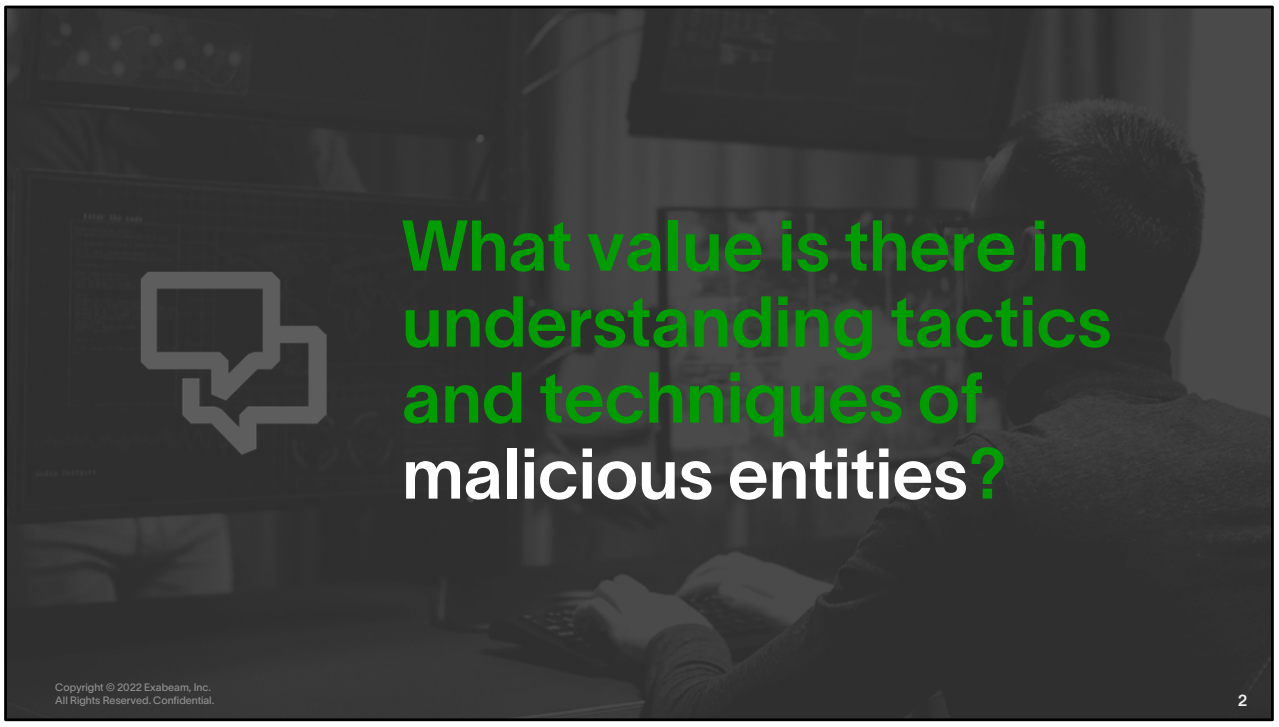
v4.00

Threat Hunting with Advanced Analytics

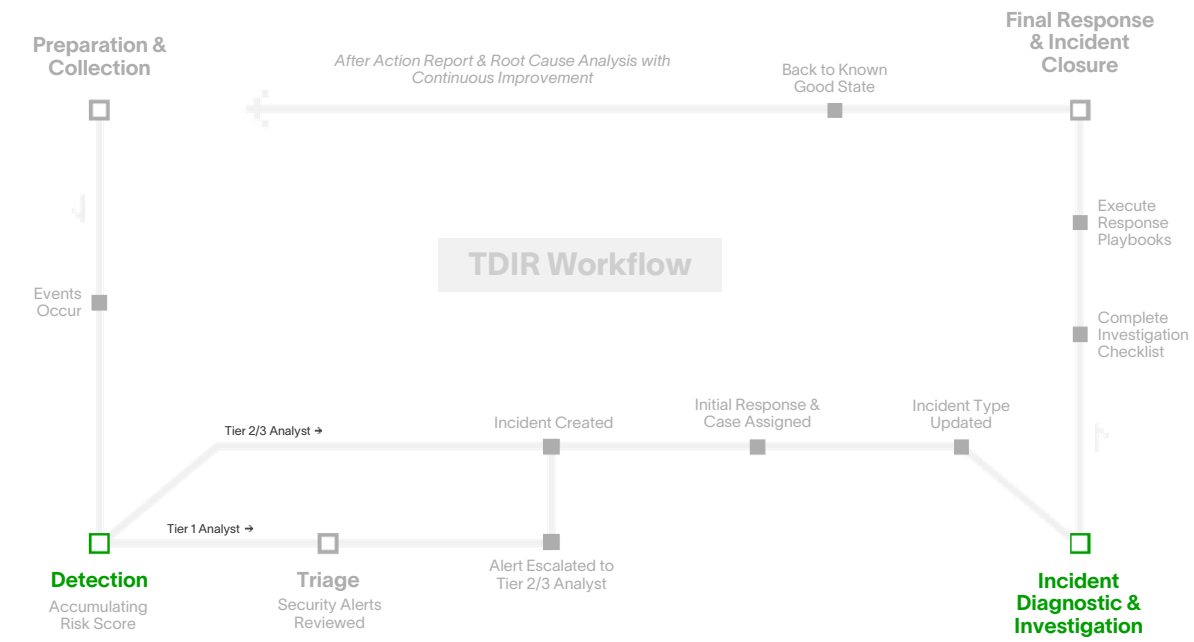
EDU-2170 : Module 5

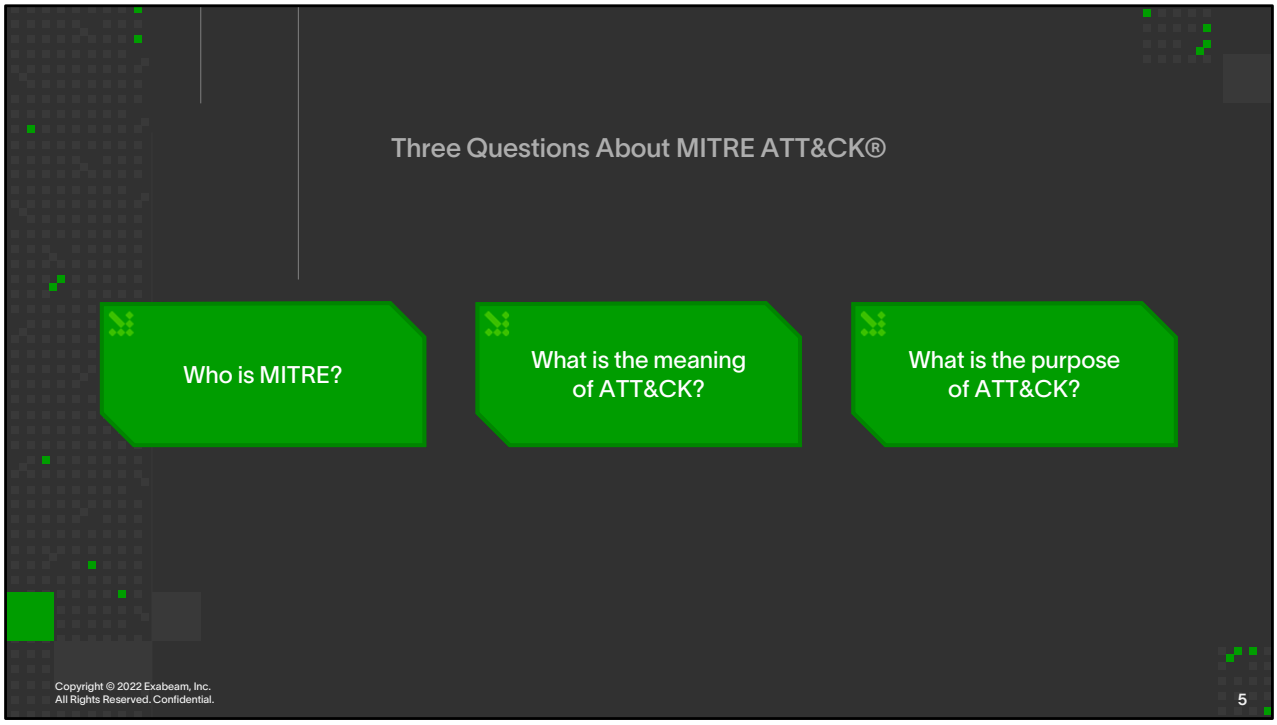

What value is there in understanding tactics and techniques of malicious entities?
Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.
2

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





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

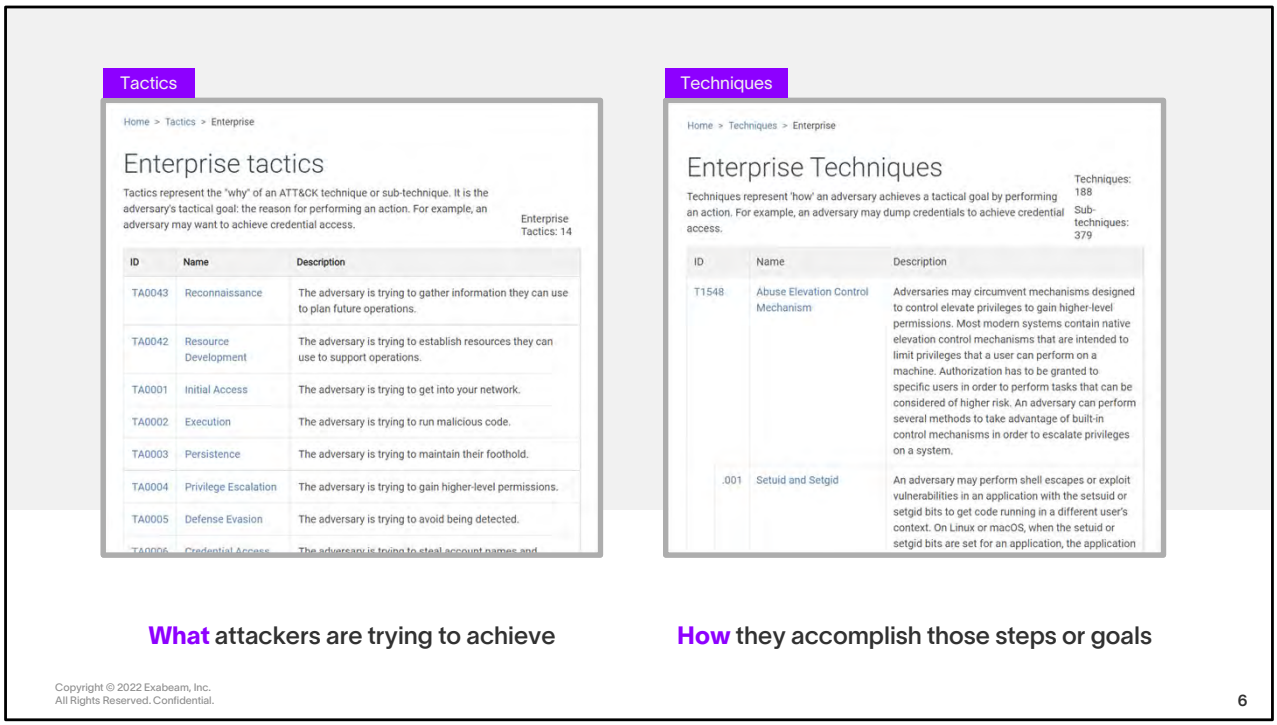
Techniques: 266 as of Aug 2019" (source: https://medium.com/mitre-attack/automating-mapping-to-attack-tram-1bb1b44bda76)

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



Student Notes

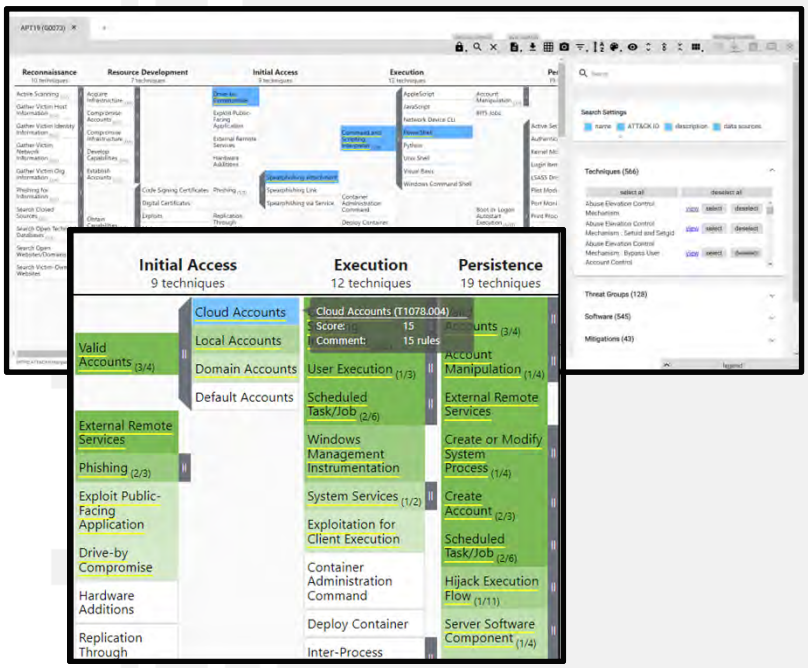
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cyberattacks.

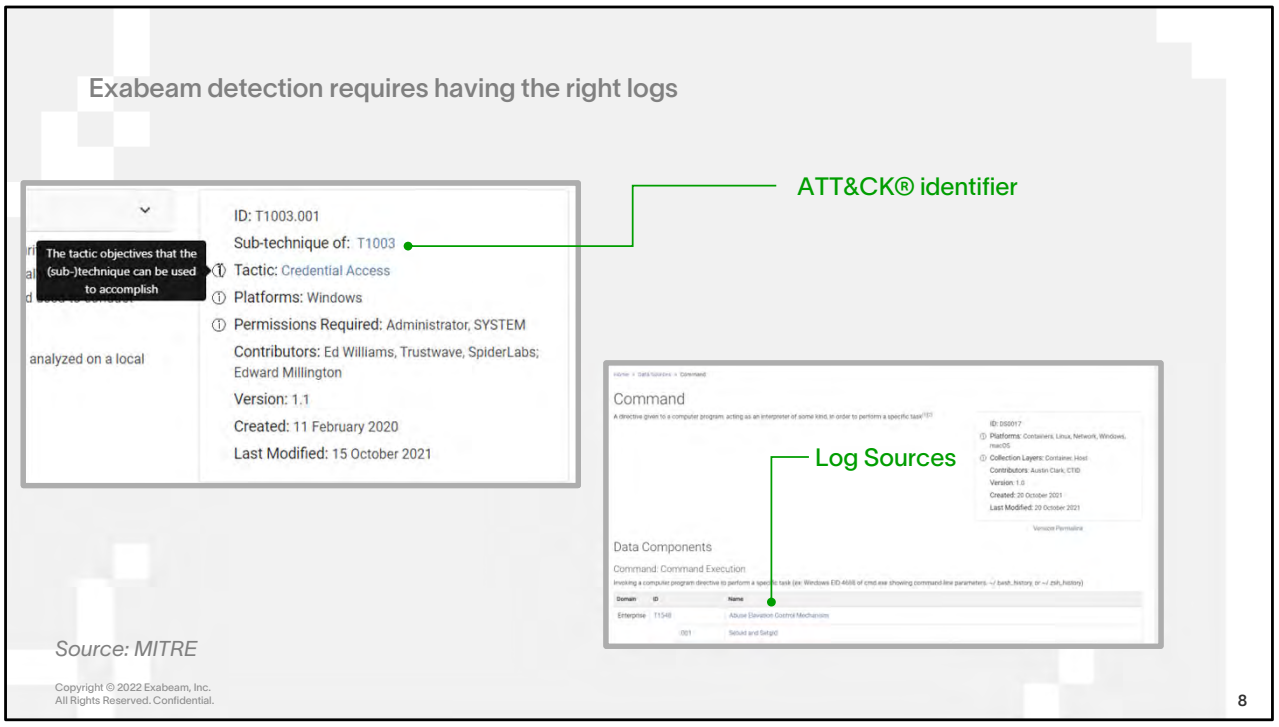
- Tactics – the *why* of an attack, e.g., Privilege Escalation, Defense Evasion
- Techniques – the *how* of an attack, e.g., Access Token Manipulation, Clear Command History
- Common Knowledge – the documented use of tactics and techniques by adversaries
- Matrices – the visual organization of Tactics 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/information-security/what-is-mitre-attck-an-explainer/

Demo





Student Notes

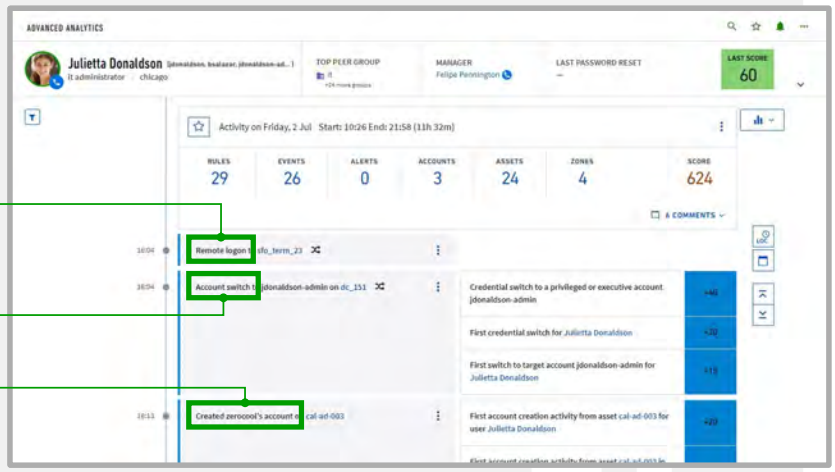
MITRE articles often indicate the needed log sources for detection and prevention.

Seeing ATT&CK® in the Smart Timeline when searching

Tactic: Lateral Movement
Technique: Remote Desktop Protocol

Tactic: Privilege Escalation
Technique: Valid Accounts

Tactic: Persistence
Technique: Account Creation



9

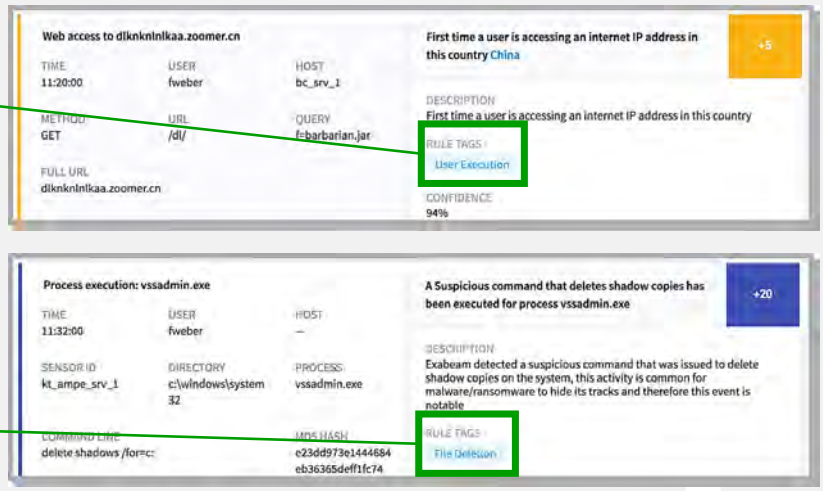
Student Notes

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



10

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

Example 1: Tactic: Execution; Technique: User Execution
Example 2: Tactique: Defense Evasion; Technique: File Deletion

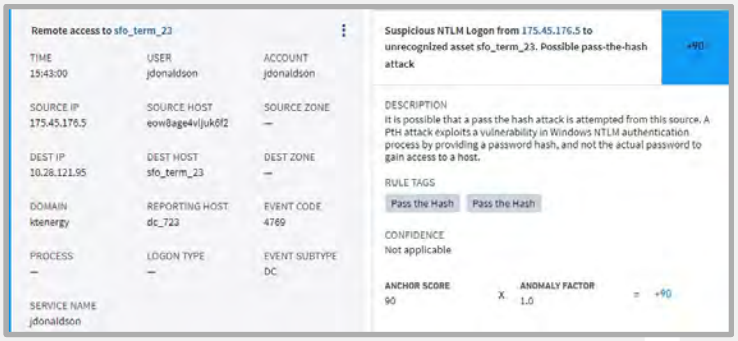
Mapping Exabeam Model to ATT&CK® Techniques

MITRE ATT&CK®
Technique T1075:
Pass the Hash

Exabeam
Identifies abnormal behaviors associated with account creation

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.



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?

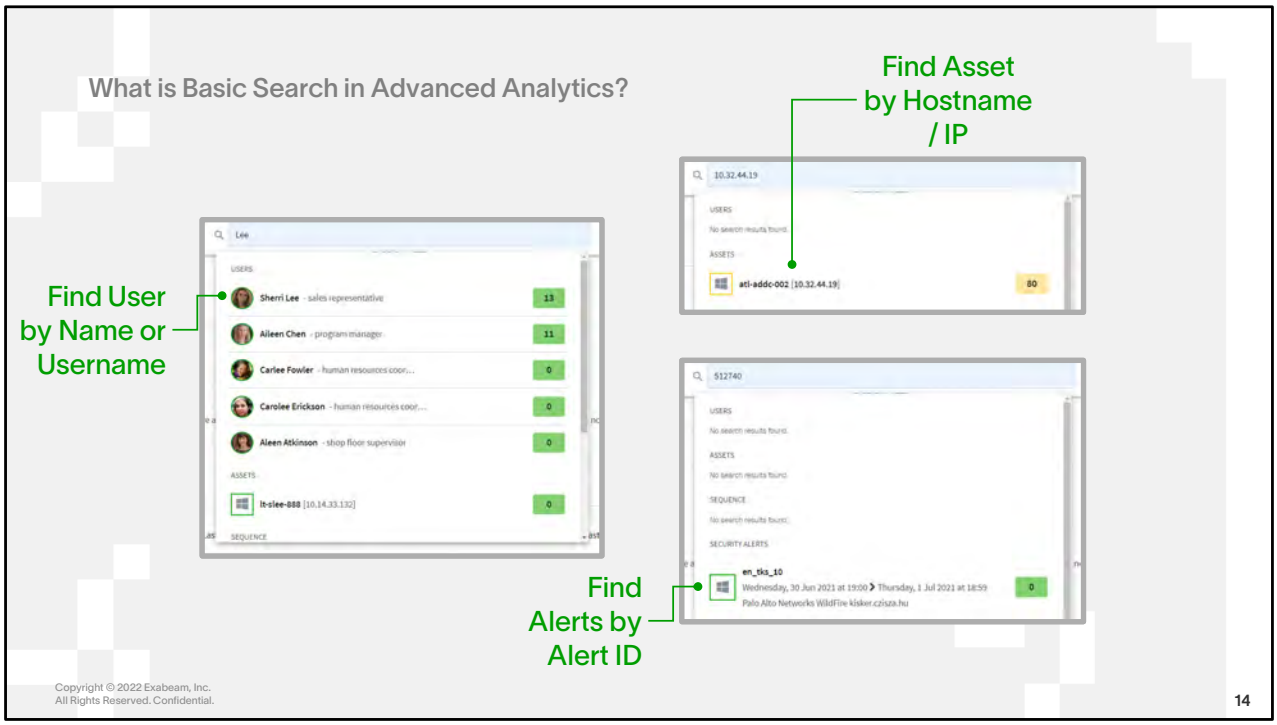
Student Notes

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/



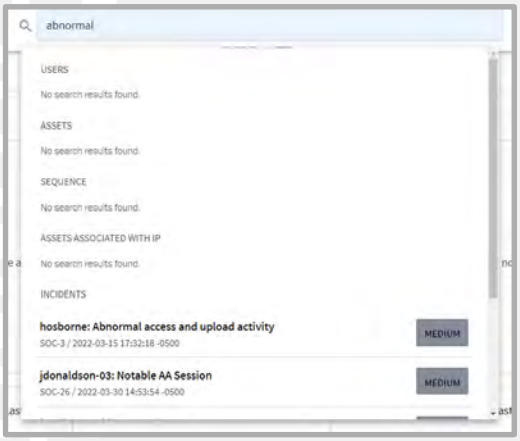
Student Notes

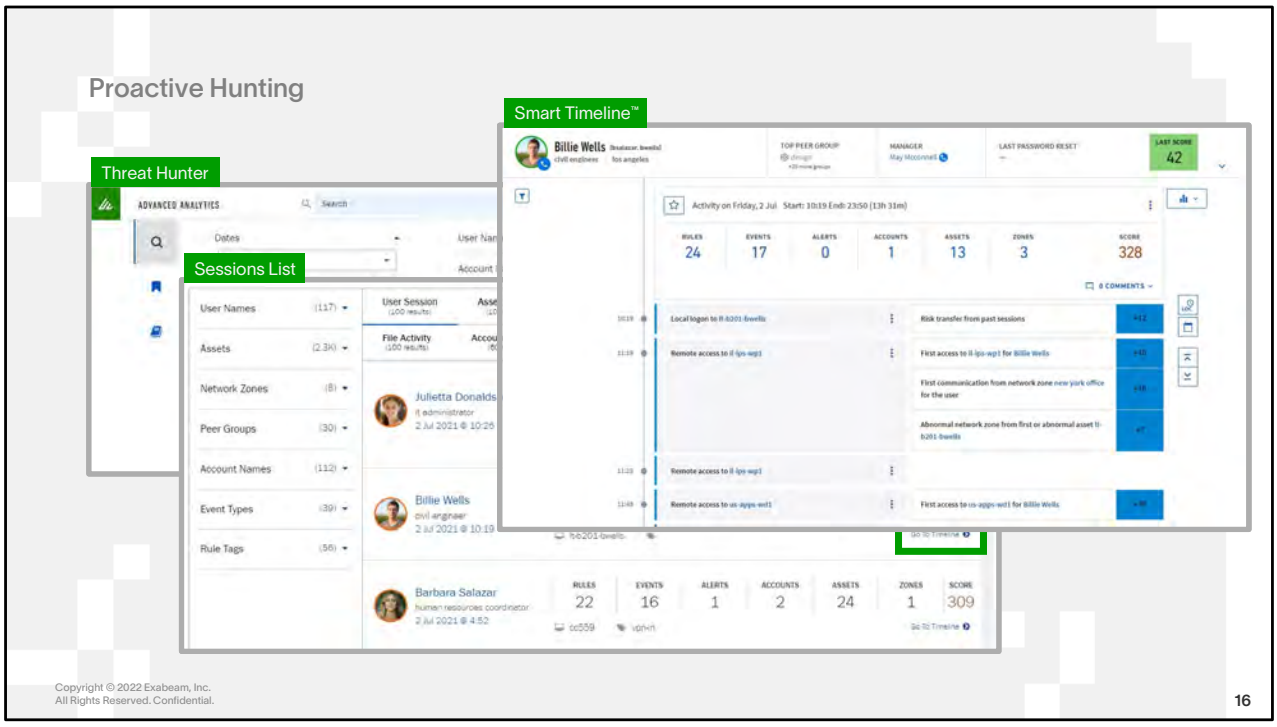
The basic search in the Advanced Analytics interface allows analysts to find entities quickly, see their current risk score, and follow links to their profile pages.

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





Source

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

Source

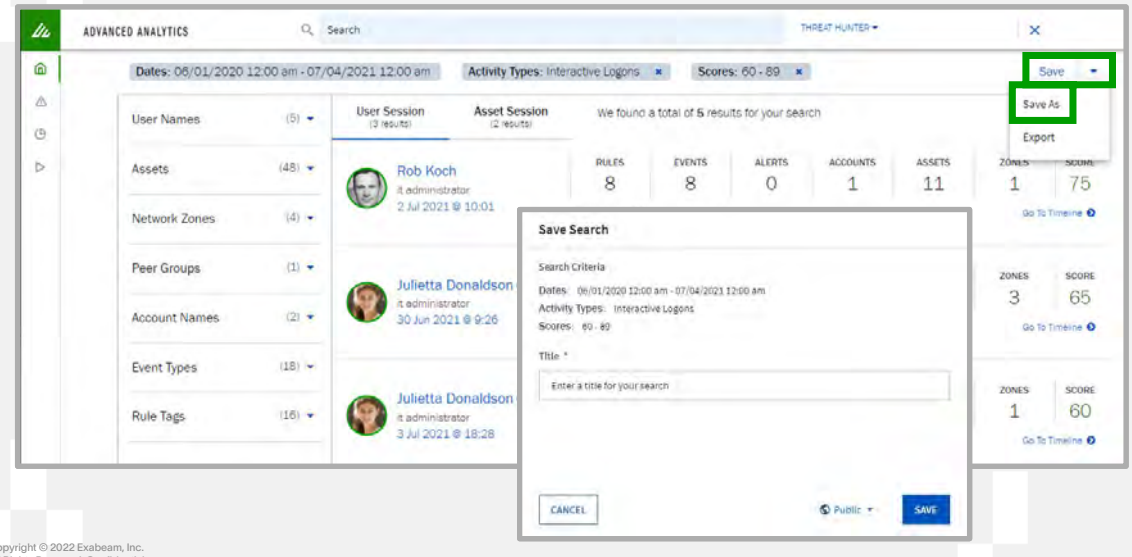
https://www.exabeam.com/siem/how-to-use-exabeam-for-threat-hunting/

{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

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



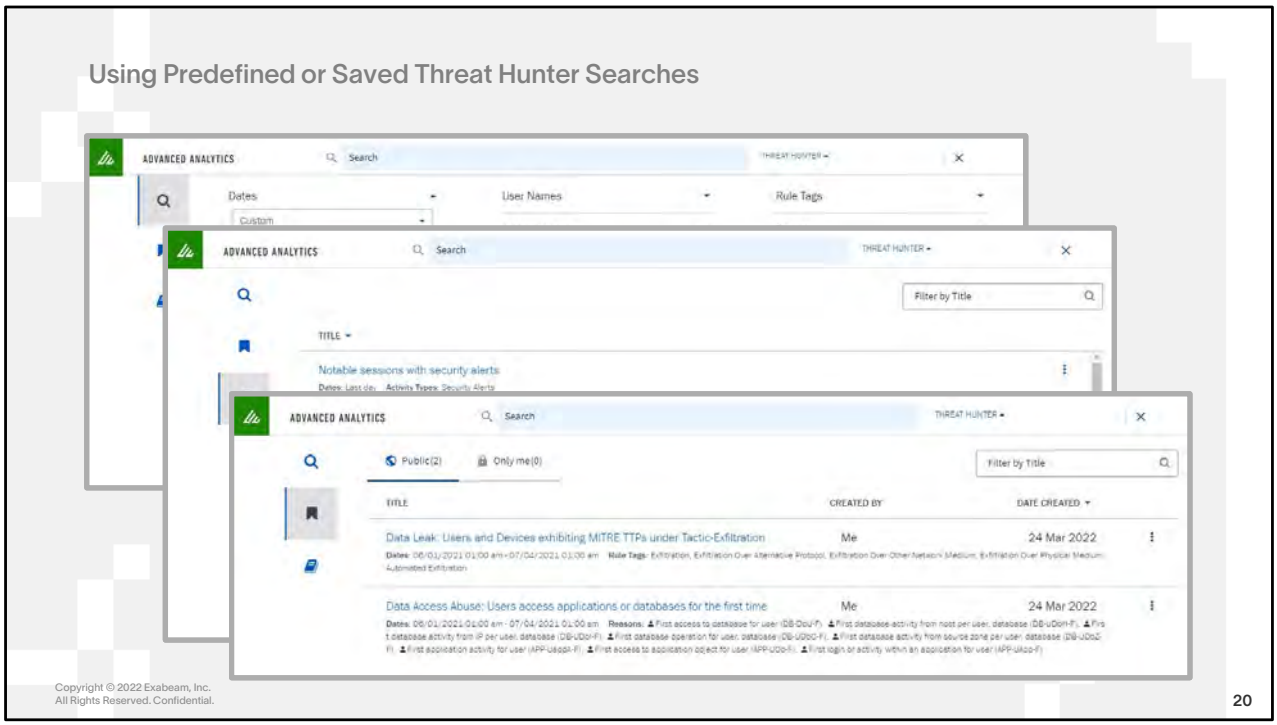
19

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/



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.

