timestamp and a brief description. On the right, the "Smart Timeline™" shows activity for Billie Wells on Friday, July 2nd, from 10:19 to 23:50. The timeline includes events like "Local login to 10.201.199.211" and "Remote access to 10.100.10.1". Below the timeline are summary statistics: RULES 24, EVENTS 17, ALERTS 0, ACCOUNTS 1, ASSETS 13, ZONES 3, and SCORE 328. At the bottom, there is another summary for Barbara Salazar with RULES 22, EVENTS 16, ALERTS 1, ACCOUNTS 2, ASSETS 24, ZONES 1, and SCORE 309.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

16

## Source

<https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/>

What to Hunt By...

- Rule Tags
- Risk Score (21+)
- Activity Types
- Data Models
- Accounts & Assets
- Anomalies
- Data Uploads

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Source

<https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/>

{Photo by [Taylor Vick](#) on [Unsplash](#)}

## Privileged Activity Risk Behavior: Failed Logons and Lockouts by Executives

User Label: executive

SEQ-UH-01, SEQ-UH-02, SEQ-UH-06, SEQ-UH-08, SEQ-UH-10, SEQ-UH-14, SEQ-UH-16, SEQ-UH-16-L, SEQ-UH-16-M, SEQ-UH-16-S, SEQ-UH-17, SEQ-UH-18

Date: Last 7 Days

The screenshot shows the Exabeam Advanced Analytics interface. On the left, there are several search filters: Dates (Last 7 days), User Names, Account Names, Rule Tags (failed), Activity Types, User Labels (executive selected), Reasons (failed selected), Activity Status, Vendors, Peer Groups, Assets, Asset Labels, and Alert IDs. On the right, there is a 'THREAT HUNTER' section with a list of threat hunting rules. One rule is highlighted: 'Abnormal direct access to an IP address by the asset belonging to an abnormal country for the asset to access has failed (N-WEBF-IP-Country-A)'. Below it are other rules like 'Abnormal failed logon to asset by user (SEQ-UH-06)', 'Abnormal number of failed application logins for user (APP-URL-COUNT)', and 'Abnormal number of failed authentications for user (AUTHN-F-...)'.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

18

## Student Notes

Different types of attacks leave different types of impressions in the logs to look for. When searching for certain types of attack symptoms there is guidance on the Exabeam community pages

Example: Privileged Activity has the “recipe” for 13 different examples of privileged activity risk behavior that might trigger an investigation, even if the overall risk score hasn’t exceeded 90

Saving Threat Hunter Searches

The screenshot shows the Exabeam Advanced Analytics interface with the 'THREAT HUNTER' tab selected. The search criteria are set to 'Dates: 06/01/2020 12:00 am - 07/04/2021 12:00 am', 'Activity Types: Interactive Logons', and 'Scores: 60 - 89'. The results table shows 5 User Sessions and 2 Asset Sessions. A context menu is open at the top right, with the 'Save As' option highlighted with a green box. A 'Save Search' modal is displayed in the foreground, containing the search criteria and a 'Title' input field. The main interface also displays summary statistics for Rules, Events, Alerts, Accounts, and Assets, along with ZONEs and SCOREs.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

19

## Student Notes

Threat Hunter Search results can change over time. To capture the results for record-keeping export the sessions list using the save feature

## Source

<https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/>

Using Predefined or Saved Threat Hunter Searches

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

20

### Student Notes

The Exabeam Search Library is the third tab on the left side of Threat Hunter. Exabeam provides powerful threat hunter searches out of the box to help with common complicated search criteria.

They are read-only but can be copied from the item menu if you would like to modify it.

Exabeam ships with the following preconfigured searches:

- Notable Sessions with Security Alerts
- Notable Sessions with Account Management
- Notable VPN Sessions
- Notable Sessions Containing Data Ex-filtration
- Notable Sessions Containing Executive Assets
- Notable Failed Logons

Additionally saved public and private saved searches can be executed as well

### Source

<https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/>

**Exporting Threat Hunter Searches**

The screenshot shows the Exabeam Advanced Analytics interface with the 'Threat Hunter' tab selected. The search parameters are set to 'Dates: 06/01/2020 12:00 am - 07/04/2021 12:00 am', 'Activity Types: Interactive Logons', and 'Scores: 60 - 89'. The results table displays 5 sessions:

User Names	(5)	User Session (3 results)	Asset Session (2 results)	We found a total of 5 results for your search						
Assets	(48)	Rob Koch it administrator 2 Jul 2021 @ 10:01	It-robkoch-888	RULES 8	EVENTS 8	ALERTS 0	ACCOUNTS 1	ASSETS 11	ZONES	SCORE
Network Zones	(4)	Julietta Donaldson* it administrator 30 Jun 2021 @ 9:26	Src_4399_prod	RULES 6	EVENTS 14	ALERTS 0	ACCOUNTS 1	ASSETS 16	3	65
Peer Groups	(1)	Julietta Donaldson* it administrator 3 Jul 2021 @ 18:28	It-jdona-888	RULES 1	EVENTS 2	ALERTS 0	ACCOUNTS 1	ASSETS 3	1	60
Account Names	(2)									
Event Types	(18)									
Rule Tags	(16)									

At the bottom left, it says 'Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential.' At the bottom right, it says '21'.

## Student Notes

Threat Hunter Search results can change over time. To capture the results for record-keeping export the sessions list using the save feature

## Source

<https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/>

**Map and Hunt: Use ATT&CK® Navigator with Threat Hunter**

The screenshot shows the ATT&CK Navigator interface. On the left, there is a tree view of various attack techniques categorized under sections like Initial Access, Persistence, Privilege Escalation, etc. A specific node, "Spearphishing Attachment", is highlighted in red. To the right of the tree view is a grid of tactics and their corresponding techniques. Below the grid is the "ADVANCED ANALYTICS" section, which includes a search bar and several dropdown filters for dates, user names, account names, activity types, peer groups, assets, asset labels, vendors, data upload, and alert IDs. To the right of the analytics is the "THREAT HUNTER" interface, which also includes a search bar and a list of rule tags such as "Code Signing", "Code Signing Certificates", and "Code Signing Policy Modification".

**Source:** MITRE

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

22

## Student Notes

Use ATT&CK Navigator to map tactics and techniques used by an adversary, then hunt for those in Advanced Analytics.

The navigator is helpful because it can help you understand the adversary and their likely threats. This has the following advantages:

- Use ATT&CK to save time in developing a hypothesis to test
- Hunt for a pattern of behavior rather than artifacts; much more efficient

## Source

<https://mitre-attack.github.io/attack-navigator/enterprise/>

# Demo

Going Threat Hunting!

The screenshot shows the Exabeam Advanced Analytics interface. At the top, there's a search bar and a 'THREAT HUNTER' button. Below the search bar, it says 'Dates: 06/01/2021 12:00 am - 07/04/2021 12:00 pm' and 'Reasons: Abnormal remote access to asset from first or abnormal zone (RA-LH-6ZA), Non-Executive user login to executive asset (AU-HT-E(EC))'. On the left, there are filters for 'User Names', 'Assets', 'Network Zones', 'Peer Groups', 'Account Names', 'Event Types', and 'Rule Tags'. The main area displays three results under 'User Session (3 results)'. Each result includes a user profile picture, name, title, date, and a timestamp. To the right of each result is a summary table with columns: RULES, EVENTS, ALERTS, ACCOUNTS, ASSETS, ZONES, and SCORE. The first result for Barbara Salazar has a score of 309, the second for Rob Koch has a score of 75, and the third for Barbara Salazar has a score of 74. There are also 'Go To Timeline' links next to each result.

User Session (3 results)	User Session (3 results)						
	RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
Barbara Salazar human resources coordinator 2 Jul 2021 @ 6:52	22	16	1	2	24	1	309
Rob Koch Administrator 2 Jul 2021 @ 10:01	8	8	0	1	11	1	75
Barbara Salazar human resources coordinator 1 Jul 2021 @ 10:32	6	17	2	1	15	3	74



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

23

## What is Anomaly Search?

The screenshot shows the Exabeam search interface with a green header bar containing the title "What is Anomaly Search?". Below the header is a search bar with the query "user\_login\_id:exabeam". The search results indicate "68,929 results" from September 29, 2022, to October 6, 2022. A timeline at the top shows activity from October 30, 2022, to October 6, 2022. The main area displays two highlighted anomalies:

**Anomaly 1 (Oct 6, 2022, 10:31:59.221):**

- Score: 5
- Rule Reason: Abnormal admin share for user exabeam-nopwose. Accessed share: C\$
- Use Case: Lateral Movement
- Techniques: T1021(02: SMB/Windows Admin Shares)
- Activity: trigger, activity\_type: alert-trigger-success, host: host23055, outcome: success, platform: Exabeam AA, product: Advanced Analytics
- Subject: alert, time: Oct 6, 2022, 10:31:59.221, vendor: Exabeam
- Raw Log: 1093 1001-1002-10-0016(11)109.2207 exabeam-analytics-master Exabeam --> [incident\_creation, time="1665073848142", id="avc-w-mopwose-20221009134910", score="5", user="svc-w-mopwose", session\_id="avc-w-mopwose-20221009134910", domain="datadocents", host="host23055", src\_ip="10.1.72.63", dest\_host="host123955", raw\_log="...ref->http://ip --> Map(s)fafade-99cf-4eeb-bc62-99541331082 --> [java.lang.String:("990014641")", event\_type:"share-access", rule\_id:"SA-Qu-A", rule\_name:"Abnor..."]]

**Anomaly 2 (Oct 6, 2022, 10:31:59.220):**

- Score: 5
- Rule Reason: Abnormal admin share for user exabeam-nopwose. Accessed share: C\$
- Use Case: Lateral Movement
- Techniques: T1021(02: SMB/Windows Admin Shares)
- Activity: trigger, activity\_type: alert-trigger-success, host: hostM00, outcome: success, platform: Exabeam AA, product: Advanced Analytics
- Subject: alert, time: Oct 6, 2022, 10:31:59.220, vendor: Exabeam

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

24



## Lesson

At the end of this lesson, you will be able to:

1. Navigate the MITRE ATT&CK® Framework and extract information useful to threat hunting
2. Use Threat Hunter to unearth hidden threats
- 3. Use Data Insights to identify trends and threats**
4. Create and utilize watchlists to monitor risky users and entities

## Use ATT&CK® with Your Security Team

Ever wish you could  
see what Advanced  
Analytics is seeing?

That is what Data  
Insights will show you:  
the models!

## Quickly Determine Normal

### Data Insights

The screenshot displays the Data Insights interface. On the left, there are two separate log entries under the heading "All activity for assets". The first log is titled "tag\_en\_061\_x1" and the second is "proxy\_360". Both logs show a table with columns: ACTIVITY, COUNT, and PCT. The logs list various system events such as account-enabled, account-switch, app-activity, app-login, database-login, dip-email-alert-out, and local-login, all with a count of 29 and a percentage of 8%. Below the logs, a copyright notice reads: "Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential." To the right of the logs is a large, dark network visualization showing numerous nodes and connections, likely representing a complex system or network structure.

All activity for assets

tag\_en\_061\_x1

ACTIVITY	COUNT	PCT
account-enabled	29	8%
account-switch	29	8%
app-activity	29	8%
app-login	29	8%
database-login	29	8%
dip-email-alert-out	29	8%
local-login	29	8%

proxy\_360

ACTIVITY	COUNT	PCT
sequence-end	30	51%
dip-email-alert-out	29	49%

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

27

{Photo by [Taylor Vick](#) on [Unsplash](#)}

**Searching For Data Insights Models**

Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential.

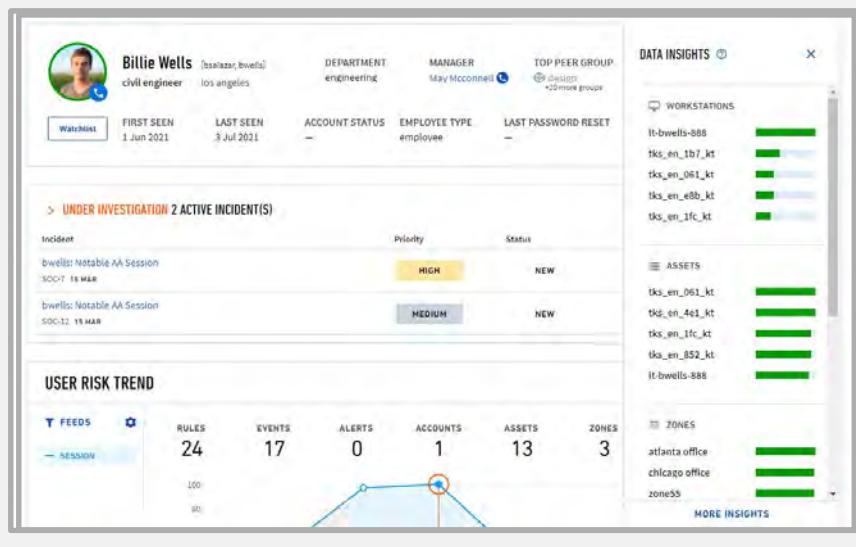
28

## Student Notes

Data Insights is revealing the models used to collect data about behavior so that rules can be run against them.

Each model has its own name and can be searched for using natural language components as well  
The Grouping Feature Value (GFV) describes how data is broken out. If the model is a per asset model, each asset will be its own GFV

## User Specific Data Insights



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

29

### Student Notes

Data Insights is revealing the models used to collect data about behavior so that rules can be run against them.

Each model has its own name and can be searched for using natural language components as well  
The Grouping Feature Value (GFV) describes how data is broken out. If the model is a per asset model, each asset will be its own GFV

## Asset Specific Data Insights



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Risk Reason Data Insights

**NTLM logon to tks\_en\_360\_kt**

TIME 11:50:00	USER bwells	ACCOUNT bwells
DEST IP 10.136.0.222	DEST HOST tks_en_360_kt	DEST ZONE chicago office
DOMAIN kt_cloud	REPORTING HOST dc_125	EVENT CODE 4776
EVENT SUBTYPE DC		

[View Logs](#)

**First NTLM/Kerberos logon to tks\_en\_360\_kt for Billie Wells**

**DESCRIPTION**  
First time user has logged on via NTLM/Kerberos authentication to this asset

**RULE TAGS**

- [Pass the Ticket](#)
- [Pass the Ticket](#)
- [Pass the Hash](#)
- [Valid Accounts](#)
- [Pass the Hash](#)
- [Steal or Forge Kerberos Tickets](#)

**CONFIDENCE**  
100%

ANCHOR SCORE 12	X ANOMALY FACTOR 1.0	± +12
--------------------	-------------------------	-------

[Rule Definition](#) [Data Insight](#)

Abnormal NTLM/Kerberos login to account tks\_en\_360\_kt

**All logons**

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Excellent - 100%	328	17	9 months ago

Enter text to filter

ASSET	COUNT	PCT.
tks_en_061_kt	27	8%
tks_en_4e1_kt	27	8%
tks_en_1fc_kt	25	8%
tks_en_852_kt	25	8%
lt-bwells-888	24	7%
tks_en_4dc_kt	24	7%
tks_en_f08_kt	24	7%

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

31

## Discussion

---

What kinds of **models**  
do you imagine being  
of most use to you?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



32

## Activity

### Using Threat Hunter and MITRE ATT&CK®

#### Objectives:

1. Use the Threat Hunter Interface to perform advanced searches.
2. Demonstrate a basic familiarity with the MITRE ATT&CK®
3. Demonstrate how to use the MITRE ATT&CK® website, matrix, and navigator for reference and research
4. Perform Threat Hunter searches in Advanced Analytics based on MITRE ATT&CK® tags

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



33



## Lesson

At the end of this lesson, you will be able to:

1. Navigate the MITRE ATT&CK® Framework and extract information useful to threat hunting
2. Use Threat Hunter to unearth hidden threats
3. Use Data Insights to identify trends and threats
- 4. Create and utilize watchlists to monitor risky users and entities**



**"If we monitor our toothbrushes and diamonds with the same [level of] zeal we will lose fewer toothbrushes and more diamonds"**

-Former national security advisor McGeorge Bundy

#### **Student Notes**

Make sure you are safeguarding the most valuable assets/individuals in your environment.

#### **Reference**

<https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis>

## Monitoring High-Risk or High-Value Users and Assets

The screenshot shows a software interface titled "Watchlists". A sub-section titled "Executive Users" is displayed, showing five users with their names, titles, and a green "0" indicating no recent activity. The users listed are Andrew Bautista (vp sales), Chelsea Mayo (vp business ...), Emely Blanch... (ceo), Emery Santiago (vp council), and Felipe Pennin... (vp informati...). Each user has a small profile picture next to their name.

User	Title	Last day
Andrew Bautista	vp sales	0
Chelsea Mayo	vp business ...	0
Emely Blanch...	ceo	0
Emery Santiago	vp council	0
Felipe Pennin...	vp informati...	0

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

36

### Student Notes

Automatic detection is done in Advanced Analytics by finding notable users who have been identified to have had risky behavior and then incidents are created in case manager for analyst workflow.

What is the difference between notables and watchlists?

The dashboard displays three main sections:

- NOTABLE USERS**: Shows users with high risk scores. One user, Julietta Donal..., has a score of 624.
- Departing Employees**: Shows employees leaving. One employee, Gary Hardin, has a score of 198.
- Executive Users**: Shows executive staff. All listed users have a risk score of 0.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

37

### Student Notes

Notables in Advanced Analytics are built in watchlists that automatically populate when a predefined threshold risk score is reached (default of  $\geq 90$  risk score). They cannot be added to or deleted from.

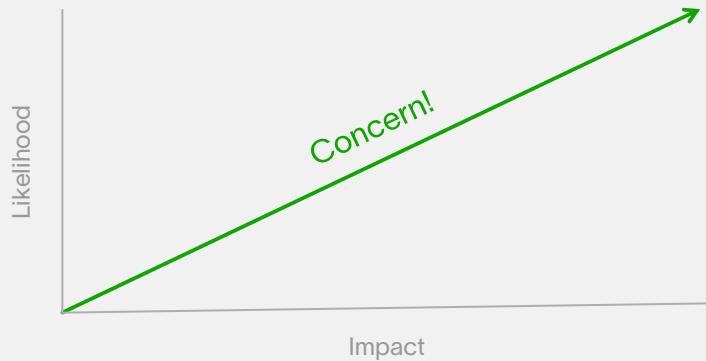
The “watchlist” however is a fundamental part of the Advanced Analytics dashboard for at-a-glance alerting based on UEBA risk score alerts. They are created by analysts to proactively monitor high-risk and/or high-value users and assets such as service accounts and executive users.

They can also be used for policy and compliance situations and other unique use cases.

### More Information

<https://www.exabeam.com/ueba/financial-institutions-and-ueba-fdic-vacation-policy-use-case/>

## When should a watchlist be created?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

38

### Source

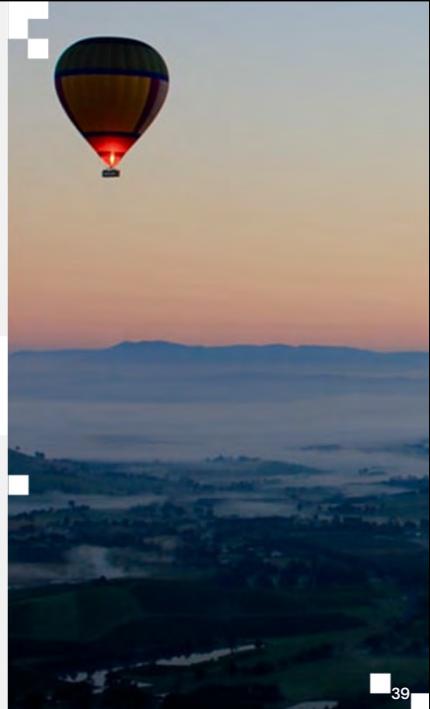
<https://www.exabeam.com/ueba/financial-institutions-and-ueba-fdic-vacation-policy-use-case/>

Concept of project management risk management: <https://intaver.com/risk-scores/>

Fast Fact: Executives are  
**12x**  
more likely to be targeted  
in a security incident

Source: Verizon, Forbes

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



**Source**

<https://www.forbes.com/sites/jeanbaptiste/2019/05/11/cybercriminals-favor-targeting-top-executives-small-businesses-money-verizon-data-breach-report/#2d96d18d30e6>

<https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf>

{Photo by [Hendra Pontomudis](#) on [Unsplash](#)}

## Account Lockouts – A Unique Watchlist

The screenshot displays the Exabeam security analytics interface. On the left, a sidebar titled "ACCOUNT LOCKOUTS" shows two users with lockout status: Mario Erickson (locked out) and Jim Coleman (locked out). The main dashboard header indicates "Activity on Tuesday, 29 Jun Start: 9:43 End: 17:50 (sh 7m)". Below the header, various metrics are displayed: RULES (0), EVENTS (128), ALERTS (0), ACCOUNTS (1), ASSETS (29), ZONES (5), and SCORE (0). A green box highlights a specific event: "Logon Failures and Lockouts on Friday, 2 Jul at 15:30 – 18:30". The bottom section contains three panels: "ACCOUNT CHANGES", "ASSETS", and "FAILURE REASONS". The "ACCOUNT CHANGES" panel shows past account activity (active on 29 Jun 2021) and current account activity (account locked out). The "ASSETS" panel lists sources (10.14.33.142, it\_x200\_manson) and destinations (10.14.33.142, it\_x200\_manson). The "FAILURE REASONS" panel is currently empty. The footer of the interface includes copyright information: "Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential." and the page number "40".

### Student Notes:

Account Lockouts is a list of users who have been locked out of their account within the timeframe selected. Clicking the caron at the top right activates a drop-down list for selecting the timeframe for that list. The account lockouts that Exabeam has deemed risky are at the top.

# Demo

## Create Custom Watchlists

The screenshot shows a software interface for creating custom watchlists. It features two main sections:

- NOTABLE USERS**: Last day
- Departing Employees**: Last day

**NOTABLE USERS** Data:

User	Title	Last Day Activity
Julietta Donaldson	it administrator	4 posts, 624 interactions
Billie Wells	civil engineer	2 posts, 328 interactions
Barbara Salazar	human resources	1 post, 309 interactions
Howard Osborne	sales representative	1 post, 302 interactions

**Departing Employees** Data:

User	Title	Last Day Activity
Gary Hardin	software engineer	3 posts, 198 interactions



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

# What are the five ways a watchlist can be populated?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

42

## Watchlist Permissions

The screenshot shows a 'SELECT WATCHLIST PERMISSIONS' interface. It lists five roles with their current permission levels: Administrator (1 user, None), Tier 3 Analyst (3 user, None), Tier 1 Analyst (0 users, None), Auditor (0 users, None), and Data Privacy Officer (0 users, None). A dropdown menu is open over the 'None' option for the Data Privacy Officer role, listing three options: 'Can view and edit members' (selected, indicated by a checked checkbox icon), 'Can only view' (indicated by an eye icon), and 'None' (indicated by a minus sign icon). At the bottom of the interface are 'BACK' and 'APPLY' buttons.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

43

### Student Notes

Watchlists permissions are simple

- None
- View members only
- View and edit the membership list (when manual additions are allowed)

## How to create a watchlist?

The screenshot shows a user interface for creating a watchlist. On the left, there's a large button labeled "ADD A WATCHLIST" with a plus sign icon. To its right is a detailed "CREATE A WATCHLIST" form. The form has fields for "Title" (with placeholder "Enter a title") and "Description" (with placeholder "(Optional) Enter description"). Below these is a section titled "Add User based on:" with two radio buttons: "User Names" (selected) and "Upload". Under "User Names", there's a field "Enter User Name" and a checkbox "Remove users from the w...". To the right of these fields is a dropdown menu titled "Who should see this list?". The "Public" option is selected, showing "All users in my organization". Other options include "Based on Role" (with a sub-note "Set view/edit permissions by role") and "Only Me" (with a sub-note "Make this list private"). At the bottom of the form are "CANCEL" and "SAVE" buttons.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

44

## Source

<https://www.exabeam.com/ueba/financial-institutions-and-ueba-fdic-vacation-policy-use-case/>

## Watchlist Tips

- ➔ Analyze business needs
- ➔ Create custom watchlists based on high-risk needs
- ➔ Use a repeatable, consistent framework
- ➔ Assess risks and models for tuning

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

45





## Summary

### Can You Do the Following?

1. Navigate the MITRE ATT&CK® Framework and extract information useful to threat hunting
2. Use Threat Hunter to unearth hidden threats
3. Use Data Insights to identify trends and threats
4. Create and utilize watchlists to monitor risky users and entities

v4.00



# Investigate and Respond with Case Manager and Incident Responder

EDU-2170 : Module 6



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

1



# What human errors derail your security investigation and resolution process?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

2



## Lesson

At the end of this lesson, you will be able to:

- 1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow**
2. Do the following:
  1. Recall how incidents are created
  2. Edit an incident in Case Manager
3. Execute a turnkey playbook in Incident Responder
4. Recall where to start an investigation and how to execute the steps in a Case Manager checklist to identify, classify, and respond to an incident
5. Perform the steps of the analyst workflow from start to completion

# What is an Incident?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

4

## Student Notes

According to NIST- Events and Incidents:

An **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

A **computer security incident** is a violation or imminent threat or violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

## Source

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

# What is an **Incident Response Plan** and why do you need one?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

5

## **Student Notes**

### **Incident Response**

Incident response is an approach to review and respond to a cyber security breach or attack utilizing a planned process or methodology.