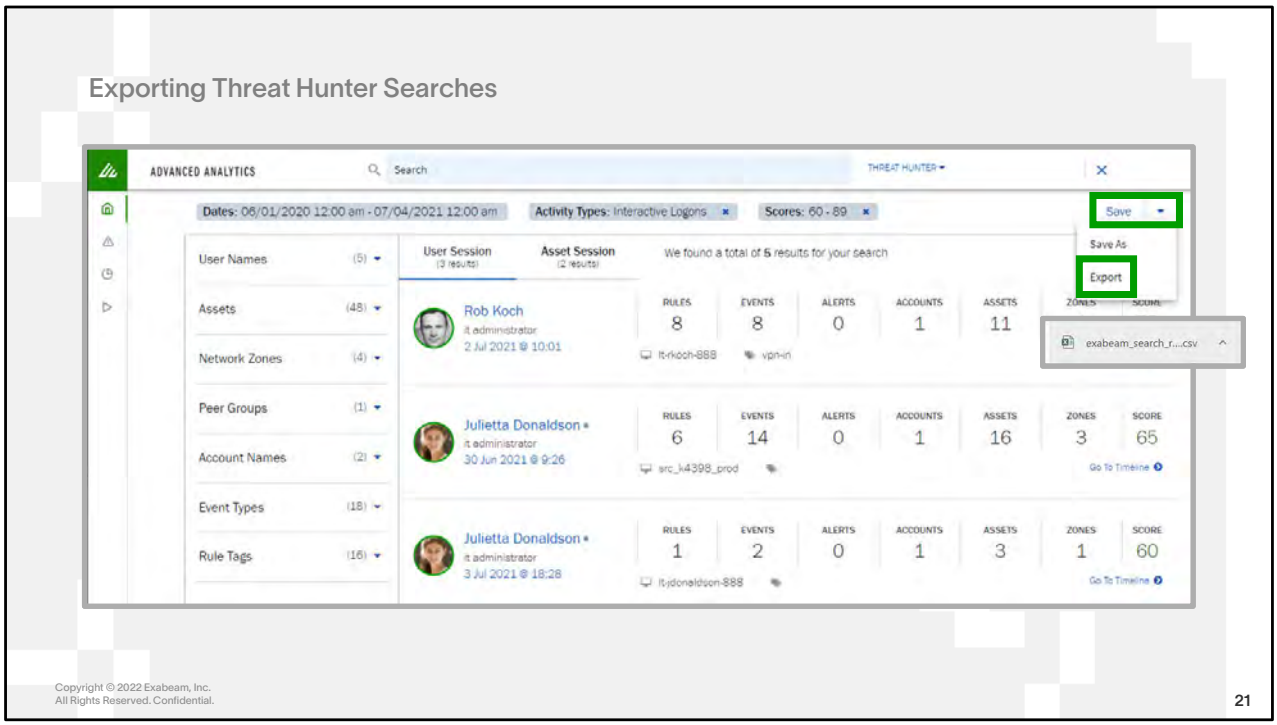
Exabeam ships with the following preconfigured searches:

- 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/

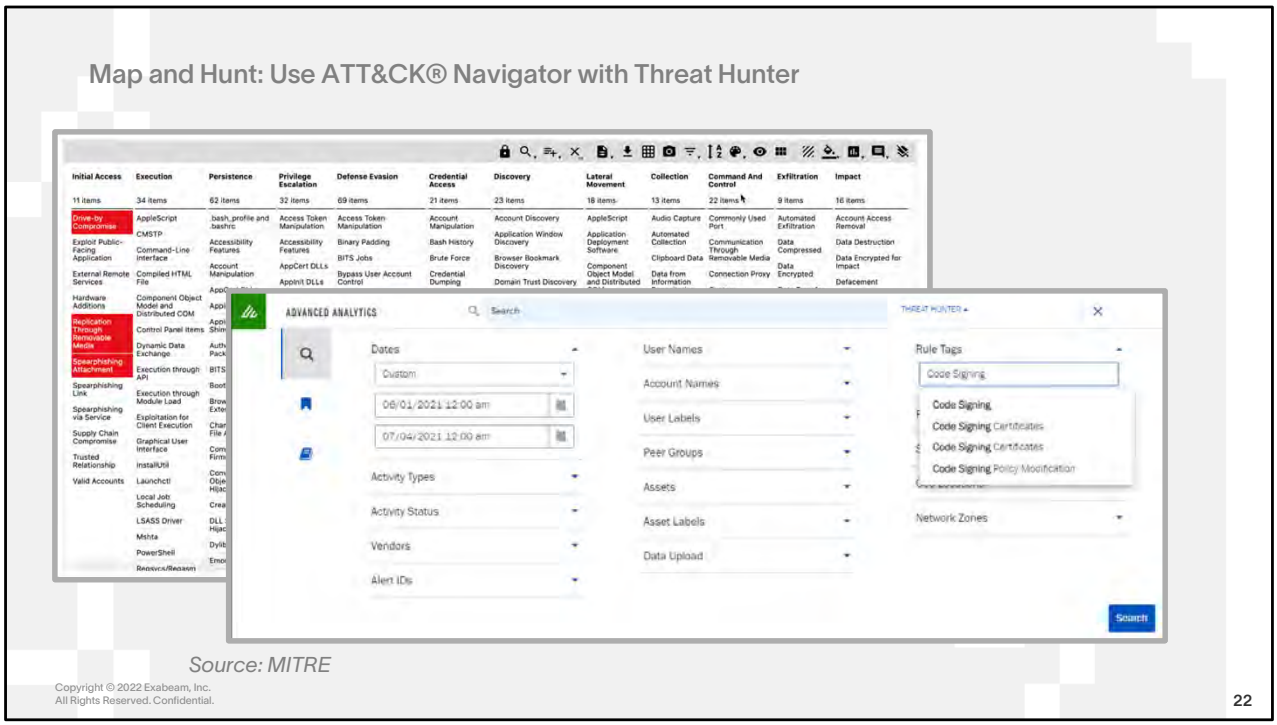


Student Notes

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/



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:

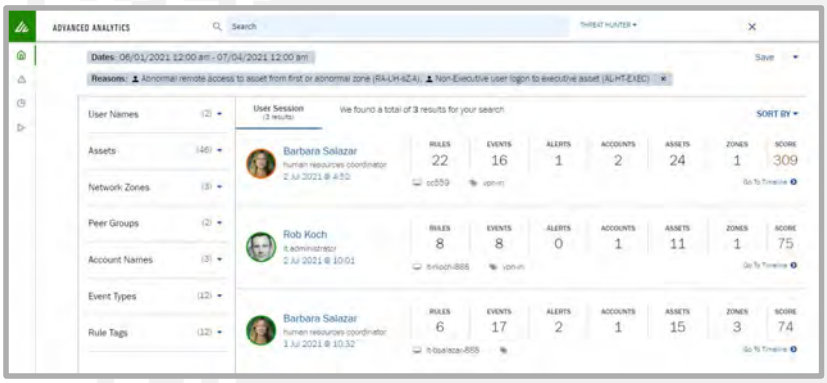
- Use ATT&CK to save time in developing a hypothesis to test
- Hunt for a pattern of behavior rather than artifacts; much more efficient

Source

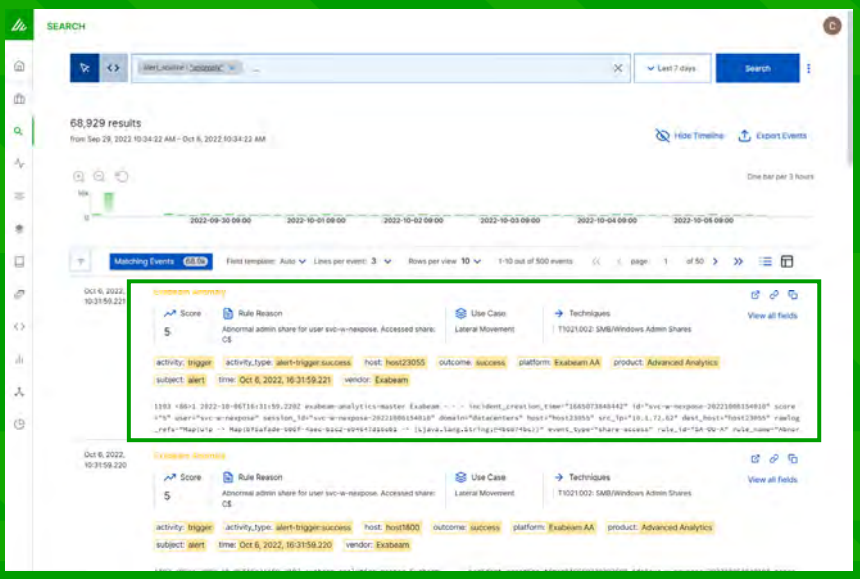
https://mitre-attack.github.io/attack-navigator/enterprise/

Demo

Going Threat Hunting!



What is Anomaly Search?



Lesson

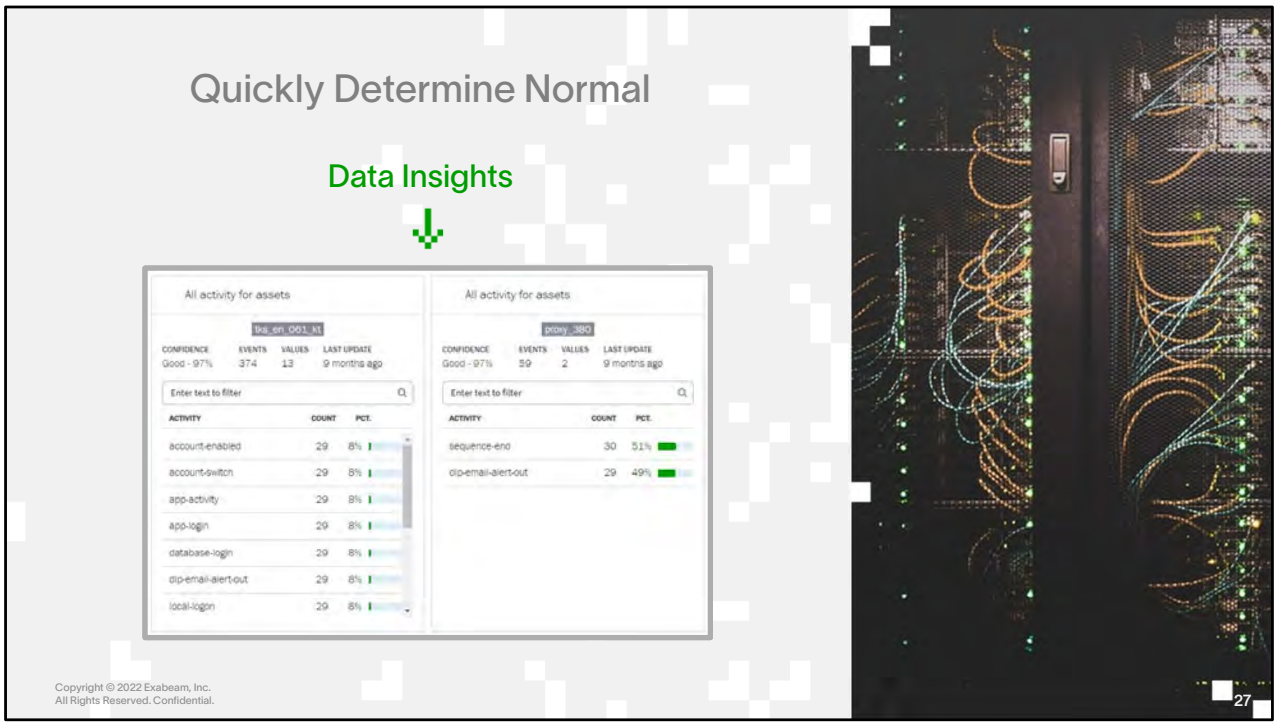
At the end of this lesson, you will be able to:

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

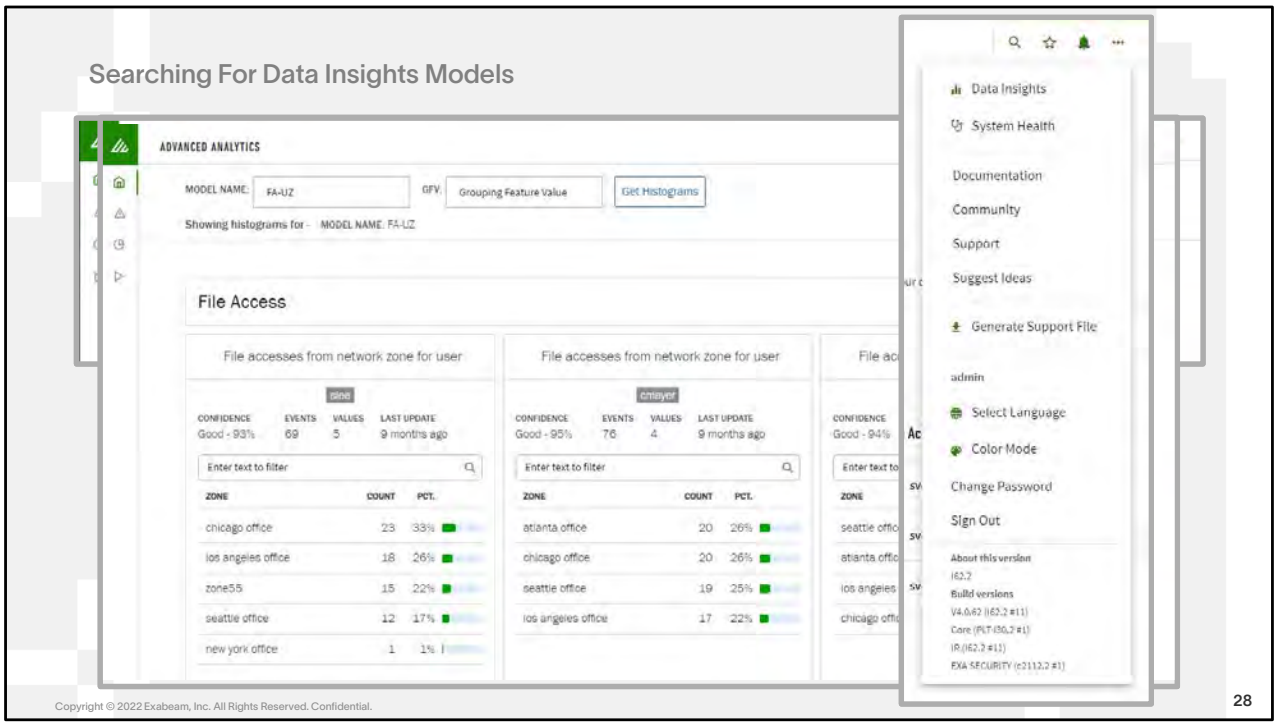
Use ATT&CK® with Your Security Team

Ever wish you could see what Advanced Analytics is seeing?

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



{Photo by Taylor Vick on Unsplash}



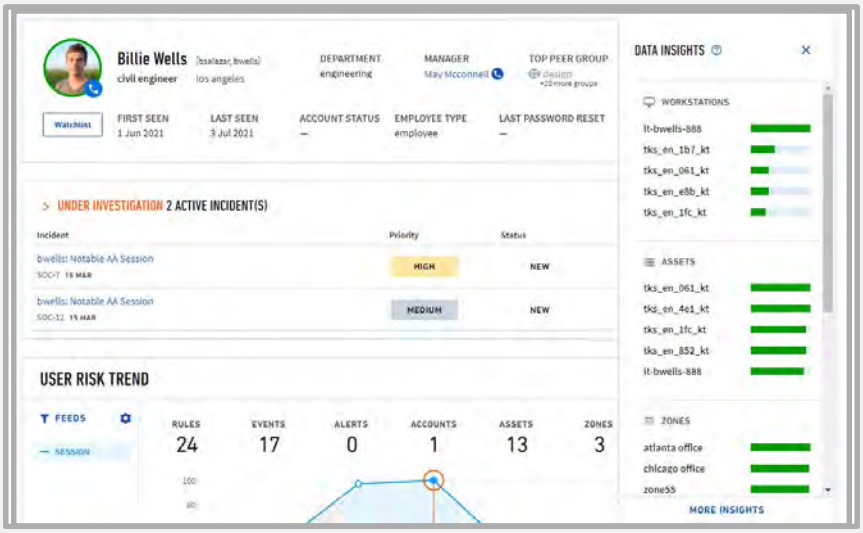
Student Notes

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



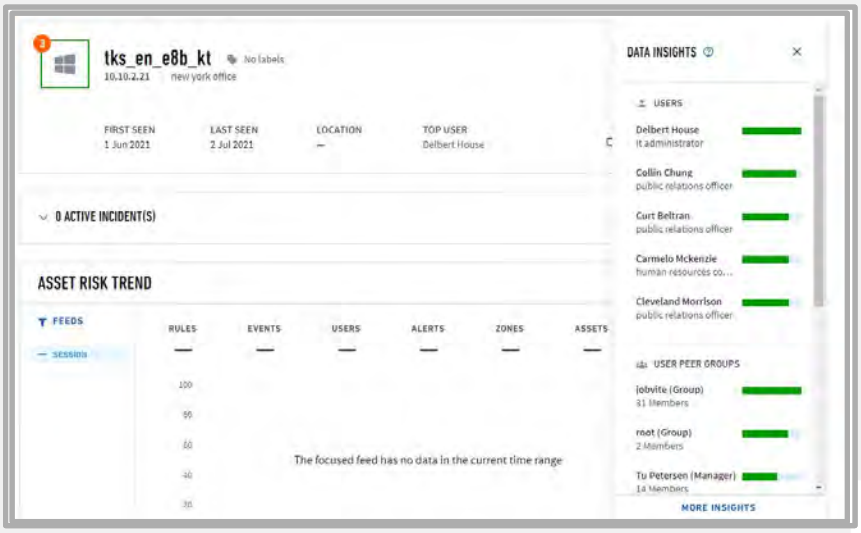
Student Notes

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

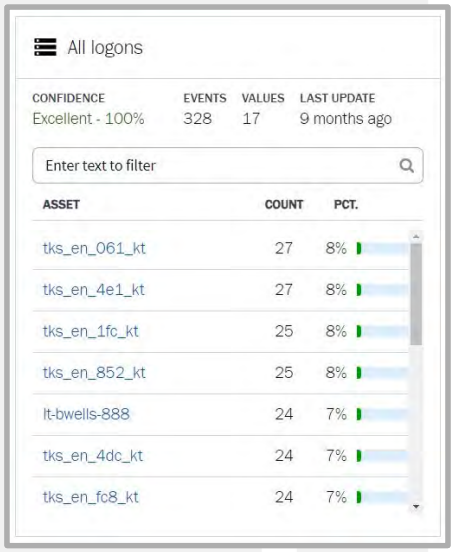
Each model has its own name and can be searched for using natural language components as well

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



Risk Reason Data Insights



Discussion

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

Activity

Using Threat Hunter and MITRE ATT@CK®

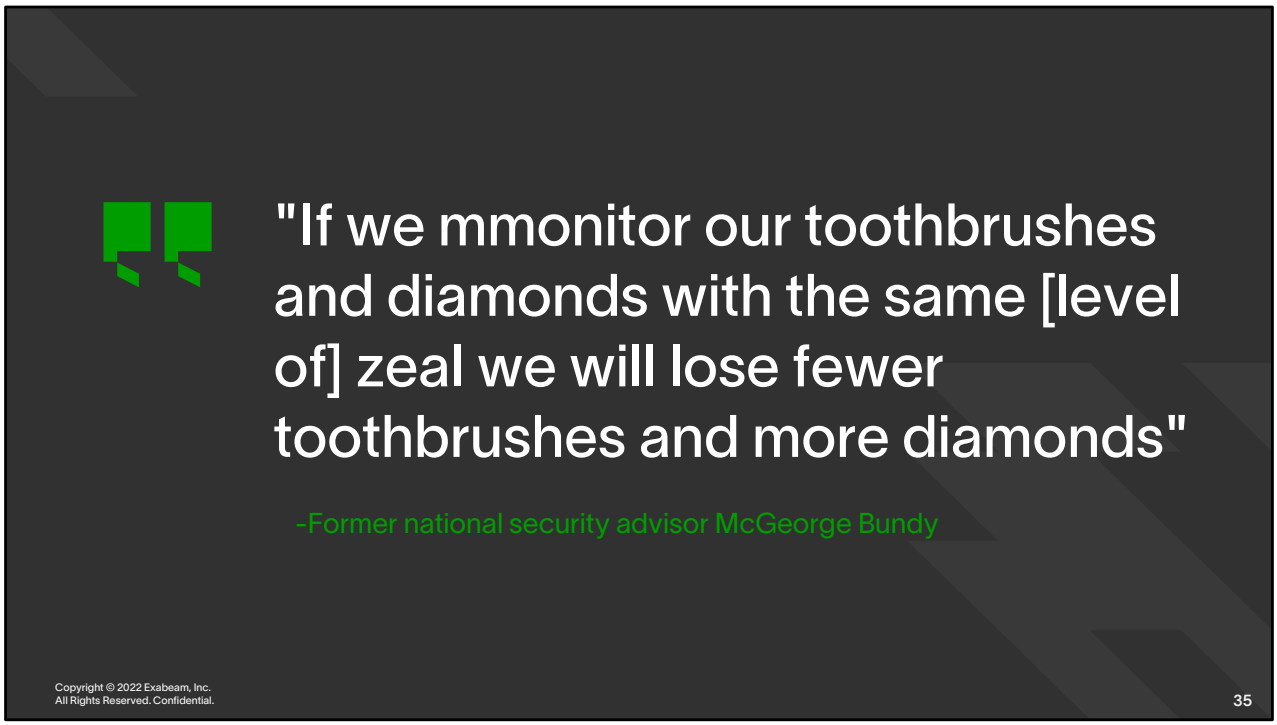
Objectives:

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

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**

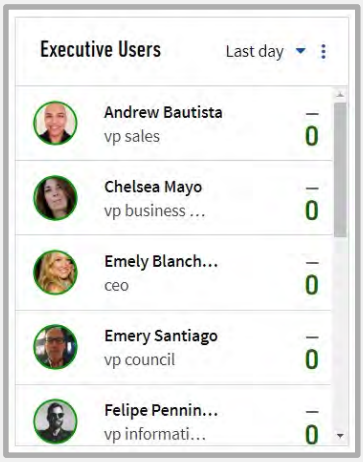


Student Notes
Make sure you are safeguarding the most valuable assets/individuals in your environment.

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

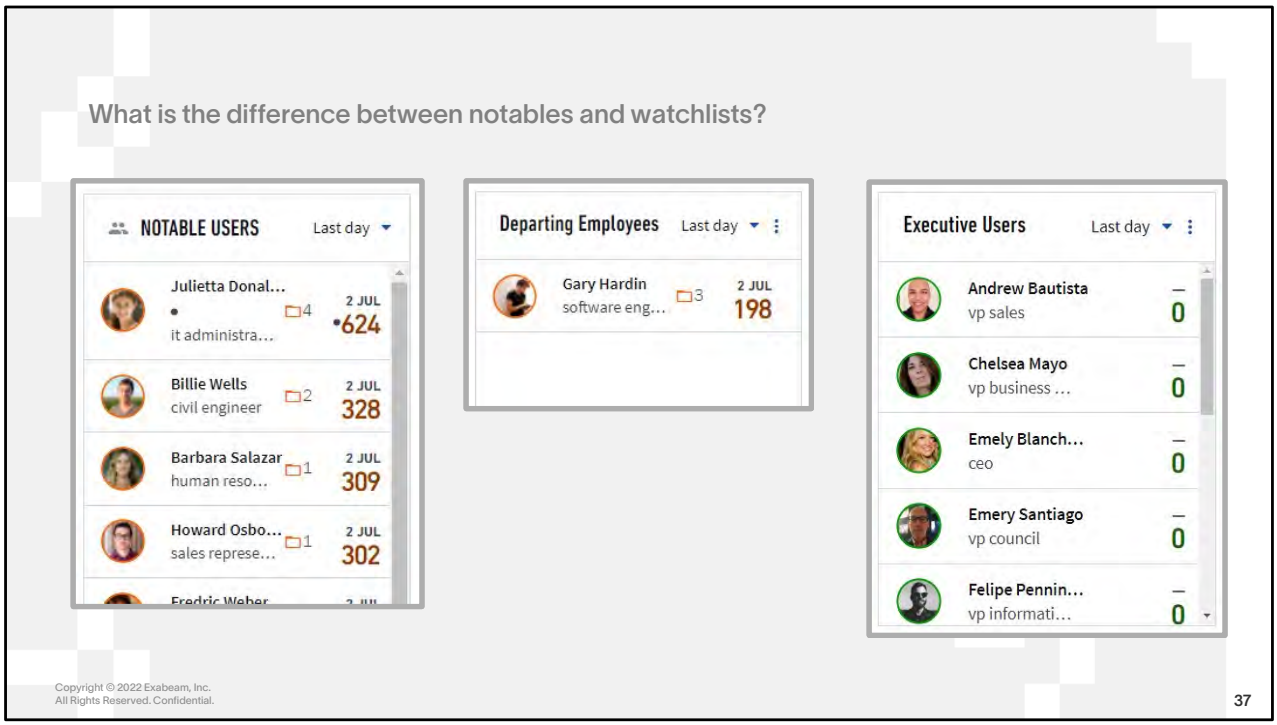
Monitoring High-Risk or High-Value Users and Assets

Watchlists



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.



Student Notes

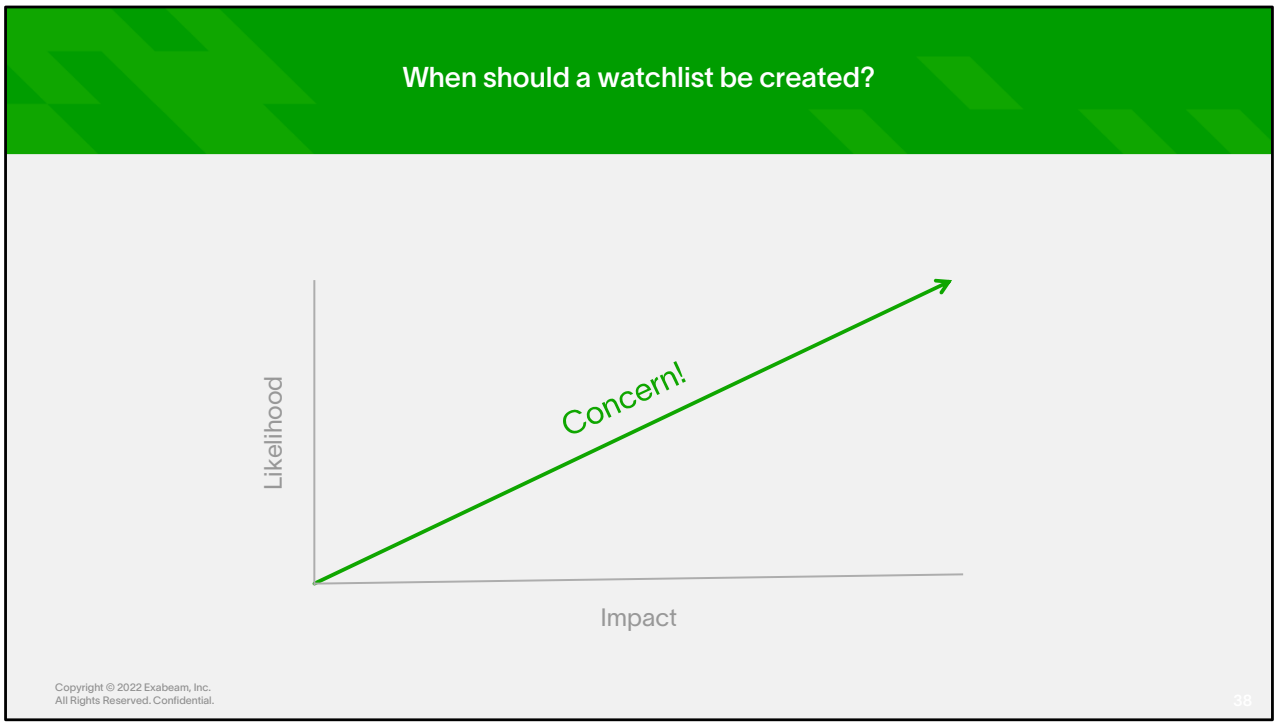
Notables in Advanced Analytics are built in watchlists that automatically populate when a predefined threshold risk score is reached (default of >=90 risk score). They cannot be added to or deleted from.