Effective incident response teams utilize procedures and technology, such as automated playbooks, to respond quickly and adequately to cyber security events, limiting the damage done by attackers.

### **Source**

<https://www.exabeam.com/incident-response/>

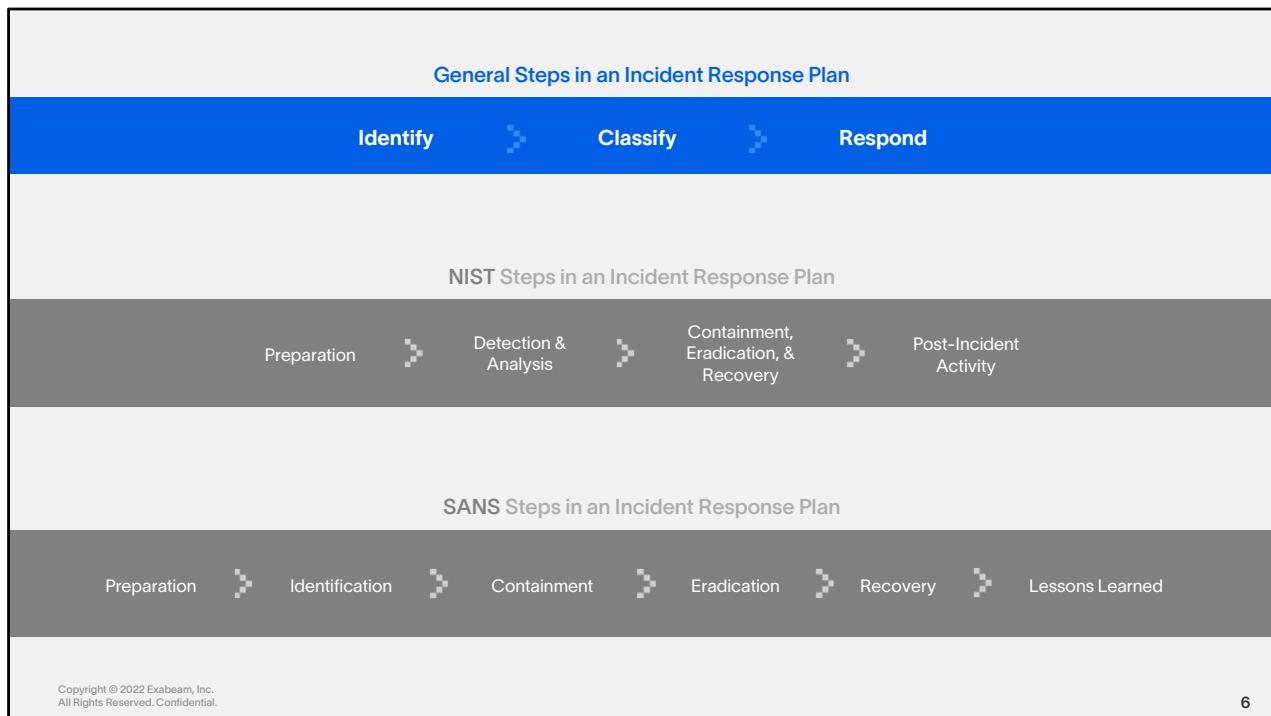
<https://www.exabeam.com/incident-response/incident-response-plan/>

According to NIST:

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger monitoring for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

### **Source**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>



### Student Notes

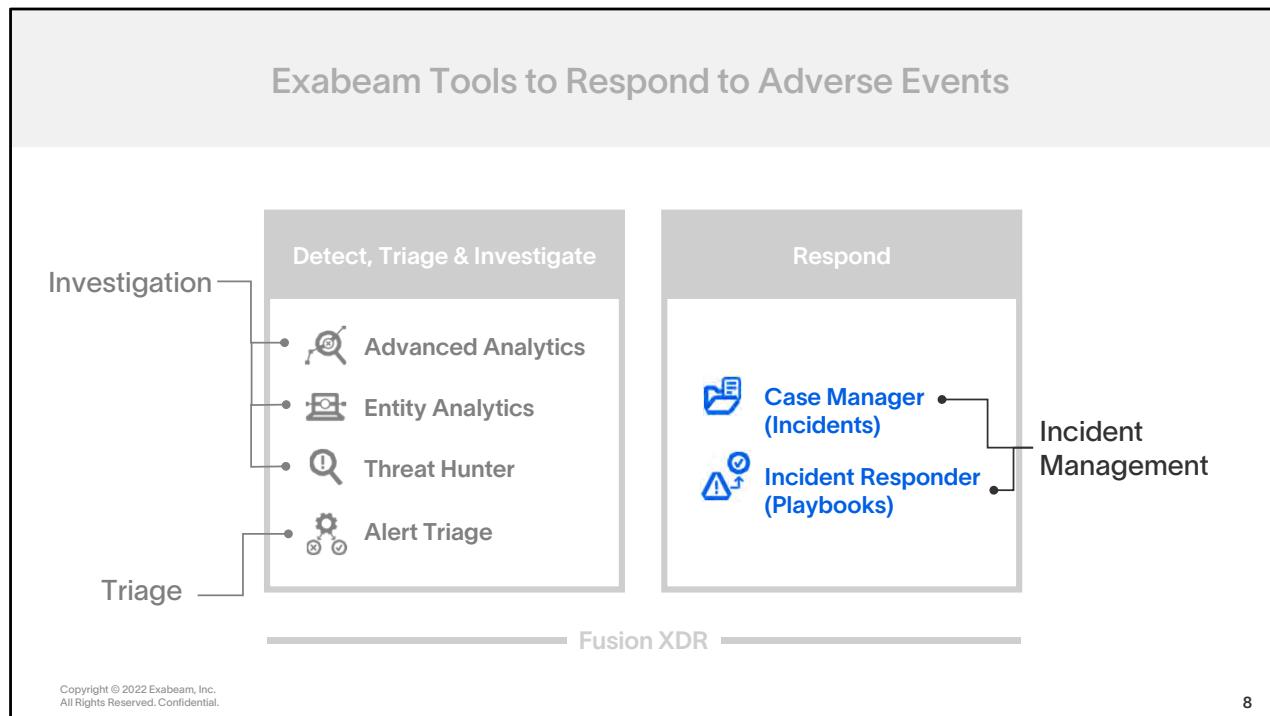
**Identify** – Determine if there is an actual cyber security incident or not.

**Classify** – Determine what systems or services are being affected and the result of the incident (scope and impact).

**Respond** – Identifies steps to contain the incident and how to restore operations.

## Five Key Analyst Questions

1. Has there been an attack?
2. Was this attack successful?
3. What is the scope of the attack?
4. What were the attacker's methods, techniques, and tactics?
5. How should we respond?



### Student Notes

Investigation and Resolution of Detected and Triaged threats is a process that requires many steps that need to be accounted for consistently, and in some cases would be better served to be performed in an automated way.

Exabeam provides tools that help analysts to do exactly that in a way that leverages the information found in user profiles and the Smart Timeline.

Exabeam Case Manager is a fully customizable case management solution that includes ticketing, messaging, and KPI dashboards to organize, track, and streamline your investigation

Case Manager includes use-case specific turnkey playbooks for automation

You can also add Incident Responder to Case Manager with a separate license to extend your custom playbook capabilities.

Advanced Analytics and Entity Analytics support resolving security concerns regarding users or entities with watchlists and search functionality

## What is a Case Manager Incident?

The screenshot shows the 'NOTABLE AA SESSION' incident details page. At the top, it displays the incident ID (JONALDSON-20230702112400), status (Tier I), priority (Info), and assigned analyst (Tier1Analyst). Below this, there's a navigation bar with icons for Home, New Incident, and New Playbook. The main area contains fields for Incident Type (Phishing Attempt), Description, Vendor (Exabeam), Source (Exabeam AA), Source Severity (Low), Source ID (JONALDSON-20230702112400), Source URL (https://12.130.0.142:8443/isa/Notes/Mail/exabeam/iconline/JONALDSON-30230702112400), Event Start Time (2 July 2021 10:28:00), and Event End Time (--). To the right, there's a sidebar titled 'ENTITIES' with tabs for ALL, FILE, DEVICE, and USER, showing one item: 'jonalson'. At the bottom, there are 'ACTIONS' and 'PLAYBOOKS' buttons, along with a note to 'Add to Incident - Internal'.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

9

- ❖ Documentation of Identification, Classification, and Response
- ❖ Integration with automation (Playbooks)
- ❖ Works well in conjunction with the automation available with the built-in phishing turnkey playbook
- ❖ Guidance throughout Identification, Classification, and Response

### Student Notes

An incident is an unusual occurrence that indicates a threat to your organization; what a security analyst investigates.

Case Manager Incident “Tickets” document and guide this process for consistency and completeness

**Consistent investigation and response with Exabeam Case Manager checklists**

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

10

Task Name	Assignee	Due Date
<input type="checkbox"/> Communicate the case to the SOC Manager	Assign	Set Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Determine adequate ...	Assign	Set Due Date
<input type="checkbox"/> Lateral Movement - Determine adequate response measures...	Assign	Set Due Date
<input type="checkbox"/> Compromised Credentials - Determine adequate response ...	Assign	Set Due Date
<input type="checkbox"/> Determine adequate response measures to contain the threat	Assign	Set Due Date

Task Name	Assignee	Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Take measures to pre...	Assign	Set Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Remediate	Assign	Set Due Date
<input type="checkbox"/> Take measures to preserve logs for impacted systems and us...	Assign	Set Due Date
<input type="checkbox"/> Reset all affected credentials	Assign	Set Due Date

### Student Notes

Exabeam tools such as Case Manager and Incident responder can take frameworks such as NIST and help analysts to stay on course in the investigation process.

Incident Assignments – Who Works on What?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

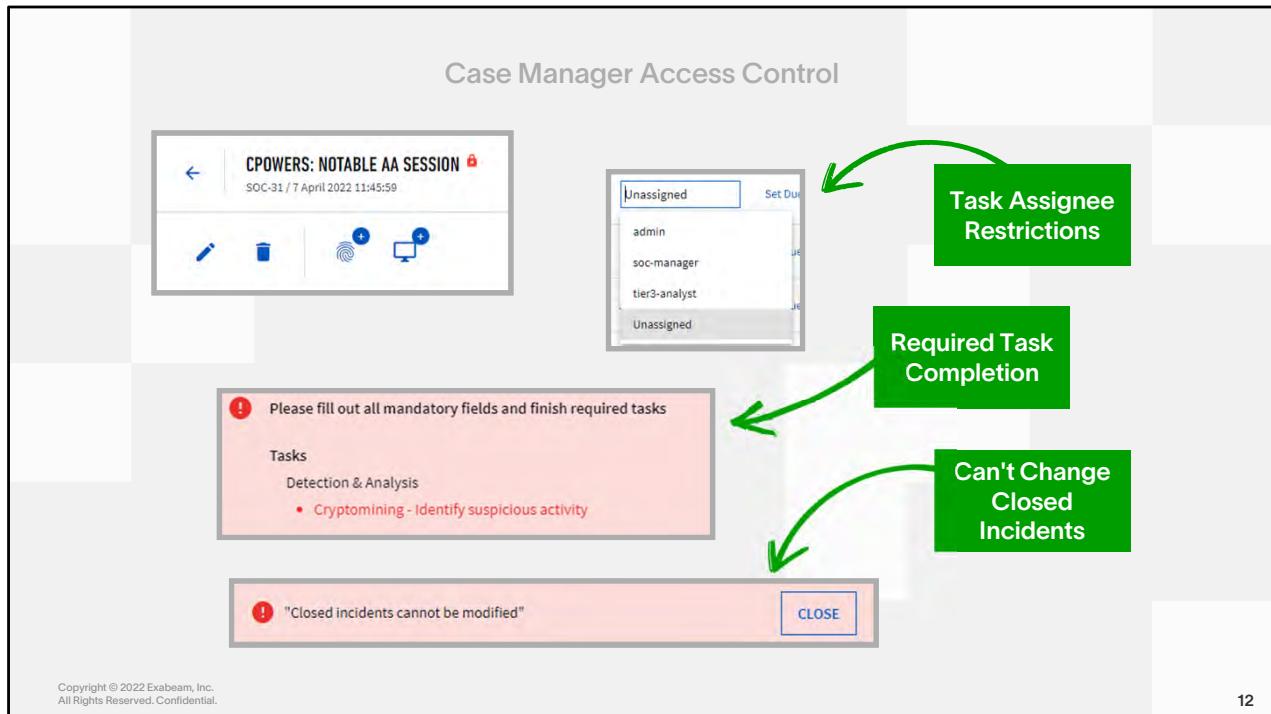
11

### Student Notes

Incidents function as tickets, and at any one time only one Advanced Analytics User can be assigned the primary responsibility to resolve that ticket.

That person is the Assignee of the incident, and they will see their assignments on the home page of Advanced Analytics under “My Incidents”

Assigning a user to a queue requires the appropriate permission. A user can only be assigned an incident if they are also a member of the queue associated with that incident.



### Student Notes

In addition to case queues and assignments, Case Manager access control restrictions have the potential to impact an analyst's interactions with the tool. Four controls in particular are worth noting:

- Incidents can be restricted to one or more roles and/or users
- Only members on the restricted list of roles and users can be assigned to a task
- Fields or tasks identified as "required" must be completed before an incident can be closed
- Closed incidents cannot be modified in any way. The incident status must be

The upcoming instructor demonstration will show these Case Manager controls in action.

### References

Case Manager Release Notes <https://docs.exabeam.com/en/cloud-delivered-case-manager/all/case-manager/171447-case-manager-release-notes.html>

Manually Create an Incident: <https://docs.exabeam.com/en/cloud-delivered-case-manager/all/case-manager/171133-investigate-a-security-incident.html#UUID-9a315bfc-d372-5bcb-4352-eebef502aa19>

Edit an Incident: <https://docs.exabeam.com/en/cloud-delivered-case-manager/all/case-manager/171133-investigate-a-security-incident.html#UUID-be6abebd-2100-2c70-2ba1-ff7c465eba2a>

**Case Manager Terminology**

The screenshot shows the Case Manager interface with the following components:

- Queue:** A blue button-like element.
- Incident Type:** A grey button-like element.
- Incident Field:** A grey button-like element.
- Task Checklist:** A grey button-like element.
- User Assignment:** A sidebar showing users assigned to a queue: tier1-analyst (selected), soc-manager, and Unassigned.
- Incidents in My Queues (6):** A list of six incidents. Each incident entry includes the reporter, subject, priority, status, and tier level.

Reporter	Subject	Priority	Status	Tier
fweber	Notable AA Session	HIGH	IN PROGRESS	Tier 3
fweber	Notable AA Session	HIGH	IN PROGRESS	Tier 3
fweber-2-02	Notable AA S...	HIGH	IN PROGRESS	Tier 3
fweber-2-01	Notable AA S...	HIGH	IN PROGRESS	Tier 3
fweber	Notable AA Session	HIGH	IN PROGRESS	Tier 3
	SOC-11 15 MAR			

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

13

### Student Notes

- Queue A group assigned to handle and investigate an incident.
- Queue member A security analyst who has been added to a queue.

### Source

Advanced Analytics User Guide

**Case Manager Terminology**

The diagram illustrates four key components of Case Manager Terminology:

- Queue**: Represented by a grey rounded rectangle.
- Incident Type**: Represented by a blue rounded rectangle.
- Incident Field**: Represented by a grey rounded rectangle.
- Task Checklist**: Represented by a grey rounded rectangle.

To the right, a screenshot of the 'Edit Incident Type' interface is shown. The interface includes a sidebar with 'Incident Type:' and a main panel listing various incident types. The listed incident types are:

- Abnormal Authentication & Access
- Compromised Credentials
- Behavioral Analytics
- Lateral Movement
- Account Manipulation
- Audit Tampering
- Brute Force Attack
- Cryptomining
- Data Access Abuse

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

14

### Student Notes

Incident type describes The nature of an incident (e.g., malware, phishing attempt, data leakage, departed employee). Based on the incident type, Incident Responder displays certain incident fields and tasks.

In other words, [Incident Types](#) are [categorizations](#) of incidents, based on [attack vector](#) or case [context](#). Incident types can be customized, or new incident types can be created by Case Manager administrators to allow for specific fields and checklists that are dialed into an organization's needs.

### Source

Advanced Analytics User Guide

**Case Manager Terminology**

The diagram illustrates four concepts of Case Manager Terminology:

- Queue**: Represented by a grey rounded rectangle.
- Incident Type**: Represented by a grey rounded rectangle.
- Incident Field**: Represented by a blue rounded rectangle.
- Task Checklist**: Represented by a grey rounded rectangle.

To the right of the diagram is a screenshot of the Exabeam SOC-13 interface. The title bar shows "FWEBER-1-01: NOTABLE AA SESSION" and the date "SOC-13 / 24 March 2022 11:51:03". Below the title are several icons: a pencil, a trash can, a fingerprint, and a monitor. The main content area displays the following incident details:

Incident Type:	Abnormal Authentication & Access		
Description:	--		
Vendor:	Exabeam	Created By:	admin
Source:	Exabeam AA	Creation Time:	24 March 2022 11:51:03
Source Severity:	--	Updated By:	admin
Source ID:	fweber-20210702145500	Updated:	24 March 2022 11:53:41
Source URL:	<a href="https://10.150.0.162:8494/uba/#user/fweber/_at=1625237700000/_st=session/_si=fweber-20210702145500">https://10.150.0.162:8494/uba/#user/fweber/_at=1625237700000/_st=session/_si=fweber-20210702145500</a>		
Event Start Time:	2 July 2021 9:55:00	Closed Time:	--
Event End Time:	2 July 2021 23:21:00	Closed Reason:	--
Source Info:	--		

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

15

## Student Notes

Incident field is an attribute of an incident, like its description or the time it was created.

### Source

Advanced Analytics User Guide

In other words, **Incident Fields** are both **unique information** to the incident type as well as **common metadata** for all incidents.

Generic Field Example: Status, Priority, Description

Malware Incident Type Field Example: Malware URL

## Case Manager Terminology

The diagram illustrates four key components of Case Manager Terminology:

- Queue**: Represented by a grey rounded rectangle.
- Incident Type**: Represented by a grey rounded rectangle.
- Incident Field**: Represented by a grey rounded rectangle.
- Task Checklist**: Represented by a blue rounded rectangle.

**Task Checklist Detail View:**

A screenshot of a software interface showing a task checklist for "Detection & Analysis". The interface includes tabs for Tasks, Artifacts (0), Messages (0), and Activity Log. Under the Tasks tab, there is a list of tasks:

- Abnormal Authentication and Access - Identify suspicious activity
- Abnormal Authentication and Access - Review the user's profile
- Account Manipulation - Perform analysis and scoping
- Account Manipulation - Identify suspicious activity
- Account Manipulation - Review the user's profile
- Account Manipulation - Perform analysis and scoping

Each task has an "Assignee" column (which is currently unassigned) and a "Due Date" column. A modal window titled "Account Manipulation - Identify suspicious activity" is open, showing detailed instructions:

**Instructions**

- Are there risky and anomalous account creation or modification activities or permission modifications obtained through group membership and inheritance?
- From the risky and anomalous account creation or permission modification activities, determine if many rights in R0 can be retained through group membership and inheritance.
- Determine potential impact based on the rights of the privileged account involved, possible systems involved and data potentially exposed as a result.

Below the instructions, there are "Notes" and "CLOSE" and "MARK AS DONE" buttons.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

16

### Student Notes

Tasks Checklists are a critical part of any case manager incident because they help analysts stay on track with all the minimum steps associated with investigating and resolving an incident

Checklists allow teams to create step-by-step instructions or 'tasks' grouped into phases aligned with NIST frameworks

Different incident types will add different tasks

Case Manager administrators can redefine the phases and tasks associated with any incident type

## Demo

### Case Manager Restrictions

CPOWERS: NOTABLE AA SESSION !  
SOC-31 / 7 April 2022 11:45:59

Unassigned Set Due  
admin  
soc-manager  
tier3-analyst  
Unassigned

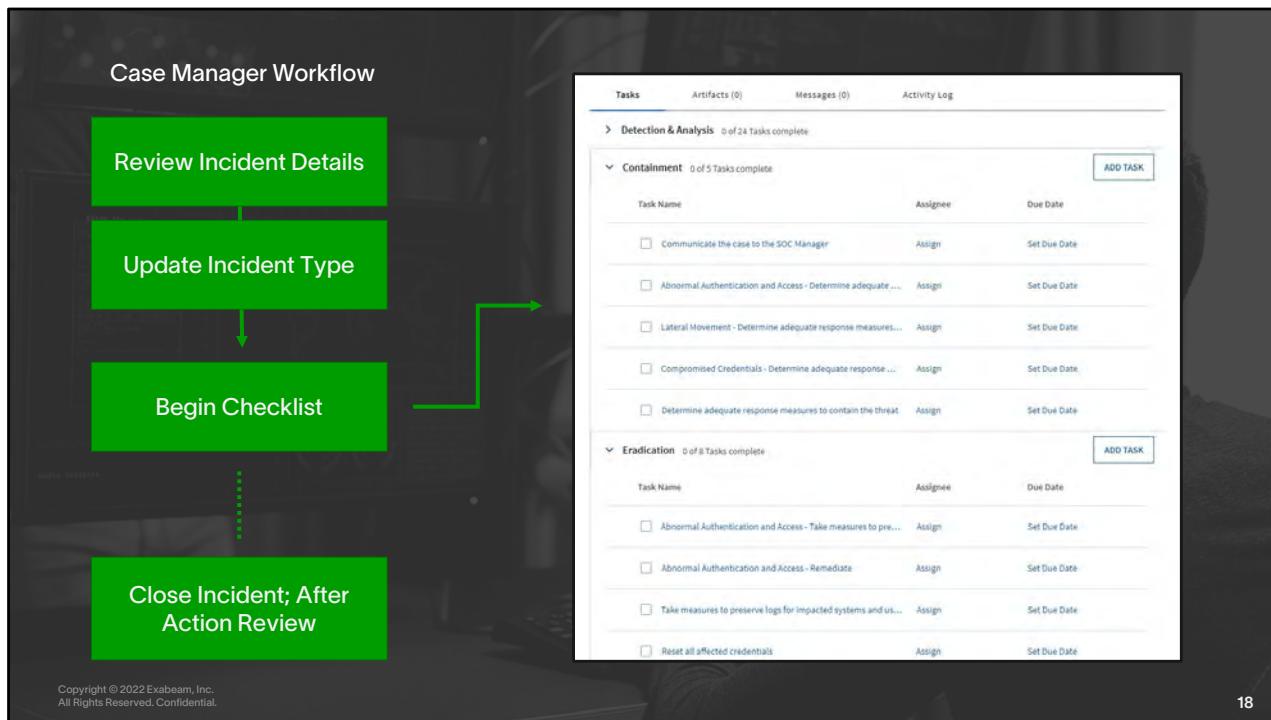
! Please fill out all mandatory fields and finish required tasks

Tasks  
Detection & Analysis  
• Cryptomining - Identify suspicious activity

! "Closed incidents cannot be modified" CLOSE



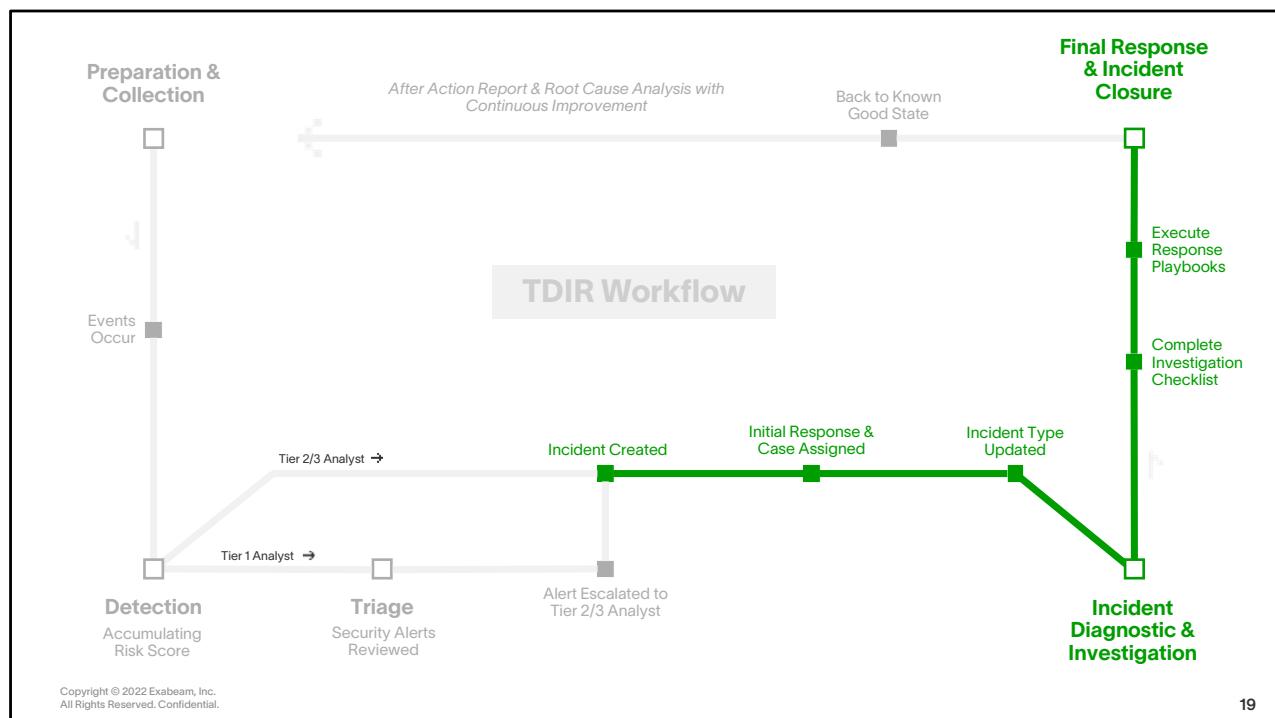
Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



18

### Student Notes

Exabeam tools such as Case Manager and Incident responder can take frameworks such as NIST and help analysts to stay on course in the investigation process.