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/

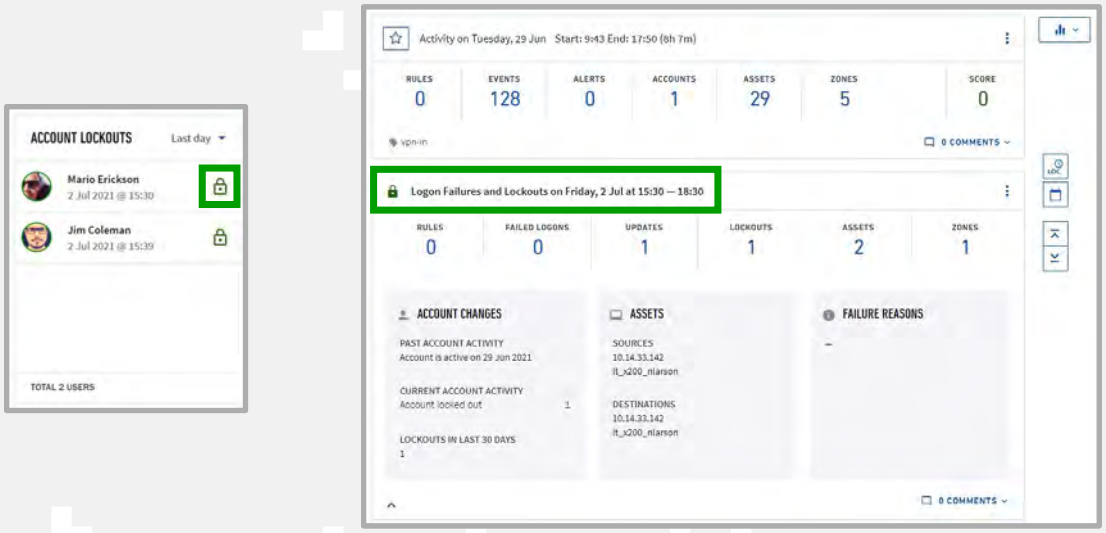


Source
https://www.exabeam.com/ueba/financial-institutions-and-ueba-fdic-vacation-policy-use-case/
Concept of project management risk management: https://intaver.com/risk-scores/

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}

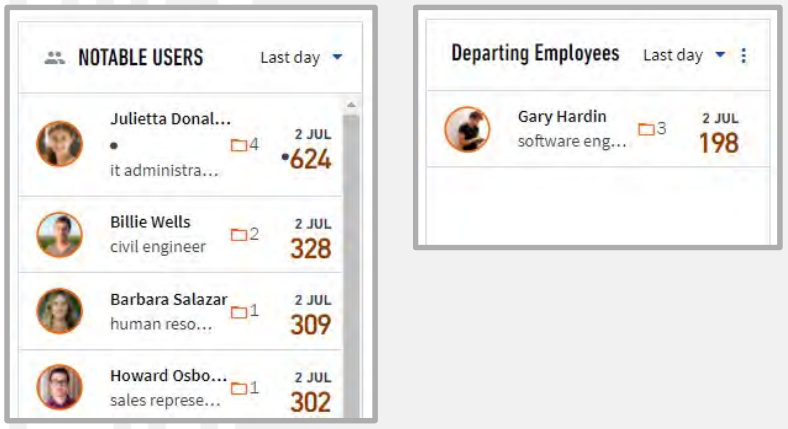
Account Lockouts – A Unique Watchlist



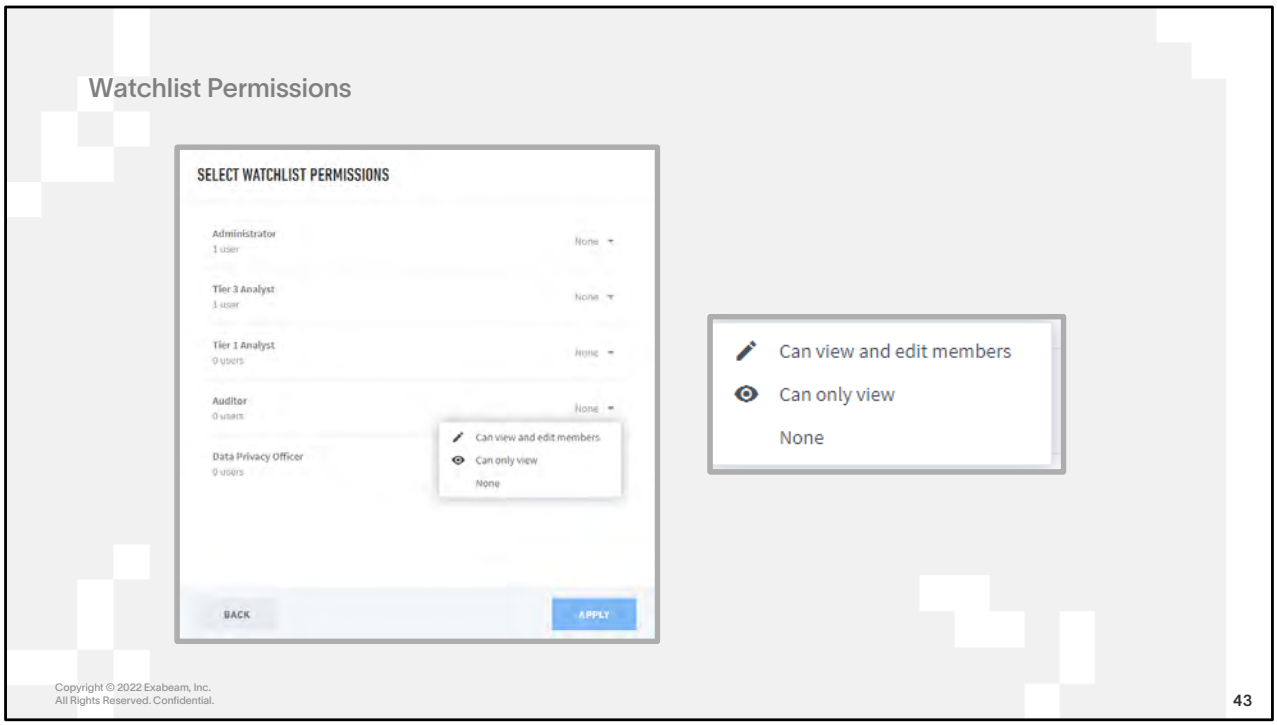
40

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



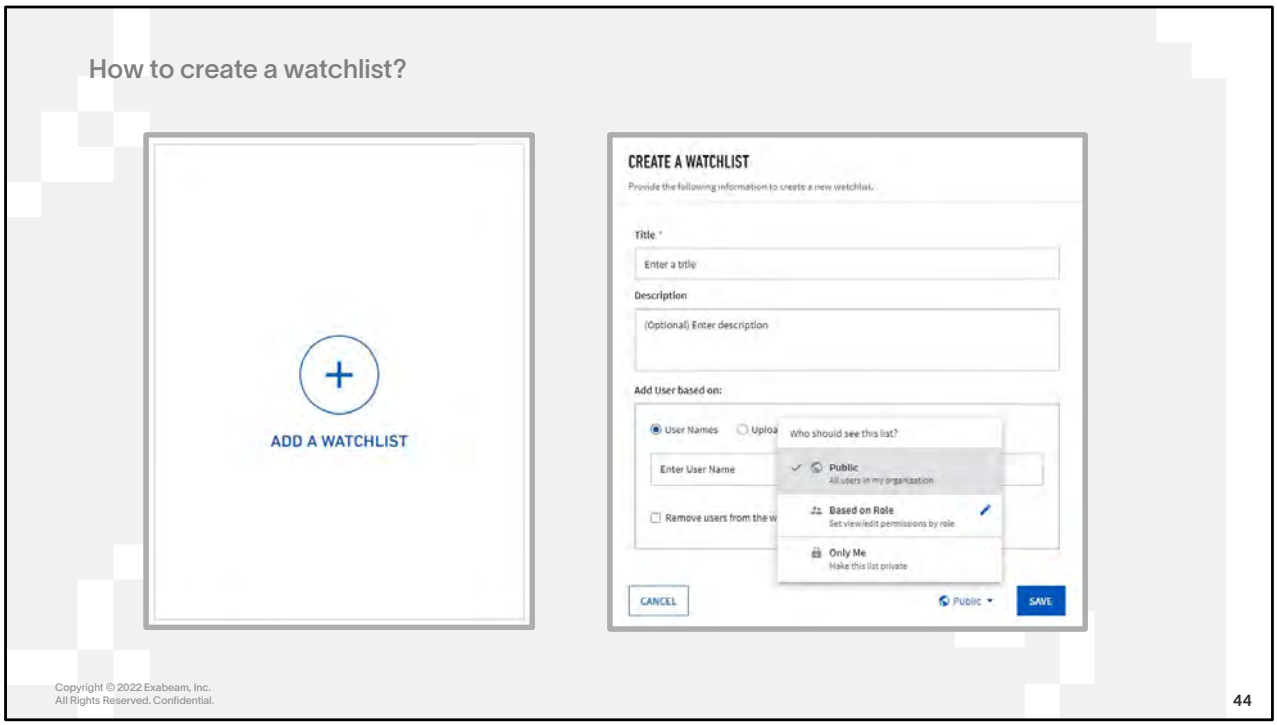
What are the five ways a watchlist can be populated?



Student Notes

Watchlists permissions are simple

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



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

Watchlist Tips

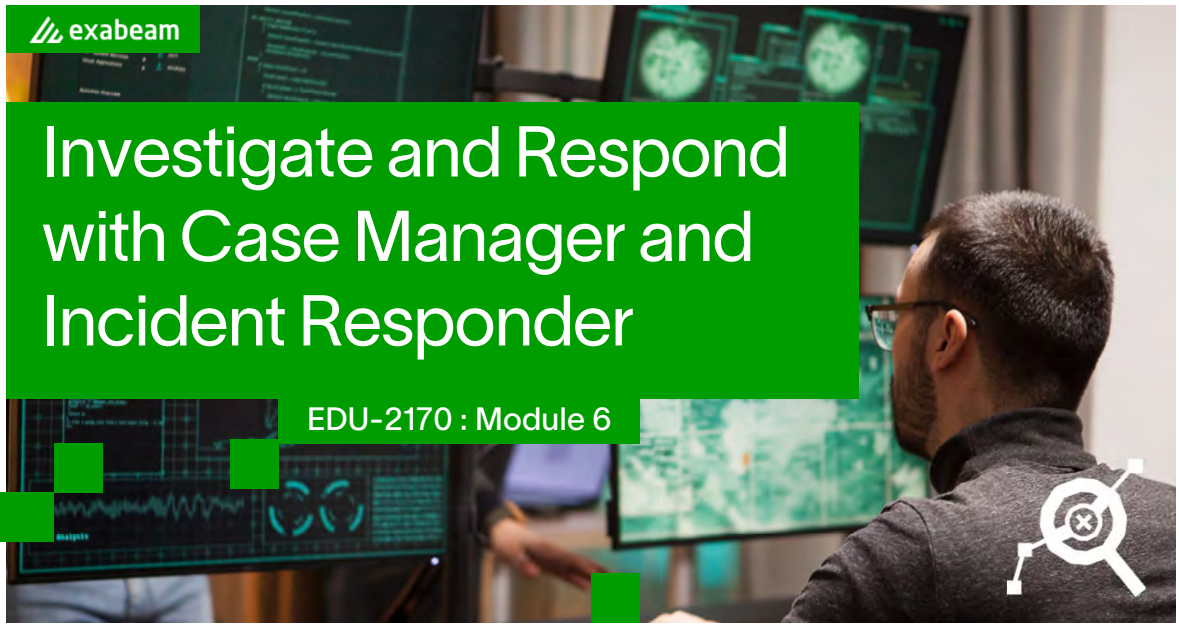
- Analyze business needs
- Create custom watchlists based on high-risk needs
- Use a repeatable, consistent framework
- Assess risks and models for tuning

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


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

Student Notes

According to NIST- Events and Incidents:

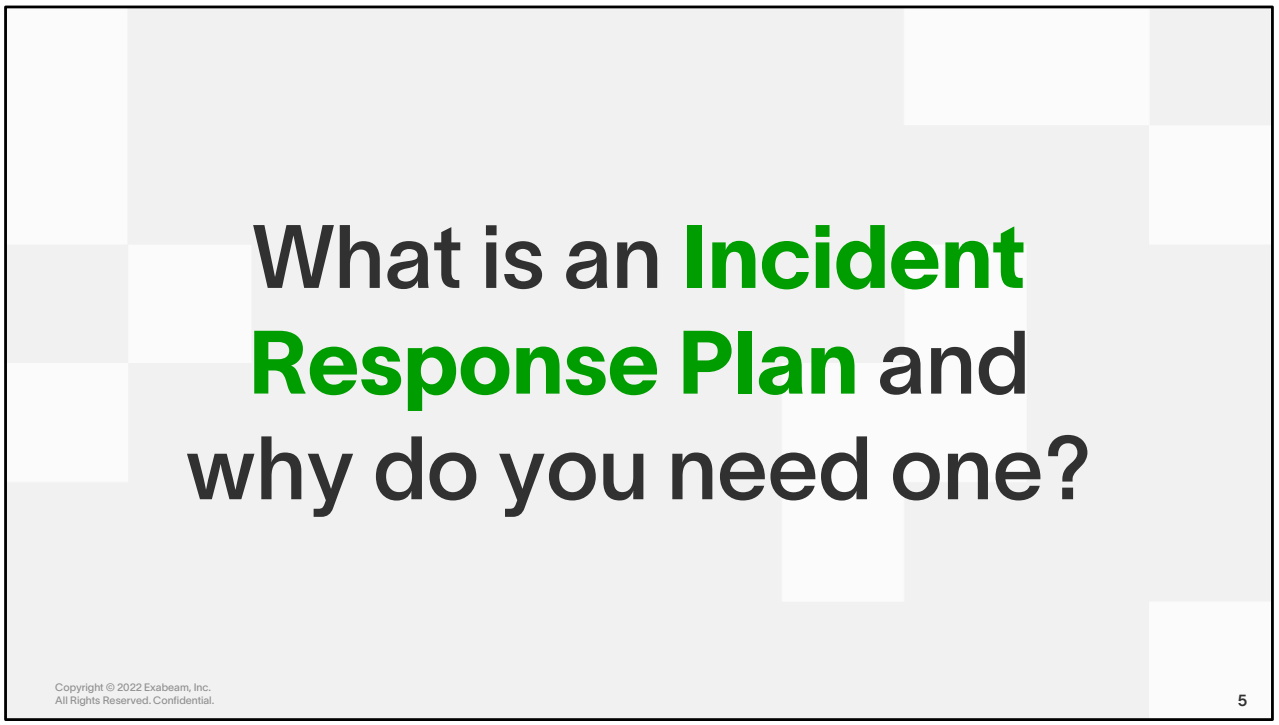
An **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, 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

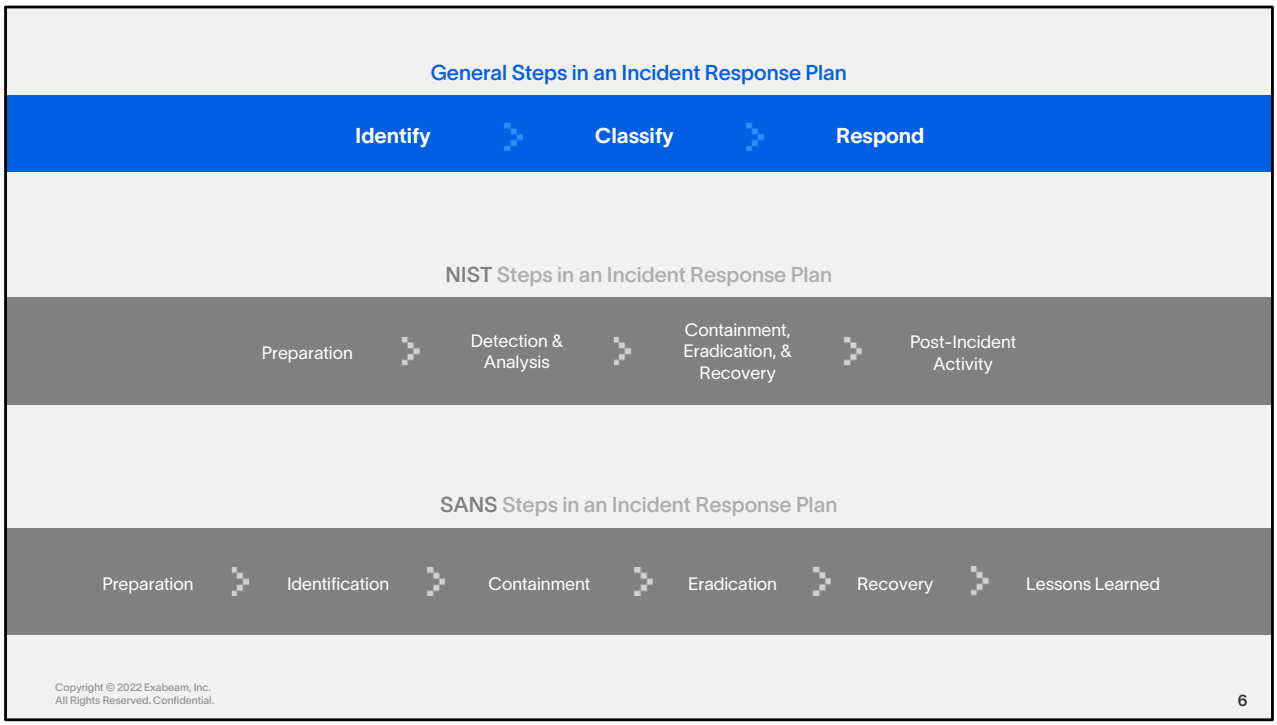


Student Notes
Incident Response
Incident response is an approach to review and respond to a cyber security breach or attack utilizing a planned process or methodology.
Effective incident response teams utilize procedures and technology, such as automated playbooks, to respond quickly and adequately to 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

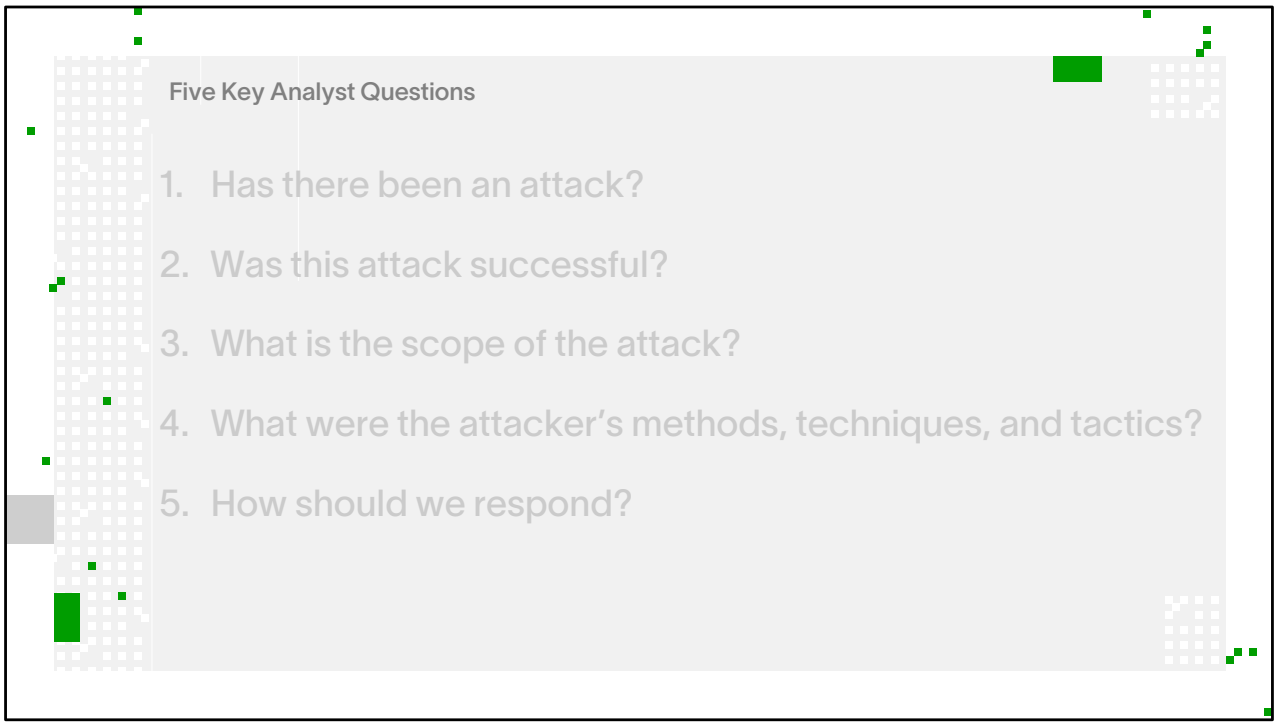


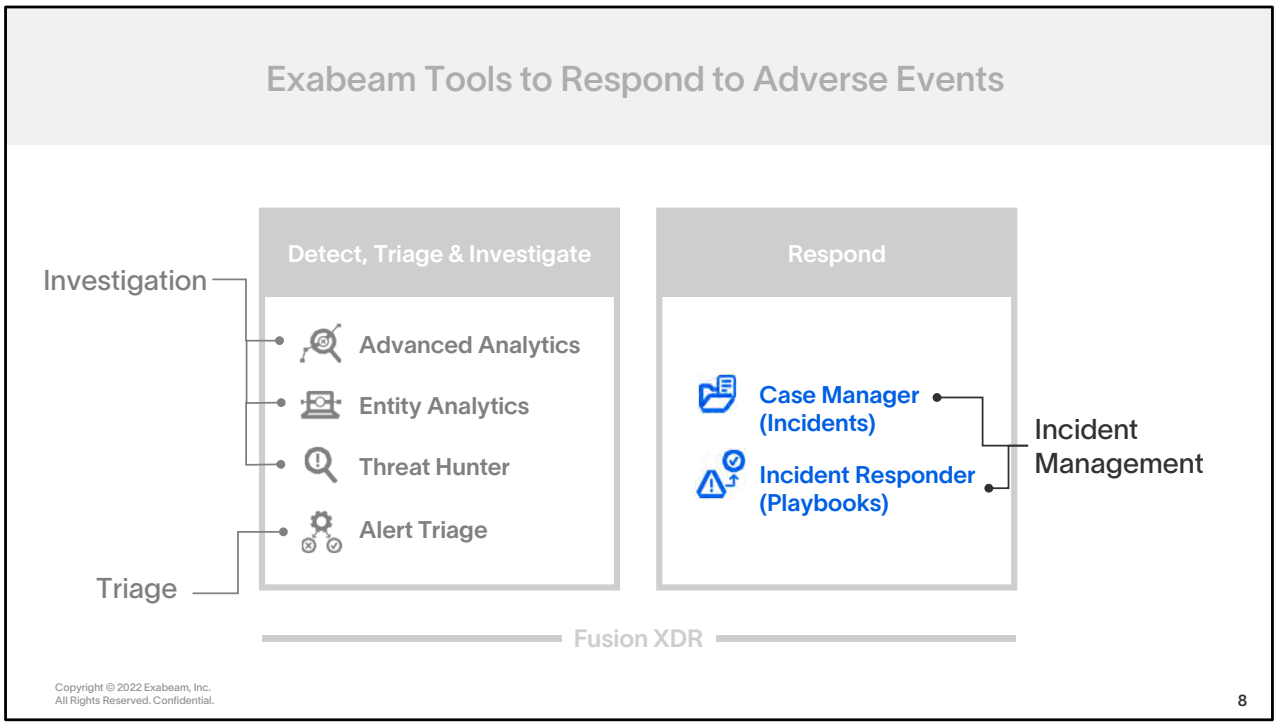
Student Notes

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.





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.

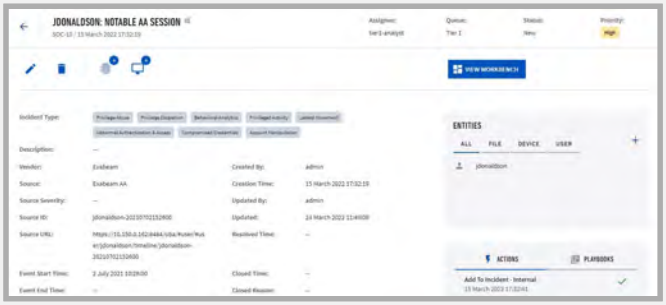
Exabeam Case Manager is a fully customizable case management solution that includes ticketing, messaging, and KPI dashboards to organize, track, and streamline your investigation

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?



- 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

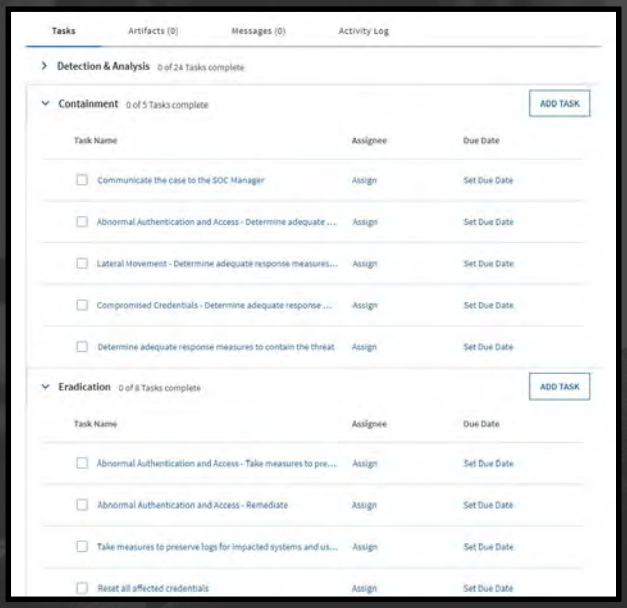
9

Student Notes

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

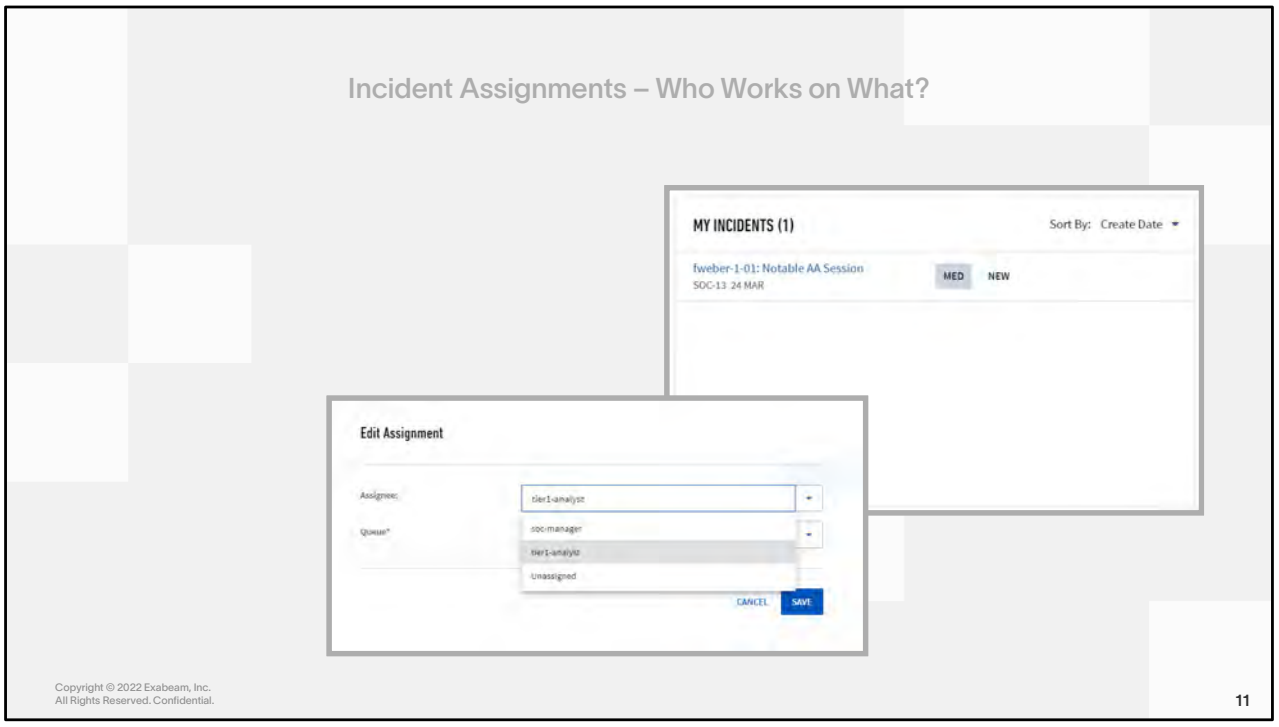
Case Manager Incident “Tickets” document and guide this process for consistency and completeness

Consistent investigation and response with Exabeam Case Manager checklists



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.