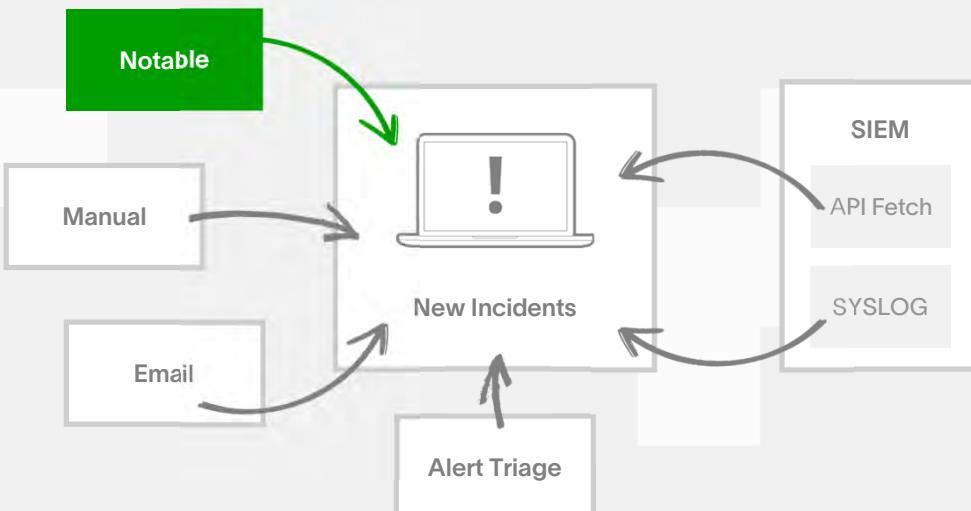


## Lesson

At the end of this lesson, you will be able to:

1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
- 2. Do the following:**
  - 1. Recall how incidents are created**
  - 2. Edit an incident in Case Manager**
3. Execute and manage turnkey and custom playbooks in Case Manager and Incident Responder
4. Recall where to start an investigation and how to execute the steps in a Case Manager checklist to identify, classify, and respond to an incident
5. Perform the steps of the analyst workflow from start to completion

## Where Do Incidents Come From?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

21

### Student Notes

An incident can be created manually, with or without initially referencing a user profile from Advanced Analytics.

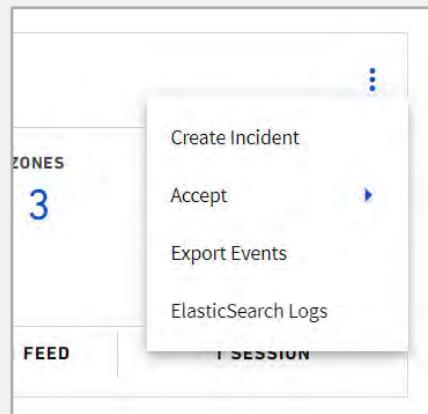
Many incidents are automatically created, such as when an Advanced Analytics user has a risk score above 90 and becomes notable or an alert is escalated in Alert Triage.

A designated phishing email box can be used to trigger the creation of phishing incidents

If there is a log source not being fed to Advanced Analytics that you would like to use to trigger incidents Case Manager can fetch those logs from the source directly using API calls or that SIEM can forward logs directly to case manager using Syslog

## Proactive Incident Creation

- What do you do when you discover suspicious behaviors proactively?
- Create an incident manually!



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Example of Email Ingestion

- ➡ Regularly pull emails from a customer inbox to create incidents
- ➡ Works well in conjunction with the automation available with the built-in phishing turnkey playbook

23

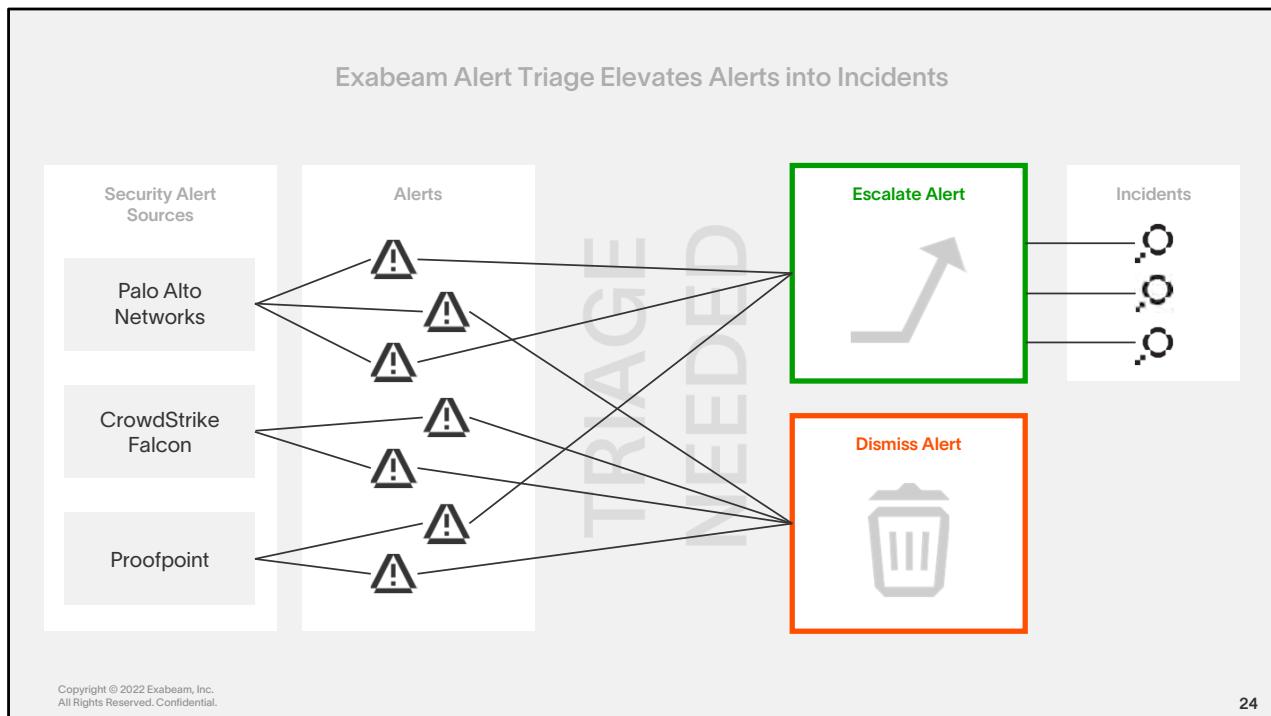
### Student Notes

Case Manager Email Ingest creates incidents from potential phishing emails. It ingests suspicious emails from a designated phishing mailbox, parses relevant fields, creates an incident, then deletes the email from the inbox.

{Photo by [Micah Tindell](#) on [Unsplash](#)}

### Source

<https://docs.exabeam.com>



### Student Notes

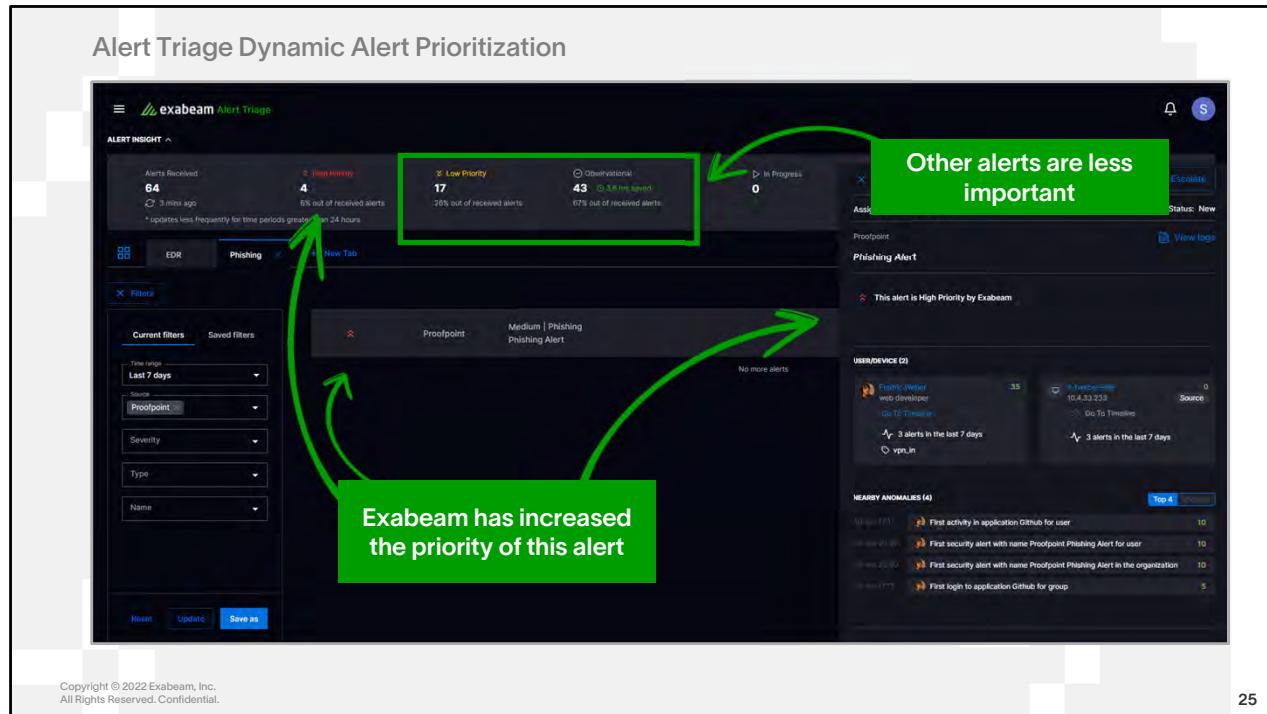
The first step of Alert Triage, usually performed by Tier 1 analysts, determines if an alert poses a risk to their organization. The first challenge is in opening the various alert sources and reviewing alerts. This can be done more quickly if a SIEM is used rather than opening each product's interface individually. If an alert does signify risk, it must be escalated to the incident response team for further review. If it is not determined to be a risk, then the alert can be dismissed and not elevated to a Case Manager Incident.

### Alert Triage on the Exabeam Cloud Platform

- Provides a unified view of third-party and Exabeam Data Lake-triggered security alerts.
- Centralizes the alert triage process and organizes an analyst's efforts, so they can review alerts faster.
- Provides full visibility into all the alerts that security tools have triggered, minimizes the likelihood that an alert is missed or overlooked, reducing the chance that a missed alert results in a breach.
- When an alert is escalated a Case Manager Incident is automatically created with relevant information injected into the incident

### More Information

<https://www.exabeam.com/information-security/introducing-exabeam-alert-triage/>



25

## Student Notes

On average, organizations deploy 30-50 security tools and receive 11,000 alerts a day. As the first step of the alert triage process, a security analyst must prioritize the alerts and identify the alerts that pose the largest threat to the organization. Many alerts classified as high or critical by other security vendors' solutions end up being false positives. On the other hand, lower-ranked alerts that represent a significant threat may fall through the cracks. Manual alert prioritization is time consuming, often inaccurate, and inefficient. Analysts struggle to understand which alerts to prioritize across vendors with varying and subjective severity rankings. And when the volume of alerts is high, prioritization becomes even more time-consuming, limiting the analyst's ability to quickly triage high-priority alerts and delaying the start time of important investigations.

Exabeam automates the prioritization of third-party security alerts and Data Lake alerts, the first step in triaging. Security analysts can filter their view to display alerts by priority. High priority alerts pose the largest threat to your organization. Low priority alerts are threats that have the potential to pose a threat, and observational alerts are alerts that Exabeam has classified as repetitive, or noisy. Classifying alerts as high-priority provides a starting point for the analyst to begin the triage process, focusing on the alerts of highest risk to the organization.

The Exabeam risk engine uses machine learning across multiple signals to categorize the alert, such as

- Rarity of the combination of alert name and type
- Rarity of the combination of the vendor (source) and alert severity
- First time the alert name and type has been observed for the organization, user, or asset in the last 30 days

Also, analyst feedback helps the ranking algorithm understand if surfacing the alert as high or low priority was correct. The Exabeam risk engine will then use this feedback to improve the ranking algorithm.

## References

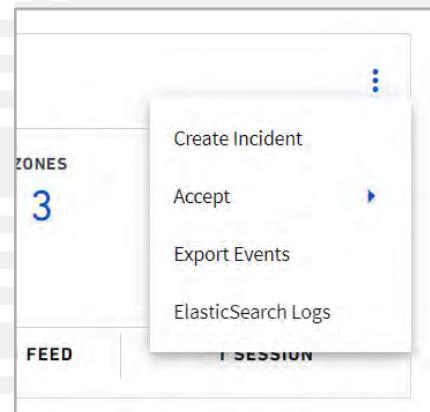
<https://www.cio.com/article/189493/how-can-cisos-tackle-the-soc-talent-shortage.html#:~:text=Embracing%20Automation%20and%20Intelligence,them%20on%20a%20given%20day.>

## Demo



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

### Create Incidents Manually in Advanced Analytics



26

#### Student Notes

The Create Incident option is found through the kebab menu in a Smart Timeline session header and in a User's Risk Reasons on their profile page.

## Editing Incidents

The screenshot shows the 'JDONALDSON: NOTABLE AA SESSION' incident details page. At the top, there are tabs for 'Privilege Abuse', 'Privilege Escalation', 'Behavioral Analysis', 'Privileged Activity', and 'Lateral Movement'. Below these are buttons for 'Abnormal Authentication & Access', 'Compromised Credentials', and 'Account Manipulation'. The top right shows assignee 'tier1-analyst', queue 'Tier 1', status 'New', and priority 'High'. A 'VIEW WORKBENCH' button is also present.

**Incident Type:** Privilege Abuse

**Description:** --

**Vendor:** Exabeam **Created By:** admin

**Source:** Exabeam AA **Creation Time:** 15 March 2022 17:32:19

**Source Severity:** -- **Updated By:** admin

**Source ID:** jdonaldson-20210702152600 **Updated:** 31 March 2022 13:29:56

**Source URL:** https://10.150.0.102:9494/uba/#user/?user=jdonaldson-timeline/jdonaldson-20210702152600 **Resolved Time:** --

**Event Start Time:** 2 July 2021 10:26:00 **Closed Time:** --

**Event End Time:** -- **Closed Reason:** --

**Source Info:** --

**Privilege Abuse:**

User Type:	User Status:
--	--

Account Type:	Access Level:
--	--

Data Accessed:	Data Type Identification:
--	--

**Entities:** ALL, FILE, DEVICE, USER. Selected: jdonaldson

**ACTIONS:**

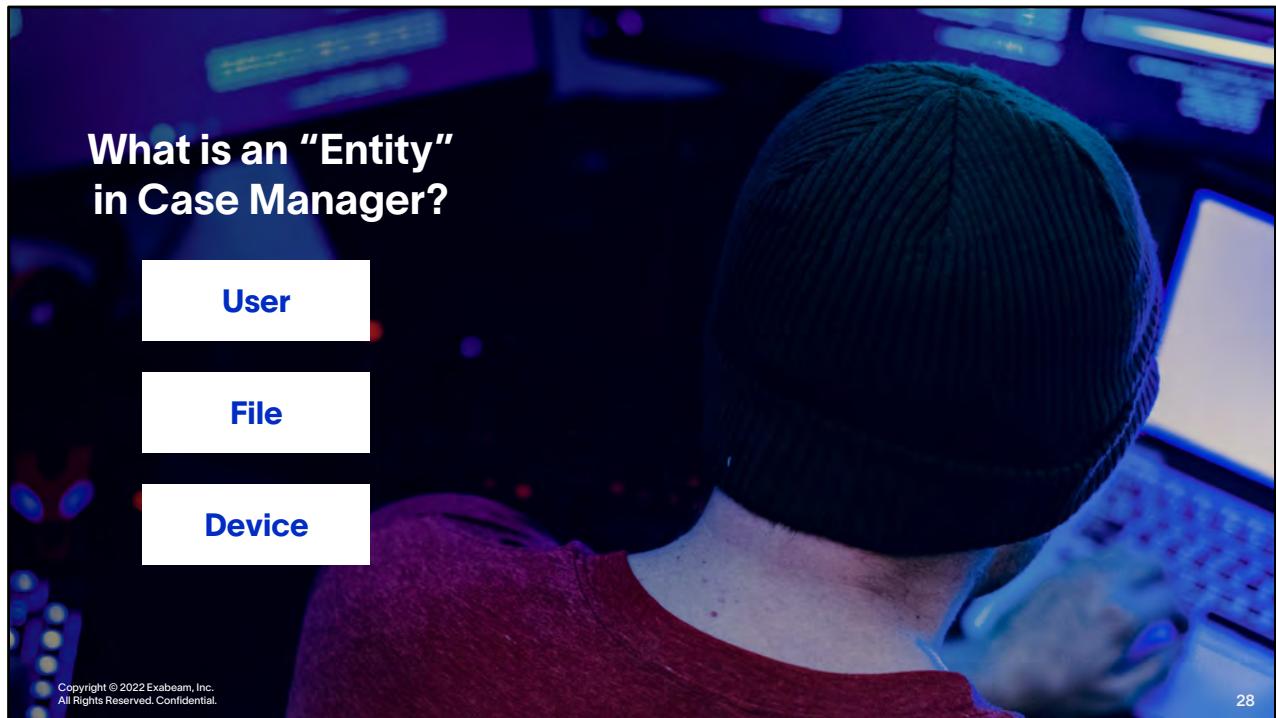
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Add To Incident - Internal 15 March 2022 17:32:41 ✓
- Run Action Based Set Operations... 15 March 2022 17:32:41 ✓

**PLAYBOOKS:**

- Run Action Based Set Operations... 15 March 2022 17:32:41 ✓

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

27



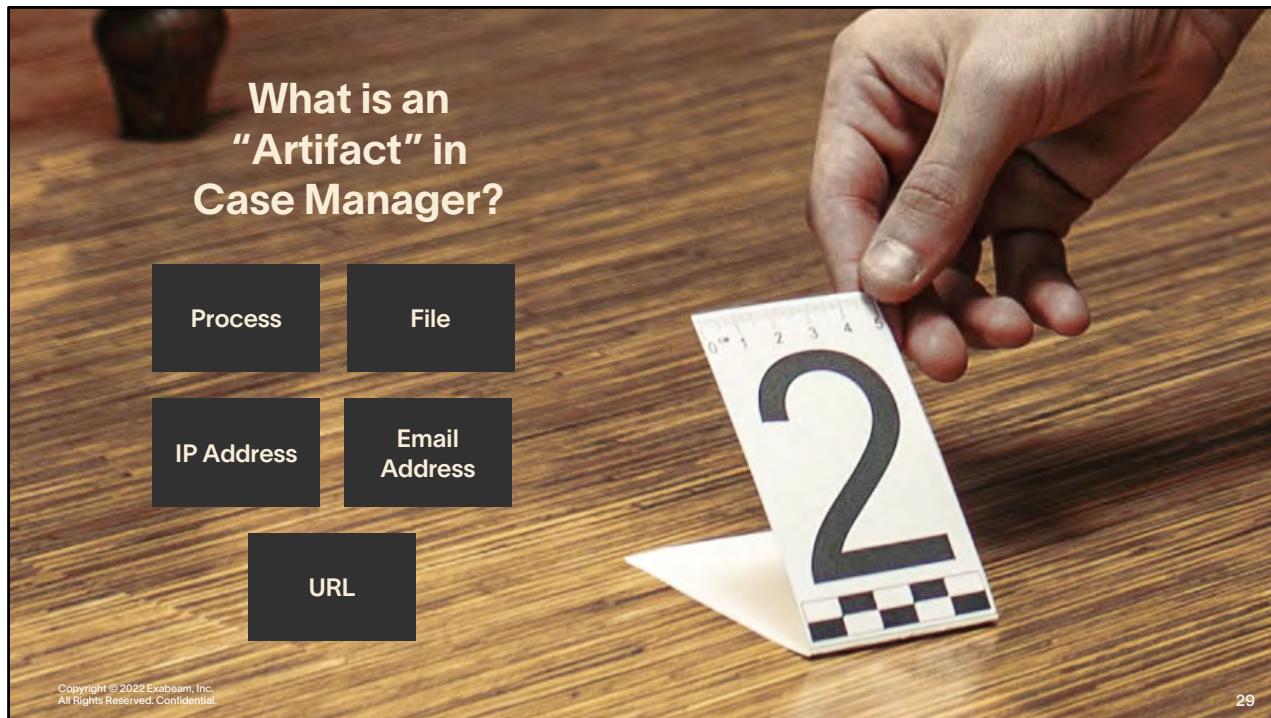
### Student Notes

Entity is the principal object you investigate. It can be a person, an internal or external machine (URL, IP, Domain), or critical data like a file (upload, hash). The default entity types are file, device, and user.

### Source

Advanced Analytics User Guide

In other words, entities are internal corporate resources impacted by an incident. Another way to view them is “internal evidence”. Example: Kathleen Mulligan, sky-eefile-wp1



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

29

### Student Notes

**Artifact** An object you collect during your investigation; a piece of evidence. Once added it can not be removed from the incident because as part of the case which may have legal implications and the digital chain of custody must be preserved.

Artifact types:

- Email Address – An email address observed on an email client or server.
- File - A file observed on a device. It may or may not have a payload. You may retrieve the file, but not download, display, or execute it because it may be malicious.
- IP - An IP address in IPv4 or IPv6 format.
- Process - A process executed by a program observed on an operating system.
- URL – A URL associated with an IP address.

Every artifact type contains a unique set of data. The IP artifact contains data about the IP's geolocation, role, threat status, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

### Source

Advanced Analytics User Guide

In other words, artifacts are external evidence or IoCs gathered during investigation. Another way to view them is "external evidence."

Example:

221.194.44.219, barbarian.jar

# Demo



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Edit Incidents in Case Manager

JDONALDSON-NOTABLE AA SESSION

SOC-32 / 13 March 2022 17:32:19

Assigned: tier1-analyst Queen: Tier 1 Status: New Priority: High

**VIEW WORKSPACE**

**ENTITIES**

ALL FILE DEVICE USER

+ jdonaldson

**ACTIONS**

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Add To Incident - Internal 13 March 2022 17:32:41 ✓

Run Action Based Set Operations. 13 March 2022 17:32:41 ✓

**PRIVILEGE ABUSE**

User Type: — User Status: —

Account Type: — Access Level: —

Data Accessed: — Data Type Identification: —

**INCIDENT DETAILS**

Incident ID: JDONALDSON-NOTABLE AA SESSION

Incident Type: Privilege Abuse

Description: —

Vendor: Exabeam

Exabeam AA

Created By: admin

Creation Time: 13 March 2022 17:32:19

Source: —

Updated By: admin

Source Severity: —

Source URL: https://10.150.5.162:8084/uba/Muse/Hot-AC/jdonaldson/timeline/jdonaldson-20221019T025000

Updated: 13 March 2022 13:29:56

Event Start Time: 2 July 2021 10:26:00

Closed Time: —

Event End Time: —

Closed Reason: —

Source Info: —

**INCIDENT LOGS**

Log ID: JDONALDSON-NOTABLE AA SESSION

Log Type: Incident Log

Log Source: Exabeam

Log Time: 13 March 2022 17:32:19

Log Message: Incident created for user jdonaldson.

Log Details: { "id": "JDONALDSON-NOTABLE AA SESSION", "type": "Incident Log", "source": "Exabeam", "time": "2022-03-13T17:32:19Z", "message": "Incident created for user jdonaldson."}

**INCIDENT FILES**

File ID: JDONALDSON-NOTABLE AA SESSION

File Name: JDONALDSON-NOTABLE AA SESSION

File Type: Incident File

File Size: 1.2 MB

File Last Modified: 13 March 2022 17:32:19

File Details: { "id": "JDONALDSON-NOTABLE AA SESSION", "name": "JDONALDSON-NOTABLE AA SESSION", "type": "Incident File", "size": 1200000, "lastModified": "2022-03-13T17:32:19Z", "details": "Incident file for JDONALDSON-NOTABLE AA SESSION."}

**INCIDENT PLAYBOOKS**

Playbook ID: JDONALDSON-NOTABLE AA SESSION

Playbook Name: JDONALDSON-NOTABLE AA SESSION

Playbook Type: Incident Playbook

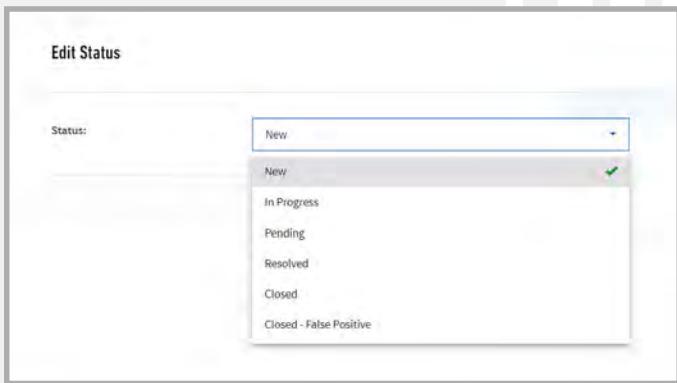
Playbook Status: Active

Playbook Last Modified: 13 March 2022 17:32:19

Playbook Details: { "id": "JDONALDSON-NOTABLE AA SESSION", "name": "JDONALDSON-NOTABLE AA SESSION", "type": "Incident Playbook", "status": "Active", "lastModified": "2022-03-13T17:32:19Z", "details": "Incident playbook for JDONALDSON-NOTABLE AA SESSION."}

## Discussion

What are the important considerations when closing an incident?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



31

### Student Notes

Resolved – means the incident threat has been mitigated.

Closed – means after resolution, all verification and documentation has been completed.

Closed-False positive – means the incident was not true threat

## Case Manager In Action

The screenshot shows the Case Manager interface for an incident titled "JDONALDSON: NOTABLE AA SESSION". The interface includes the following components:

- Incident:** A blue bracket points to the title bar.
- Facilitate Assignment:** A blue bracket points to the top right corner where status and priority are listed.
- Incident Types:** A blue bracket points to the "Incident Type" section, which lists several categories: Privilege Abuse, Privilege Escalation, Behavioral Analytics, Compromised Credentials, Lateral Movement, Abnormal Authentication & Access, and Account Manipulation.
- Entities:** A blue bracket points to the "Entities" sidebar on the right, which displays a list of entities under the "USER" tab, with "jdonaldson" selected.
- Incident Fields:** A blue bracket points to the main incident details table, which contains fields such as Vendor, Source, Source Severity, Source ID, Source URL, and Event Start Time.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

32

## Case Manager In Action

Incident Type

**Behavior Analytics**

Exabeam Risk Score:	93	Reasons Count:	9
User ID:	shahar	Alert Count:	0
Risk Reasons:	First time anyone in the organization has performed this activity in the application First time operating system and browser combination were observed for this user in the event First time a user in this peer group has performed this activity in the application Members of this group do not usually log into this application.		
Timeline Page:	<a href="#">Go to page</a>	Event Count:	196
User Page:	—	Asset Count:	1

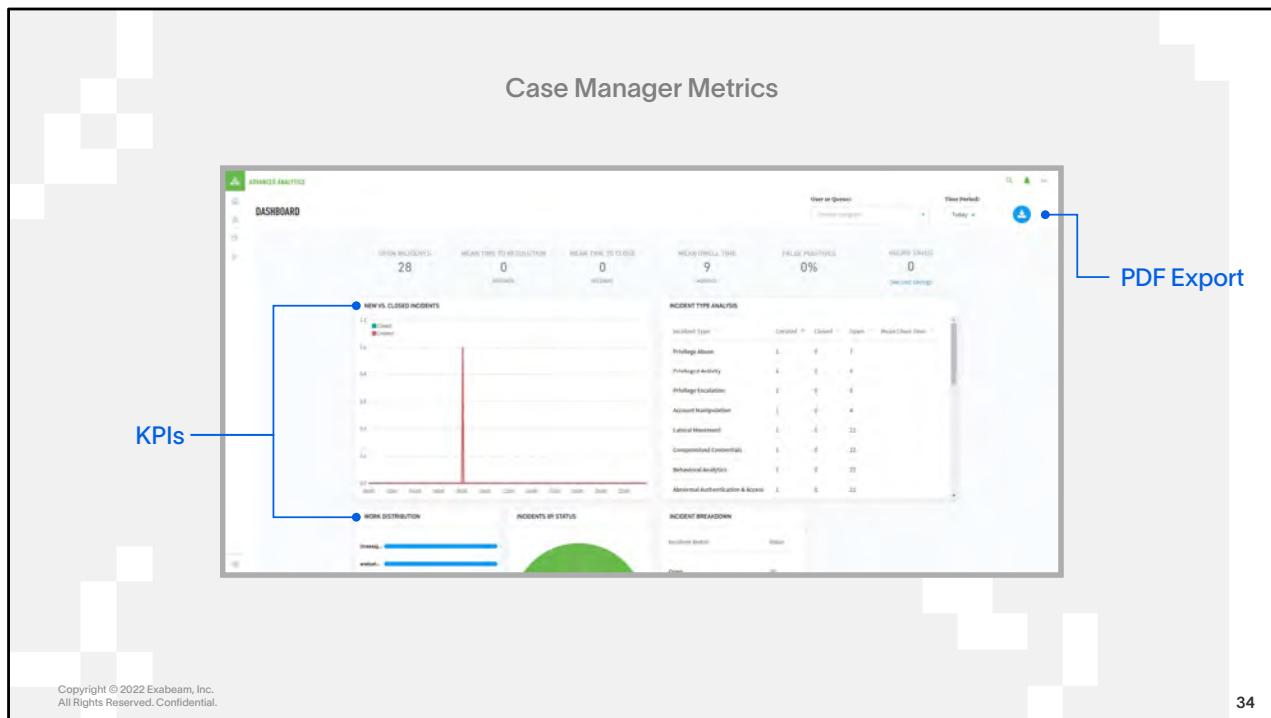
**Malware**

Malware Name:	barbarian malware	Victim Host:	lt-fweber-888
Malware Category:	strain command and control channel	Attacker URL:	221.194.44.219
Knowledge Base:	<a href="https://support.crowdstrike.com/en_US/article/TECH105518.html">https://support.crowdstrike.com/en_US/article/TECH105518.html</a>		
Attacker IP:	221.194.44.219		
Source System:	--		
test field 23:	—		

Incident Type Fields

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

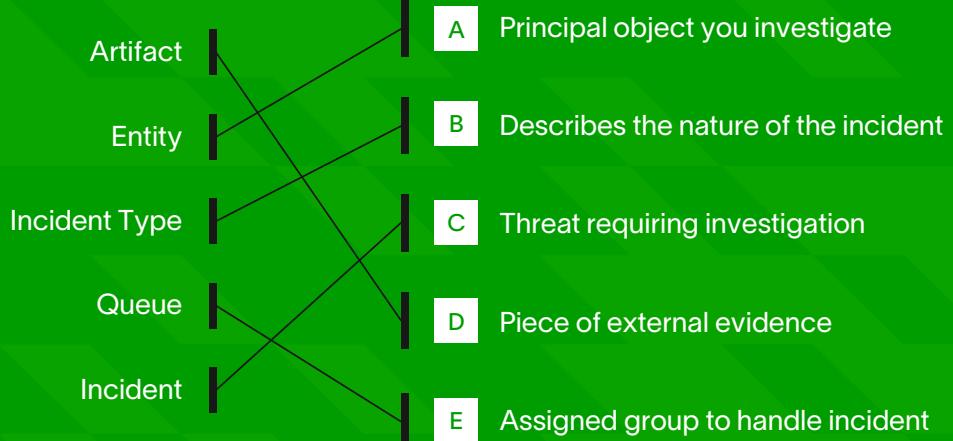
33



### Student Notes

Case Manager Metrics are useful for quantifying the work being done by the SOC team, especially for managers who need to see and report on the big picture.

## Pop Quiz Hotshot!





## Lesson

At the end of this lesson, you will be able to:

1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
2. Do the following:
  1. Recall how incidents are created
  2. Edit an incident in Case Manager
- 3. Execute a turnkey playbook in Incident Responder**
4. Recall where to start an investigation and how to execute the steps in a Case Manager checklist to identify, classify, and respond to an incident
5. Perform the steps of the analyst workflow from start-to-completion

## Discussion

---

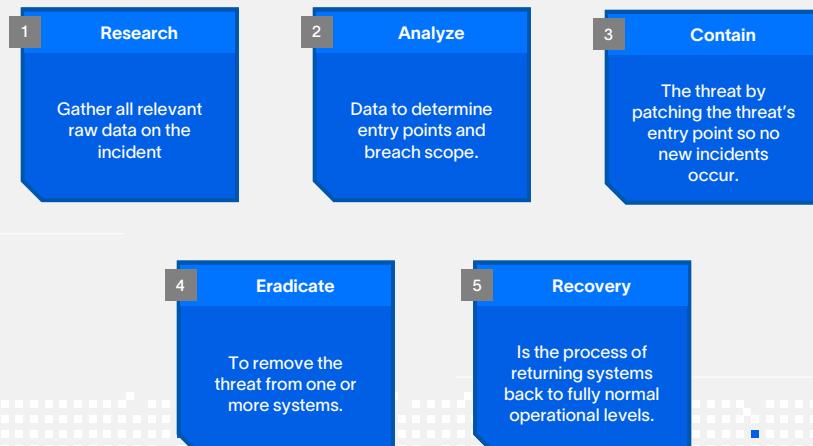
What are **common responses**  
when a threat investigation  
reveals compromise?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



37

## How Long Does This Take?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

38

### Student Notes

- **Research** to gather all relevant raw data on the incident.
- **Analyze** data to determine entry points and breach scope
- **Contain** the threat by patching the threat's entry point so no new incidents occur.
- **Eradication** is about removing the threat from one or more systems
- **Recovery** is the process of returning systems back to fully normal operational levels



## What are Playbooks?\*

Playbooks provide step-by-step actions to respond to high-risk threats

Helps ensure that the Incident Response Plan is followed completely and consistently

\*Requires Exabeam Security Investigation or similar license

# Demo

## A Peek at Playbooks

The screenshot shows a website for the Incident Response Consortium. At the top, there's a navigation bar with links for HOME, ABOUT, RESOURCES (with a dropdown menu), IRC EVENTS, BLOG, FORUMS, and CONTACT. Below the navigation is a section titled "PLAYBOOKS GALLERY". It features a message encouraging users to check out pre-defined playbooks derived from standard IR policies and industry best practices, and to sign up for the newsletter. Below this message are six cards, each representing a different type of incident:

Icon	Name	Description
Malware icon	MALWARE OUTBREAK	Malware is running rampant on the network.
Phishing icon	PHISHING	Someone is trying to take advantage of users.
Data theft icon	DATA THEFT	Data is being extracted by external or internal parties.
Virus icon	VIRUS OUTBREAK	A virus is running rampant on the network.
Denial of service icon	DENIAL OF SERVICE	System performance or availability is compromised.
Unauthorized access icon	UNAUTHORIZED ACCESS	User gains access to network illegally.

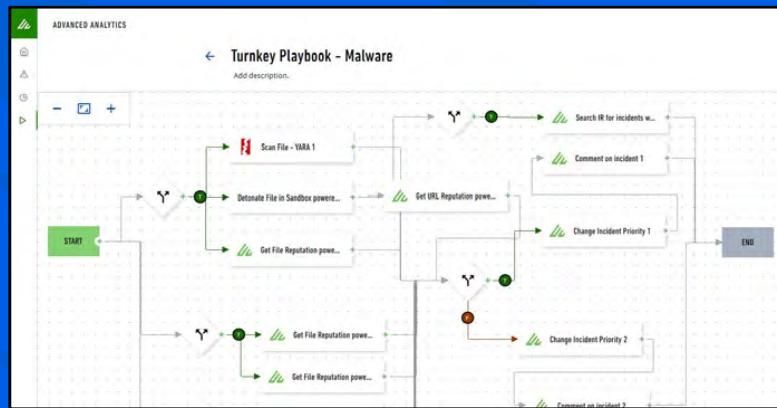


Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

40

## What are Playbooks in Exabeam Incident Responder?

Incident Responder allows analysts to streamline Case Manager workflows by running a **playbook** which contains automated response **actions**



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

41

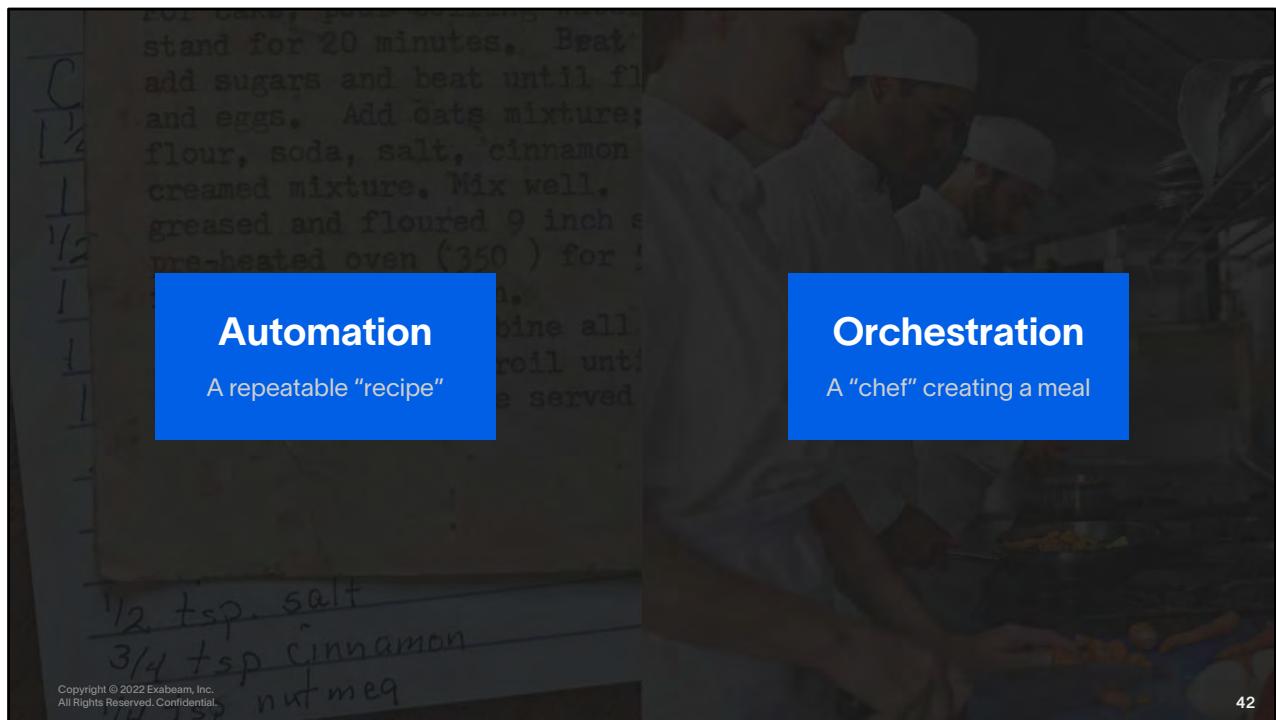
### Student Notes

Incident Responder playbooks are what enables automation and provides orchestration with support for integrating with third-party tools and services.

If you are an overburdened analyst, integrated services and automated workflows help you avoid repetitive tasks and switch between security tools. If you are a SOC manager, Incident Responder helps you deal with talent shortage. You create and maintain playbooks using a simple drag-and-drop editor—you don't need to know how to code. You can even use playbook templates to teach junior analysts about your organization's best practices for common scenarios, like phishing and malware.

### Source

Advanced Analytics User Guide



## Automation

A repeatable "recipe"

## Orchestration

A "chef" creating a meal

### Student Notes

**Automation** is having a computer do a task normally done manually.

- Executes a predefined rigid template
- Decision paths are pre-chosen, and a computer executes tasks

**Orchestration** is having a computer do something based on predefined a set of rules and parameters and input

- The computer "decides" how to get to a result and uses all the various tools available

Image from: [Brown Paper Bag Recipe Cards \(craftingagreenworld.com\)](http://craftingagreenworld.com) – listed as free for commercial use image on Bing image search for recipe card

[Free cozinheiro Stock Photo - FreImages.com](#)

## Playbook Types

**Turnkey**

**Templates**

**Custom**

ADVANCED ANALYTICS

← Turnkey Playbook - Malware

Add description.

```

graph TD
    START([START]) --> Scan[Scan File - YARA 1]
    Scan --> Detonate[Detonate File in Sandbox power...]
    Detonate --> GetURL[Get URL Reputation power...]
    GetURL --> GetFile1[Get File Reputation power...]
    GetFile1 --> GetFile2[Get File Reputation power...]
    GetFile2 --> GetFile3[Get File Reputation power...]
    GetFile3 --> Decision(( ))
    Decision --> ChangePriority1[Change Incident Priority 1]
    ChangePriority1 --> Comment1[Comment on incident 1]
    ChangePriority1 --> END([END])
    Decision --> ChangePriority2[Change Incident Priority 2]
    ChangePriority2 --> Comment2[Comment on incident 2]
    ChangePriority2 --> END
  
```

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

43

### Student Notes

Fully pre-configured turnkey playbooks are ready to run out of the box.

Turnkey playbooks are pre-configured [playbooks](#) that are ready for you to run, without having to purchase additional services to get the actions you need.

They are listed along other playbooks you created on the **PLAYBOOKS** page. Like a playbook you created yourself, you can run them manually or automatically with a [playbook trigger](#).

These playbooks leverage an in-house service, [Exabeam Actions](#), that is available out-of-the-box and free to use. The service supports basic actions, including:

- Get Domain Reputation
- Get URL Reputation
- Get Email Reputation
- Get IP Reputation
- Get File Reputation

To customize a turnkey playbook, you can also use it as a [template](#).

Threat Intelligence Reputation Lookup Turnkey Playbook

Learn about the Threat Intelligence Reputation Lookup [turnkey playbook](#) and how it works.

The Threat Intelligence Reputation Lookup turnkey playbook helps you analyze and triage suspicious emails, like potential spam and phishing emails. It changes a Case Manager incident's priority based on the reputation of an [email entity](#) and its [artifacts](#).

First, the playbook assesses the reputation of the incident's entities and artifacts, including:

- Files attached to the email
- IP addresses
- Domains of any URLs in the email body
- Domain of the sender's email address

If the playbook finds any IP addresses with a malicious reputation, it searches for other incidents that has the same IP address entity or artifact. View the output in the incident's [workbench](#).

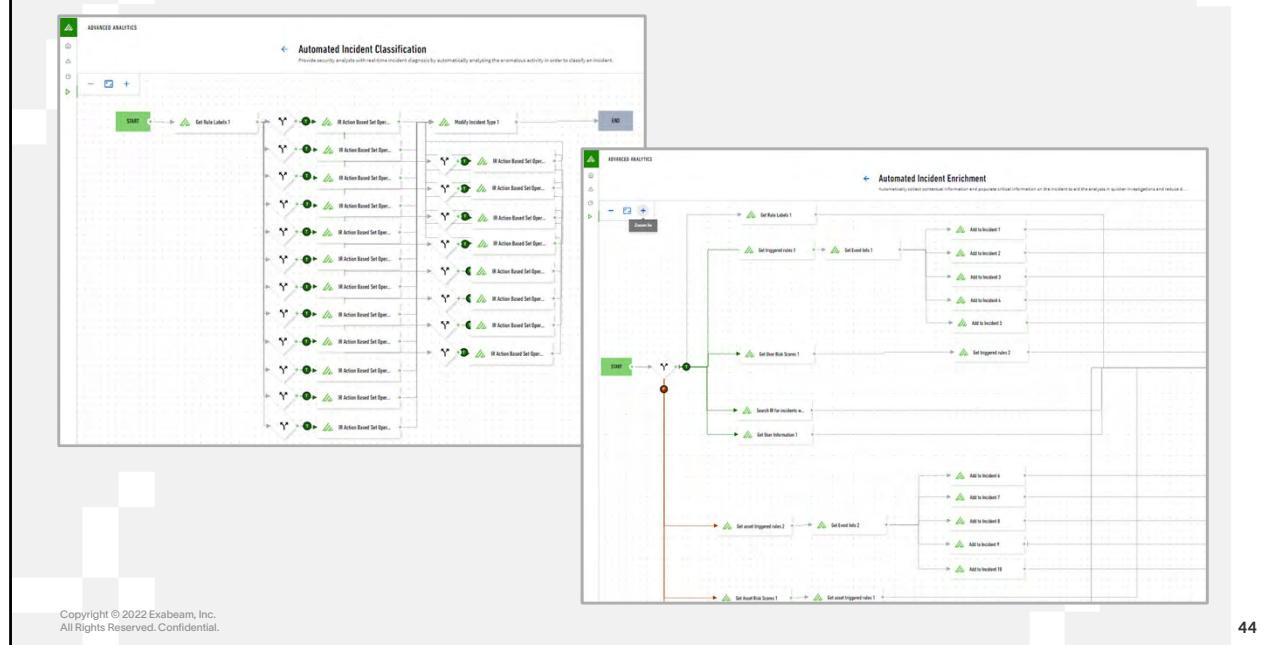
If any entity or artifact has a malicious reputation, the playbook escalates the incident's priority to critical. If none of the artifacts have a malicious reputation, the playbook de-escalates the incident's priority to low.

### Source

<https://docs.exabeam.com/en/incident-responder/i53/respond-to-security-incidents/106286-turnkey-playbooks.html>

Advanced Analytics User Guide

## Automatic Classification & Enrichment Turnkey Playbooks



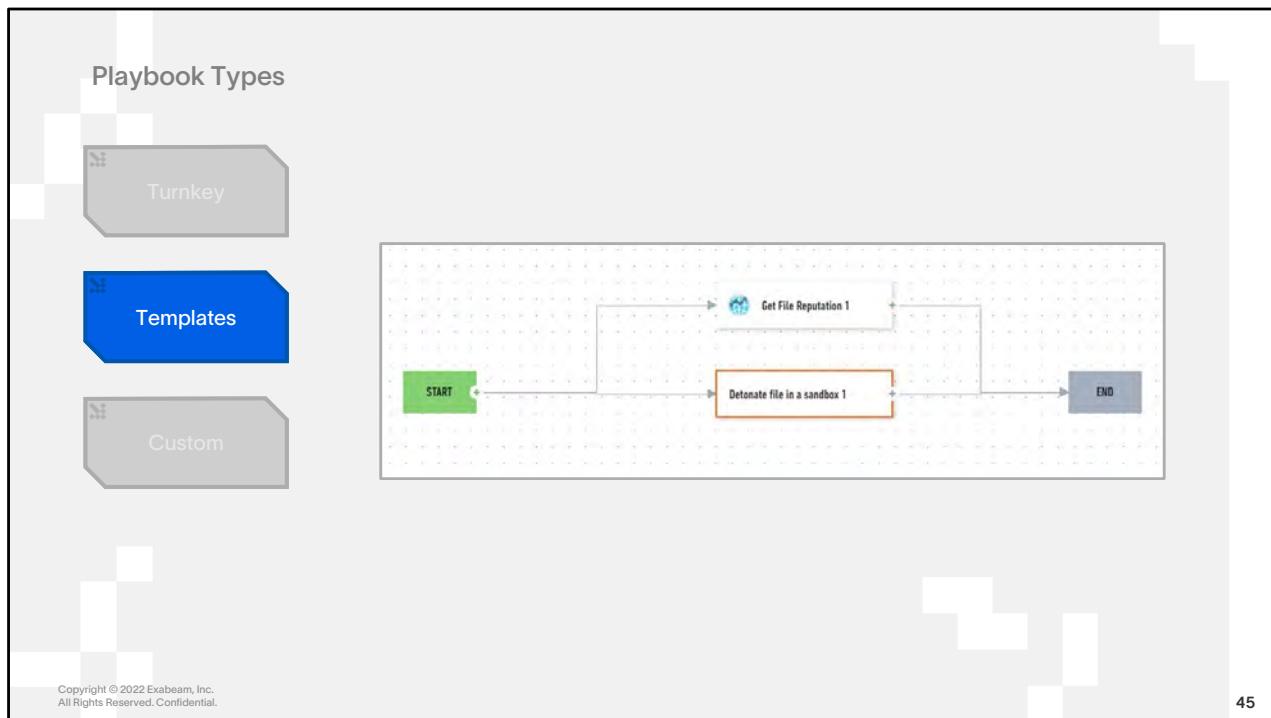
### Student Notes

When an Advanced Analytics user or asset session becomes notable, Case Manager automatically creates an incident with the *Behavior Analytics* incident type. The Automated Incident Classification turnkey playbook analyzes the labels of the triggered rules in the session to accurately change the incident's type, helping you make sense of all the evidence in Advanced Analytics and quickly diagnose what threat you're investigating.