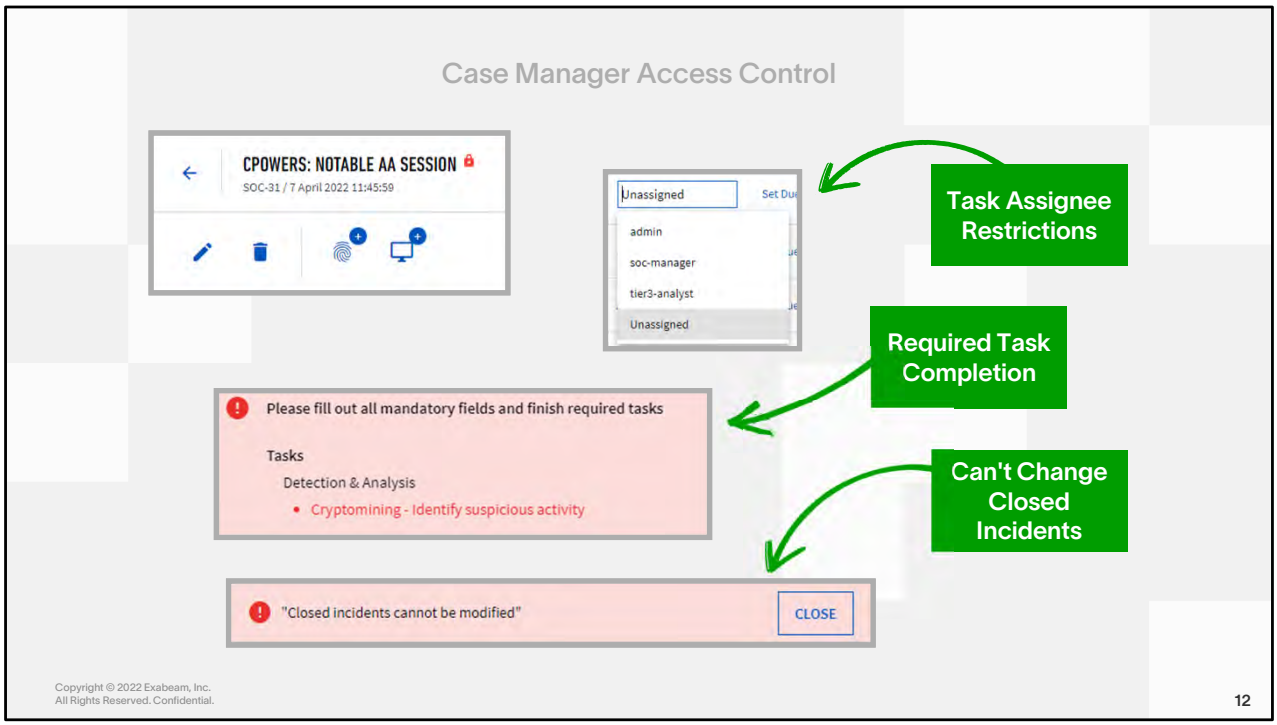


Student Notes

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

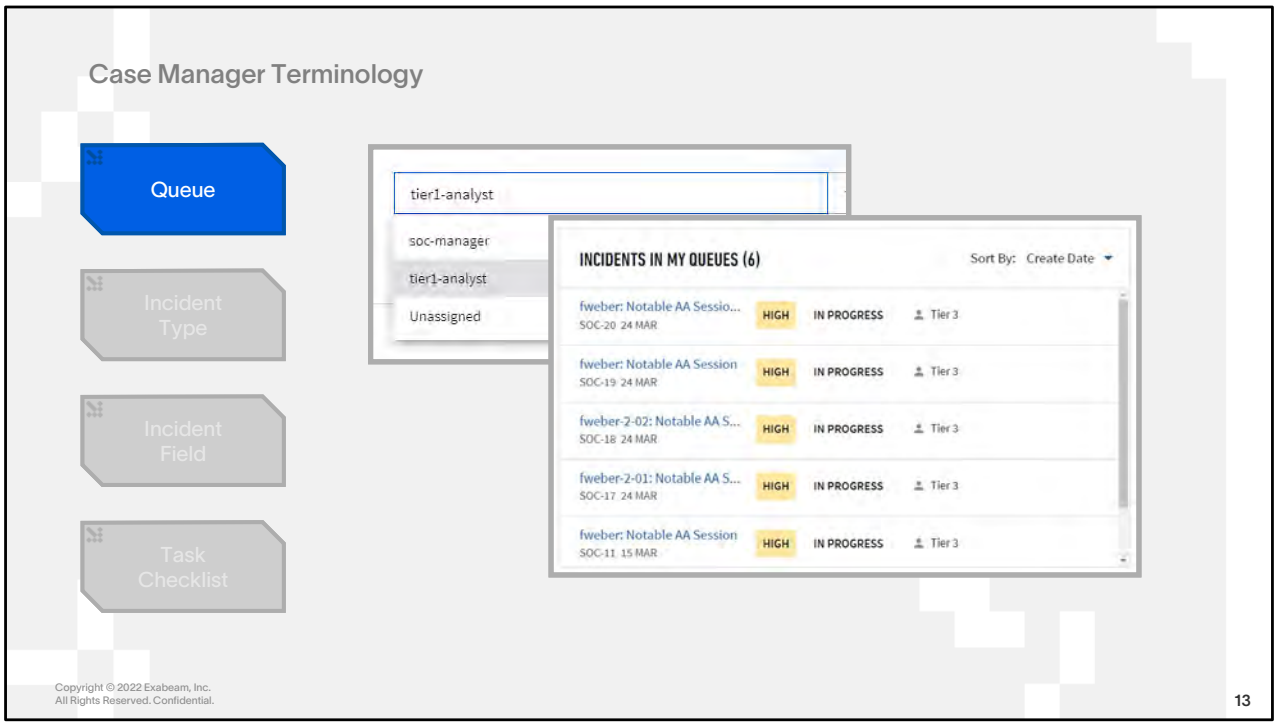
In addition to case queues and assignments, Case Manager access control restrictions have the potential to impact an analyst's interactions with the tool. Four controls in particular are worth noting:

- 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 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

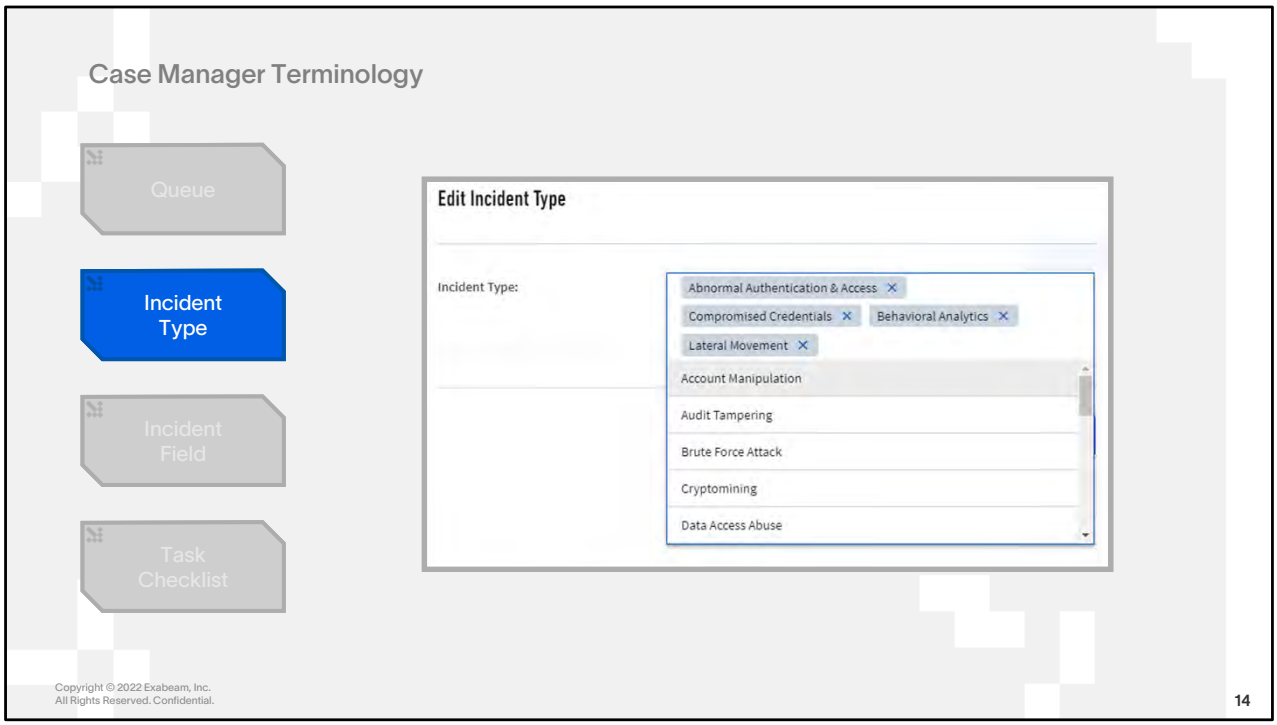


Student Notes

- 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



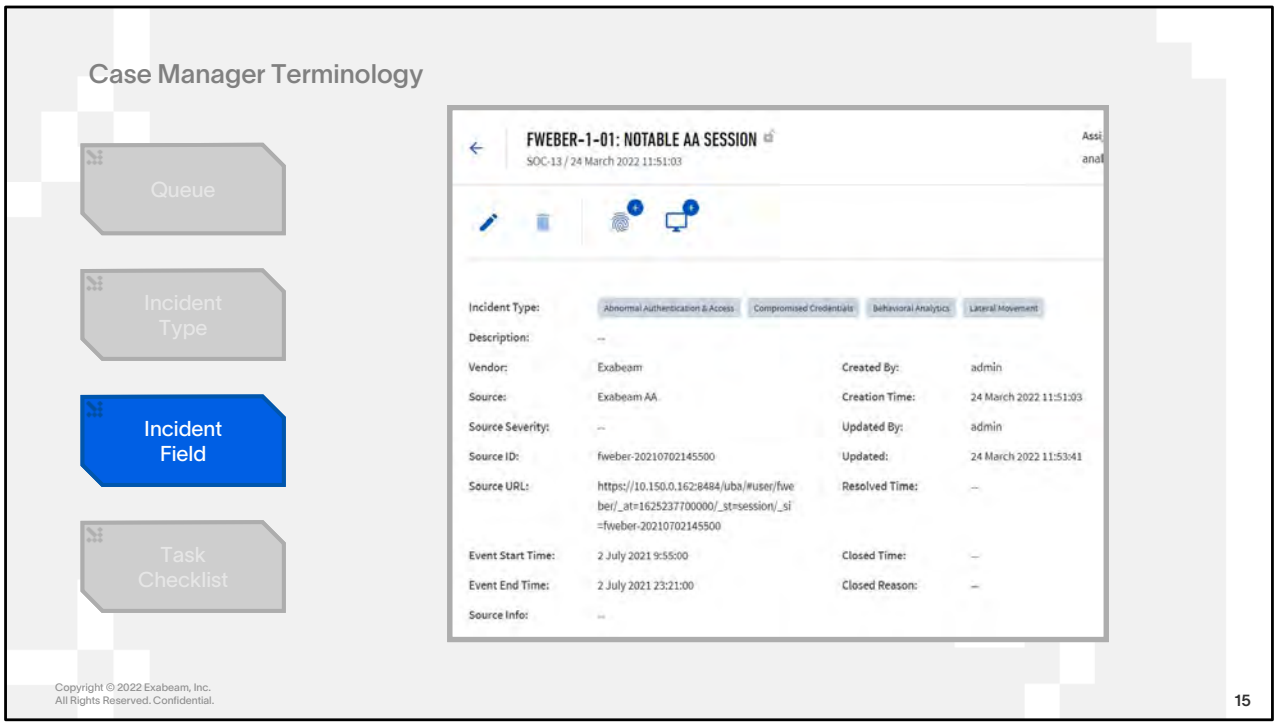
Student Notes

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



Student Notes

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

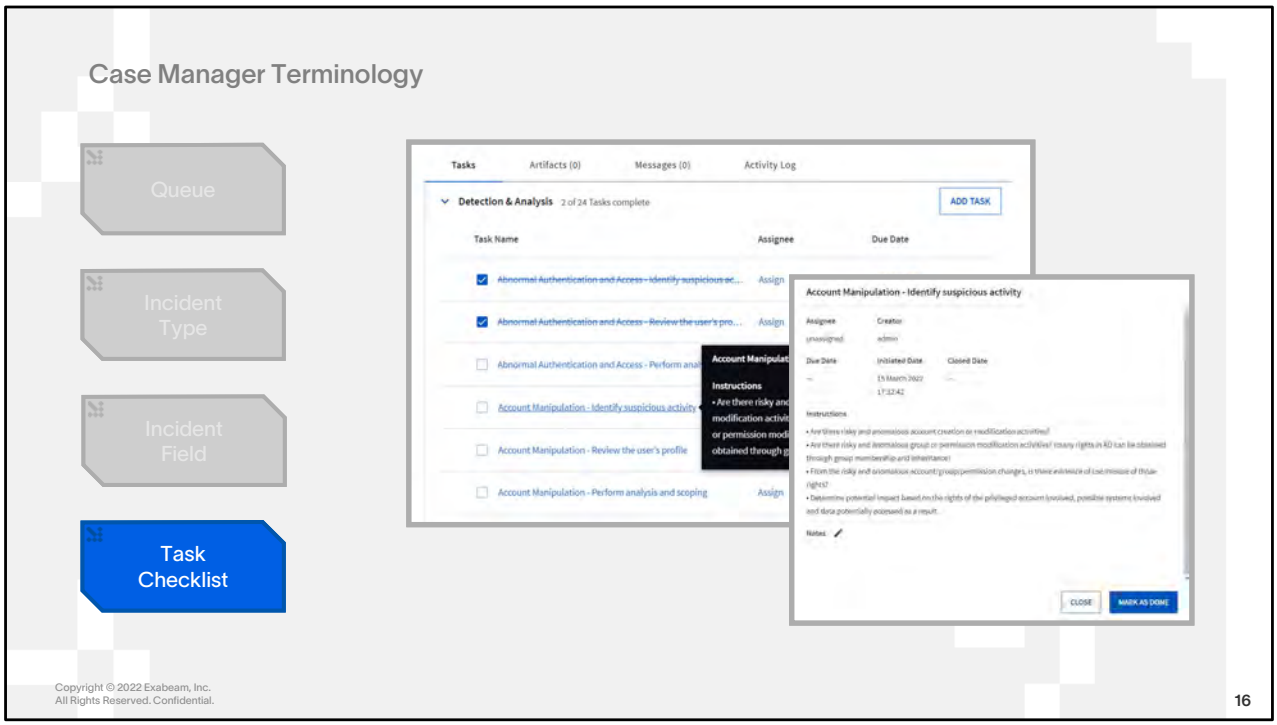
Source

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



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

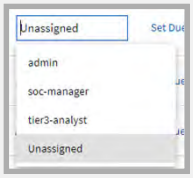
Checklists allow teams to create step-by-step instructions or 'tasks' grouped into phases aligned with NIST frameworks

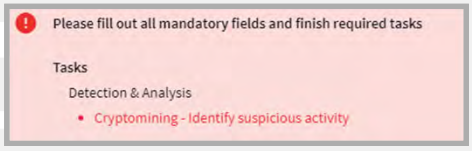
Different incident types will add different tasks

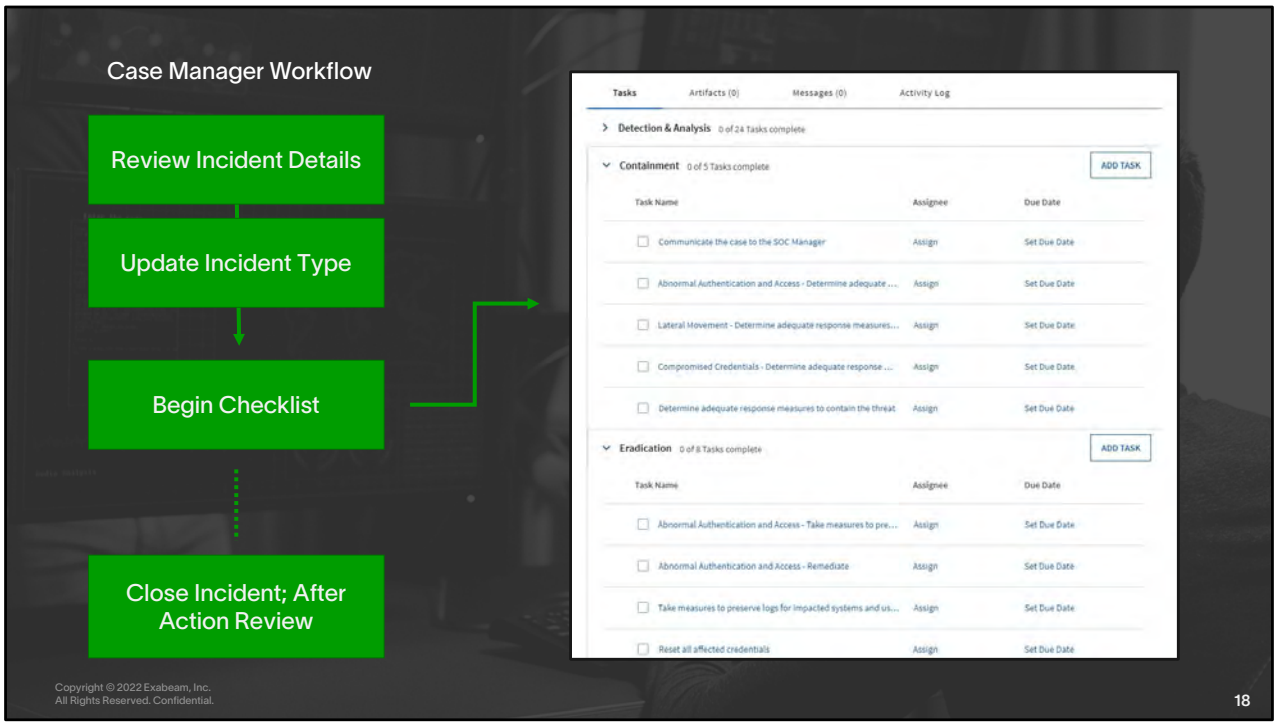
Case Manager administrators can redefine the phases and tasks associated with any incident type

Demo

Case Manager Restrictions

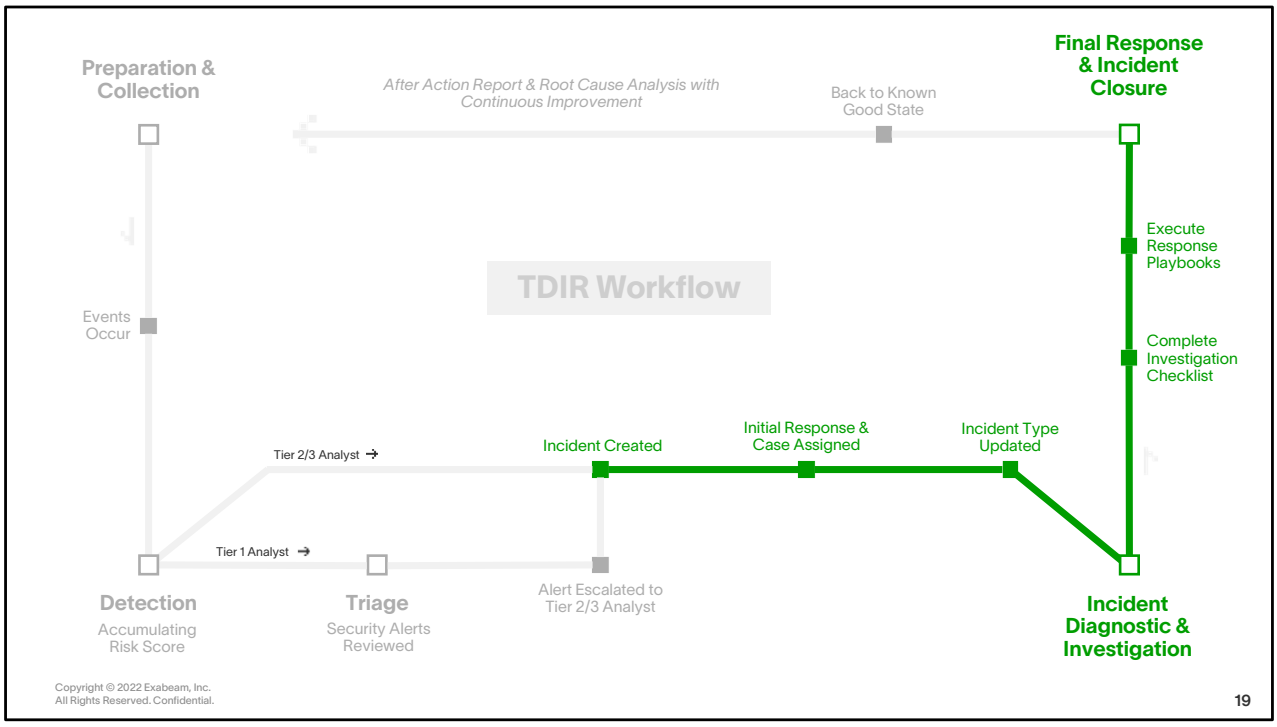






Student Notes

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:

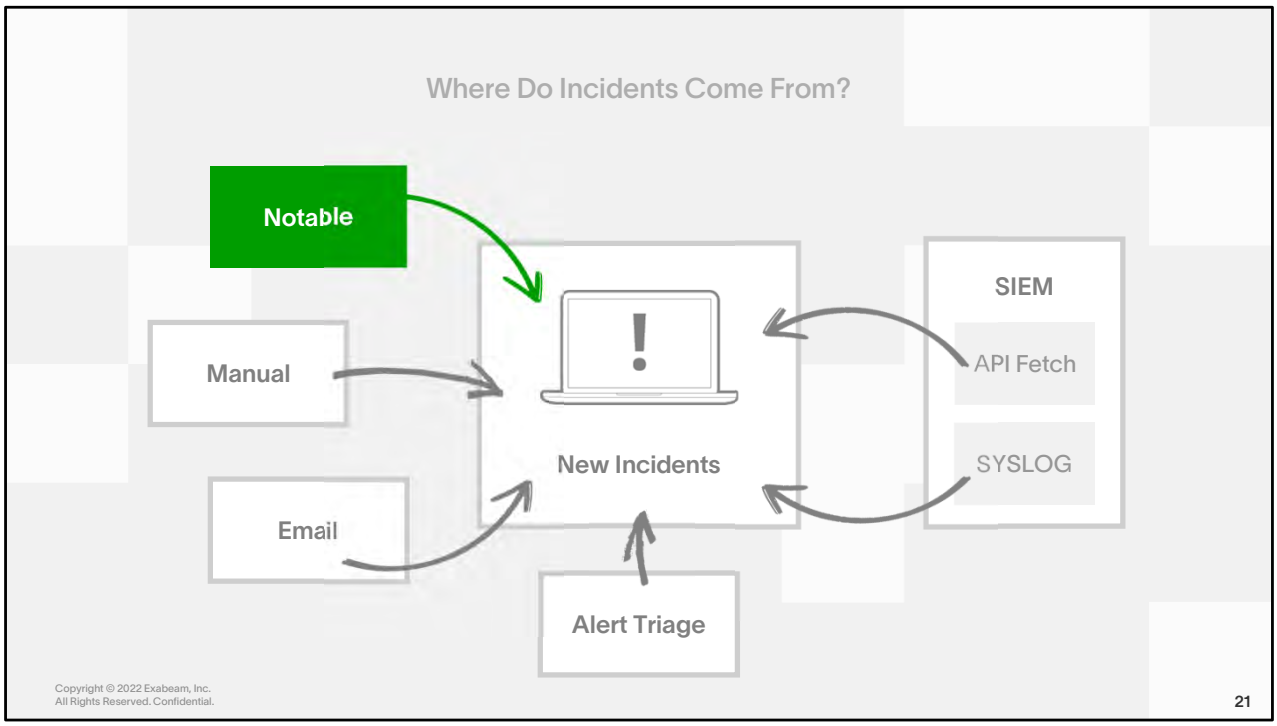
1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow

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



Student Notes

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

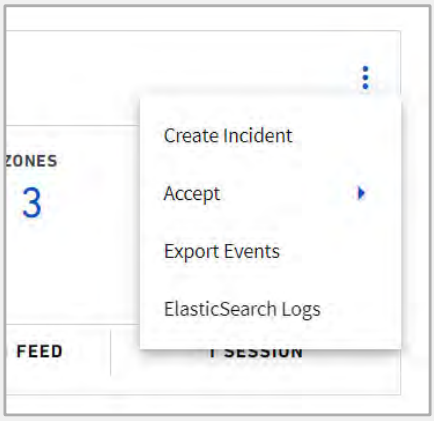
Many incidents are automatically created, such as when an Advanced Analytics user has a risk score above 90 and becomes notable or an alert is escalated in Alert Triage.

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

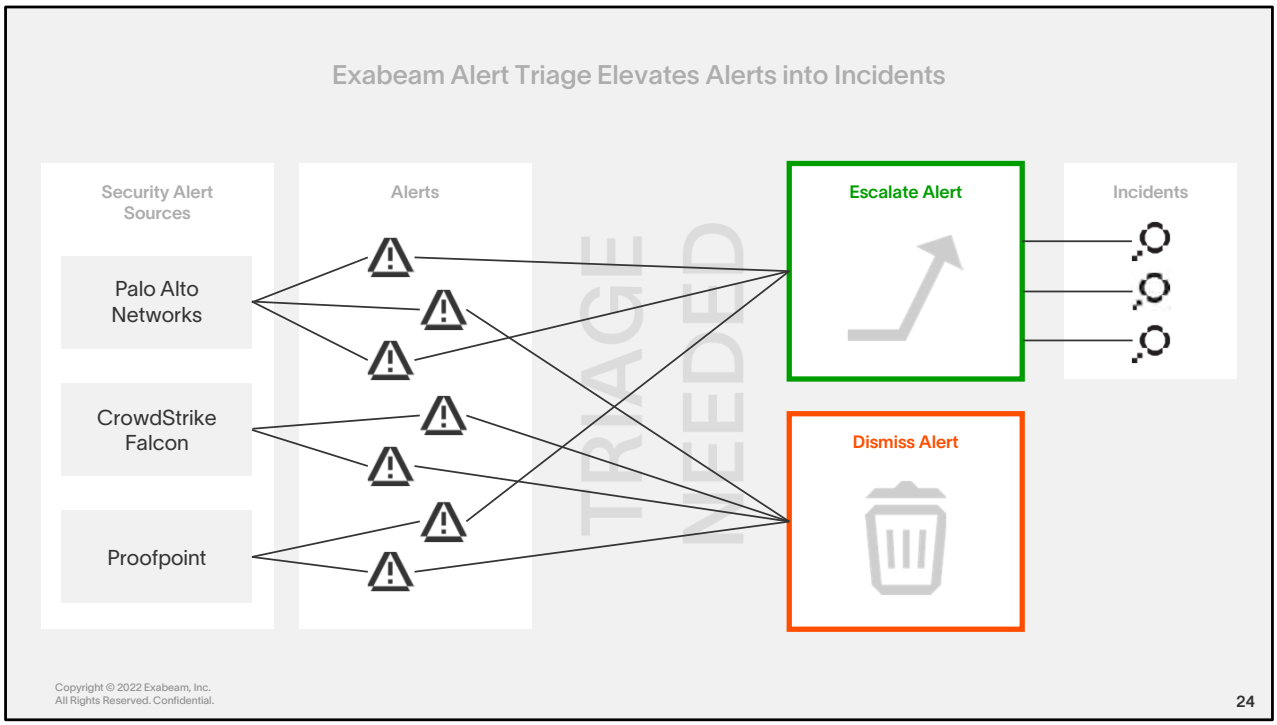
- What do you do when you discover suspicious behaviors proactively?
- Create an incident manually!



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

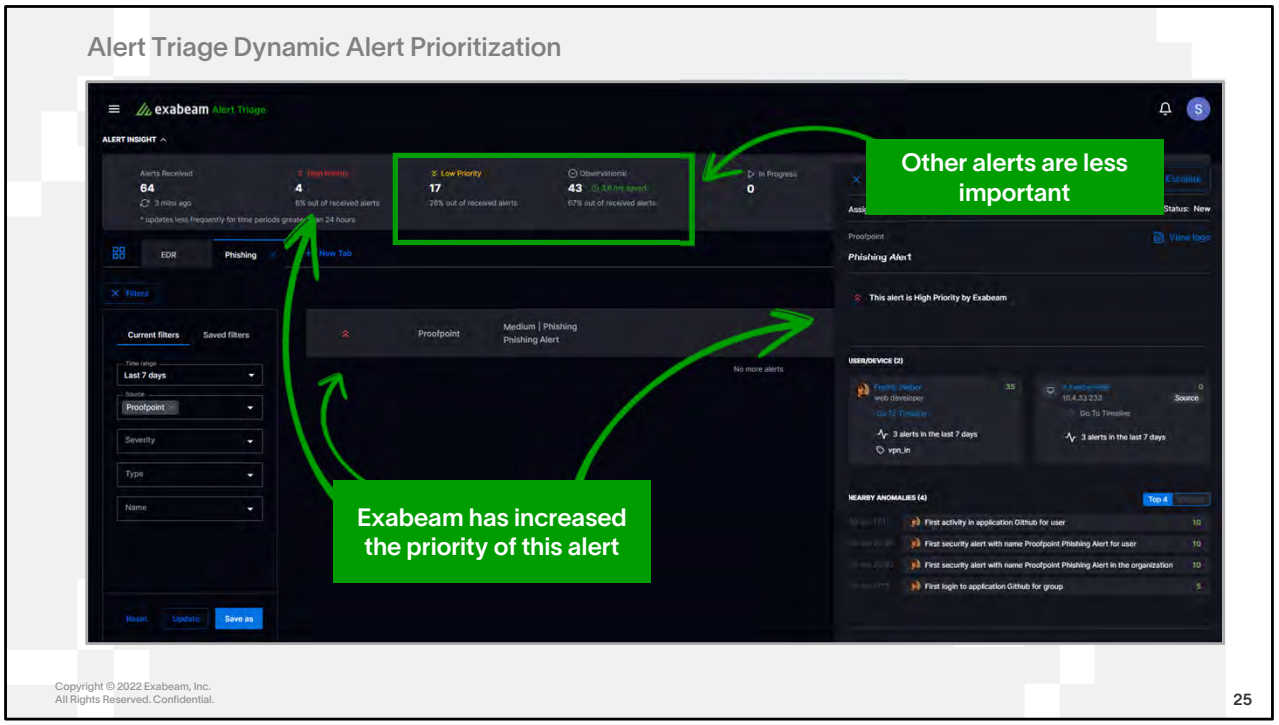
The first step of Alert Triage, usually performed by Tier 1 analysts, determines if an alert poses a risk to their organization. The first challenge is in opening the various alert sources and reviewing alerts. This can be done more quickly if a SIEM is used rather than opening each product's interface 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/



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 use 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

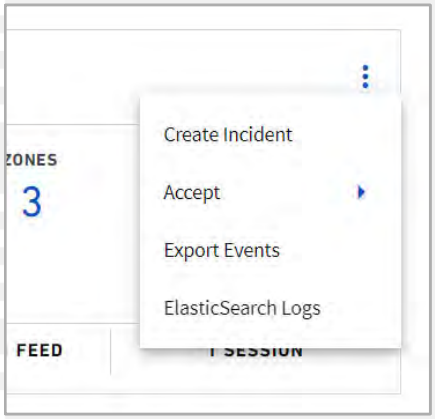
Also, analyst feedback helps the ranking algorithm understand if surfacing the alert as high or low priority was correct. The Exabeam risk engine will then use this feedback to improve the ranking algorithm.

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

Create Incidents Manually in Advanced Analytics

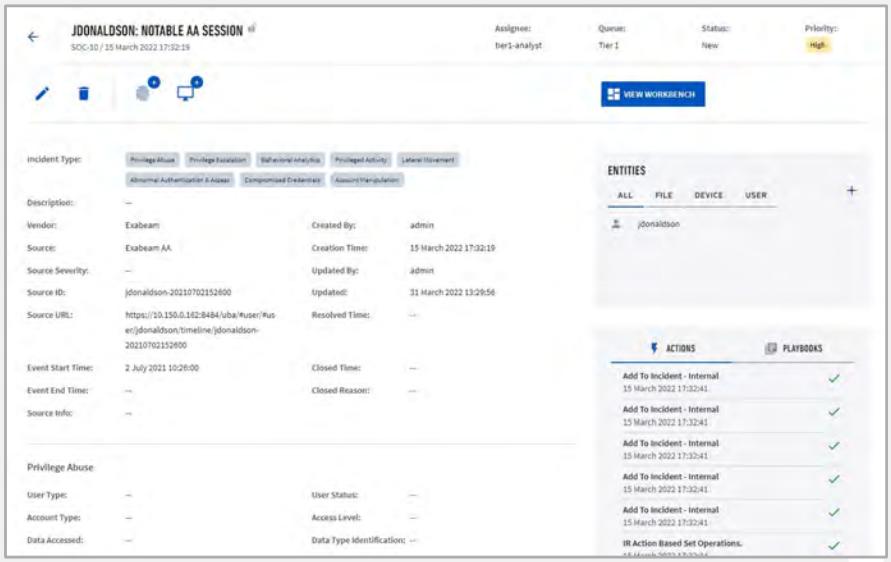


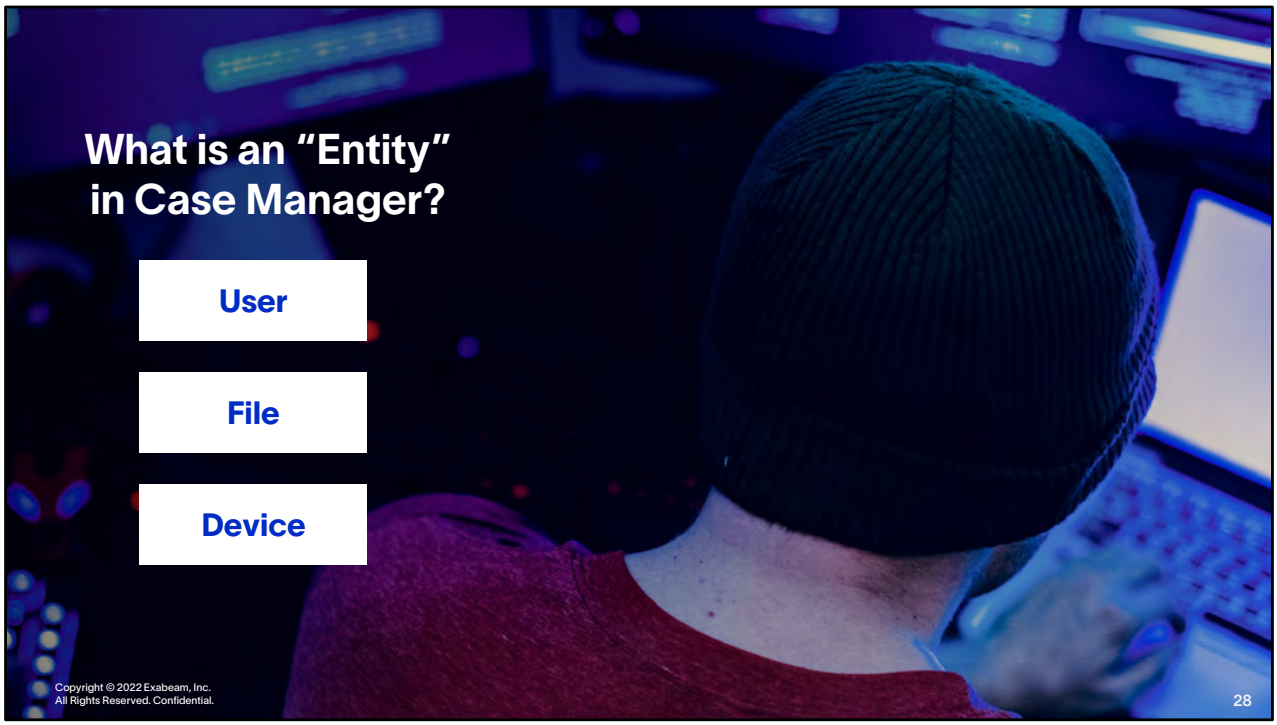
26

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





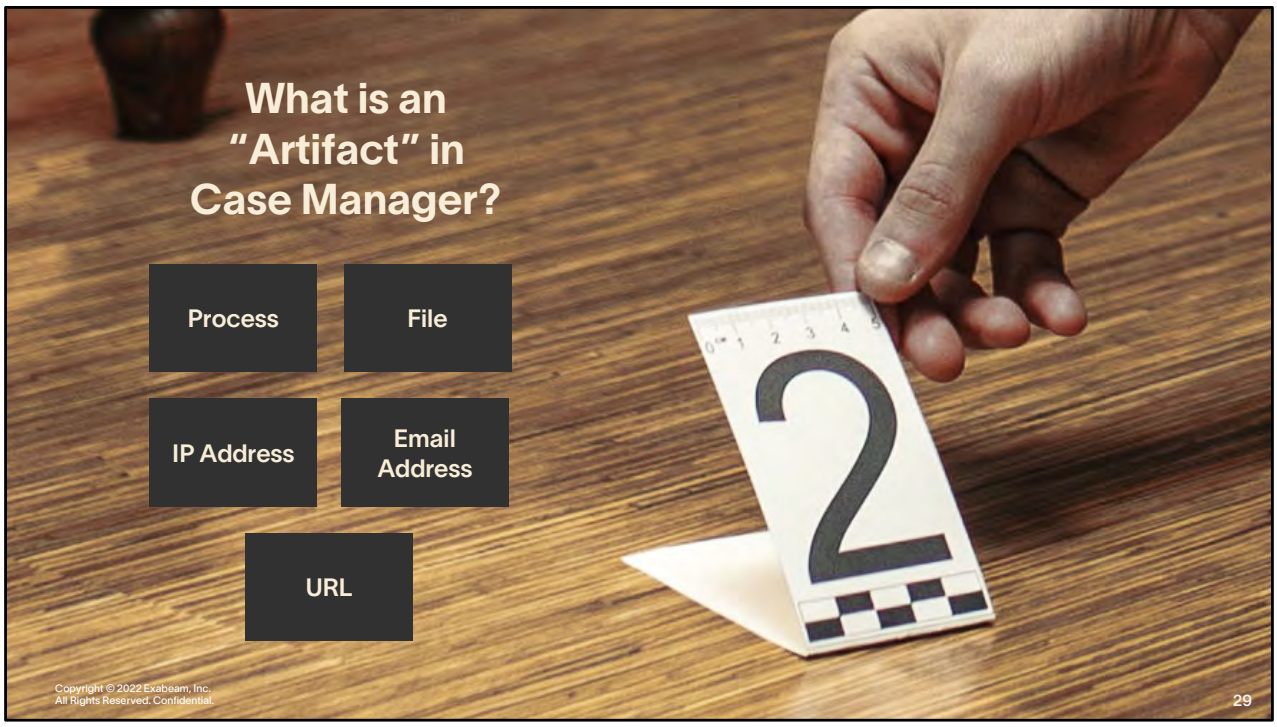
Student Notes

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



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.

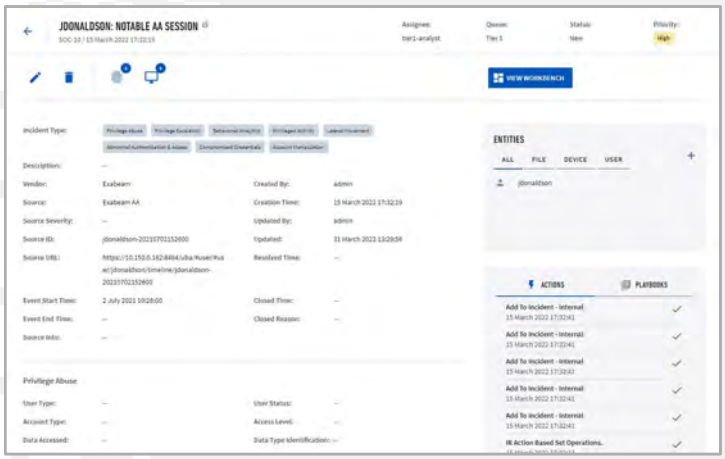
Source
Advanced Analytics User Guide

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

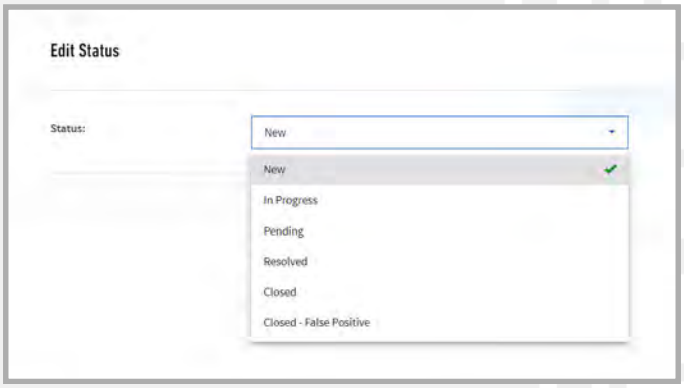
Demo

Edit Incidents in Case Manager



Discussion

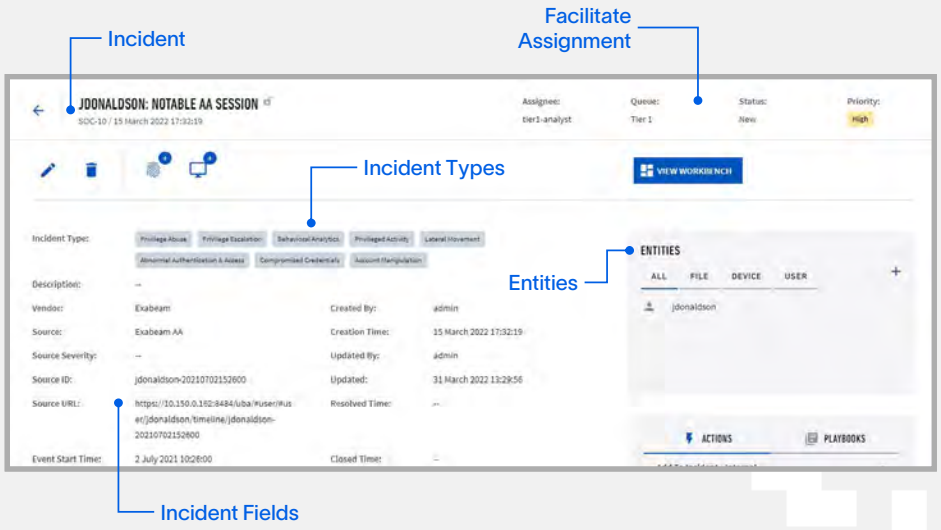
What are the important considerations when closing an incident?



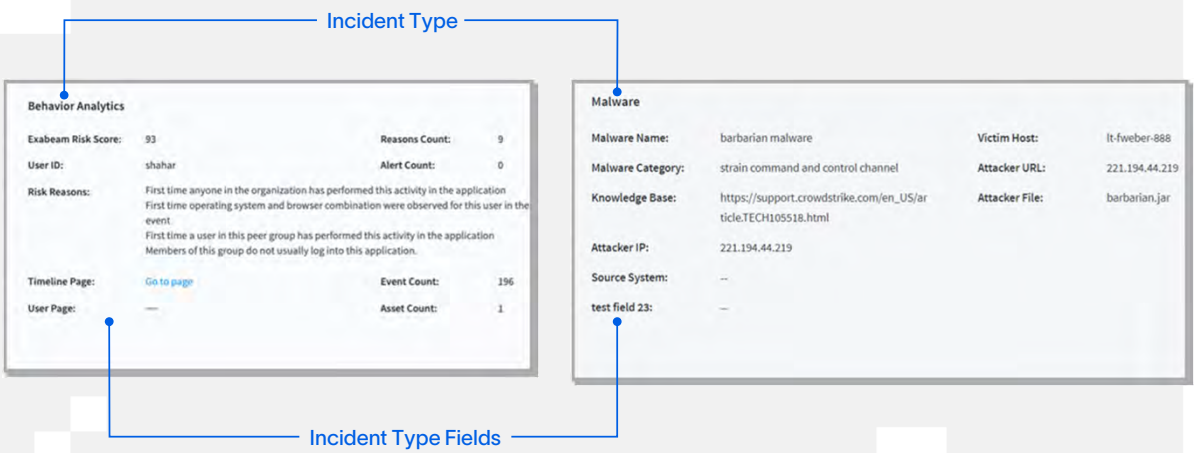
Student Notes

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



Case Manager In Action

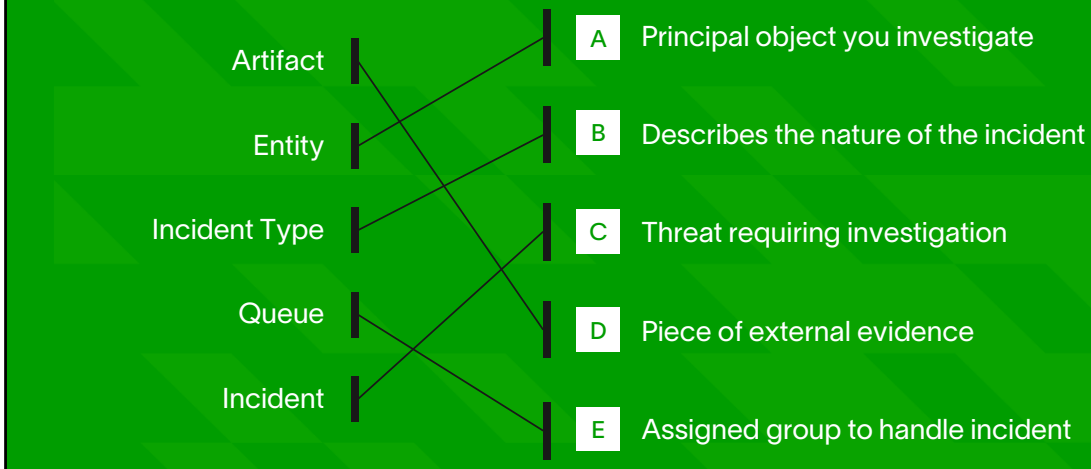


Case Manager Metrics

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

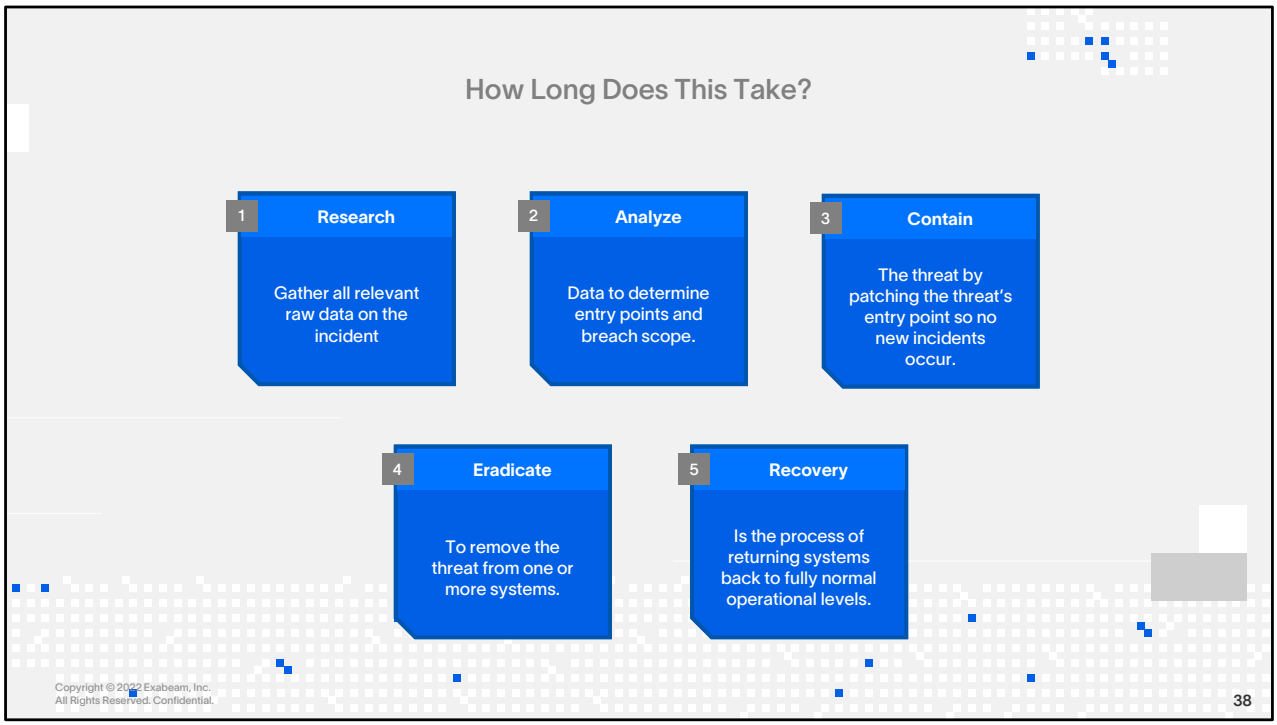
3. **Execute a turnkey playbook in Incident Responder**

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

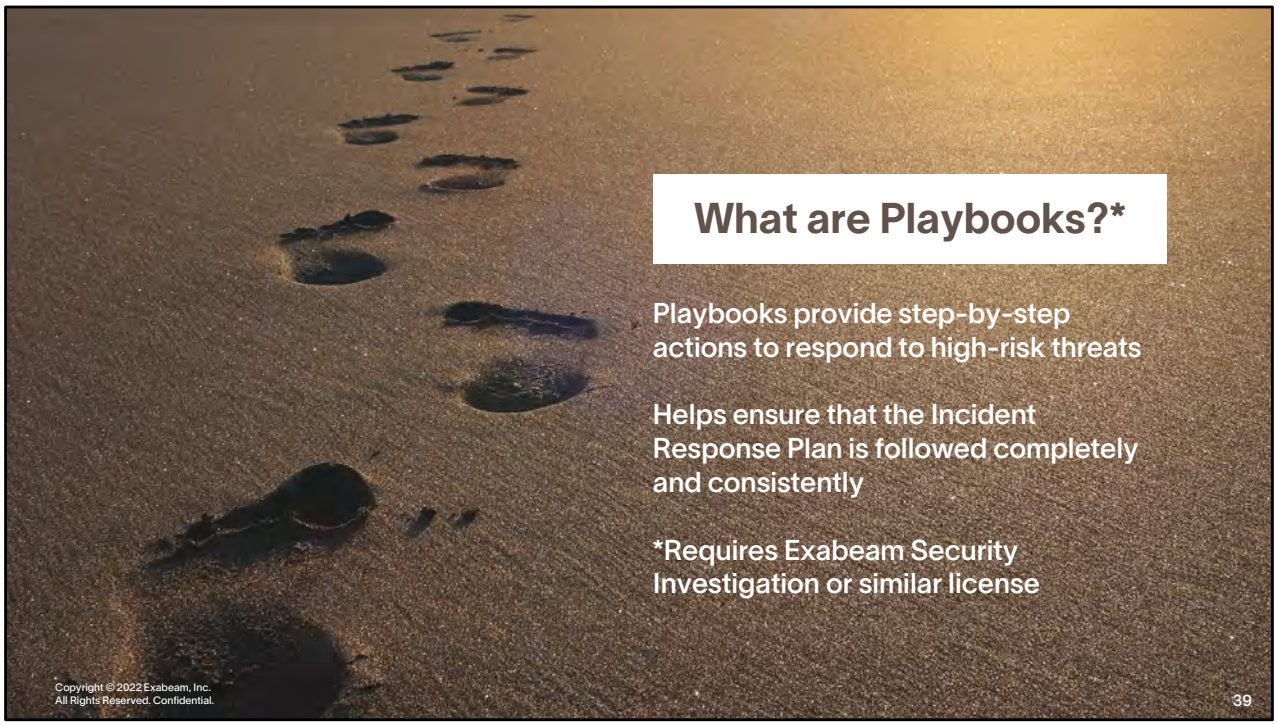
Discussion

What are common responses when a threat investigation reveals compromise?



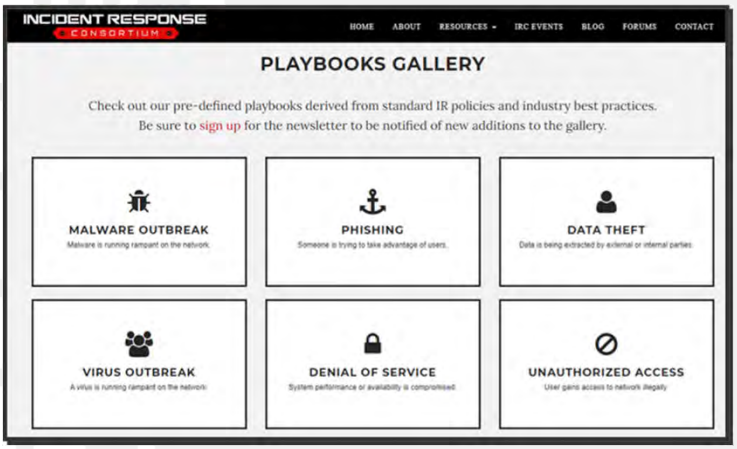
Student Notes

- **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
Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.
39

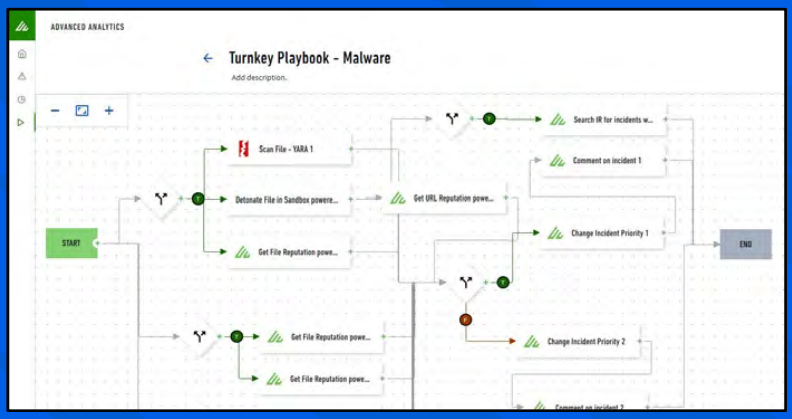
Demo

A Peek at Playbooks



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**



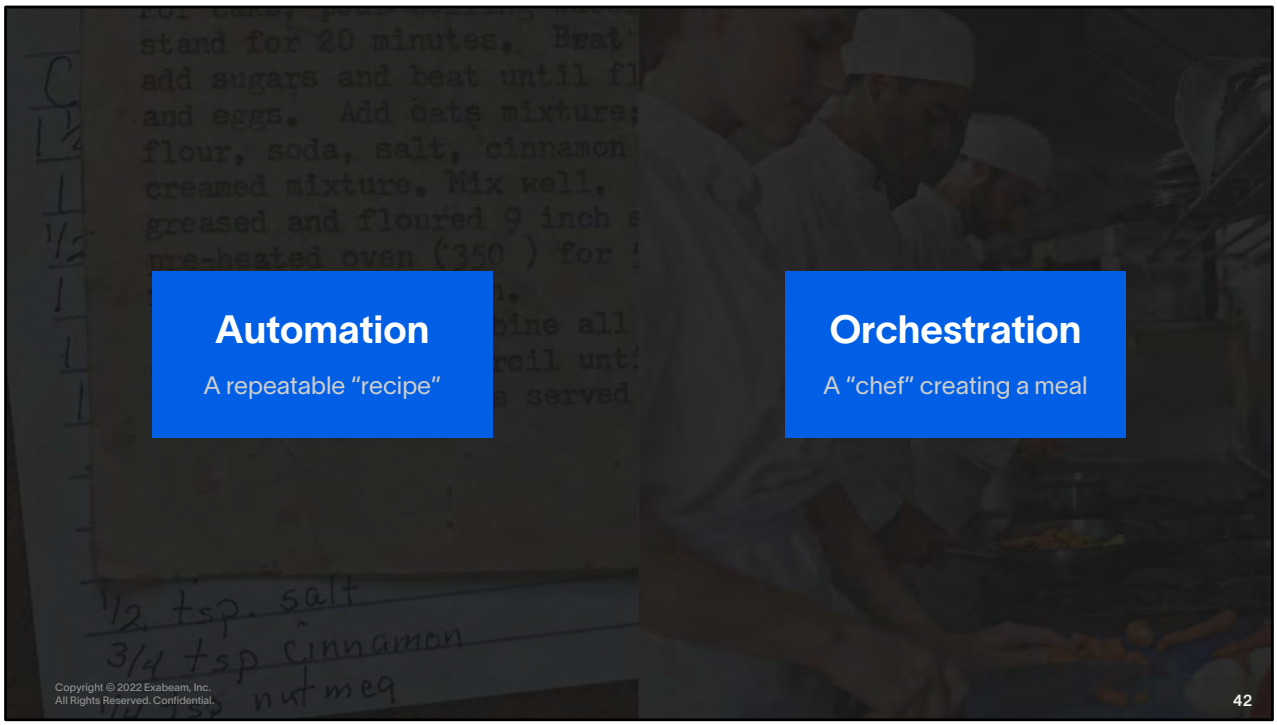
Student Notes

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



Student Notes

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

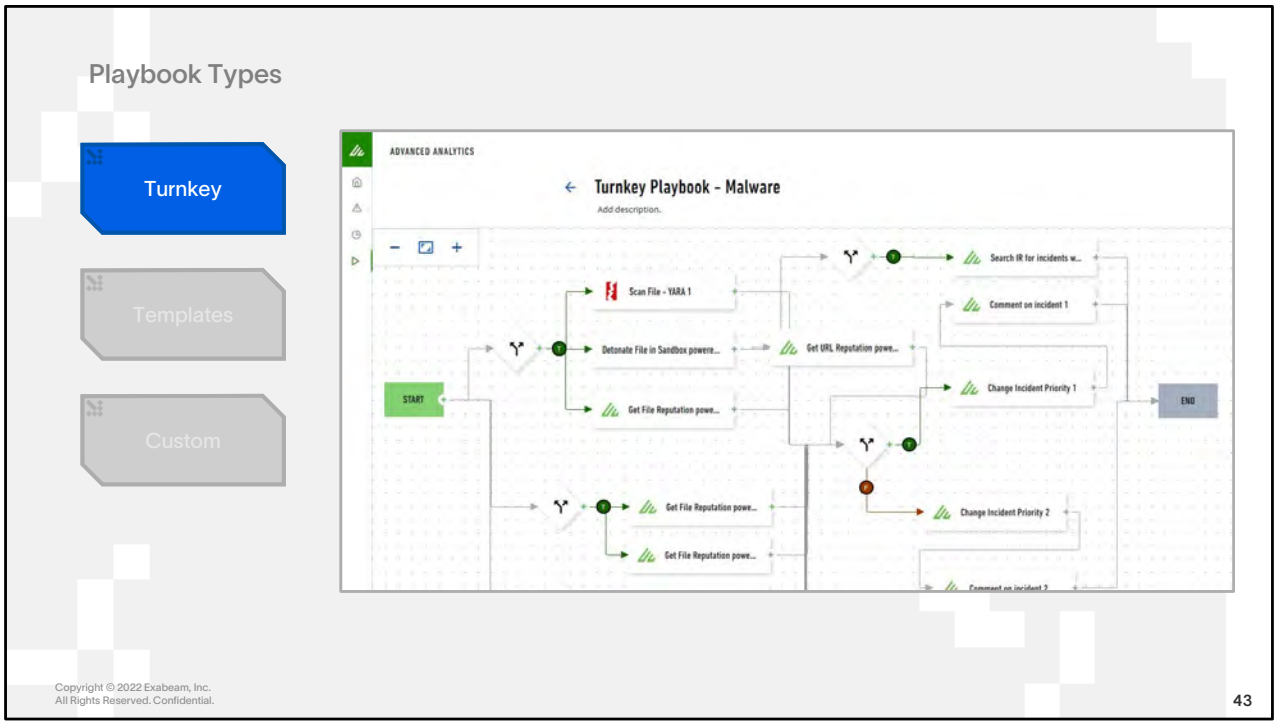
- Executes a predefined rigid template
- Decision paths are pre-chosen, and a computer executes tasks

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) – listed as free for commercial use image on Bing image search for recipe card

Free cozinheiro Stock Photo - FreeImages.com



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

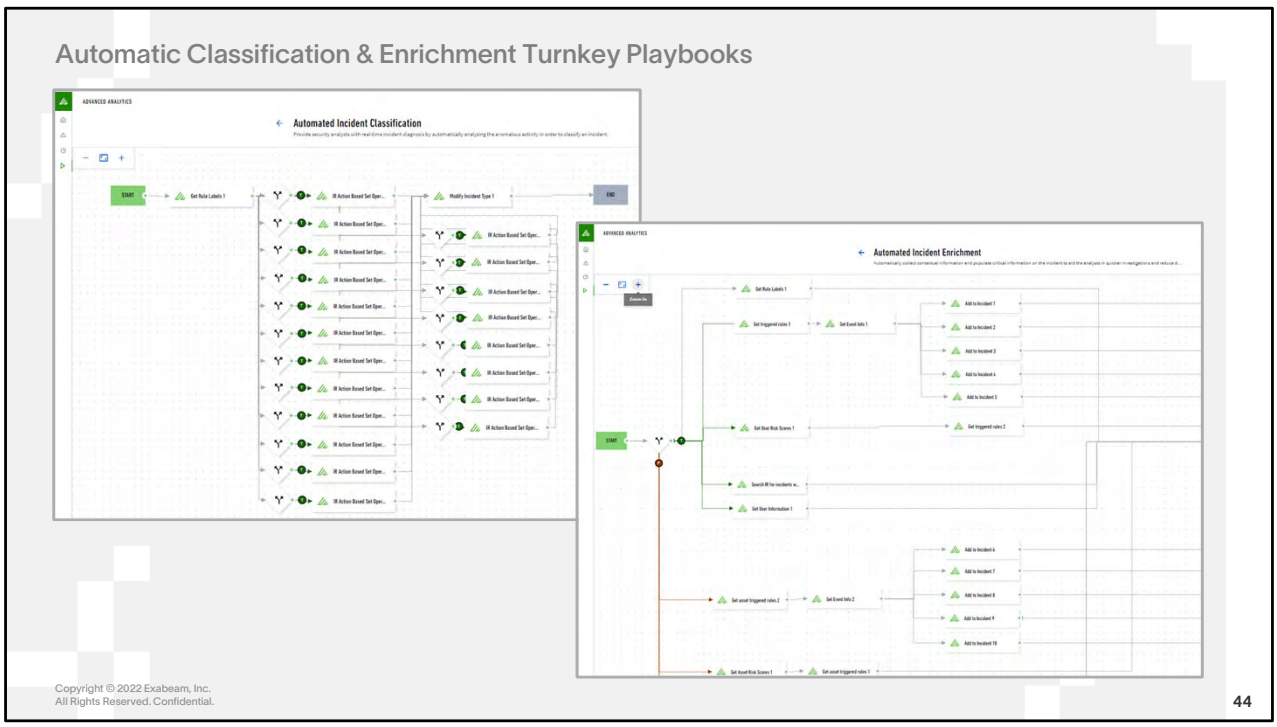
If the playbook finds any IP addresses with a malicious reputation, it searches for other incidents that has the same IP address entity or artifact. View the output in the incident's workbench.