The Automated Incident Enrichment turnkey playbook gathers additional contextual or supporting information from the Advanced Analytics session and populates the Case Manager incident, so you have everything you need to investigate the incident.

### References

- <https://docs.exabeam.com/en/cloud-delivered-incident-responder/all/incident-responder/172044-respond-to-security-incidents.html#UUID-de815c14-968c-e52a-2e65-a97541c6709a>
- <https://docs.exabeam.com/en/cloud-delivered-incident-responder/all/incident-responder/172044-respond-to-security-incidents.html#UUID-1252c0f6-72dc-b033-d736-373f89ba180b>



### Student Notes

If you don't want to create a playbook from scratch, use a template. These templates come out-of-the-box, or you can import your own from an existing playbook.

Playbook templates are frameworks that are already designed and ready for you to use. When you create a playbook from a template, just indicate the service you want to use.

There are 16 templates available out of the box, including ones for malware and [phishing](#).

### Source

Advanced Analytics User Guide

## Playbook Types

The diagram illustrates three categories of Playbooks:

- Turnkey**: Represented by a grey rounded rectangle.
- Templates**: Represented by a grey rounded rectangle.
- Custom\***: Represented by a blue rounded rectangle, indicating it requires an additional license.

\*Requires an IR add-on license

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

46

### Student Notes

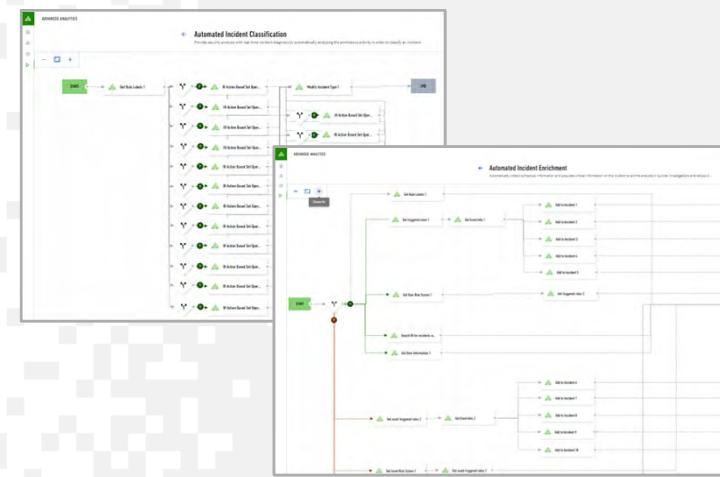
A Playbook can be built from scratch with no predefined nodes in place. This requires an additional license.

### Source

Advanced Analytics User Guide

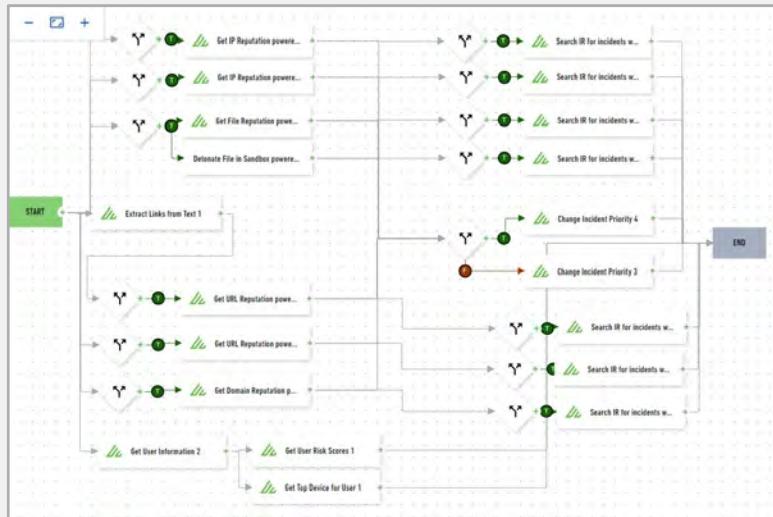
# Demo

## A Look at Turnkey Playbooks in Incident Responder



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## How Long Would This Take If Executed Manually?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

48

### Student Notes

Below are the steps in the phishing playbook that is available out of the box. How long would it take to do this manually?

1. Trigger playbook when suspicious email is forwarded to phishing-triage inbox
2. Enrich links and other information from an email with **threat intelligence**
3. If present, detonate file attachments in a sandbox using **malware analysis**
4. Hunt for files in across an environment with an **endpoint detection and response (EDR) tool**
5. Summarize and report via **email**



## Lesson

At the end of this lesson, you will be able to:

1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
2. Do the following:
  1. Recall how incidents are created
  2. Edit an incident in Case Manager
3. Execute a turnkey playbook in Incident Responder
- 4. Recall where to start an investigation and how to execute the steps in a Case Manager checklist to identify, classify, and respond to an incident**
5. Perform the steps of the analyst workflow from start to completion

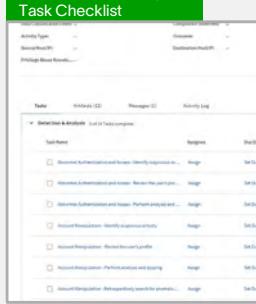
## Incident-driven Analyst Workflows

Notable Users, Alert Triage, SIEM, or Email Ingestion trigger the creation of Incidents that need analyst attention

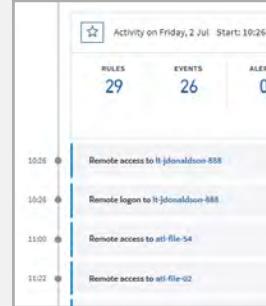
### Open your incident



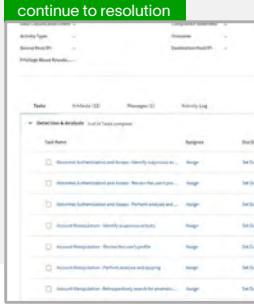
### Read and start using the Task Checklist



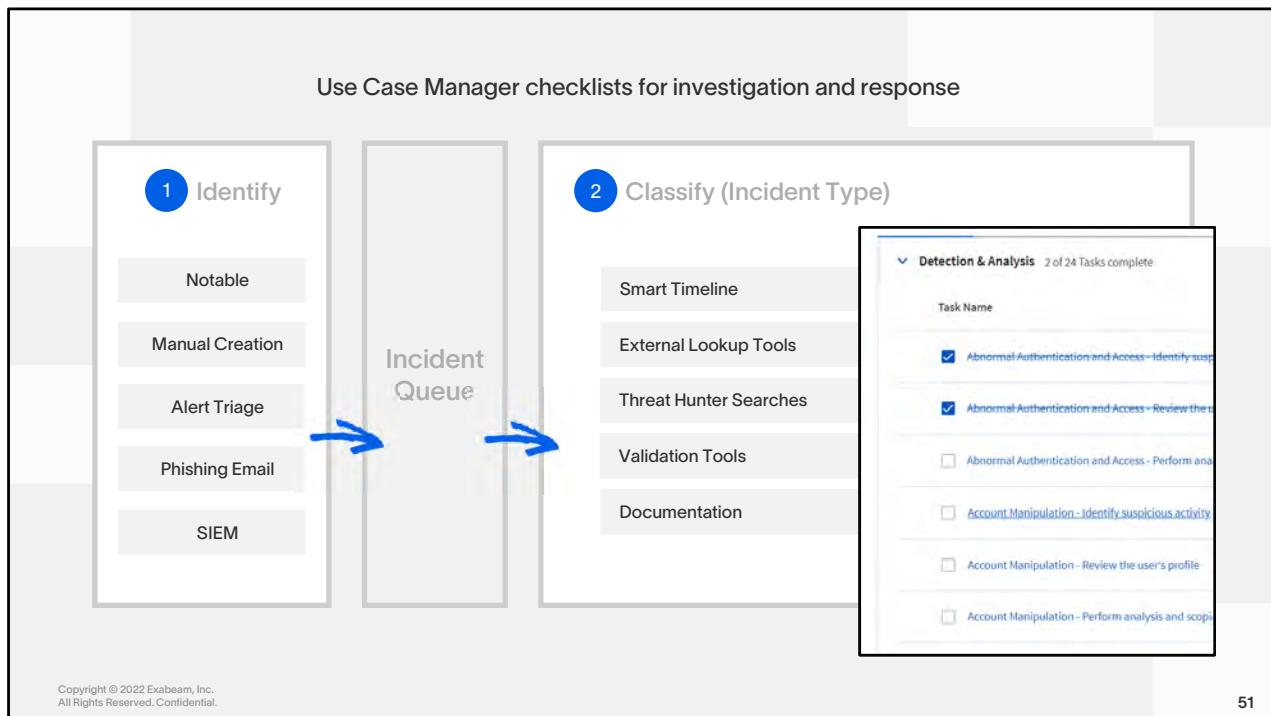
### Investigate using Exabeam and third party tools



### Complete tasks and continue to resolution



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



### Student Notes

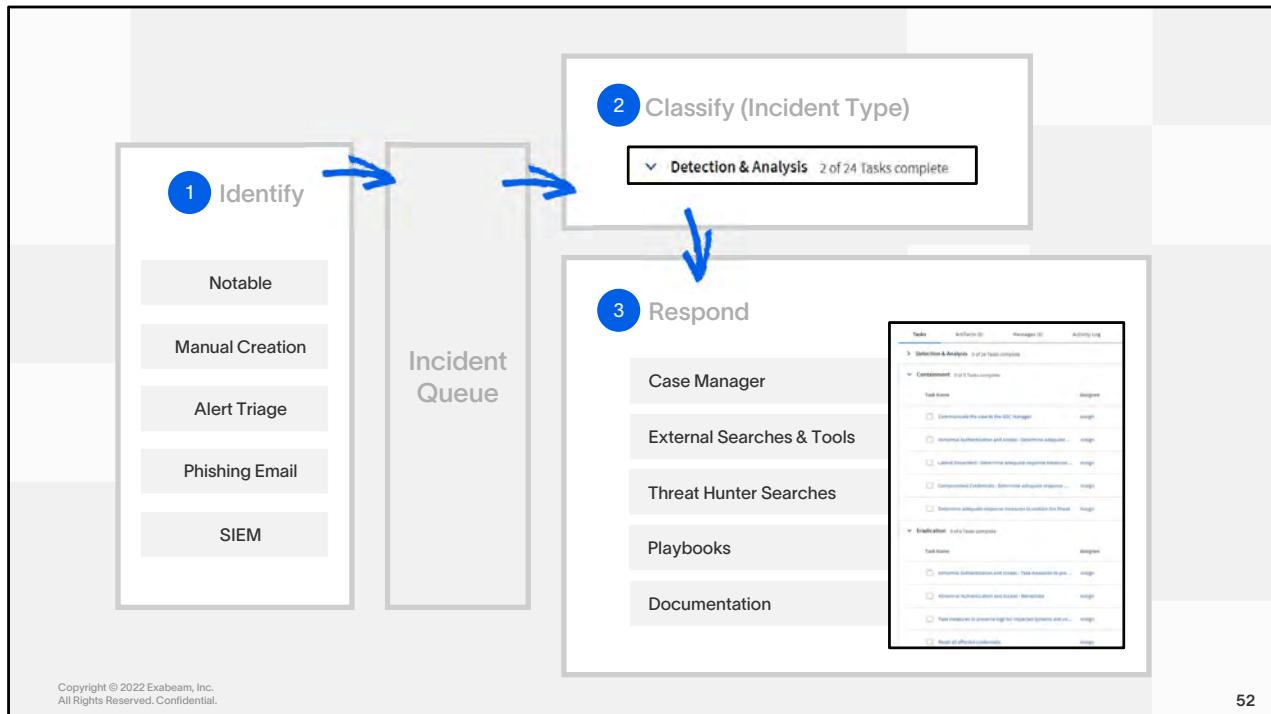
#### Case Management in CMIR

Step One:

The first step is to identify the type of the incident, e.g. is it malware, phishing etc.?

Step Two:

Once the incident type has been identified, additional details each response phase should be listed for consistent efficient workflow.



## **Student Notes**

### **Case Management in CMIR**

**Step Three:**

The next step is to respond by running threat hunter and external searches, playbooks and providing documentation and team communication.

## Proactive Searches that May Lead to an Incident

When analysts discover a potential threat they can manually create an incident

The screenshot displays the Exabeam security analytics platform interface across four main panels:

- Watchlists:** Shows a list of "Executive Users" with their roles and counts of notable events. The users listed are Andrew Bautista (vp sales), Chelsea Mayo (vp business ...), Emely Blanch... (CEO), and Emery Santiago (vp council). A total of 11 users are tracked, with 0 notable events.
- Basic Search:** A search interface for "fredric". It shows results for "USERS" (Fredric Weber, Fredric Hanna, Fredric Leach, Fredric Lowery, Fredric Odem) and "ASSETS" (no search results found). It also includes a "SEQUENCE" section (no search results found).
- Threat Hunter:** A search interface for "THREAT HUNTER". It allows filtering by "Rule Tags", "Reasons", "Scores", "Geo Locations", and "Network Zones". A "Search" button is at the bottom right.
- Data Insights:** Shows histograms for "MODEL NAME: RL-UH" and "GPV: Green". The "Assets" section displays "Remote logins" for the user "administrator". A summary table shows metrics: CONFIDENCE Excellent - 100%, EVENTS 39, VALUES 4, LAST UPDATE 9 months ago. A "Enter text to filter" input field and a "Search" button are also present.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

53

### Student Notes

Analysts and threat hunters may discover potential threats using the following:

- Watchlists allow analysts to keep tabs on the “crown jewels”
- Basic Search feature is very handy for SOC analyst who already have a suspicious username or alert from a security system
- Threat hunter allows analysts to find sessions that match certain criteria related to actions and risk
- Data insights allows analysts to focus on behavior types monitored by the analytics engine

Any of these starting points could lead analysts to investigate a user, review their timeline, and determine that there is a possible threat and a need to manually create an incident

# Demo



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

**Watchlists**  
Executive Users Last day  
Andrew Bautista vp sales 0  
Chelsea Mayo vp business ... 0  
Emely Blanch... CEO 0  
Emery Santiago vp council 0  
TOTAL 11 USERS 0 NOTABLE

**Basic Search**  
users  
Fredric Weber - web developer  
Fredric Hanna - web developer  
Fredric Leach - machine  
Fredric Lowery - program manager  
Fredric Odom - sales coordinator  
ASSETS  
No search results found  
SEQUENCE  
No search results found

**Threat Hunter**  
THREAT HUNTER Rule Tags Reasons Scores Geo Locations Network Zones Search

**Data Insights**  
MODEL NAME: RI-UH OFV Gross  
Showing histograms for - MODEL NAME: RI-UH  
**Assets**  
Remote logons  
CONFIDENCE EVENTS VALUES LAST UPDATE  
Excellent - 100% 39 4 9 months ago  
Enter text to filter  
REMOTE LOGON COUNT PCT.

What is the difference between notables and watchlists?

NOTABLE USERS		
	Julietta Donaldson it administr...	2 JUL 624
	Billie Wells civil engineer	2 JUL 328
	Barbara Salazar human reso...	2 JUL 309

Departing Employees		
	Gary Hardin software eng...	2 JUL 198

Executive Users		
	Andrew Bautista vp sales	0
	Chelsea Mayo vp business ...	0
	Emely Blanch...	0

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

55

### Student Notes

Notables in Advanced Analytics are built in watchlists that automatically populate when a predefined threshold risk score is reached (default of >=90 risk score). They cannot be added to or deleted from.

The “watchlist” however is a fundamental part of the Advanced Analytics dashboard for at-a-glance alerting based on UEBA risk score alerts. They are created by analysts to proactively monitor high-risk and/or high-value users and assets such as service accounts and executive users.

They can also be used for policy and compliance situations and other unique use cases.

### More Information

<https://www.exabeam.com/ueba/financial-institutions-and-ueba-fdic-vacation-policy-use-case/>

## Watch the Watchlist

Attend to vulnerable users and assets

Executive Users		
Last day		
	Andrew Bautista vp sales	0
	Chelsea Mayo vp business ...	0
	Emely Blanch... ceo	0

Observe  
Watchlist

Review  
User Profile

Review  
Timeline

Create  
Incident

Search for someone

Search for “interesting” users and assets

The screenshot shows a search interface with the query 'fredinc'. The results are categorized into 'USERS' and 'ASSETS'. Under 'USERS', there are five entries: Fredric Weber (web developer), Fredric Hanna (web developer), Fredric Leach (machinist), Fredric Lowery (program manager), and Fredric Odom (sales coordinator). Under 'ASSETS', it says 'No search results found.' At the bottom, there is a timeline bar with a red marker at position 624, and a note stating 'There are currently no notable assets in selected time range'.

Run  
Search

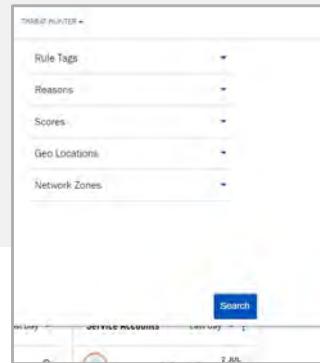
Review  
User Profile

Review  
Timeline

Create  
Incident

**Threat Hunter elevates the non-notable**

**Search for specific symptoms for threats  
you are concerned about**



Run  
Threat  
Hunter  
Search

Review  
User Profile

Review  
Timeline

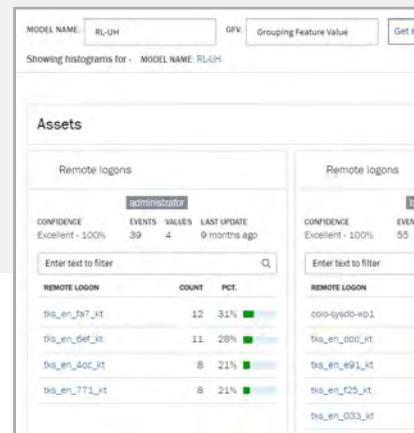
Create  
Incident

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

58

## Data Insights Exposes Models

Search for Models to look for trends among the results



Data  
Insights  
Search

Review  
User Profile

Review  
Timeline

Create  
Incident

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

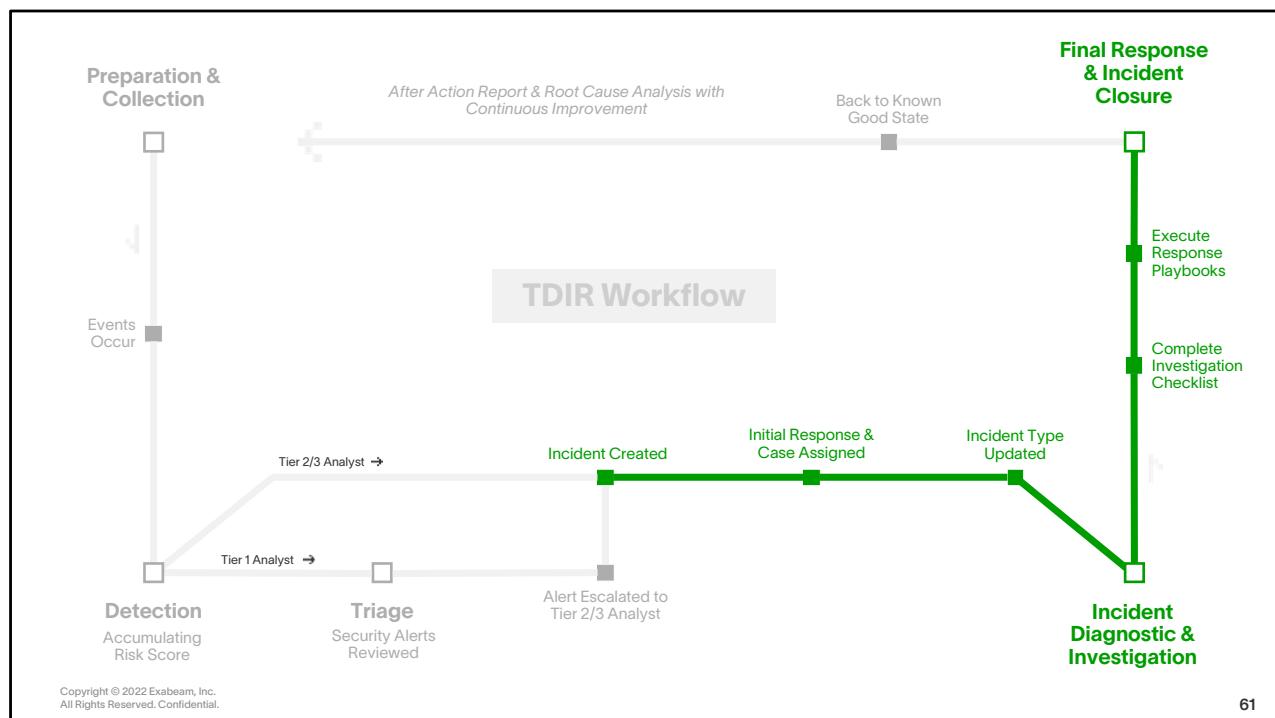
59



## Lesson

At the end of this lesson, you will be able to:

1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
2. Do the following:
  1. Recall how incidents are created
  2. Edit an incident in Case Manager
3. Execute a turnkey playbook in Incident Responder
4. Recall where to start an investigation and how to execute the steps in a Case Manager checklist to identify, classify, and respond to an incident
- 5. Perform the steps of the analyst workflow from start to completion**



# Demo

Putting it all together: end-to-end workflow

Tasks	Artifacts (0)	Messages (0)	Activity Log
> Detection & Analysis 0 of 24 tasks complete			
▼ Containment 0 of 5 Tasks complete			
Task Name	Assignee	Due Date	
<input type="checkbox"/> Communicate the case to the SOC Manager	Assign	Set Due Date	<a href="#">ADD TASK</a>
<input type="checkbox"/> Abnormal Authentication and Access - Determine adequate ...	Assign	Set Due Date	
<input type="checkbox"/> Lateral Movement - Determine adequate response measures...	Assign	Set Due Date	
<input type="checkbox"/> Compromised Credentials - Determine adequate response ...	Assign	Set Due Date	
<input type="checkbox"/> Determine adequate response measures to contain the threat	Assign	Set Due Date	
▼ Eradication 0 of 8 Tasks complete			
Task Name	Assignee	Due Date	
<input type="checkbox"/> Abnormal Authentication and Access - Take measures to pre...	Assign	Set Due Date	
<input type="checkbox"/> Abnormal Authentication and Access - Remediate	Assign	Set Due Date	
<input type="checkbox"/> Take measures to preserve logs for impacted systems and us...	Assign	Set Due Date	
<input type="checkbox"/> Reset all affected credentials	Assign	Set Due Date	