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



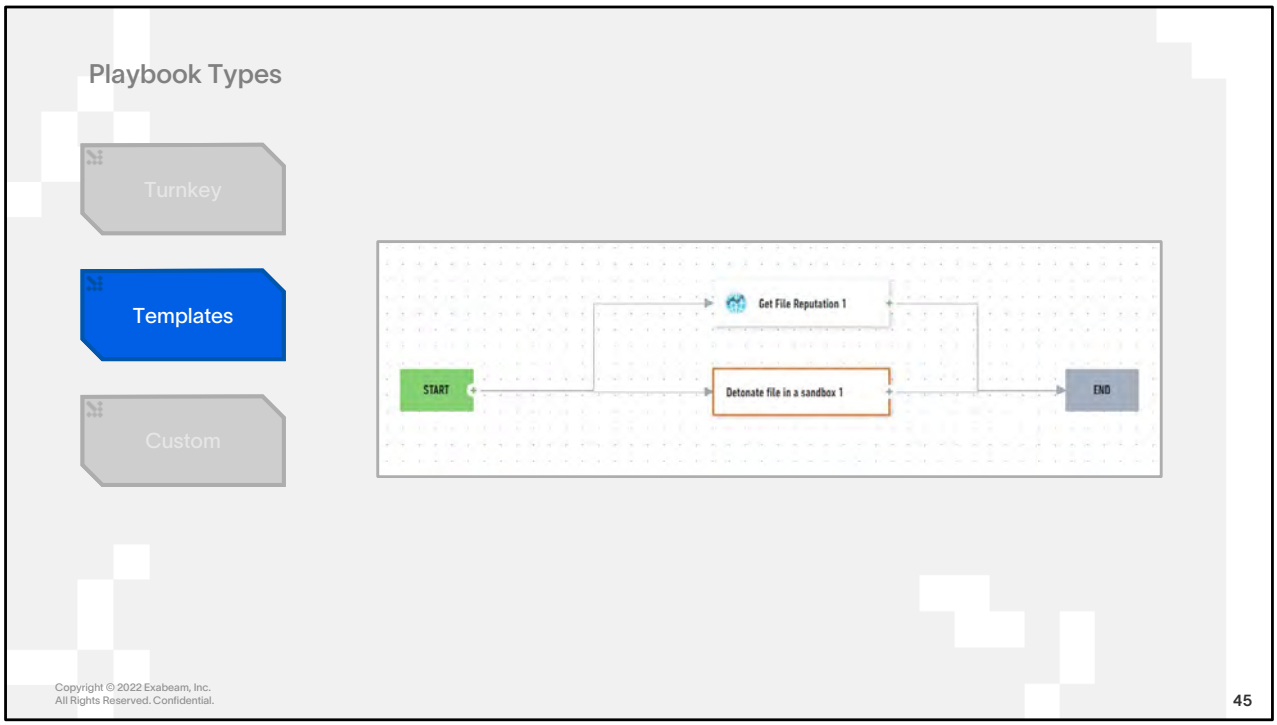
Student Notes

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

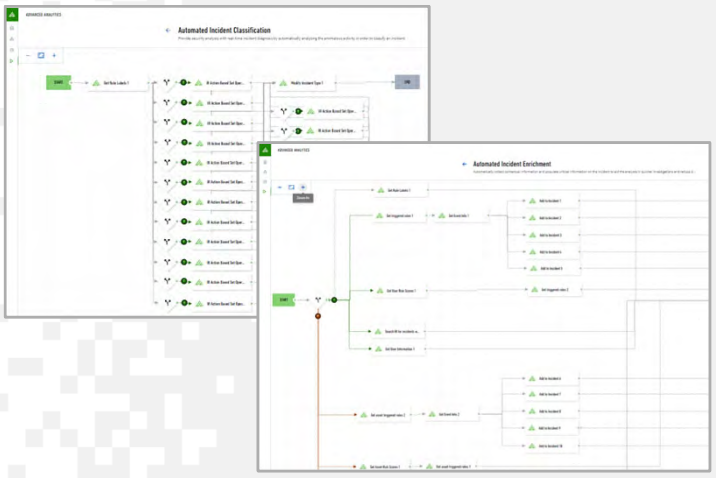
Advanced Analytics User Guide

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

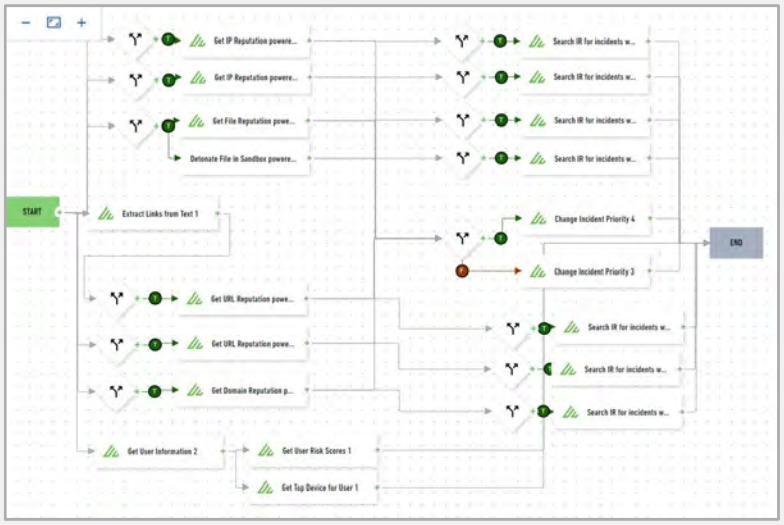
Source
Advanced Analytics User Guide

Demo

A Look at Turnkey Playbooks in Incident Responder



How Long Would This Take If Executed Manually?



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

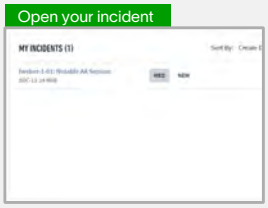
At the end of this lesson, you will be able to:

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

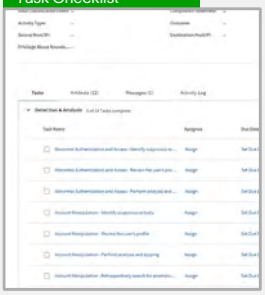
Incident-driven Analyst Workflows

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

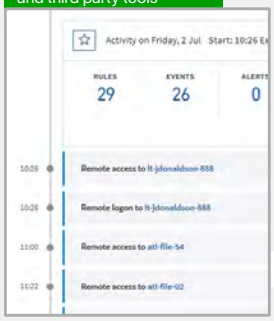
Open your incident



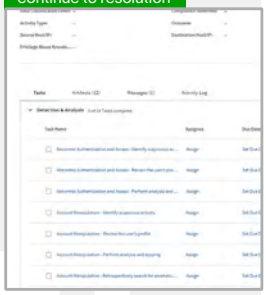
Read and start using the Task Checklist

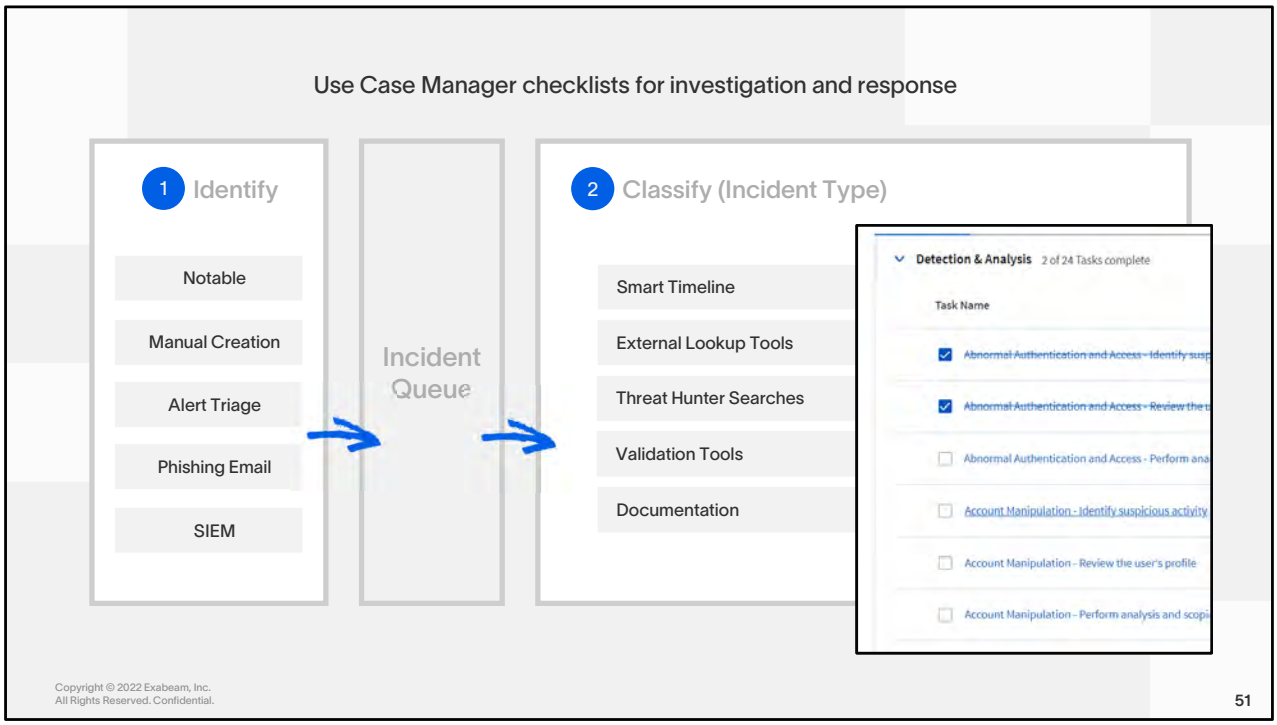


Investigate using Exabeam and third party tools



Complete tasks and continue to resolution





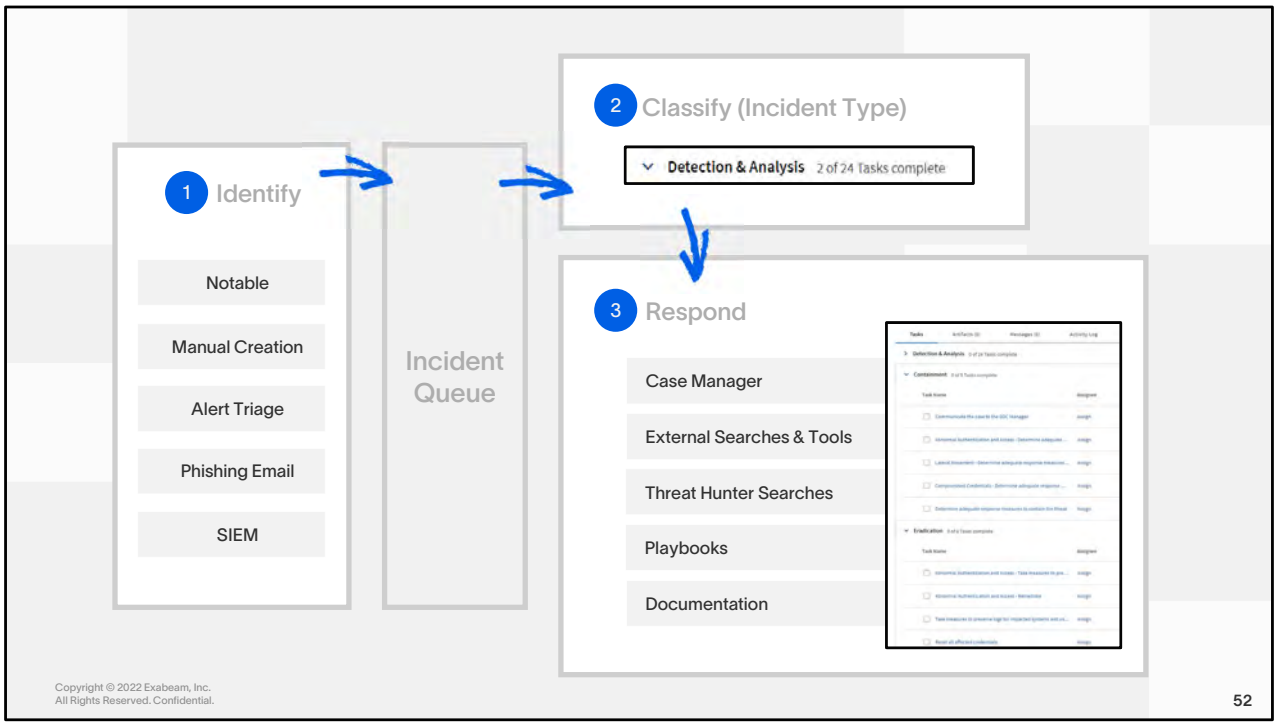
Student Notes
Case Management in CMIR

Step One:

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

Step Two:

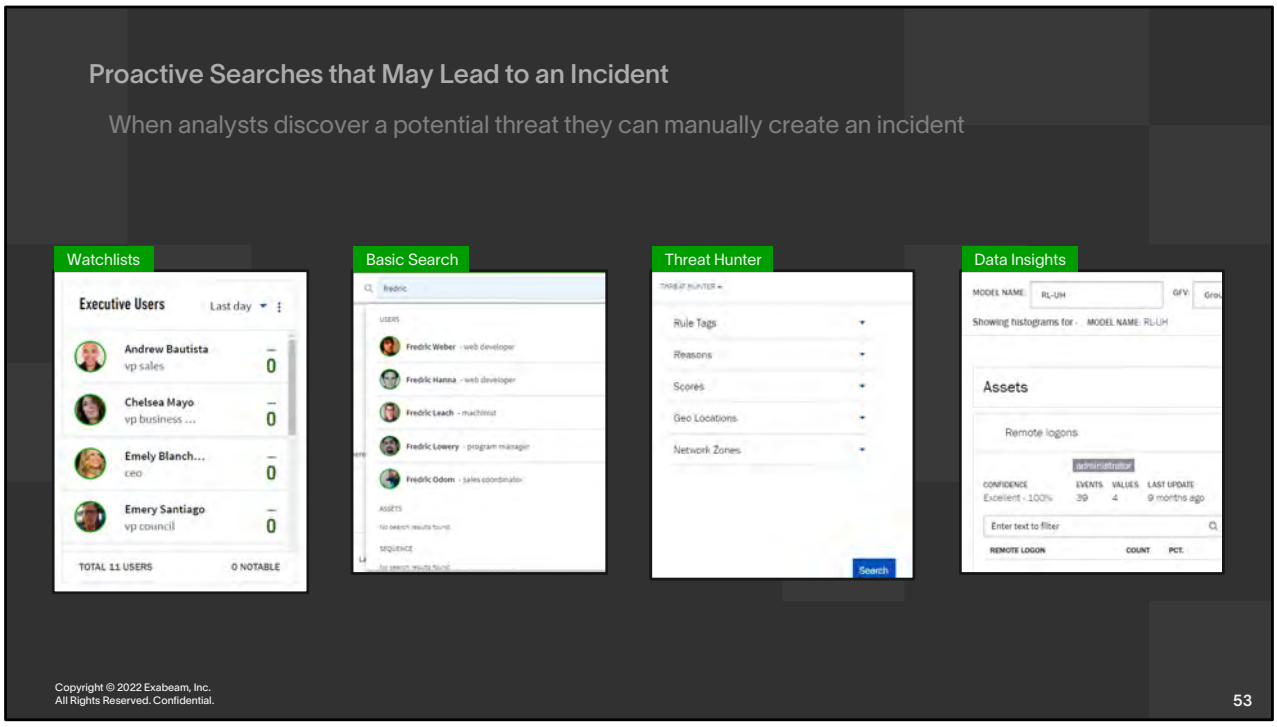
Once the incident type has been identified, additional details each response phase should be listed for consistent efficient workflow.



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.



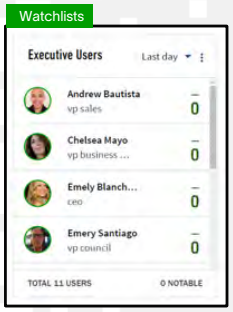
Student Notes

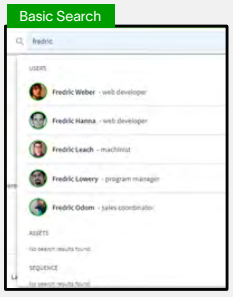
Analysts and threat hunters may discover potential threats using the following:

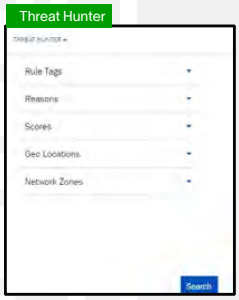
- Watchlists allow analysts to keep tabs on the “crown jewels”
- Basic Search feature is very handy for SOC analyst who already have a suspicious username or alert from a security system
- Threat hunter allows analysts to find sessions that match certain criteria related to actions and risk
- Data insights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

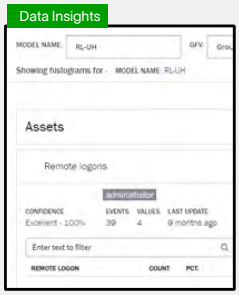
Any of these starting points could lead analysts to investigate a user, review their timeline, and determine that there is a possible threat and a need to manually create an incident

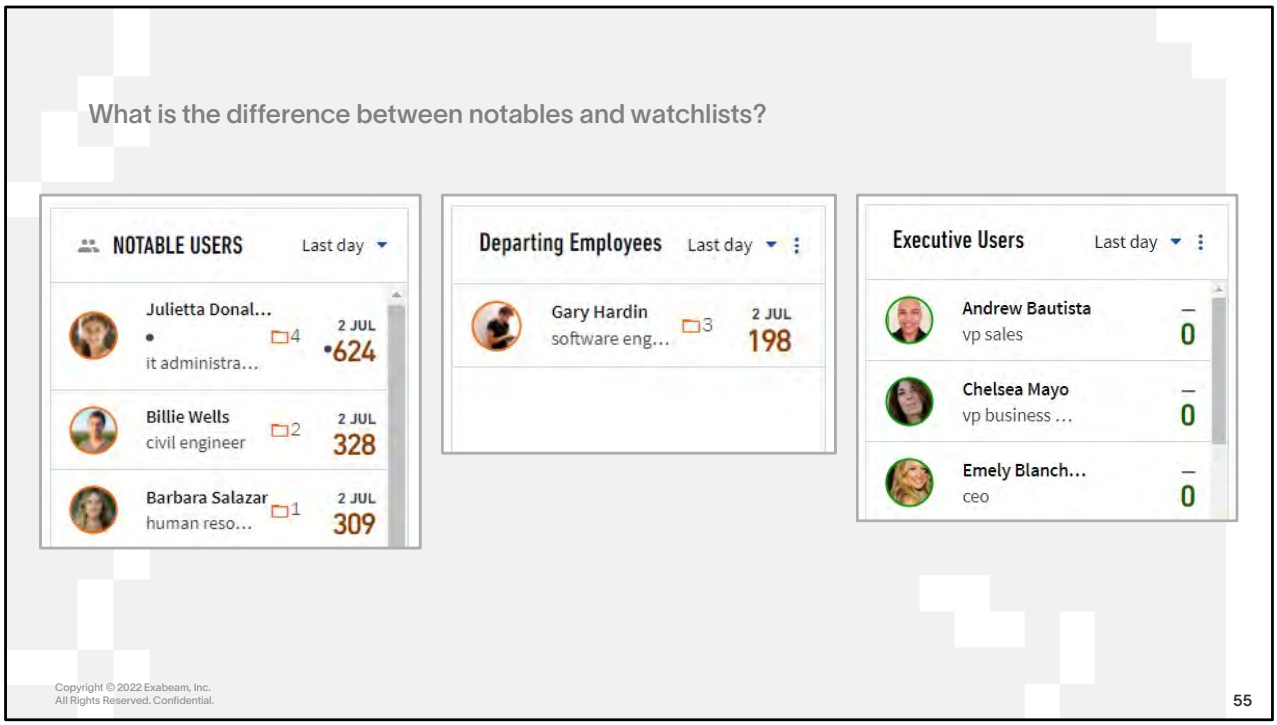
Demo











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.

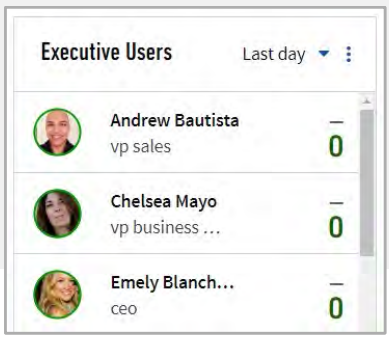
They can also be used for policy and compliance situations and other unique use cases.

More Information

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

Watch the Watchlist

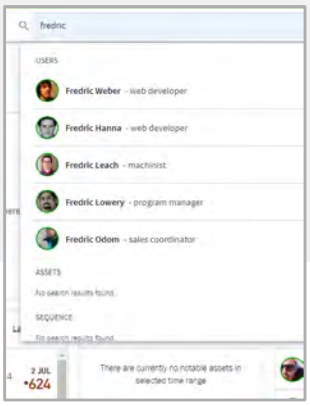
Attend to vulnerable users and assets



Observe Watchlist › Review User Profile › Review Timeline › Create Incident

Search for someone

Search for “interesting” users and assets



Run Search › Review User Profile › Review Timeline › Create Incident

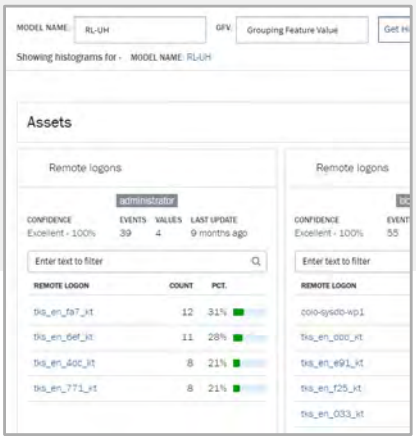
Threat Hunter elevates the non-notable

Search for specific symptoms for threats you are concerned about

Run Threat Hunter Search › Review User Profile › Review Timeline › Create Incident

Data Insights Exposes Models

Search for Models to look for trends among the results

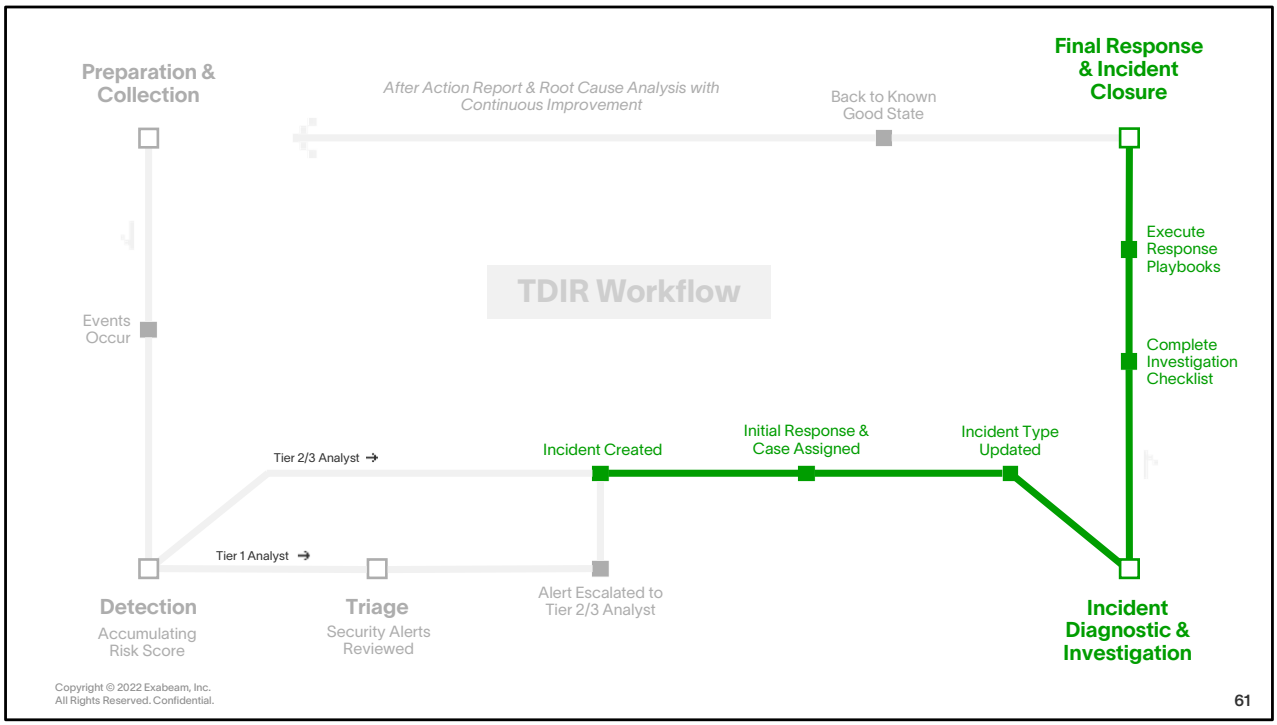


Data Insights Search > Review User Profile > Review Timeline > Create Incident

Lesson

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

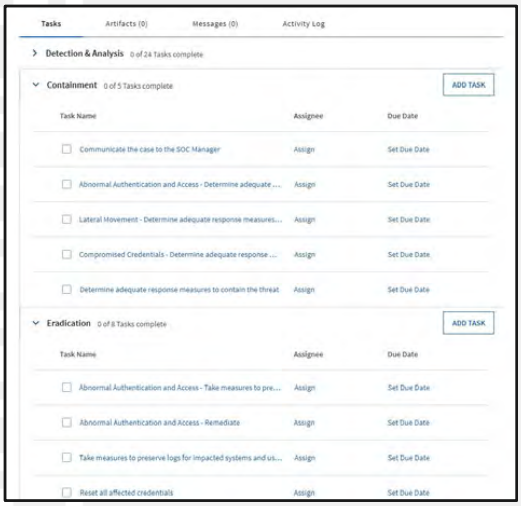
1. Define a security incident and recall the function of the Case Manager checklist in the Exabeam analyst workflow
2. Do the following:
    1. Recall how incidents are created
    2. Edit an incident in Case Manager
3. Execute a turnkey playbook in Incident Responder
4. Recall where to start an investigation 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**

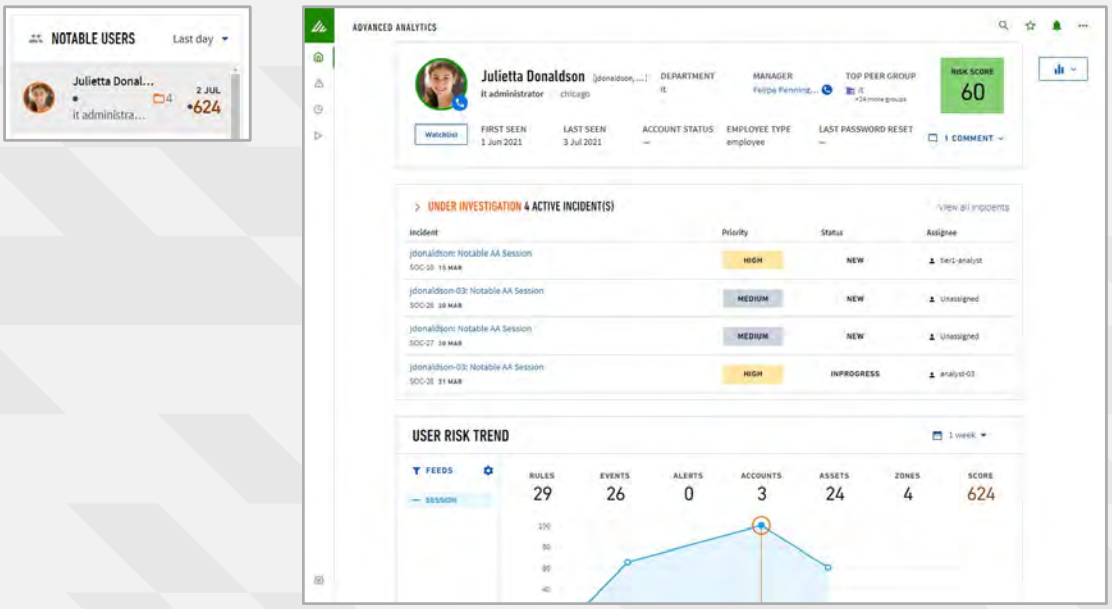


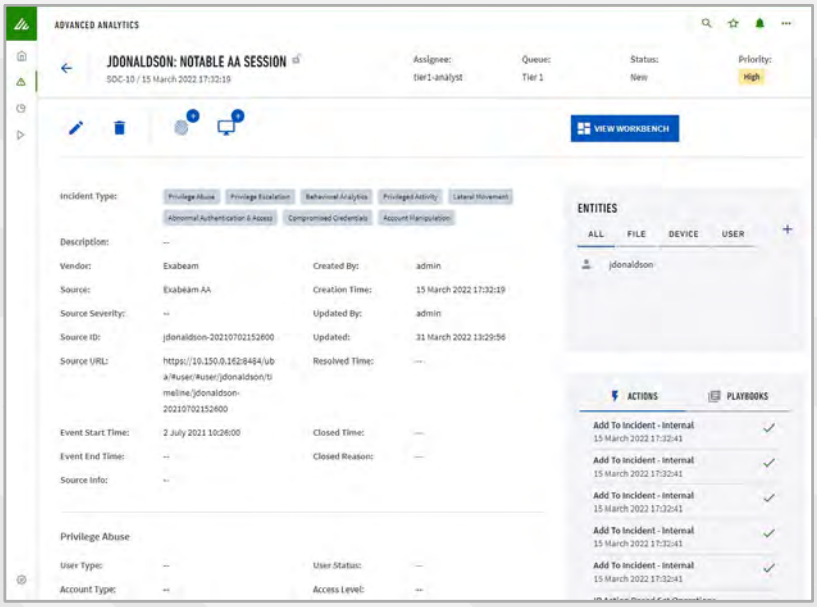
61

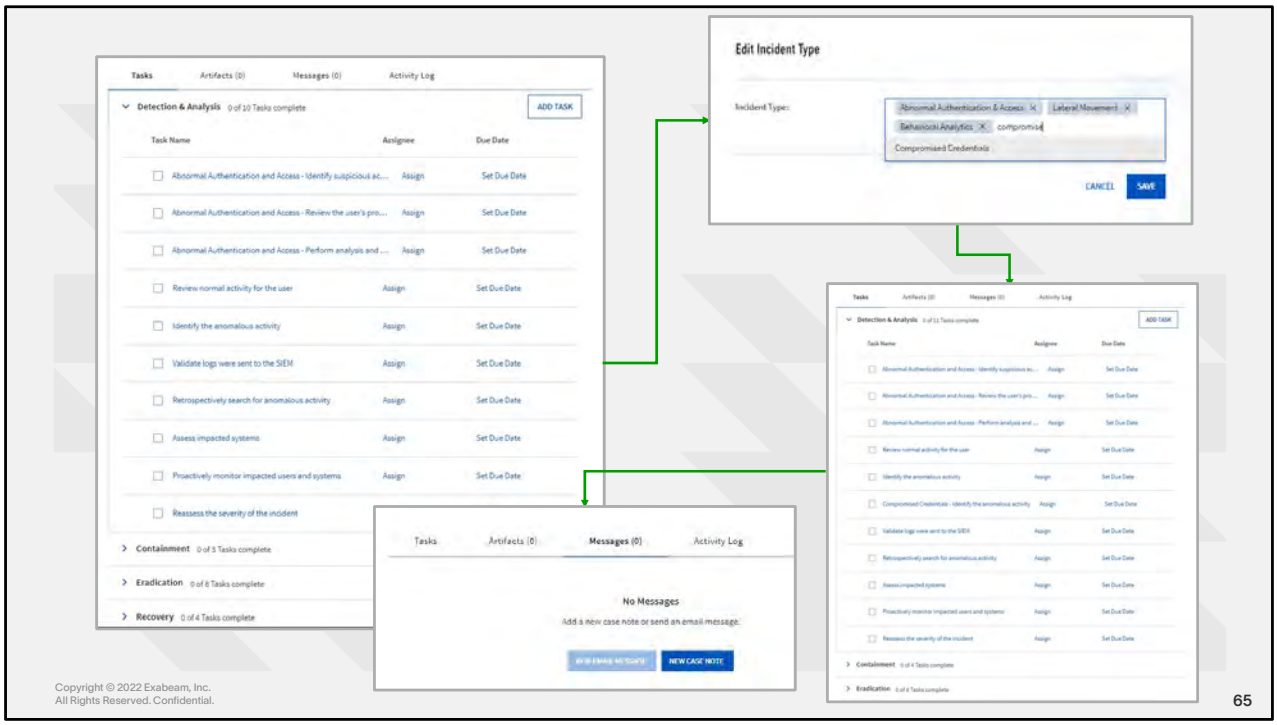
Demo

Putting it all together: end-to-end workflow

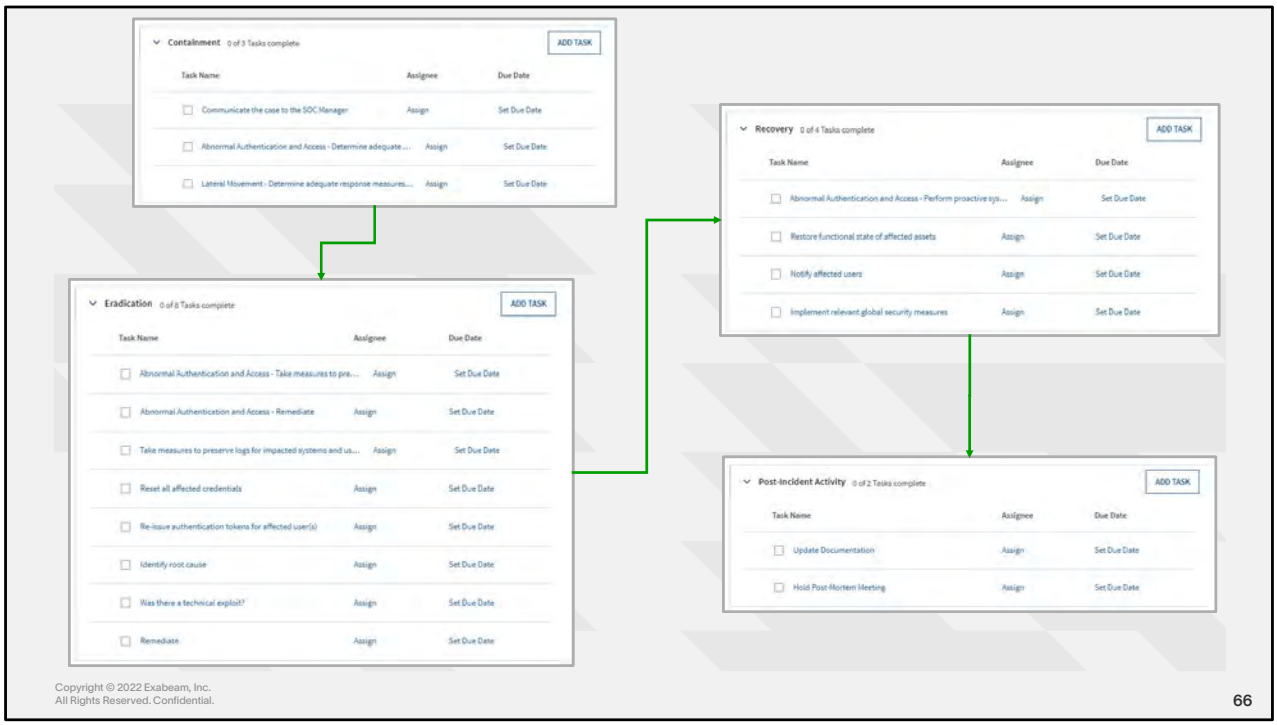


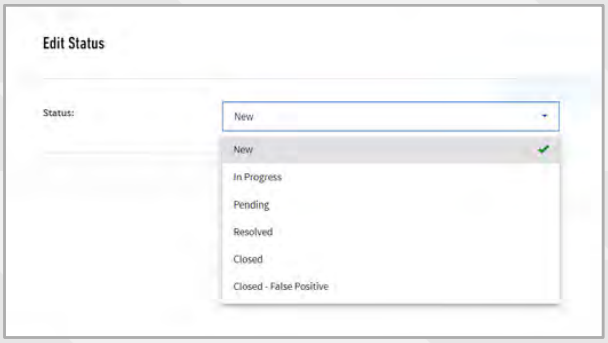






65





Activity

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

Objectives:

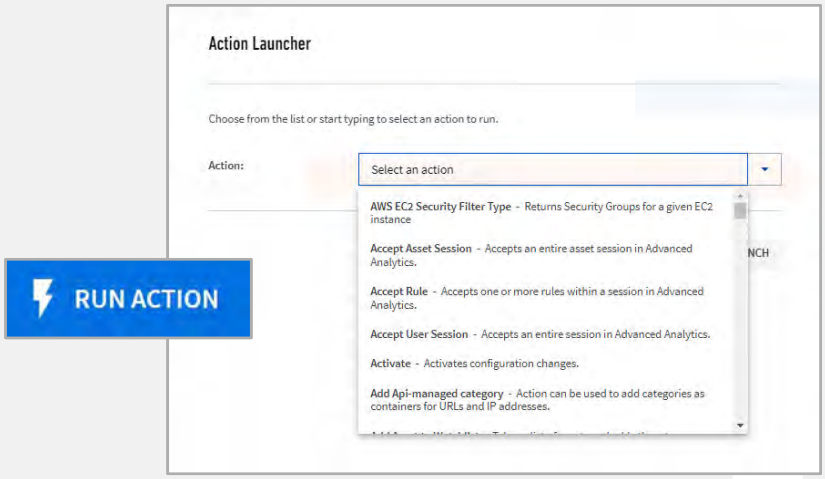
1. Open an incident from incident queue
2. Review incident details and update incident type
3. Use the built-in checklist to investigate, contain, respond, and close an incident
4. Start an investigation proactively using Watchlists or Search
5. Investigate proactively by searching for rules in Data 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

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?



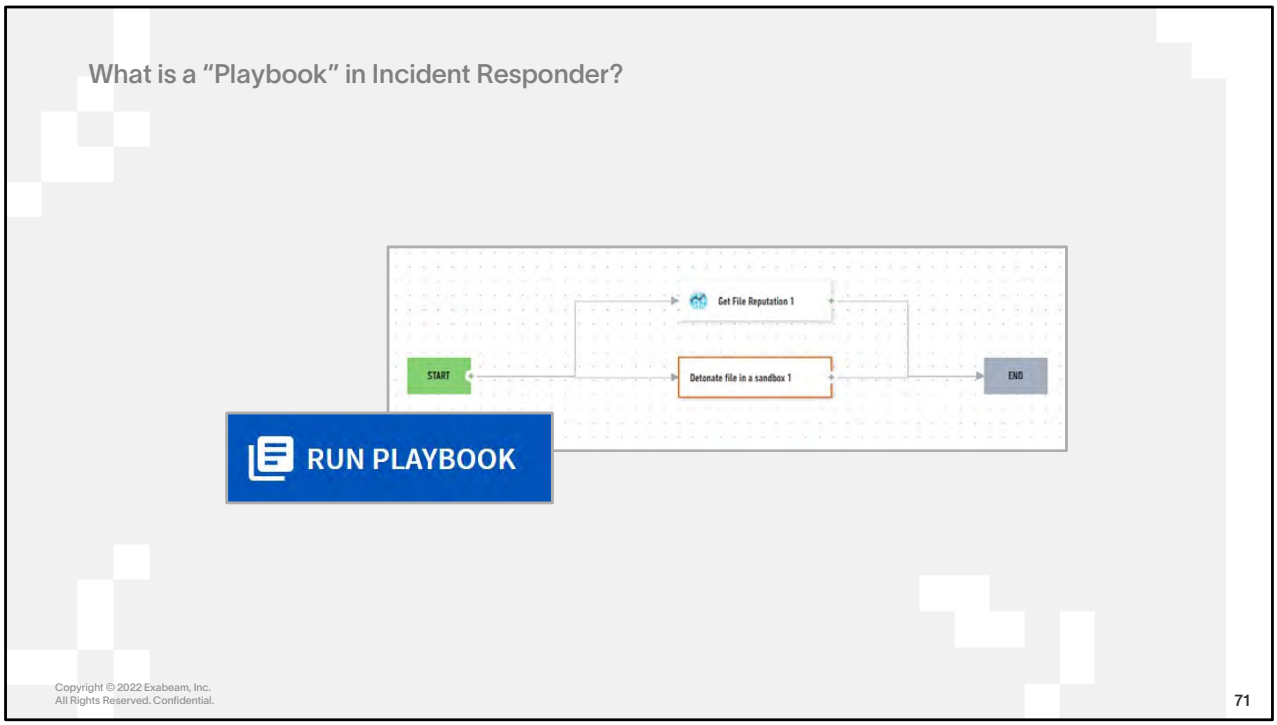
70

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.



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

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

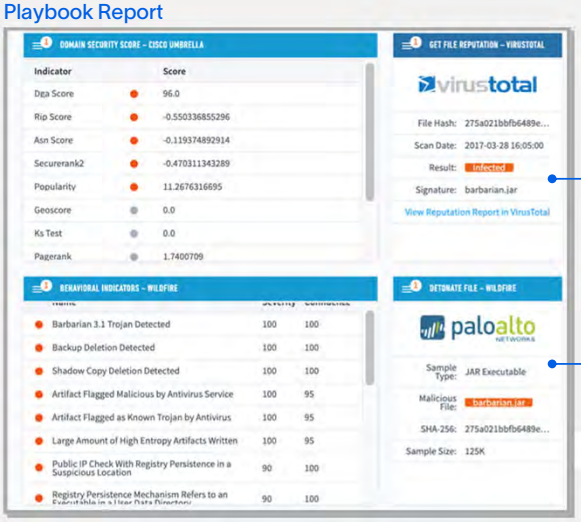
- Active Directory
- Exabeam Data Lake
- Palo Alto Wildfire
- SERVICENOW

Action Examples

- Get domain reputation
- Detonate File
- Kill Process
- Block URL

Example of Service Integrations in Playbook

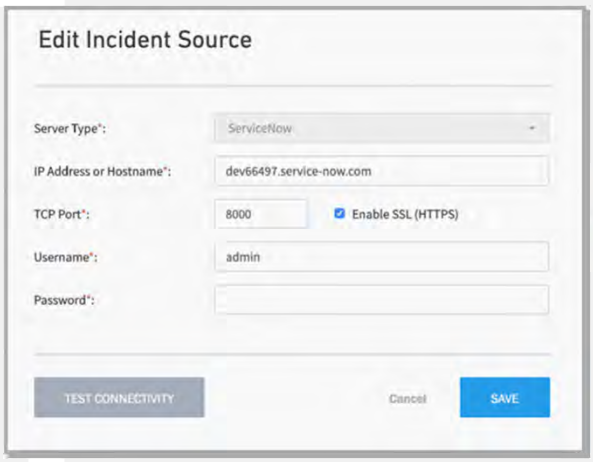
Playbook Report



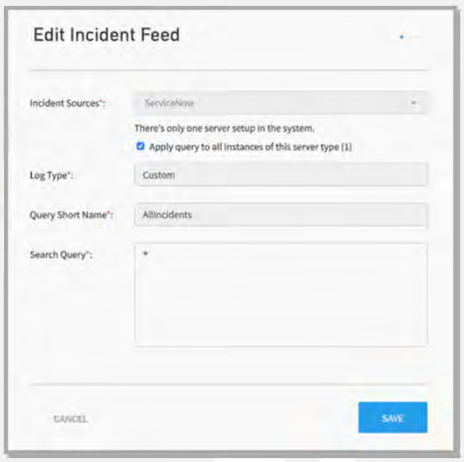
Service Integrations

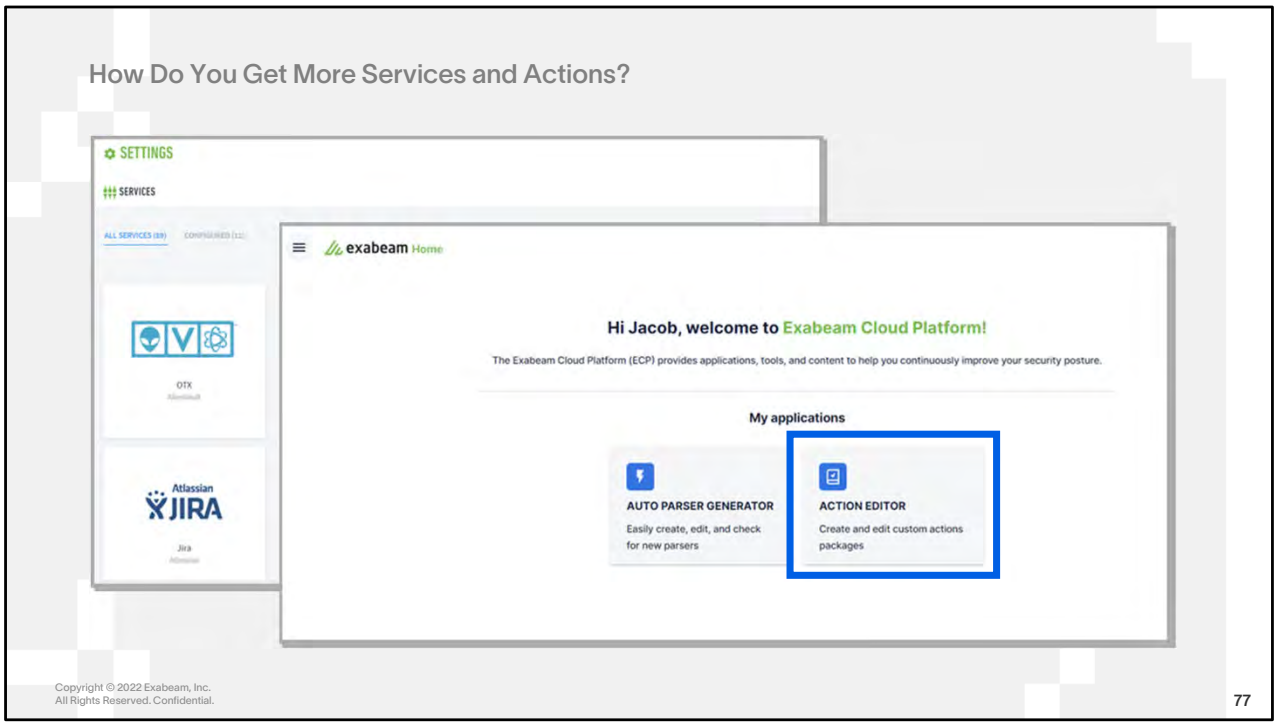
Example of Configuring ServiceNow Ingest

Incident Source



Incident Feed

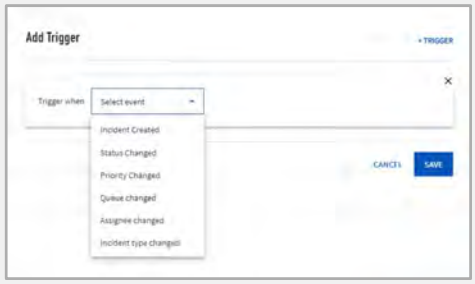


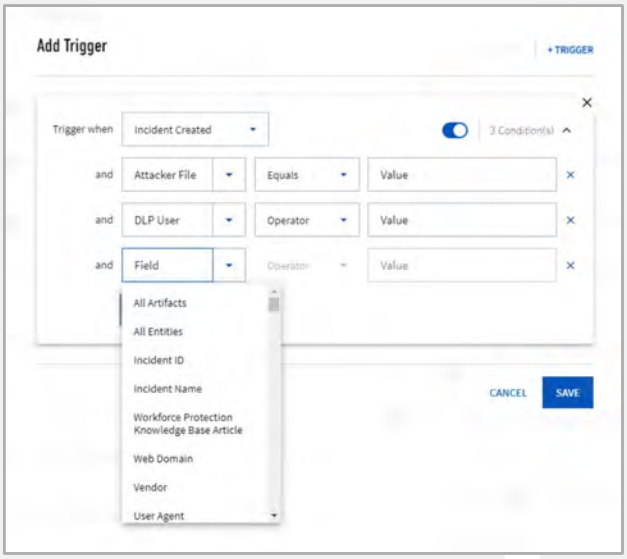


Student Notes

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.

Playbook Triggers





78

Student Notes

Playbooks can be launched manually from case manager

OR

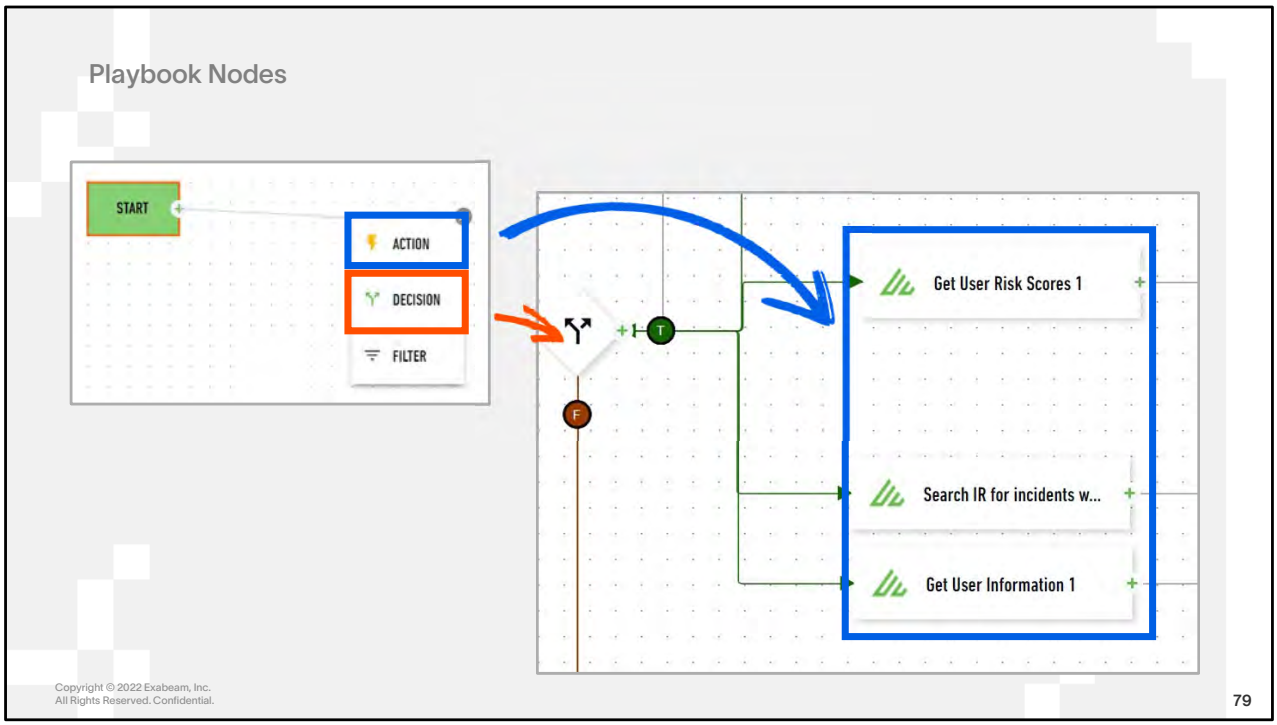
You can automatically run playbooks using triggers. Playbooks automatically run when you prescribe it to run under a certain circumstance, and that circumstance happens. This circumstance is called a trigger. There are three circumstances that trigger a playbook:

- 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

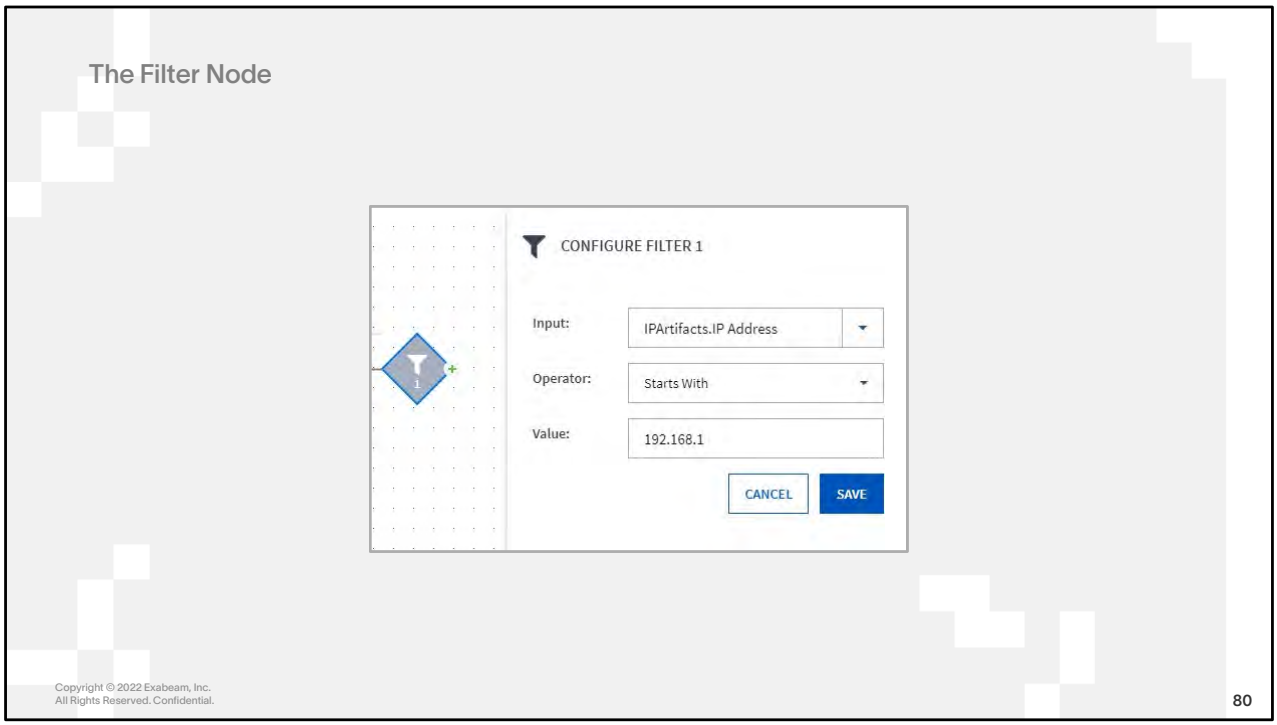


Student Notes

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



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.

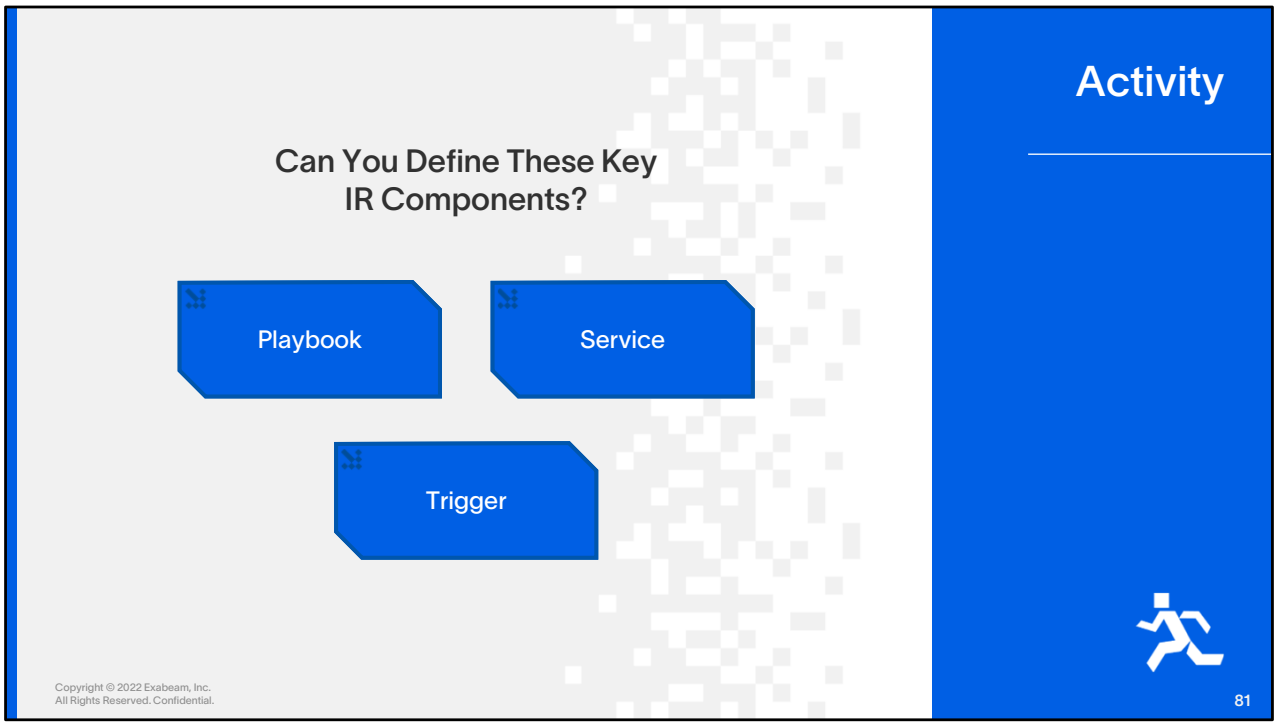
•Allow listed URLs, so the next node evaluates block listed URLs only.

•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

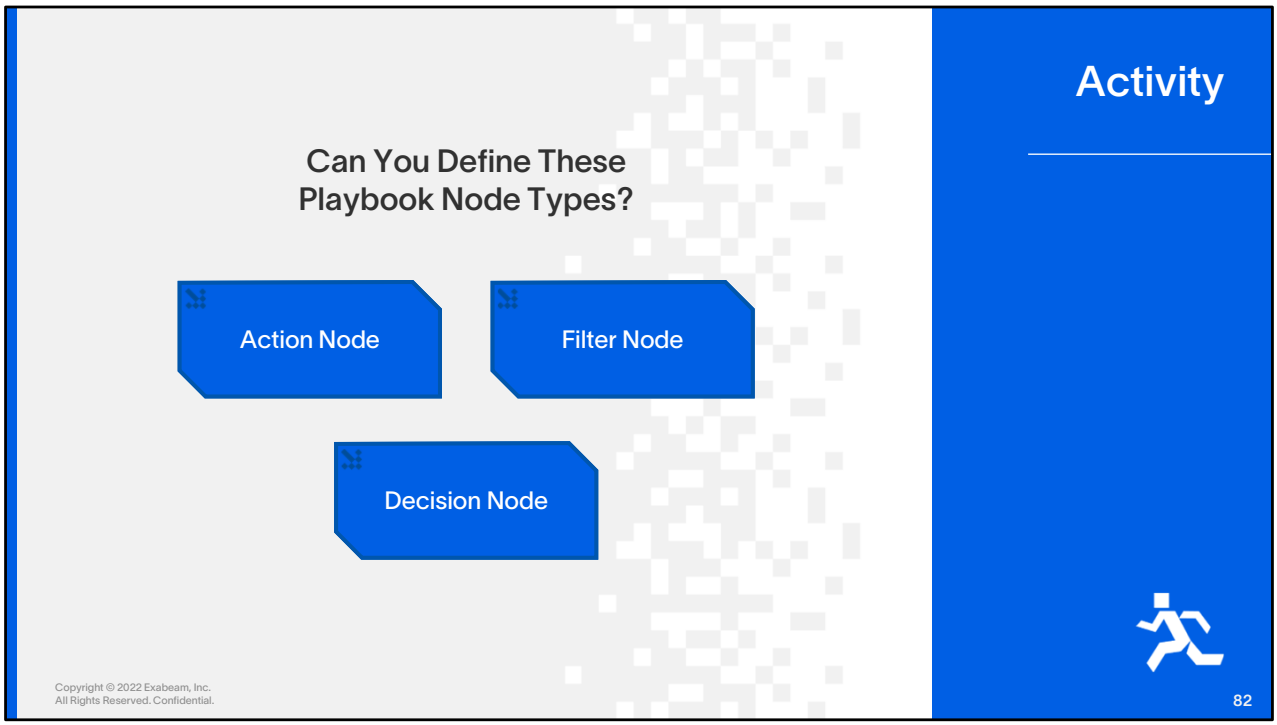
Advanced Analytics User Guide



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



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

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

Discussion

What type of Playbook implementation would aid your processes most?

Activity

Practice using Playbooks and Incident Responder

v4.00

External Threats

EDU-2170 : Module 7

Student Notes
Of course, Ransomware:

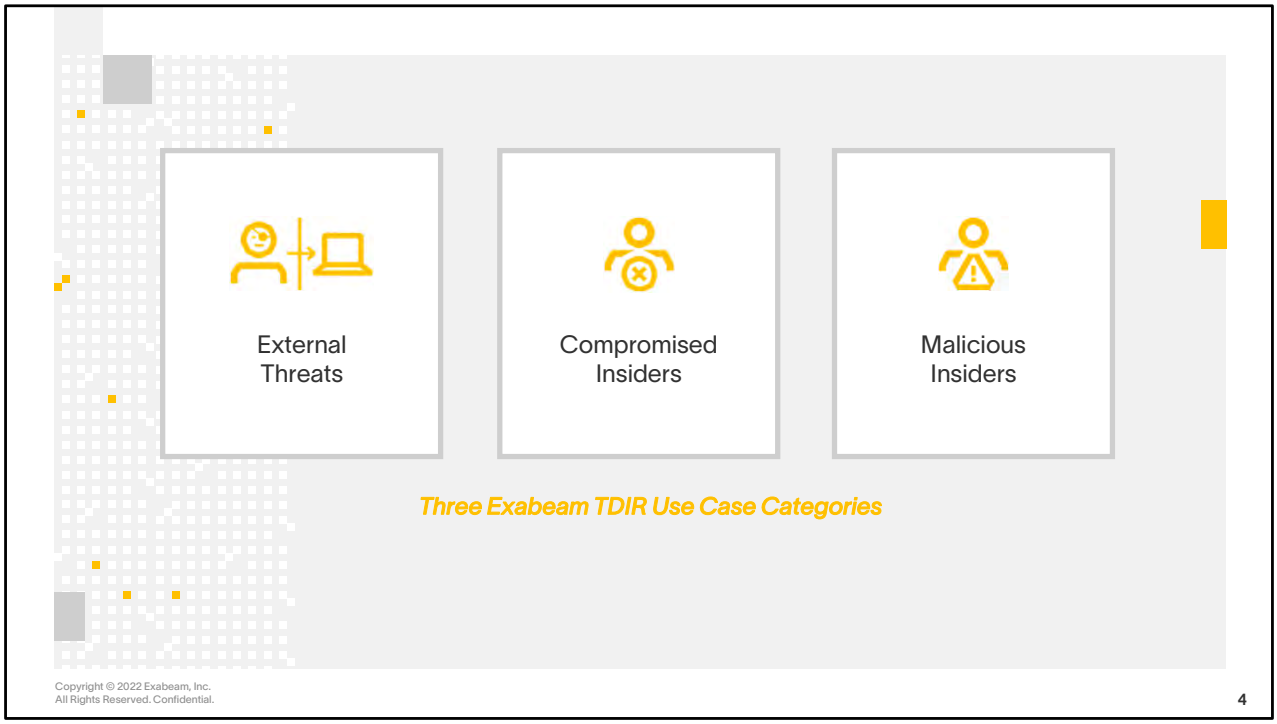
- Kaseya, impacting up to 1,500 companies
- Colonial Pipeline
- JBS Foods

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



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.