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

**NOTABLE USERS** Last day

Julietta Donaldson (jdonaldson,...) It administrator Chicago 2 JUL 624

**ADVANCED ANALYTICS**

**Julietta Donaldson** (jdonaldson,...) It administrator Chicago Manager Felipe Penning... Top Peer Group Risk Score 60

FIRST SEEN 1 Jun 2021 LAST SEEN 3 Jul 2021 ACCOUNT STATUS — EMPLOYEE TYPE employee LAST PASSWORD RESET — 1 COMMENT

**UNDER INVESTIGATION 4 ACTIVE INCIDENT(S)**

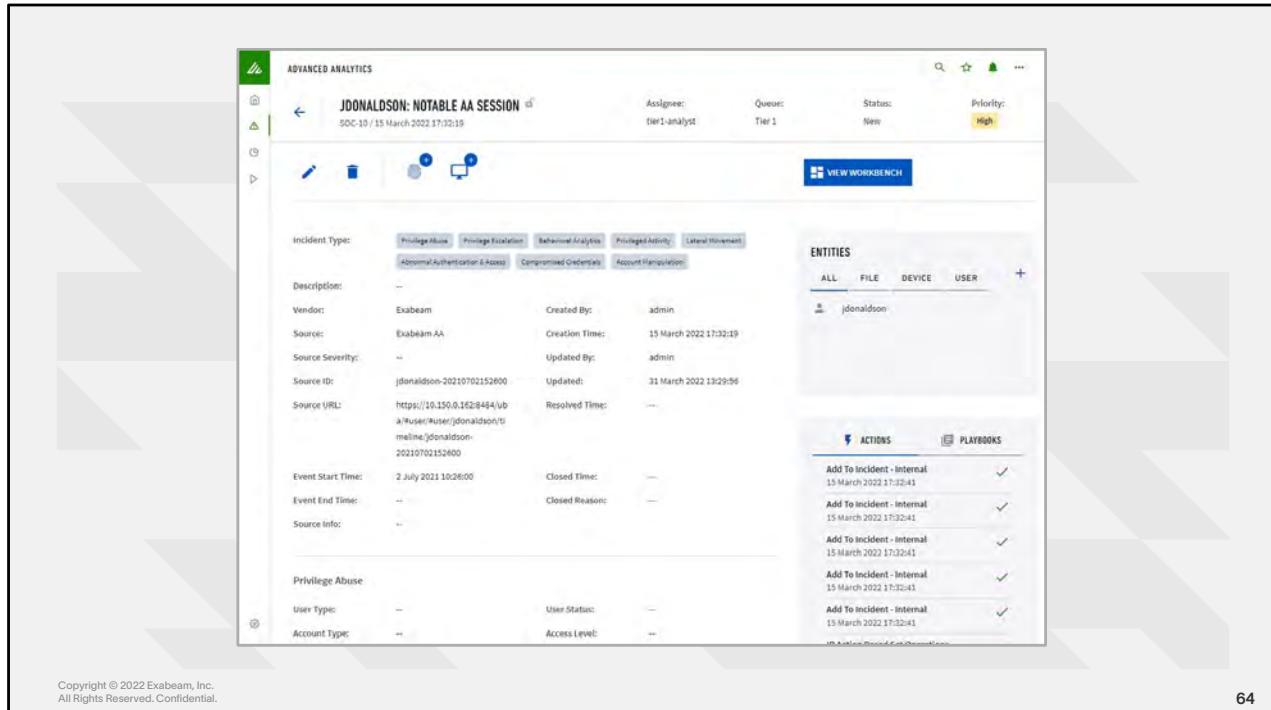
Incident	Priority	Status	Assignee
jdonaldson: Notable AA Session SOC-10- 15 MAR	HIGH	NEW	Ser1-analyst
jdonaldson-03: Notable AA Session SOC-26- 10 MAR	MEDIUM	NEW	Unassigned
jdonaldson: Notable AA Session SOC-27- 10 MAR	MEDIUM	NEW	Unassigned
jdonaldson-03: Notable AA Session SOC-26- 11 MAR	HIGH	INPROGRESS	analyst-03

**USER RISK TEND** 1 week

**FEEDS** SESSION RULES 29 EVENTS 26 ALERTS 0 ACCOUNTS 3 ASSETS 24 ZONES 4 SCORE 624

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

63



The diagram illustrates the flow of data and relationships between four different user interface components:

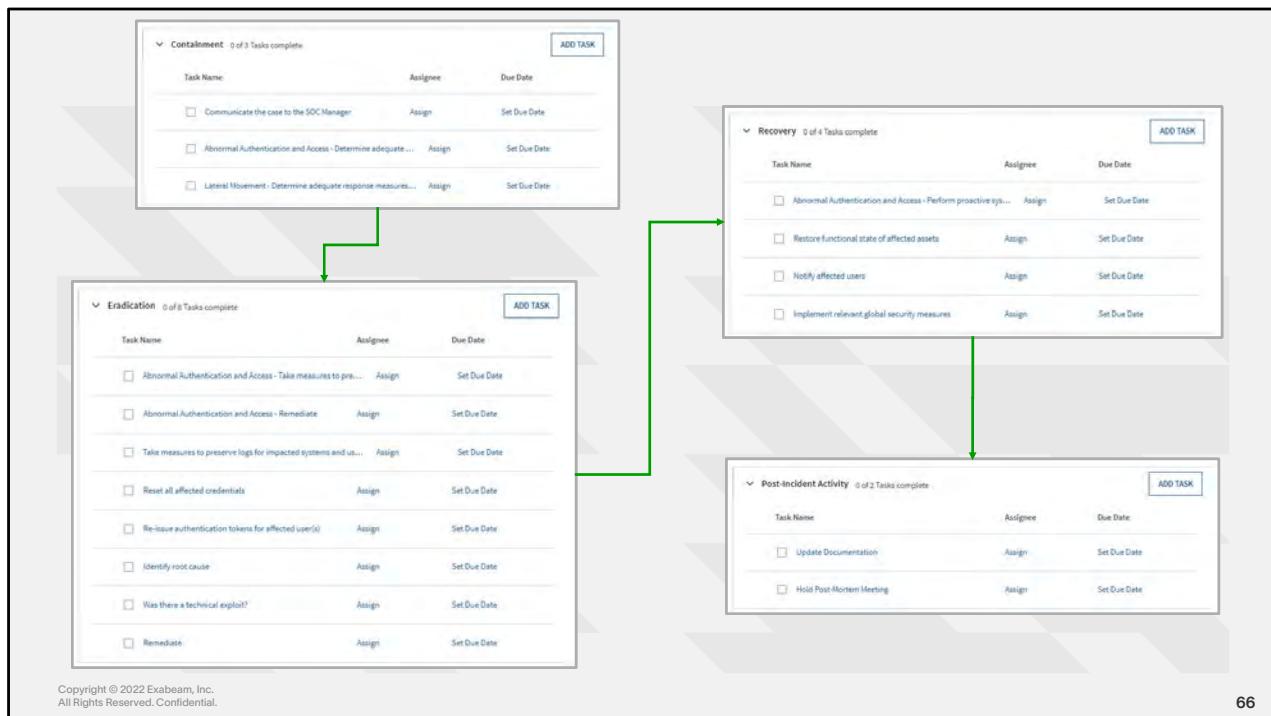
- Detection & Analysis**: A list of tasks under categories like 'Detection & Analysis', 'Containment', 'Eradication', and 'Recovery'. It includes columns for Task Name, Assignee, and Due Date.
- Edit Incident Type**: A modal dialog for editing incident types. It shows a list of selected incident types: 'Abnormal Authentication & Access' (selected), 'Lateral Movement' (selected), 'Behavioral Analytics' (selected), and 'Compromised Credentials'. Buttons for 'CANCEL' and 'SAVE' are at the bottom.
- Case Details**: A panel showing 'No Messages' and a note to 'Add a new case note or send an email message.' It has buttons for 'EMAIL MESSAGE' and 'NEW CASE NOTE'.
- Case Log**: A list of tasks similar to the main interface, showing progress (e.g., 0 of 10 Tasks complete) and columns for Task Name, Assignee, and Due Date.

Green arrows indicate the flow of data or relationships:

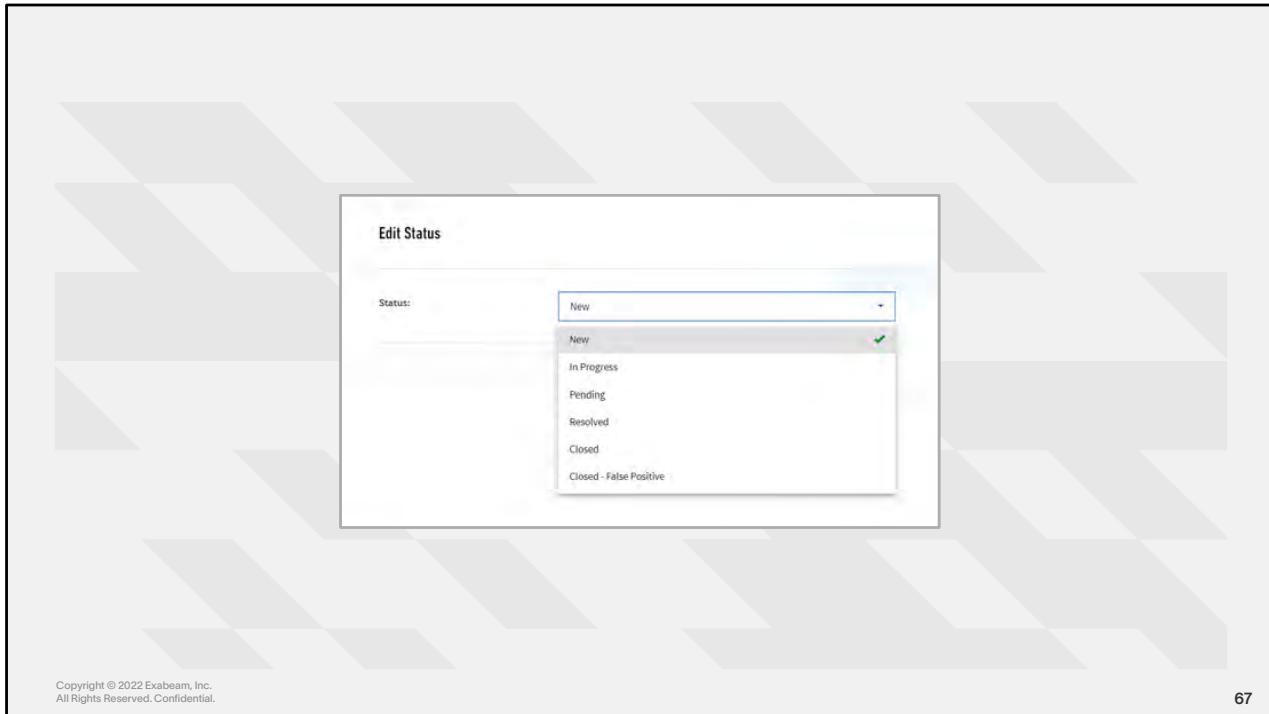
- An arrow points from the 'Edit Incident Type' window down to the 'Case Details' panel.
- A curved arrow points from the 'Edit Incident Type' window down to the 'Case Log' panel.
- A vertical arrow points from the 'Case Details' panel up to the 'Case Log' panel.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

65



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



## Activity

Practice executing analyst workflow  
using Case Manager, Incident  
Responder, and Alert Triage

### Objectives:

1. Open an incident from incident queue
2. Review incident details and update incident type
3. Use the built-in checklist to investigate, contain, respond, and close an incident
4. Start an investigation proactively using Watchlists or Search
5. Investigate proactively by searching for rules in Data Insights
6. Use Histograms to detect normal and erratic behavior
7. Search using Threat Hunter to find obscure threats
8. Use Alert Triage to Escalate a concerning Alert to an Incident

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



68



## Summary

### Can You Do the Following?

1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
2. Do the following:
  1. Recall how incidents are created
  2. Edit an incident in Case Manager
3. Execute a turnkey playbook in Incident Responder
4. Execute the steps of the Exabeam analyst workflow
5. Become practically familiar with the analyst workflow

## What is An "Action" in Incident Responder?

The screenshot shows the 'Action Launcher' interface. At the top, it says 'Action Launcher' and 'Choose from the list or start typing to select an action to run.' Below this is a dropdown menu labeled 'Action:' with the placeholder 'Select an action'. A list of actions is displayed in a scrollable window:

- AWS EC2 Security Filter Type - Returns Security Groups for a given EC2 instance
- Accept Asset Session - Accepts an entire asset session in Advanced Analytics.
- Accept Rule - Accepts one or more rules within a session in Advanced Analytics.
- Accept User Session - Accepts an entire session in Advanced Analytics.
- Activate - Activates configuration changes.
- Add Api-managed category - Action can be used to add categories as containers for URLs and IP addresses.

On the left side of the interface, there is a blue button with a white lightning bolt icon and the text 'RUN ACTION'.

At the bottom left, there is a copyright notice: 'Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential.' On the right side, the number '70' is visible.

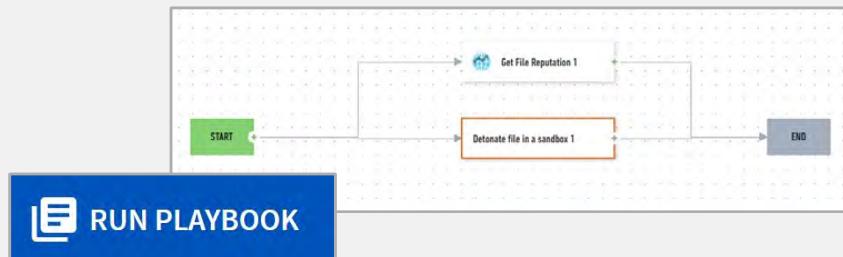
### Student Notes

An Action is the command issued to a service (via an API call written in python)

Turnkey playbooks have access to out-of-the-box services

Custom playbooks with Incident Responder allow custom services and custom actions to existing services.

## What is a “Playbook” in Incident Responder?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

71

### Student Notes

Automate your tasks, immediately neutralize attacks, and mitigate damages with Exabeam playbooks. A playbook is a standard, repeatable sequence of actions that responds to specific incident types, like phishing or malware, based on your best practices. It automates your workflow and completes complex, manual, and repetitive tasks so you quickly identify and address incidents.

You design a logic flow that triggers the playbook under certain conditions. Then, the playbook automatically runs the relevant responses. You make workflows semi-automated, so it runs at the push of a button, or fully automated so it runs without any human intervention.

You manage a playbook and track its history in an incident's workbench.

### Source

Advanced Analytics User Guide



**Services Provide 3<sup>rd</sup> Party Automation Integration**

Service Integration

VirusTotal ThreatGrid

Wildfire EC2

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

72

### Student Notes

A third-party product or vendor you integrate with Incident Responder to run actions and playbooks.

For example: Cisco Threatgrid, Palo Alto Networks Wildfire.

You interact with multiple instances of a service from within Incident Responder.

Information about a service, like how to connect to it and which actions are defined, is stored in the Incident Responder server.

### Source

Advanced Analytics User Guide

## Service Examples

Active Directory

Exabeam Data Lake

Palo Alto Wildfire

SERVICENOW

## Action Examples

Get domain reputation

Detonate File

Kill Process

Block URL



## Service Examples

**Active Directory**

**Exabeam Data Lake**

**Palo Alto Wildfire**

**SERVICENOW**

## Action Examples

Get domain reputation

Detonate File

Kill Process

Block URL

## Example of Service Integrations in Playbook

Playbook Report

The screenshot displays a 'Playbook Report' interface with three main sections:

- DOMAIN SECURITY SCORE - CISCO UMBRELLA:** A table showing various indicators and their scores:

Indicator	Score
Dga Score	96.0
Rip Score	-0.550336855296
Asn Score	-0.119374892914
Securerank2	-0.470311143289
Popularity	11.2676316695
Geoscore	0.0
Ks Test	0.0
Pagerank	1.7400709
- GET FILE REPUTATION - VIRUSTOTAL:** A summary of a file scan:

File Hash	Scan Date	Result	Signature
275a021bbfb6489e...	2017-03-28 16:05:00	infected	barbarian.jar

[View Reputation Report in VirusTotal](#)
- DETECTIVE FILE - WILDFIRE:** A list of detected artifacts:

Artifact Type	Count	Severity
Barbarian 3.1 Trojan Detected	100	100
Backup Deletion Detected	100	100
Shadow Copy Deletion Detected	100	100
Artifact Flagged Malicious by Antivirus Service	100	95
Artifact Flagged as Known Trojan by Antivirus	100	95
Large Amount of High Entropy Artifacts Written	100	95
Public IP Check With Registry Persistence in a Suspicious Location	90	100
Registry Persistence Mechanism Refers to an Suspicious Location	90	100

A blue callout labeled "Service Integrations" points from the right side of the VirusTotal section towards the Palo Alto Networks section.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Example of Configuring ServiceNow Ingest

**Incident Source**

**Edit Incident Source**

Server Type\*: ServiceNow

IP Address or Hostname\*: dev66497.service-now.com

TCP Port\*: 8000  Enable SSL (HTTPS)

Username\*: admin

Password\*:

**TEST CONNECTIVITY** Cancel **SAVE**

**Incident Feed**

**Edit Incident Feed**

Incident Sources\*: ServiceNow  
There's only one server setup in the system.  
 Apply query to all instances of this server type [i]

Log Type\*: Custom

Query Short Name\*: AllIncidents

Search Query\*: \*

**CANCEL** **SAVE**

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



How Do You Get More Services and Actions?

The screenshot shows the Exabeam Cloud Platform (ECP) interface. On the left, there is a sidebar with 'SETTINGS' and 'SERVICES' sections. Under 'SERVICES', there are two items: 'OTX' and 'Atlassian JIRA'. On the right, the main area is titled 'exabeam Home' and displays a welcome message: 'Hi Jacob, welcome to Exabeam Cloud Platform!'. Below this, there is a section titled 'My applications' which lists 'AUTO PARSER GENERATOR' and 'ACTION EDITOR'. The 'ACTION EDITOR' card is highlighted with a blue border. The bottom left of the screen has a copyright notice: 'Copyright © 2022 Exabeam, Inc. All Rights Reserved. Confidential.' and the bottom right corner has the number '77'.

### Student Notes

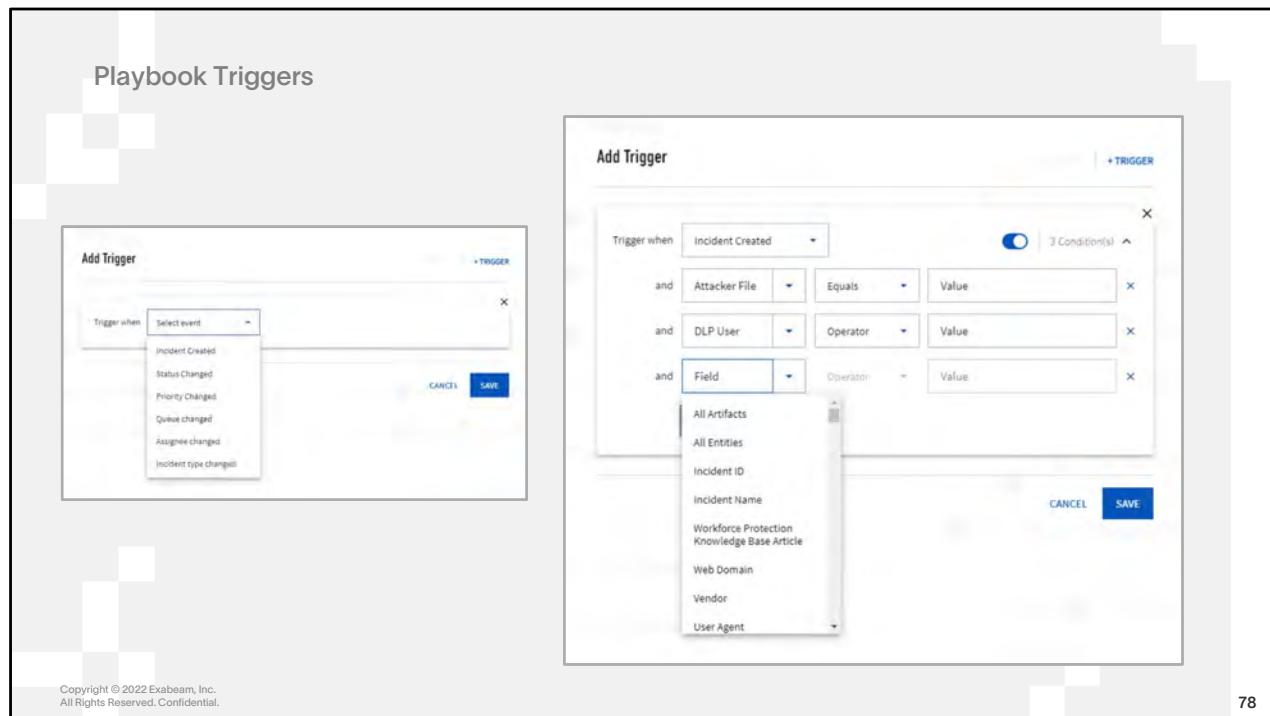
The Exabeam Cloud Platform provides access to the Action Editor

The action editor allows for:

- Editing of existing services and actions

- Creation of new actions with existing services

- Defining new services and the actions for those services.



### Student Notes

Playbooks can be launched manually from case manager

OR

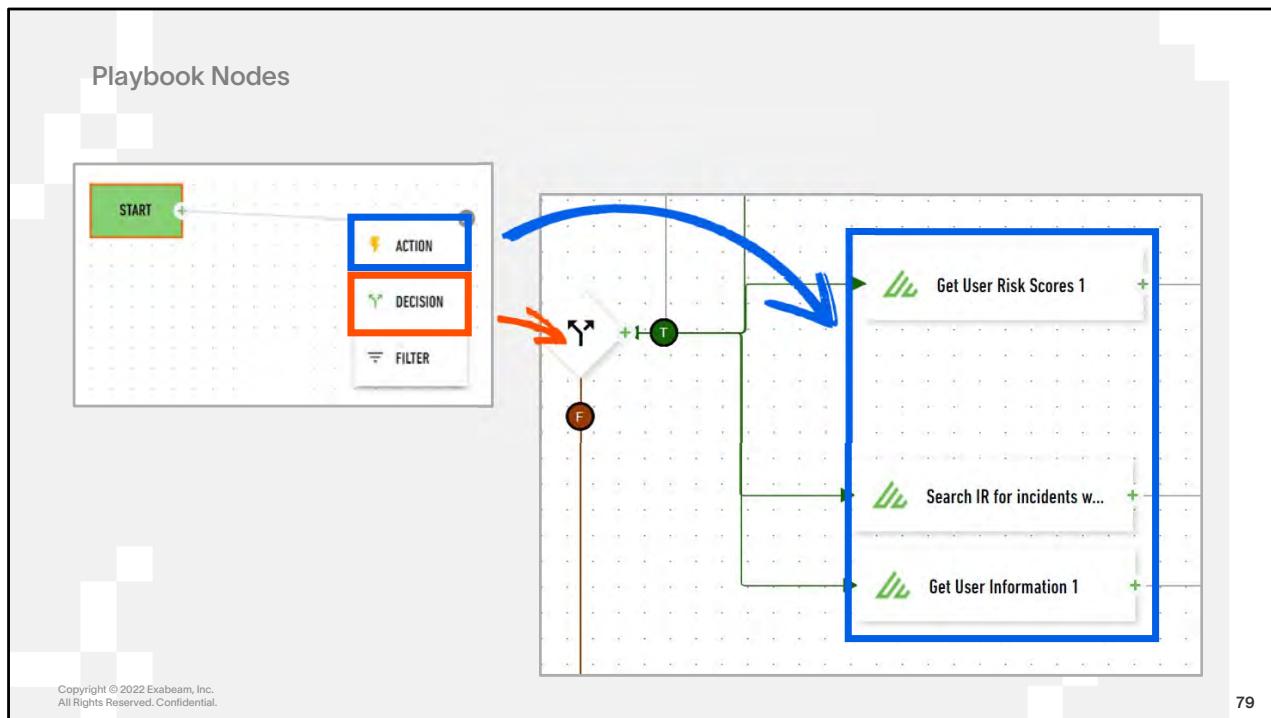
You can automatically run playbooks using triggers. Playbooks automatically run when you prescribe it to run under a certain circumstance, and that circumstance happens. This circumstance is called a trigger. There are three circumstances that trigger a playbook:

- Incident Created – When you create a new incident.
- Status Changed – When you change the state of an incident.
- Priority Changed – When you change the priority of an incident.

If you've already created an incident manually and the details match the conditions of a playbook trigger, the playbook will not trigger automatically.

### Source

Advanced Analytics User Guide

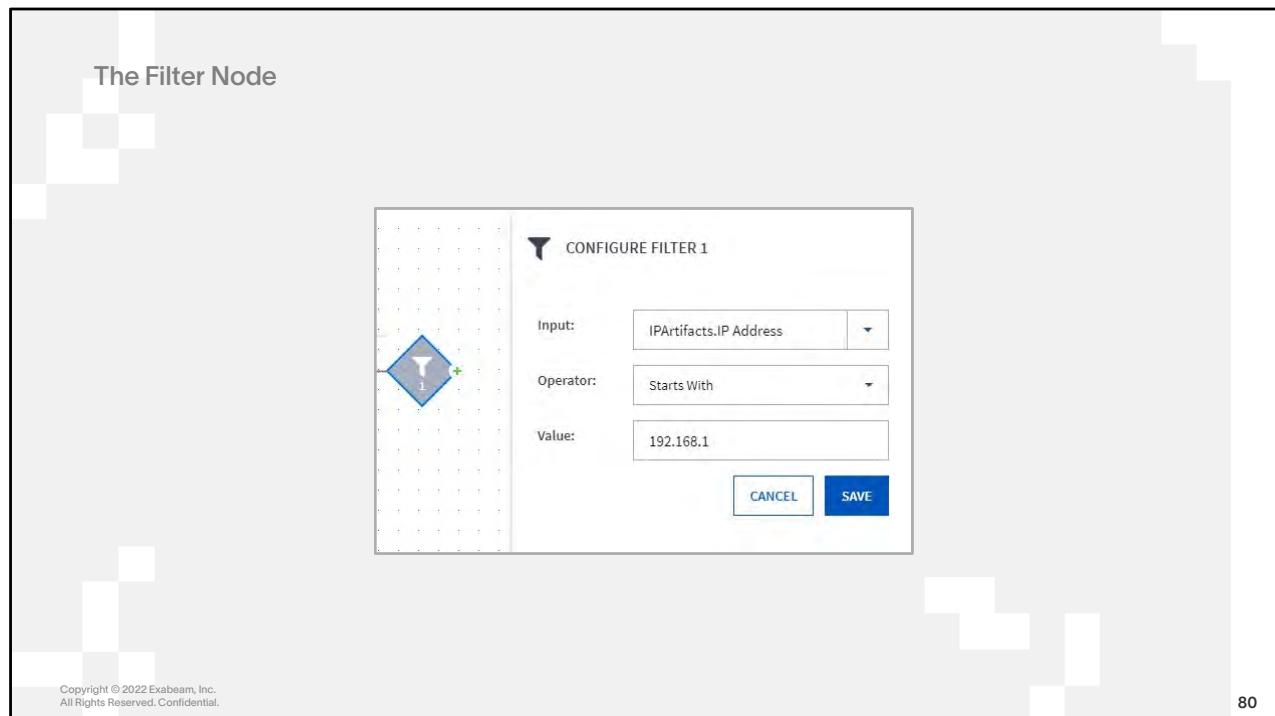


### Student Notes

Node is the fundamental building blocks of playbooks. Each one represents an action, decision, start, or end. Input is data passed from one node to another; data from a Case Manager incident, entity, or artifact. You use action nodes in playbooks. It has an inbound port on the left and an outbound on the right. Each node has at least one inbound port and one outbound port that connects it to another node (except the start node and end node). An inbound port receives data from another note, and an outbound node sends data. You use A decision node to indicate a Boolean (if/else) decision. It has one inbound node on the left, an if/true node on the right, and else/false nodes on the top and bottom.

### Source

Advanced Analytics User Guide



80

### Student Notes

Add a filter node to narrow down multiple input values to a specific subset.

You use a filter node to filter out a subset of the input source, based on conditions you specify when you configure the node. The filter node outputs the remaining subset and passes it on to the next node. The next node only evaluates this remaining subset. For example, you can use a filter node to remove:

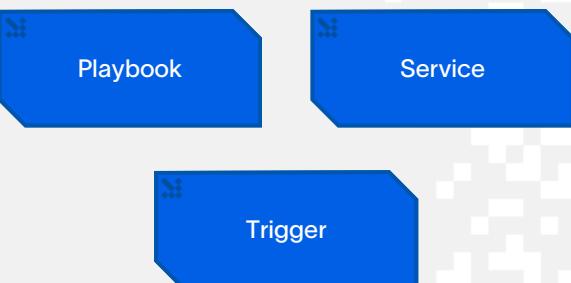
- Normal domains, so the next node evaluates malicious domains only.
- Allow listed URLs, so the next node evaluates block listed URLs only.
- Email attachments with a risk score below 90, so the next node evaluates attachments with a risk score above 90 only.
- IP addresses from other countries, so the next node evaluates IP addresses from a specific country only.

### Source

Advanced Analytics User Guide

## Activity

Can You Define These Key IR Components?



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

81



### Student Notes

Playbook:

A standard, repeatable sequence of actions that responds to specific incident types

Service:

A third-party product or vendor you integrate with Incident Responder to run actions and playbooks.

Trigger:

A certain circumstance that causes a Playbook to run automatically

## Activity

Can You Define These Playbook Node Types?

Action Node

Filter Node

Decision Node

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

82



### Student Notes

Action:

A scripted task to call a third-party API service and gather data

Filter:

Conditionally reduce the results of an input to only a subset that is passed to the next node

Decision:

A boolean (if/else) branching node

## Enable & Disable Playbooks

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

83

### Student Notes

- Playbooks with errors are disabled by default
- Disable playbooks to prevent from running
- Commonly used when created new playbooks for testing

## Import and Export Playbooks

### Import Playbook Template

You will be able to use the template(s) you are importing when creating a new playbook.



CHOOSE TEMPLATE FILE

.JSON is the only supported file type

CLOSE

## Discussion

---

**What type of Playbook implementation would aid your processes most?**



85

## Activity

---

# Practice using Playbooks and Incident Responder

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



86

v4.00

 exabeam

# External Threats

EDU-2170 : Module 7



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

1



# What are the most common cyber threats making headlines today?

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

2

## Student Notes

Of course, Ransomware:

- Kaseya, impacting up to 1,500 companies
- Colonial Pipeline
- JBS Foods

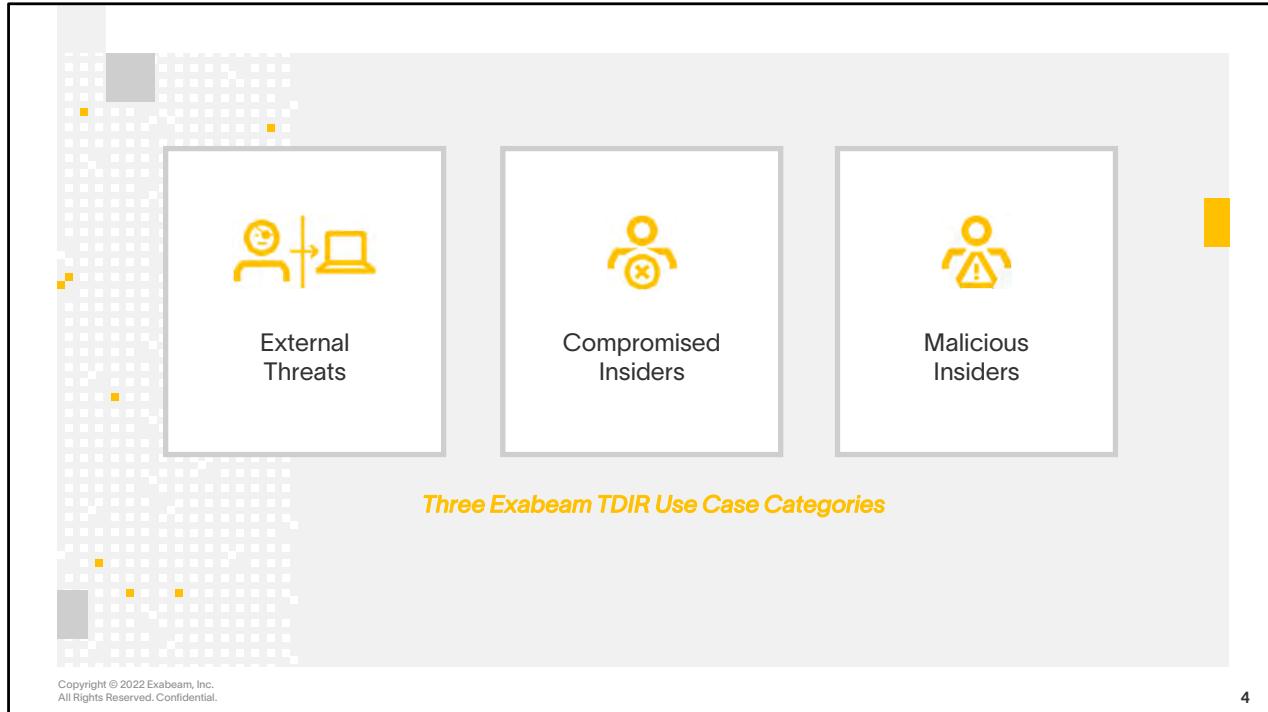
But consider the other types listed in this article by HP - <https://www.hp.com/us-en/shop/tech-takes/most-common-types-of-cyber-attacks>



## Lesson

At the end of this lesson, you will be able to:

- 1. Recall with general familiarity the principles of the Exabeam Use Case methodology**
2. Describe and Identify External Threat Activity
3. Investigate and Respond to External Threat Activity



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

4

### Student Notes

Exabeam organizes use cases into three broad categories:

- External Threats
- Compromised Insiders
- Malicious Insiders

A use case category is an umbrella term used to group a collection of related use cases; all use cases under each category complement one another and align to an adoption maturity path.

Each use case within the category defines a set of functionalities across all Exabeam's products to deliver measurable outcomes for detection, investigation, response, hunting and compliance to provide prescriptive, end-to-end solutions.

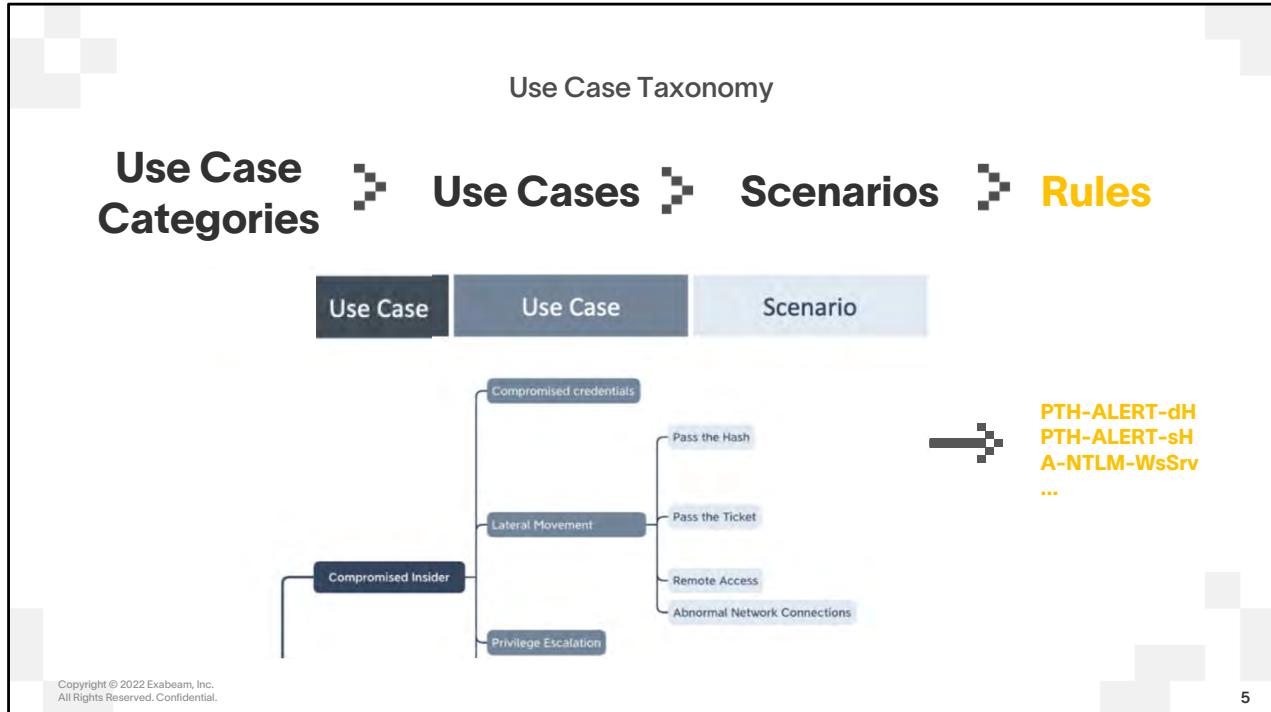
**External Threats** - Protect Against Prevalent Attack Vectors Attack vectors like phishing or malware provide adversaries ample opportunities to breach a company's defenses. With the sheer volume of attacks on a daily basis, SOCs must be prepared to properly detect, investigate, and respond at a moment's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

### References

<https://github.com/ExabeamLabs/Content-Doc/blob/master/Exabeam%20Use%20Cases.md>



### Student Notes

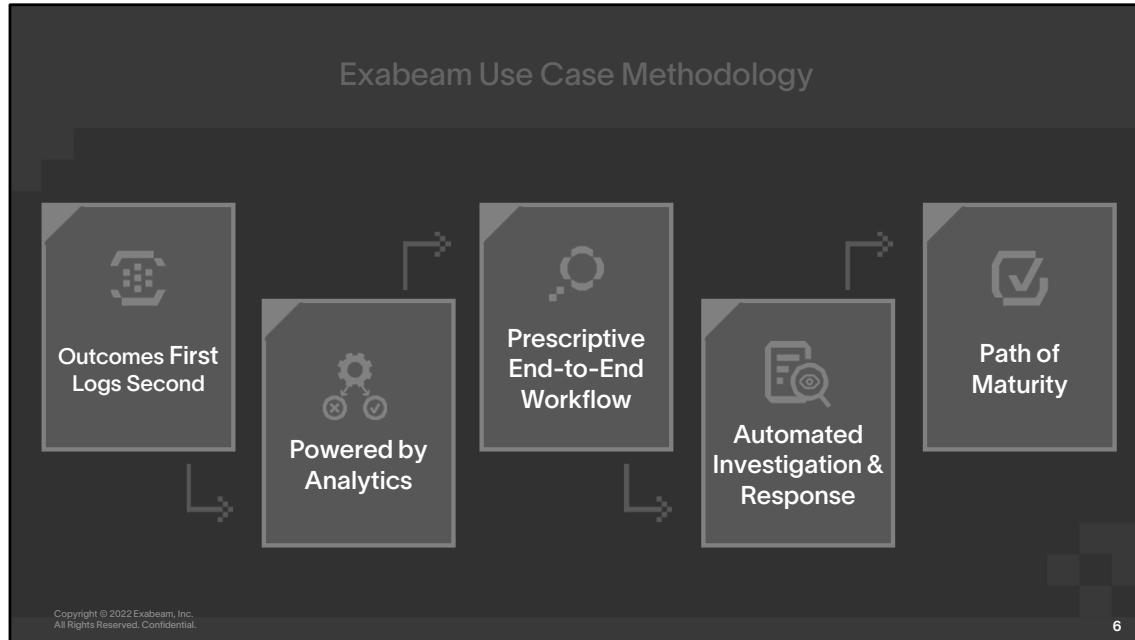
The TDIR Use Case framework organizes threats in a hierarchy, from a broad category down to specific detection insights.

- **Use Case Package (Category)** – 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. Not all use cases contain scenarios; for example, the *External Threats* use cases don't have scenarios.

### Source

<https://docs.exabeam.com/en/use-cases/all/get-started-with-tdir-use-case-packages/159618-threat-detection,-investigation,-and-response--tdir--use-case-packages-hierarchy.html>



## Student Notes

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.

Exabeam provides Threat Detection, Investigation, and Response (TDIR) Use Cases which are an outcome-based framework for using your Exabeam product. It describes what threats you can detect, investigate, hunt, and respond to using a prescribed end-to-end workflow. Exabeam also provides clear guidance on the data sources that are needed for security teams to protect against external and internal threats.

How does Exabeam provide coverage for use cases?

- Exabeam use case coverage helps organizations solve specific problems by providing visibility, detection logic and response procedures out-of-the-box.
- You can employ use case content and features for each stage of the workflow, not just detection.

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.

### Outcomes First, Logs Second

Instead of pushing every available log into a SIEM, it's important to identify what outcomes and security goals are needed first, then determine the logs and data sources. In some cases, additional logs are needed. In other cases, it is important to optimize the log collection for your specific results. Exabeam supports cloud sources and hundreds of integrations.

### Powered by Analytics

Exabeam draws from the organization's log management system and enriches the logs with identity, asset, and network information. It follows user sessions by tracking the state of the users' presence within the IT environment, building an added layer of intelligence from the logs collected.

### Prescriptive End-to-End Workflow

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.

#### Automated Investigation & Response

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.

#### Path of Maturity

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.

#### **References**

<https://www.exabeam.com/wp-content/uploads/TDIR-Use-Case-Packages-Overview.pdf>

"Demystifying the SOC: Part 5": <https://gorkasadowski.medium.com/demystifying-the-soc-part-5-the-new-soc-maturity-model-based-on-outcomes-7746402130e0>



## Lesson

At the end of this lesson, you will be able to:

1. Recall with general familiarity the principles of the Exabeam Use Case methodology
- 2. Describe and Identify External Threat Activity**
3. Investigate and Respond to External Threat Activity



## External Threats

Techniques commonly employed by adversaries to deceive users, gain access to valid credentials, or exploit corporate assets.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

8

### Student Notes

Cybercriminals carry out external threats – these can be criminal syndicates, lone wolves, or state-sponsored hackers.

In days gone by, attackers often used trial and error in their attacks, but many have gotten far more sophisticated. All they need to do is to keep trying through actions such as phishing, malware, ransomware, DDoS attack, or Malvertising, until they break into our systems. Other methods external attackers may use include:

- Hacking through security loopholes
- Ransomware and malware
- Physical theft of devices that can offer unauthorized user access
- 3<sup>rd</sup>-party apps
- Malicious USB drops

The External Threats use case category currently includes the following five use cases:

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

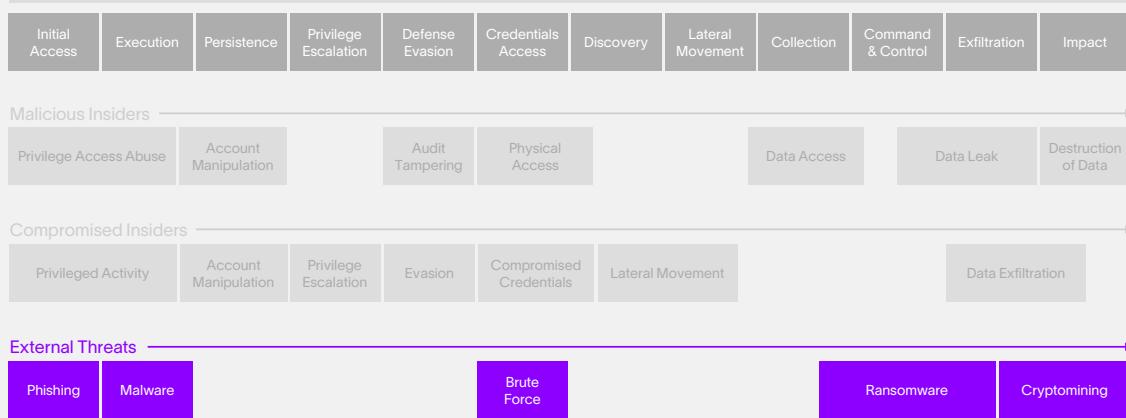
### References

- <https://github.com/ExabeamLabs/Content-Doc/blob/master/Exabeam%20Use%20Cases.md>
- <https://github.com/ExabeamLabs/Content-Doc/blob/master/Exabeam%20Use%20Cases.md>
- <https://www.tripwire.com/state-of-security/featured/understanding-external-security-threats/>
- <https://syspeace.com/internal-external-threats/>

Photo by [Gerald Schömbs](#) on [Unsplash](#)

## Mapping Exabeam Use Cases to MITRE ATT&CK

MITRE ATT&CK® Matrix



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

9

### Student Notes

#### References:

“Demystifying the SOC: Part 5”: <https://gorkasadowski.medium.com/demystifying-the-soc-part-5-the-new-soc-maturity-model-based-on-outcomes-7746402130e0>

	<b>Malware</b> Detect and respond to malicious programs or code developed by adversaries with the intent to cause damage to data or a system or gain unauthorized access to a network
	<b>Phishing</b>
	<b>Ransomware</b>
	<b>Brute Force Attack</b>
	<b>Cryptomining</b>

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

10

## Student Notes

Traditional anti-malware solutions are ineffective in the face of:

- Outdated signatures
- Alert fatigue
- Known vendor bypasses
- Fireless, in-memory attacks
- "Living off the Land" attacks

The Exabeam Malware use case augments your existing anti-virus and EDR alerts with advanced detection and response capabilities. Beyond static file hashing to identify known malware threats, Advanced Analytics flags first-time and anomalous behaviors often associated with malware, such as abnormal process execution and spawning, privileged service accounts running on unusual systems, PowerShell and other strange command line activity (possibly an indication of "living off the land"-types of attacks), DLL abuse, and scheduled task abnormalities. And these behaviors and the rules that alert on them are further enriched with up-to-date context, such as known dangerous URLs, domains, and IPs. The turnkey Malware Playbook, included in all Fusion deployments without requiring additional licensing, can speed the analyst's investigation and time to resolution by automating several tasks commonly associated with a malware response. And for customers with an IR license, the playbook can be customized, or entirely new playbooks created, to meet the unique needs for malware response of your incident response team.

In summary, the Exabeam SOC platform augments existing logs, AV, and EDR alerts in the malware use case by

- detecting anomalies, not just signature matches
- creating end-to-end user and entity activity timelines
- providing contextual enrichment and threat intelligence via the following context tables:
  - `is_ranked_domain`
  - `is_dynamicdns_domain`
  - `web_malicious_categories`

- `web_ioc`
- `is_ip_threat`
- `reputation_domains`
- `reputation_urls`
- integrating with the malware turnkey playbook and supporting actions
- leveraging built-in Data Lake reports

## References

<https://community.exabeam.com/s/article/Malware-Use-Case-Chapter-3-Detect>



Malware



**Phishing**

Detect and respond to social engineering attacks over email or other messaging services designed to deceive users into taking action to assist the adversary



Ransomware



Brute Force Attack



Cryptomining



## Phishing

Detect and respond to social engineering attacks over email or other messaging services designed to deceive users into taking action to assist the adversary

### Example

#### Collection

- dlp-email-alert-out
- session-end
- vpn-logout
- web-activity-allowed
- web-activity-denied

#### Context

- is\_ranked\_domain
- web\_phishing
- web\_malicious\_categories

#### Detection

- First/Abnormal email domain
- Abnormal email size
- Abnormal email volume
- First/abnormal email country
- Suspected phishing domain activity

#### Hunt

- Email received from new domain(s)
- Users with abnormal email and process activity
- Users with abnormal email and geo login activity
- Spearphishing MITRE TTPs
- Sessions with Proofpoint phishing alerts

#### Investigation

- Escalate and/or triage Incidents
- Smart Timelines
- Data Insight models
- Self-guided investigations with curated steps per detection scenario
- Data Lake for additional detail

#### Response

- Delete suspicious email in user(s) mailboxes
- Block malicious ips, URLs, email addresses, and/or domains
- Block malicious files by hash
- Rotate credentials/reset password if necessary

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

12

## Student Notes

Additional Phishing Use Case notes:

### Data Sources

- Data loss prevention
- Email security and management
- Web security and monitoring
- Endpoint security (EPP/EDR)
- VPN/Zero Trust Network Access

### MITRE Techniques

- T1566: Phishing
- T1048: Exfil over Alternative Protocol
- T1071: Application Layer Protocol

### Email Ingestion

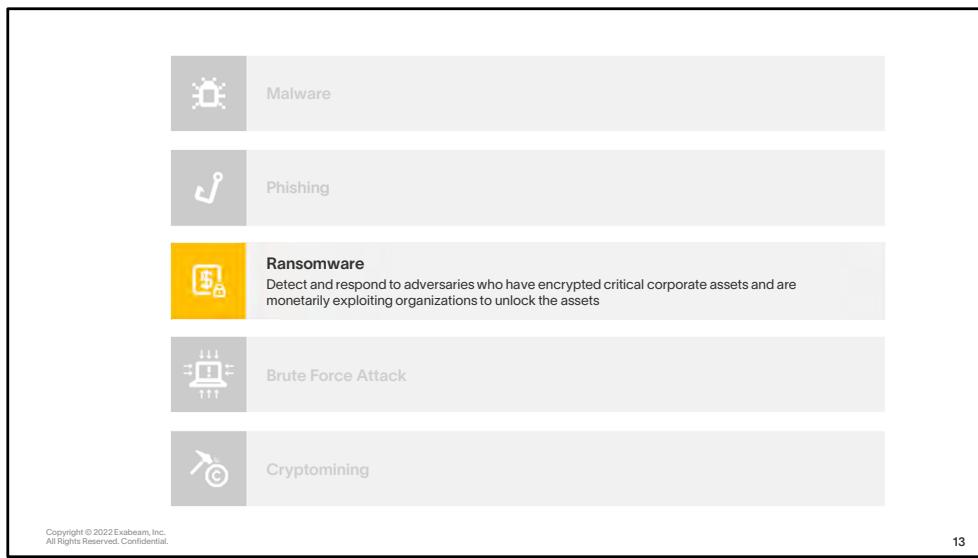
Train employees to forward suspicious emails directly to a designated corporate phishing mailbox. Case Manager extracts any file attachments or URLs/links in the email and adds them as artifacts on a new incident with the details regarding the potential phishing scam.

### Data Lake Reports

- Cisco OpenDNS Umbrella Summary
- User/Host-based DLP Activity
- DLP Activity Summary

### References

<https://github.com/ExabeamLabs/Content-Doc/blob/master/Exabeam%20Use%20Cases.md>



## Student Notes

Sobering statistics about ransomware:

- 59% of companies consider ransomware to be their biggest threat [1]
- \$1.85 million is the average cost to recover from a ransomware attack
- \$170,404 is the average ransom paid by medium-sized organizations
- 37% of companies polled reported that their organization had been hit by a ransomware attack within the last year

Ransomware poses many challenges to modern organizations, including

- ransomware may be difficult to detect
- response is largely reactive
- an average of 287 days to fully recover from an attack
- investigating using IoCs alone only identifies existing strains

To support the ransomware use case, the Exabeam SOC Platform enriches existing logs with threat intelligence stored in the following context tables:

- is\_ransomware\_domain
- is\_ransomware\_ip
- ransomware\_extensions

The built-in malware turnkey playbook supports the ransomware use case by performing reputational lookups on suspicious files and URLs, as well as detonating potentially dangerous files in a secure sandbox. For customers with an Incident Responder license, the turnkey playbook can be customized, or entirely new playbooks can be created, to perform even more advanced operations, such as

- quarantining/isolating affected hosts
- suspending users
- reset/expire passwords
- block malicious domains, URLs, and/or IPs
- Kill processes

## References

- <https://community.exabeam.com/s/article/Ransomware-Use-Case-Chapter-1-Introduction>
- <https://www.sophos.com/en-us/mediabinary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469>
- [https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force\\_Final\\_Report.pdf](https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf)
- <https://www.cisa.gov/stopransomware>

Malware

Phishing

Ransomware

**Brute Force Attack**  
Detect and respond to automated bots generating a large number of fake credentials in an attempt to guess a valid user's password

Cryptomining

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

14

## Student Notes

Brute Force attacks attempt to authenticate by iterating through a list of potential passwords, such as all words in the dictionary or combinations of words, symbols, and numbers in hopes that it will match. Credential stuffing attacks attempt to reuse breached passwords on other sites. For example, the credentials exposed in a breach of EvilCorp might be replayed successfully at Acme Corporation. Password spraying distributes a small number of common passwords across a large number of user accounts in the hopes that one of the accounts is using the insecure password(s).

Weak and reused passwords are vulnerable to these types of attacks and are often the first step in compromising a user's credentials. Once a password attack is successful, legitimate access can be difficult (if not impossible) to discriminate without behavior analytics. The Exabeam SOC platform aids in detecting and responding to password compromise activity by

- Intelligently prioritizing high-risk users to investigate based on the relative risk score of their suspicious activity
- Tracking failed logins across hosts
- Surfacing abnormal numbers of failed logons
- Surfacing first and abnormal password vault interactions

## References

[https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc\\_brute\\_force\\_attack.md](https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_brute_force_attack.md)

	Malware
	Phishing
	Ransomware
	Brute Force Attack
	<b>Cryptomining</b> Detect and respond to adversaries exploiting high-performance corporate computing systems to engage in crypto mining

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

15

### Student Notes

Cryptomining code typically gains a foothold in an organization through malware, hacking the IT infrastructure, or attacking the company's cloud infrastructure, leading to increased costs and potentially introducing new vulnerabilities. In addition to behavioral analytics that aid in detecting unwanted activities, Exabeam's Incident Responder can automate the process of blocking IPs, domains, and/or URLs suspected of crypto mining.



## Lesson

At the end of this lesson, you will be able to:

1. Recall with general familiarity the principles of the Exabeam Use Case methodology
2. Describe and Identify External Threat Activity
- 3. Investigate and Respond to External Threat Activity**

## Example Phishing Use Case Resources

### Threat Hunter Searches

- Users with abnormal email and process activity
- Users with abnormal email and geo login activity
- Emails received from new domain
- Spearphishing MITRE TTPs
- ...

### Rules

- Abnormal email domain for org/user/group
- Web activity to phishing domain
- Asset access to suspected phishing domain
- Abnormal email countries
- ...

### Data Insights

- Domains per user
- Email countries from/to user

### Data Lake Reports

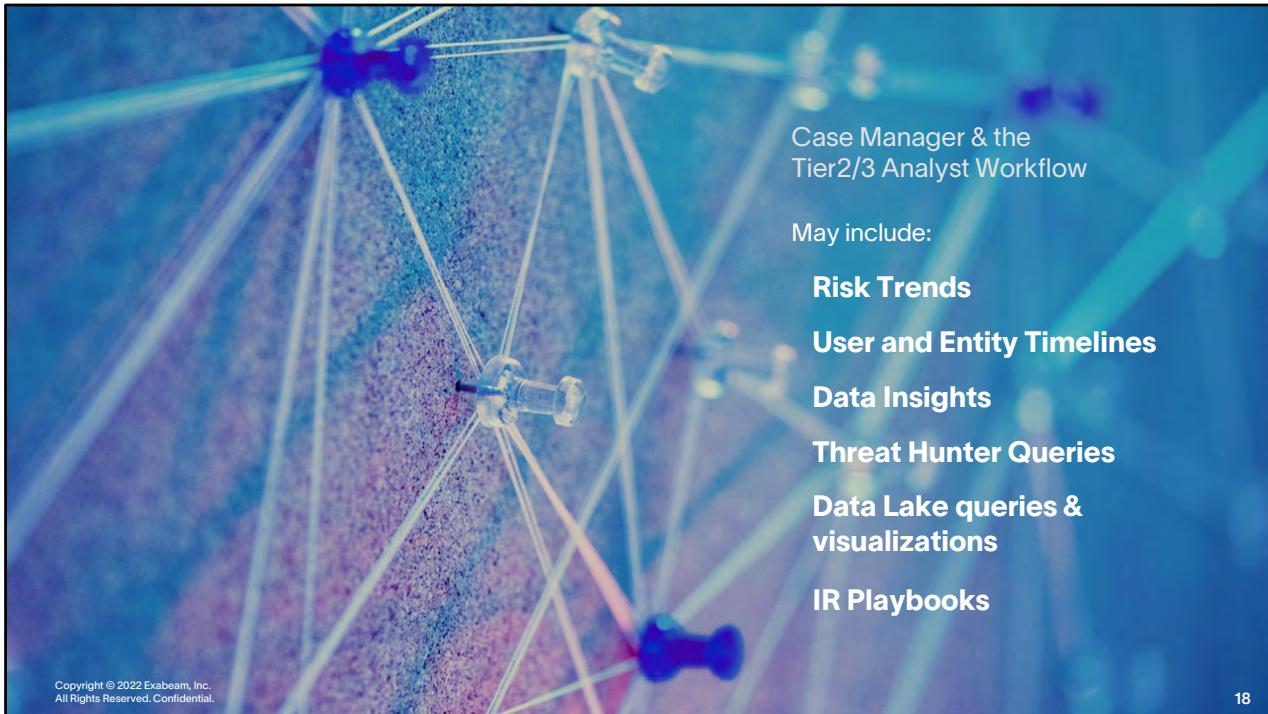
- Cisco OpenDNS Umbrella
- DLP Activity (host & user based)
- DLP Activity Summary

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

17

### Student Notes

Use case categories include resources such as Threat Hunter searches, rules, data insight visualizations, and Data Lake reports for each use case. The items above are examples of some of the resources included to support the phishing use case.



Case Manager & the  
Tier2/3 Analyst Workflow

May include:

**Risk Trends**

**User and Entity Timelines**

**Data Insights**

**Threat Hunter Queries**

**Data Lake queries &  
visualizations**

**IR Playbooks**

The screenshot shows the Case Manager Incident screen for a new session. A green bracket on the right side groups several elements:

- Incident Type**: Points to the 'Behavior Analytics' tab under 'Incident Type'.
- Status, Assignments, & Priority**: Points to the top right corner showing 'Assigned: Unassigned', 'Queue: Unassigned Queue', 'Status: New', and 'Priority: Medium'.
- Impacted Entities**: Points to the 'ENTITIES' section at the bottom right, which lists 'ALL', 'FILE', 'DEVICE', and 'USER' categories, each with a count of '0'.

A red box highlights the 'Compromised Credentials' section in the center-left of the screen. The text within this box is as follows:

**Compromised Credentials**

User Type: --	User Status: --
Account Type: --	Access Level: --
Asset Count: 0	Asset Type: --
Source Host/IP: --	Destination Host/IP: --
Data Accessed: --	Data Type Identification: --

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

19

### Student Notes

Commonly workflows will begin with incidents assigned to a specific analyst and/or a queue to which the analyst has been assigned. Incidents created automatically when a user or entity becomes notable are assigned the “Behavior Analytics” incident type in Case Manager. The corresponding **Behavior Analytics** section of the incident is populated with the details of the user’s **risk score**, **User ID**, **Risk Reasons**, and counts for risk **Reasons**, **Alerts**, and **Events**. All fields in an incident can be edited, and additional fields can be created as necessary. **Entities** represent files, devices, and users that may have been impacted by the event. The new incident shown above has not been assigned to an analyst or queue, and it currently has a priority of **medium**.

## Case Manager Incident continued

Hover over  
a task for  
additional  
details

The screenshot shows the 'Containment' phase of an incident response checklist. The task 'Communicate the case to the SOC Manager' is highlighted with a green box. The task details are as follows:

**Task Name:** Communicate the case to the SOC Manager

**Instructions:**

- Inform SOC Manager, if needed
- Include the expected start and end date of the case.
- Determine the required involvement of additional team members or teams. (HR, Legal, Physical Security, etc.)

Other tasks listed under Containment include: Abnormal Authentication and Access, Lateral Movement, and Compromised Credentials. There are also sections for Detection & Analysis, Eradication, Recovery, and Post-Incident Activity.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

20

### Student Notes

Checklist tasks provide use case-specific guidance and allow your response team to track the progress of an investigation. All incidents regardless of use case classification will include generic tasks, such as “Identify impacted users” and “Identify lessons learned.” Incidents created automatically when a user or entity becomes notable are assigned the “Behavior Analytics” incident type, which adds several additional tasks to the Detection & Analysis, Containment, and Post-Incident Activity response phases. Assigning additional incident types to a case will add checklist items to guide the analyst through the response process.

User Profile Page

The screenshot shows a user profile for Sherri Lee. At the top right, her Risk Score is 13. Below it, her profile picture, name, title (sales representative), location (Los Angeles), and department (Sales) are displayed. Her manager is Andrew Bautista, and she is in the Top Peer Group with a score of 110. A comment from 'admin' dated 24 Mar 12:16 indicates a recent role/department change. Below the profile, there is a section for 'Active Incidents' which lists one active incident related to her account.

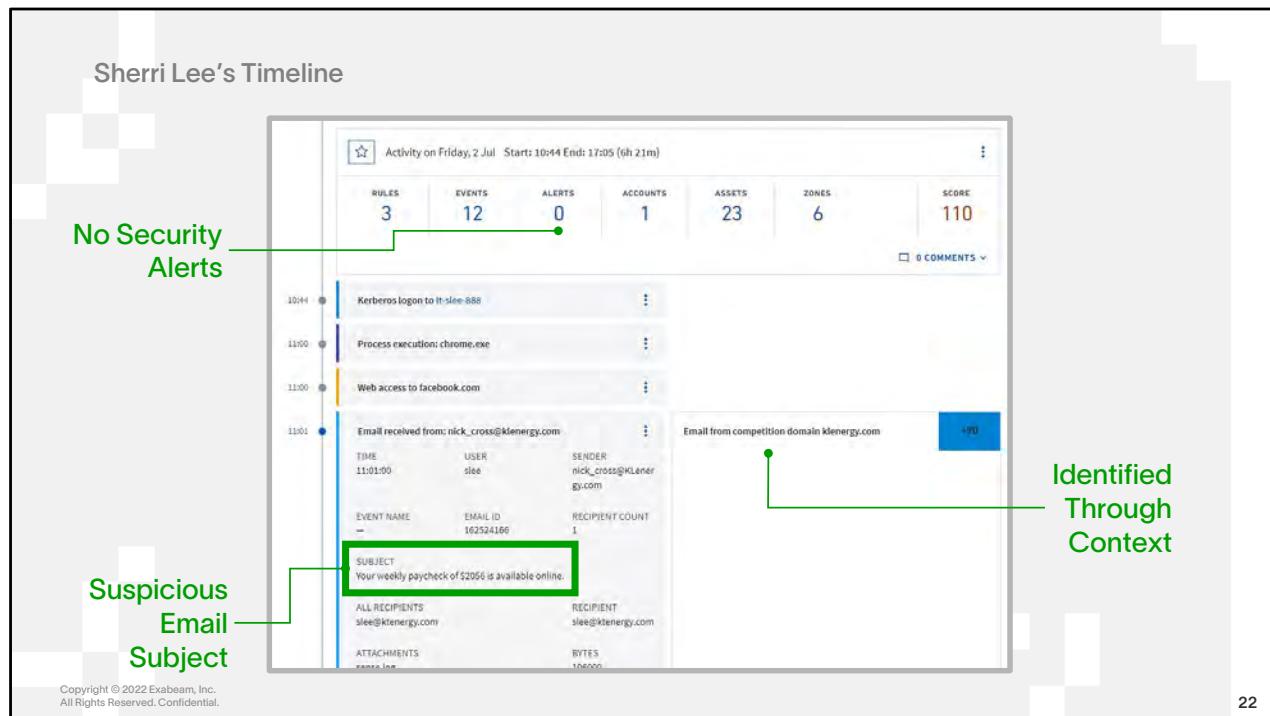
**Active Incidents**

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

21

### Student Notes

We see from Sherri Lee's profile page that her current risk score is only 13, but there is an active incident tied to her account. The comment on her profile indicates a recent role/department change, a valuable piece of information for the analyst to have when investigating anomalies. Comments can be added to sessions as well as user profiles, and analysts can add case notes to the incident itself and/or send email messages through Case Manager.



22

### Student Notes

When we pivot to Sherri Lee's timeline for her notable session, we see that it doesn't contain any security alerts (AV, EDR, DLP, etc.), so this activity wouldn't have surfaced in Alert Triage. The first concerning event in Sherri's timeline is the receipt of an email from a "competition domain," which is defined through the **is\_competition** context table. The details of the event include the suspicious subject line "Your weekly paycheck of \$2056 is available online."

## Sherri Lee's Timeline continued



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

23

### Student Notes

About one minute after receiving the email, anomalous activity associated with “tor.exe” appears in Sherri’s timeline. TOR is a well-known proxy system used for anonymous communications, and although it has perfectly legitimate uses, the system is also used for access to the dark web and should usually be considered suspicious in an enterprise setting.

### Sherri Lee's Timeline continued

The screenshot shows a timeline interface for an incident. At the top, there are two events:

- 11:04 Web access to iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
- First access to this domain iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com which has been identified as DGA +10

In the middle section, there is a green box labeled "Can Add to Incident" pointing to a specific event:

- 11:06 Remote access to us\_sales\_app\_1
- First access to us\_sales\_app\_1 for Sherri Lee +10
- First communication from network zone new york office for the user -10

Below this, there are two file read events:

- 11:07 177x File Read
- 11:07 55x File Read

A detailed view of the second file read event is shown:

TIME	USER	SOURCE
11:47:00	slee	Windows
ACCESS TYPE	PROCESS	BYTES
READ	taskbar.exe	9347
DESTINATION PATH	DESTINATION FILE	Add to incident
\REGISTRY\USER\test_\...ive\...\Software\Microsoft\Windows\CurrentVersion	EdmGen.docx	
SOURCE PATH	SOURCE FILE	-
SOURCE IP	SOURCE HOST	-
SOURCE ZONE	-	-

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

24

### Student Notes

The web access and subsequent file manipulation events in Sherri Lee's timeline shortly after confirm our suspicions. We see a web connection to what appears to be a “domain generating algorithm” domain—i.e., a pseudo-random hostname assigned to an internet-facing system, often used in command-and-control for botnets and other malware. The remaining file system activity seems to indicate a WannaCry ransomware infection.

You can easily add relevant events from a timeline and their details to an existing incident in Case Manager use the “kebab” menu and selecting “Add to Incident.”

Additional SIEM Research

Recipients

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

25

### Student Notes

Recall that the suspicious email Sherri Lee received that prompted this investigation did not trigger an EPP/EDR alert. Pivoting to Data Lake and performing a simple, unstructured text search on the string "paycheck" reveals that a similar email was sent to Barbara Salazar (bsalazar@ktenergy.com). The analyst should update the Case Manager incident with this new information and consider opening a new incident for Barbara Salazar if one doesn't already exist.

**Update the Incident**

Add Appropriate Types

Checklists Are Updated

Update Priority

Task Name	Assignee	Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Identify suspicious ac...	Assign	Set Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Review the user's pro...	Assign	Set Due Date
<input type="checkbox"/> Abnormal Authentication and Access - Perform analysis and ...	Assign	Set Due Date
<input type="checkbox"/> Review normal activity for the user	Assign	Set Due Date
<input type="checkbox"/> Identify the anomalous activity	Assign	Set Due Date
<input type="checkbox"/> Compromised Credentials - Identify the anomalous activity	Assign	Set Due Date
<input type="checkbox"/> Validate logs were sent to the SIEM	Assign	Set Due Date
<input type="checkbox"/> Retrospectively search for anomalous activity	Assign	Set Due Date
<input type="checkbox"/> Assess impacted systems	Assign	Set Due Date
<input type="checkbox"/> Proactively monitor impacted users and systems	Assign	Set Due Date
<input type="checkbox"/> Reassess the severity of the incident	Assign	Set Due Date

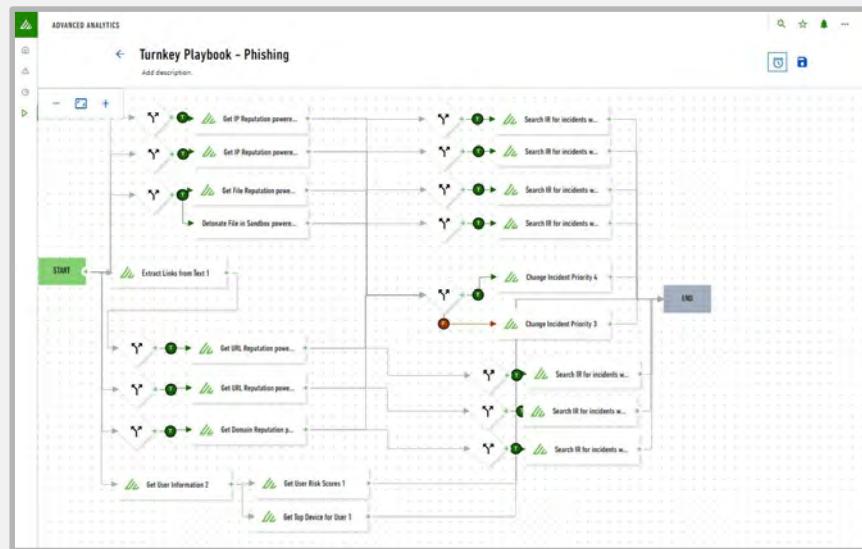
Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

26

### Student Notes

Based on what we've learned, we should update the incident types with the **Malware** and **Phishing** labels, which will automatically add relevant checklist items to the case. Considering the potential damage of a ransomware incident, we should consider changing the priority of the case to **Critical**. Depending on your team's processes, it may also be appropriate to escalate the case to a Tier3 analyst and/or queue, or the equivalent in your organization.

## Respond to Phishing



Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

27

## Student Notes

Playbooks in incident responder provide automated ways of gathering data points from 3<sup>rd</sup> party security tools for triage and further response. For instance, the phishing playbook shown here, provides for extracting links, getting reputations and YARA file scanning amongst other tasks.

## References

<https://docs.exabeam.com/en/incident-responder/cloud-delivered/get-started-with-incident-responder/153864-playbooks.html>

## Turnkey Playbook Actions for Phishing Use Case

The screenshot displays the Exabeam security platform's user interface. On the left, a sidebar titled "ACTIONS" lists several turnkey playbook actions for a phishing use case, each with a green checkmark indicating completion. The actions include: Get URL Reputation - Email Links, Detonate File - VxStream, Scan File - YARA, Expert Rules - Phishing, Text Scan - YARA, Extract Links, and GET FILE REPUTATION FOR PHISHING. The main area contains two cards: "DOMAIN CATEGORIZATION - CISCO UMBRELLA" and "DOMAIN SECURITY SCORE - CISCO UMBRELLA". The "DOMAIN CATEGORIZATION" card shows two URLs: https://filmirrors.com/p... (Phishing) and https://google.com (None). The "DOMAIN SECURITY SCORE" card lists various metrics with their scores: Viral Score (90.0), Rip Score (-0.550336855296), Asn Score (-0.119374892914), Securrank2 (-0.470311343289), Popularity (11.2676316695), Geoscore (0.0), Ks Test (0.0), Pagerank (1.7400709), Entropy (3.0), Prefix Score (-0.16665521266), and Perplexity (0.563936155017).

28

### Student Notes

The Exabeam security platform provides turnkey playbook actions for phishing incidents to provide you with out of the box response for this type of attack.

### References

<https://docs.exabeam.com/en/incident-responder/cloud-delivered/release-notes/156151-what-s-new.html>

## Turnkey Playbook Actions for Phishing Use Case continued

The image displays three separate windows from a security platform, likely VxStream, illustrating the analysis of a phishing sample named "payroll.zip".

- DETONE FILE – VXSTREAM:** This window shows the "PAYLOAD SECURITY" logo at the top. Below it, the attachment name is listed as "Attachment Name: payroll.zip". Further down, the SHA-256 hash is shown as "SHA-256: 9335e1404d1aa005...". A "Threat Score:" field contains the value "99" in red. The "Sample Type:" is identified as "HTML document, AS...". The "Sample Size:" is given as "7960 Bytes". At the bottom, there is a link: "View Detonation Report in VxStream".
- EXTRACTED NETWORK INDICATORS – VXSTREAM:** This window lists network resources. It includes:

Type	Network Resource
TCP	192.229.233.16:80
TCP	205.198.123.9:80
UDP	84.200.69.80:53
- BEHAVIORAL INDICATORS – VXSTREAM:** This window displays behavioral indicators with their names and descriptions:

Name	Description
Detected Emerging Threats Alert	100
Sample was identified as malicious by a large number of Antivirus engines	100
Sample was identified as malicious by at least one Antivirus Engine	80
All indicators are available only in the private webservice or standalone version	80
Sends UDP traffic	25
Found potential IP address in binary/memory	25
Malicious artifacts seen in context of a contacted host	25

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Turnkey Playbook Actions for Phishing Use Case continued

SCAN FILE - YARA	
Rule Name	Rule Description
Network vulnerability	Found queries for sensitive IE security settings
URL binary match	Found potential URL in binary/memory
POS_FastPOS	Used to detect FastPOS keylogger + scraper
Additional scripts in payload	Found additional scripts within payload to install hooks/patches during the running process.

TEXT SCAN - YARA	
Rule Name	Rule Description
Scam content detected	Detects scam emails with phishing attachment.
Masked link detected	Link hidden behind URL shortener.
Low reputation sender	Email sender domain from low reputation.

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Turnkey Playbook Actions for Phishing Use Case continued

The screenshot displays three windows from a Turnkey Playbook interface:

- VirusTotal Scan Results:** Shows a file hash (275a021bbfb6489e54d47...), result (Infected), attachment name (payroll.zip), signature (EXE.payroll.zip), and scan date (2017-03-28 16:05:00). A link to "View Reputation Report in VirusTotal" is present.
- Expert Rules - Phishing:** A table showing rule matches for 2021-07-28 at 14:53:38 +0000. It lists two rules:
  - Masked Link:** Details: HTML link https://goo.gl/pay4rollrepoxx masked behind link https://filermirrors.com/payroll.zip
  - New Sender Domain:** Details: Domain KLEnergy.com is younger than 30 days
- Extract Links:** A table showing URLs and their expanded forms:

URL	Expanded
http://goo.gl/pay4rollrepoxx	https://filermirrors.com/payroll.zip
https://www.google.com	-

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.

## Activity

### DETECT, INVESTIGATE, & RESPOND TO EXTERNAL THREATS

#### Objectives:

1. Review the Exabeam Content Library and External Threat use case category
2. Investigate an External Threat Incident
3. Use Advanced Analytics to Continue an Investigation
4. Respond to the Malware Use Case

Copyright © 2022 Exabeam, Inc.  
All Rights Reserved. Confidential.



32



## Summary

Can You Do the Following?

1. Recall with general familiarity the principles of the Exabeam Use Case methodology
2. Describe and Identify External Threat Activity
3. Investigate and Respond to External Threat Activity