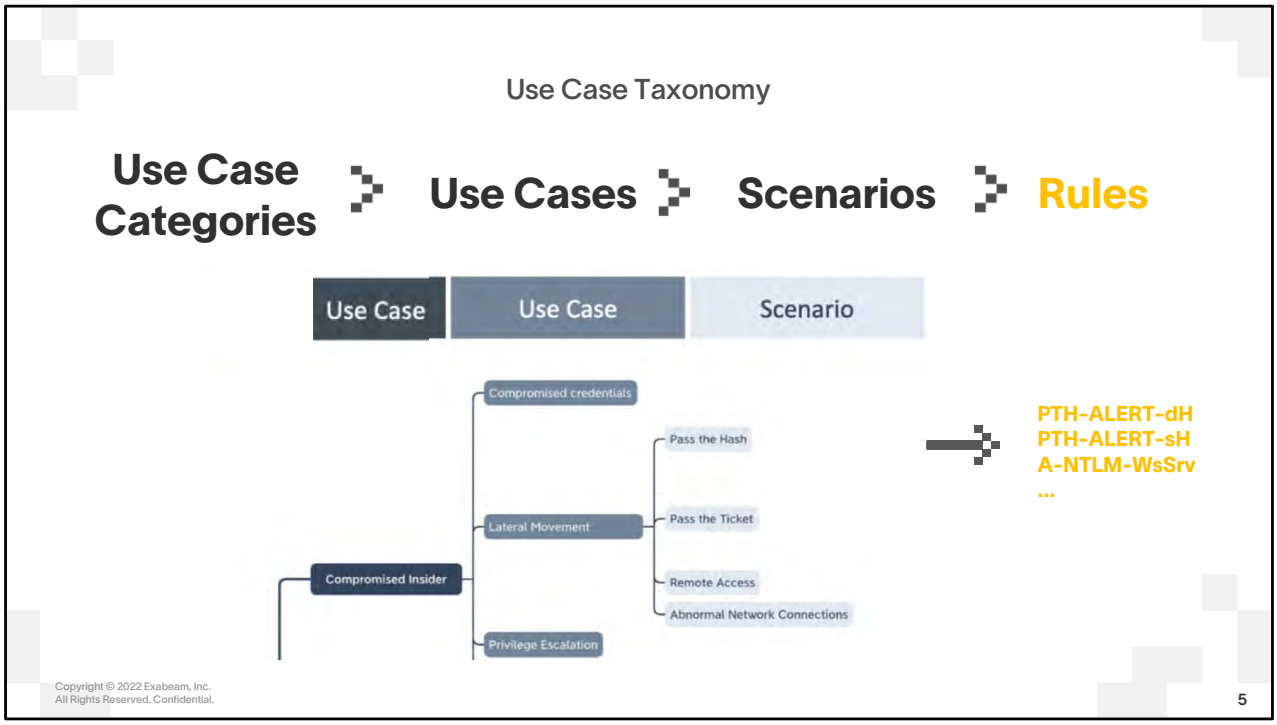
External Threats - Protect Against Prevalent Attack Vectors Attack vectors like phishing or malware provide adversaries ample opportunities to breach a company's defenses. With the sheer volume of attacks on a daily basis, SOCs must be prepared to properly detect, investigate, and respond at a moment's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

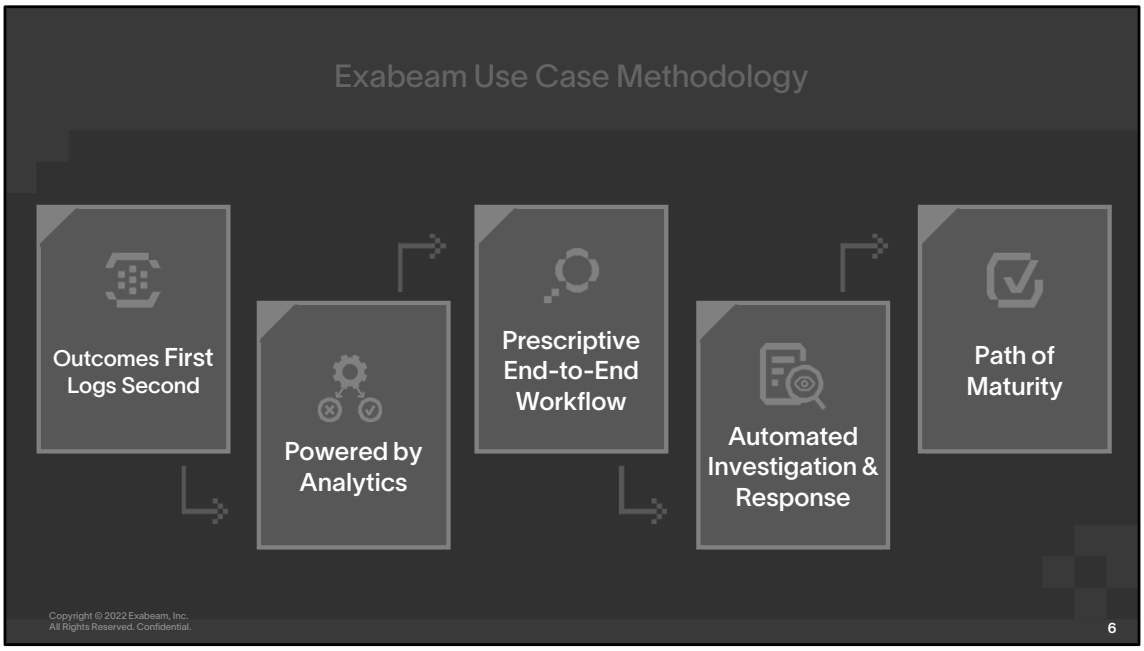
The TDIR Use Case framework organizes threats in a hierarchy, from a broad category down to specific detection insights.

•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

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 Malvertizing, until they break into our systems. Other methods external attackers may use include:

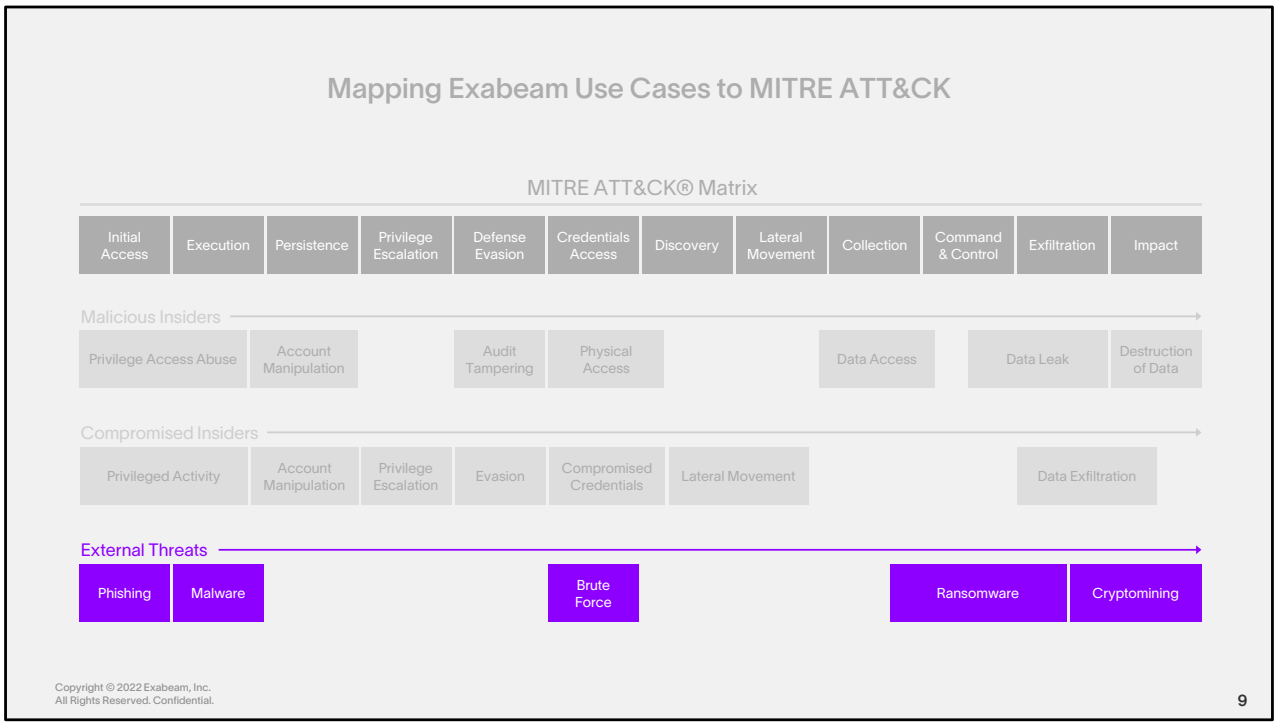
•Hacking through security loopholes
•Ransomware and malware
•Physical theft of devices that can offer unauthorized user access
•3rd-party apps
•Malicious USB drops

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/

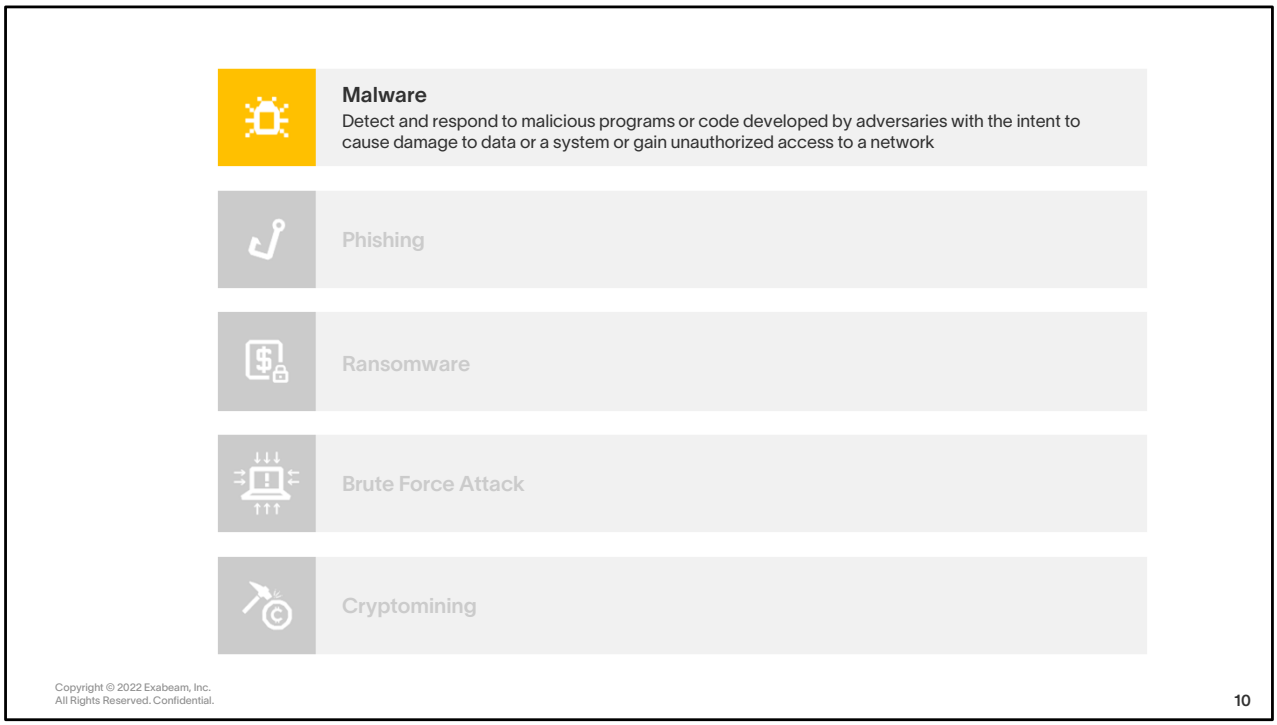
Photo by Gerald Schömbs on Unsplash



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



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

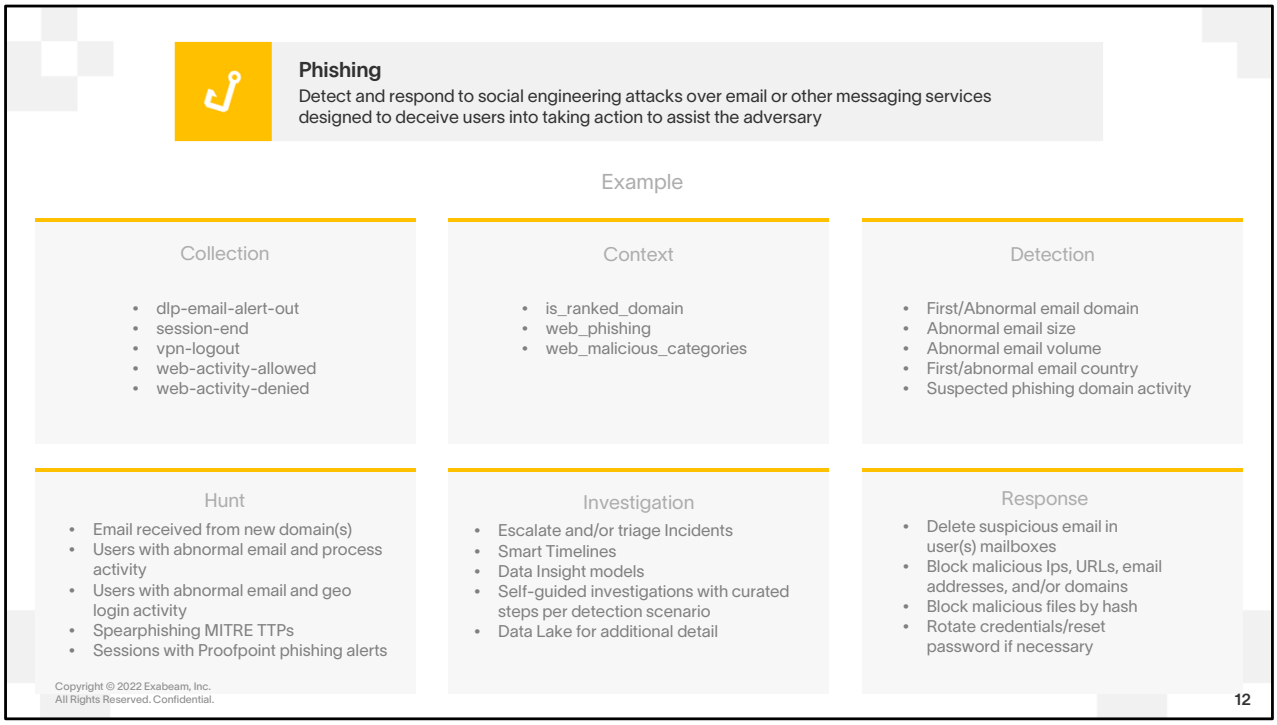
Phishing

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



Student Notes
Additional Phishing Use Case notes:

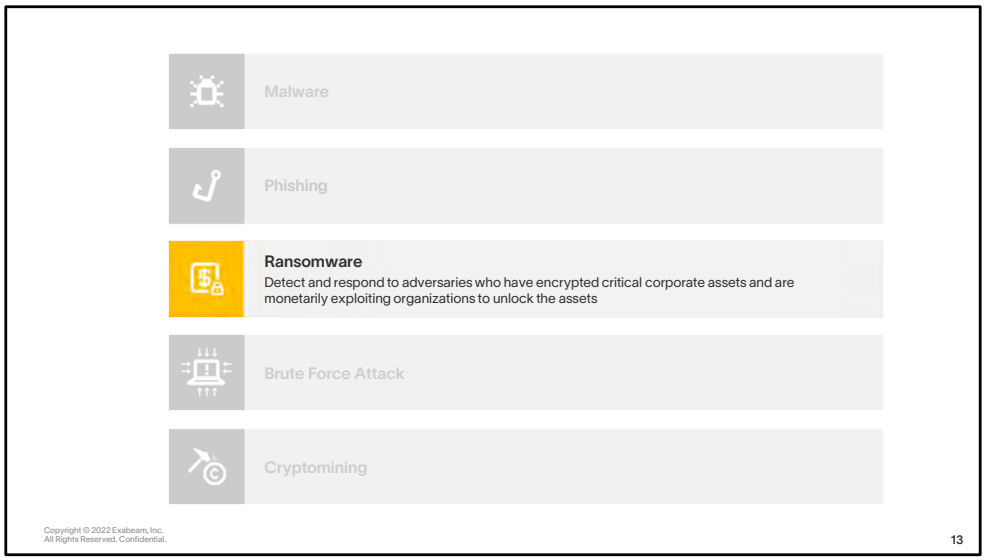
Data Sources
- Data loss prevention
- Email security and management
- Web security and monitoring
- Endpoint security (EPP/EDR)
- VPN/Zero Trust Network Access

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

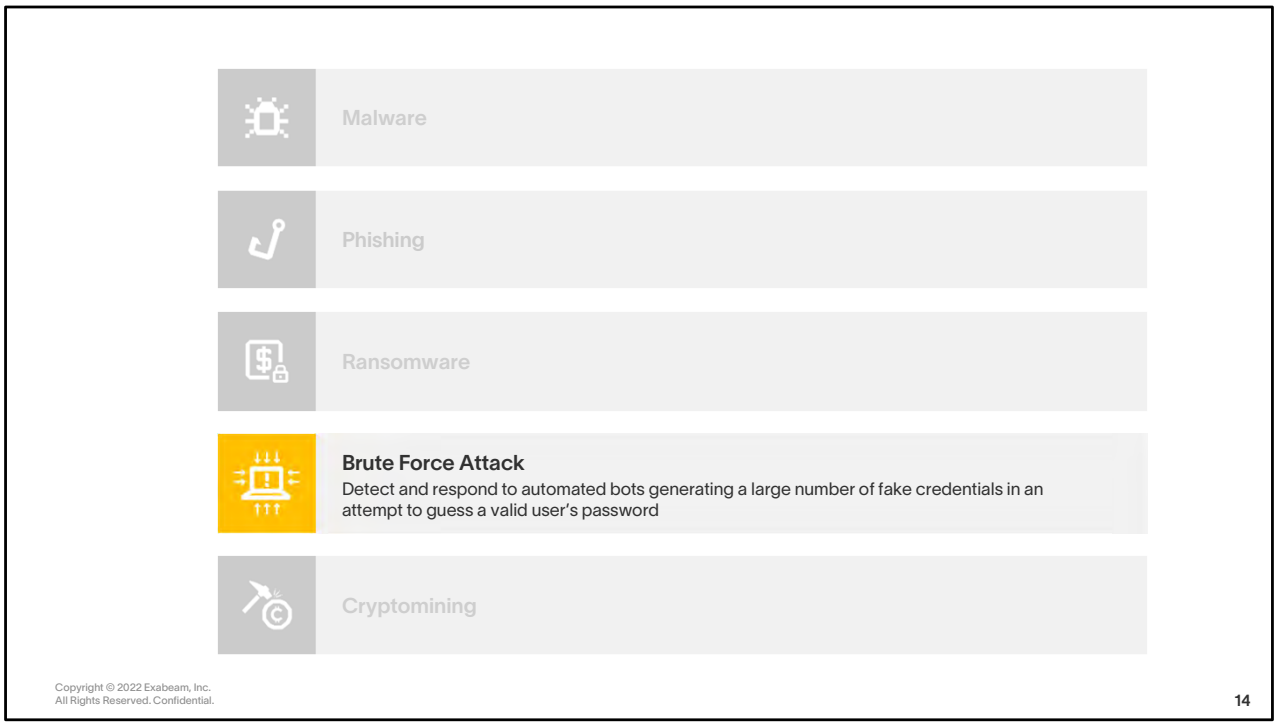
To support the ransomware use case, the Exabeam SOC Platform enriches existing logs with threat intelligence stored in the following context tables:

- 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/medialibrary/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://www.cisa.gov/stopransomware



Student Notes

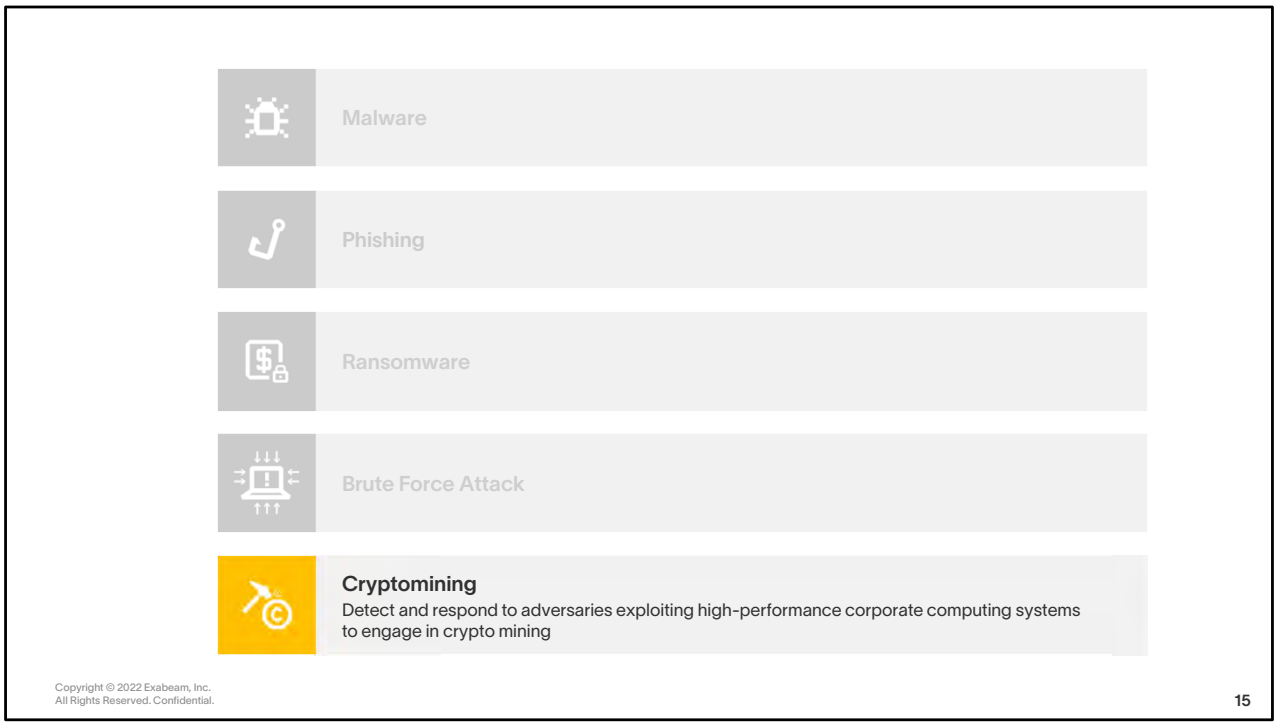
Brute Force attacks attempt to authenticate by iterating through a list of potential passwords, such as all words in the dictionary or combinations of words, symbols, and numbers in hopes that it will match. Credential stuffing attacks attempt to reuse breached passwords on other sites. For example, 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



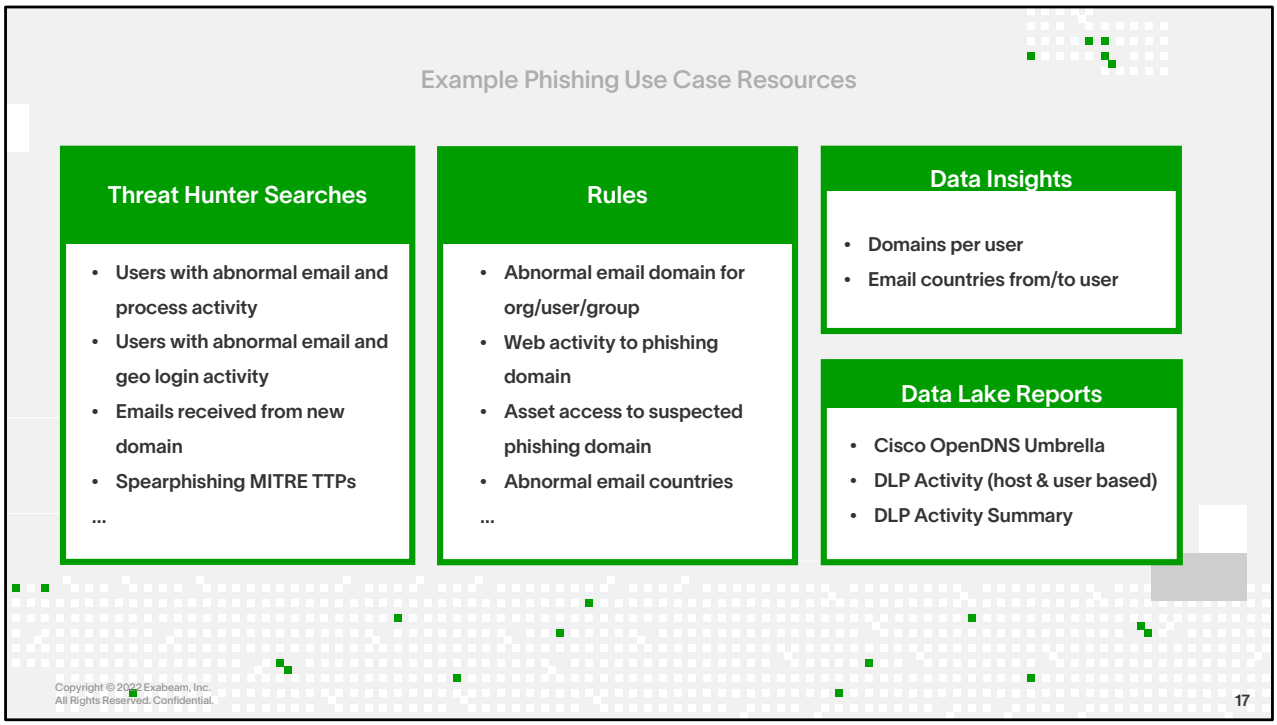
Student Notes

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:

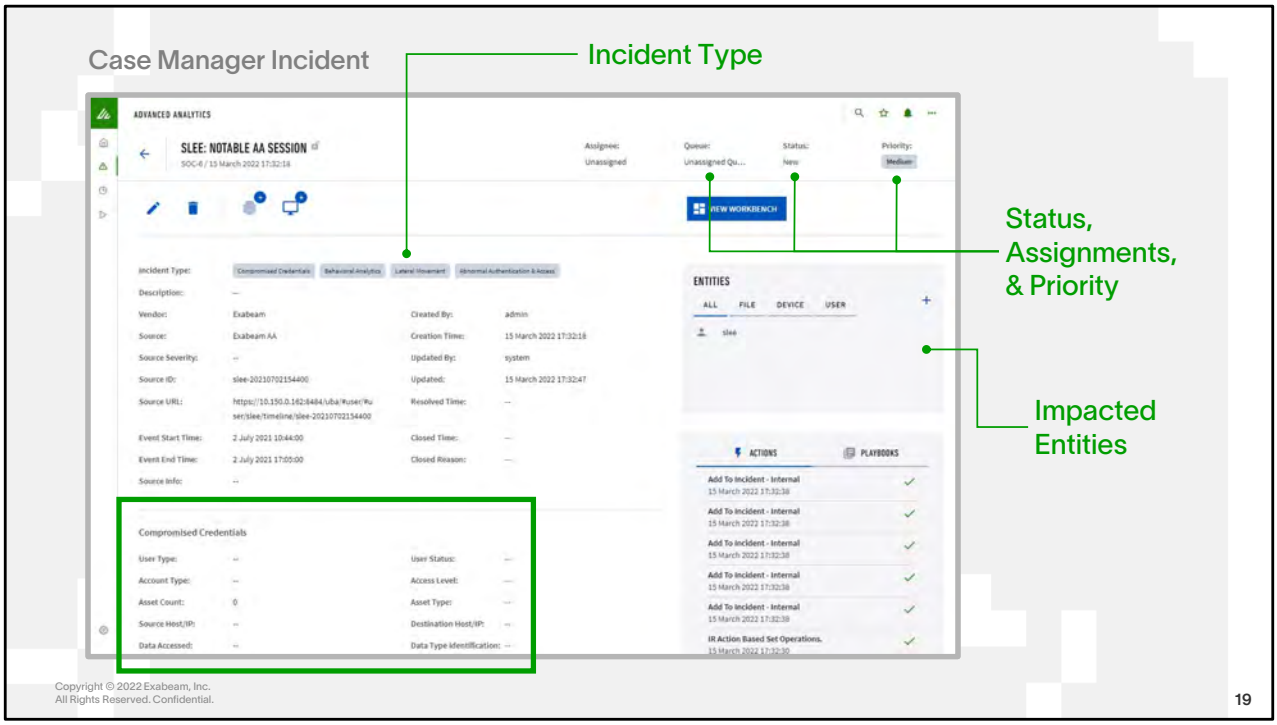
1. Recall with general familiarity the principles of the Exabeam Use Case methodology
2. Describe and Identify External Threat Activity
3. **Investigate and Respond to External Threat Activity**



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
Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.
18

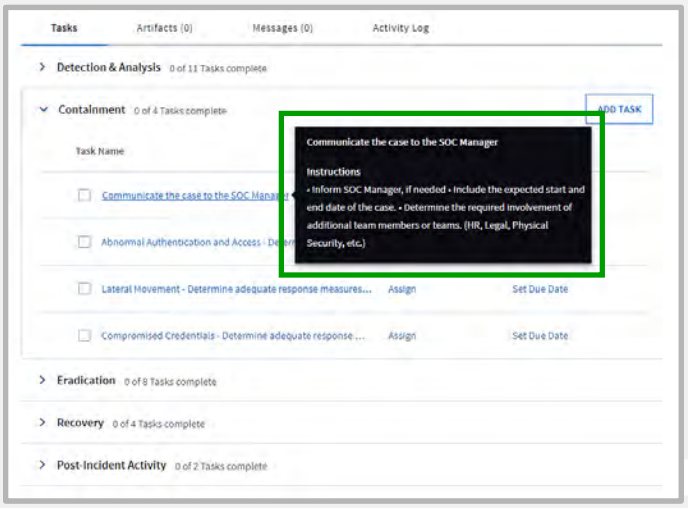


Student Notes

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

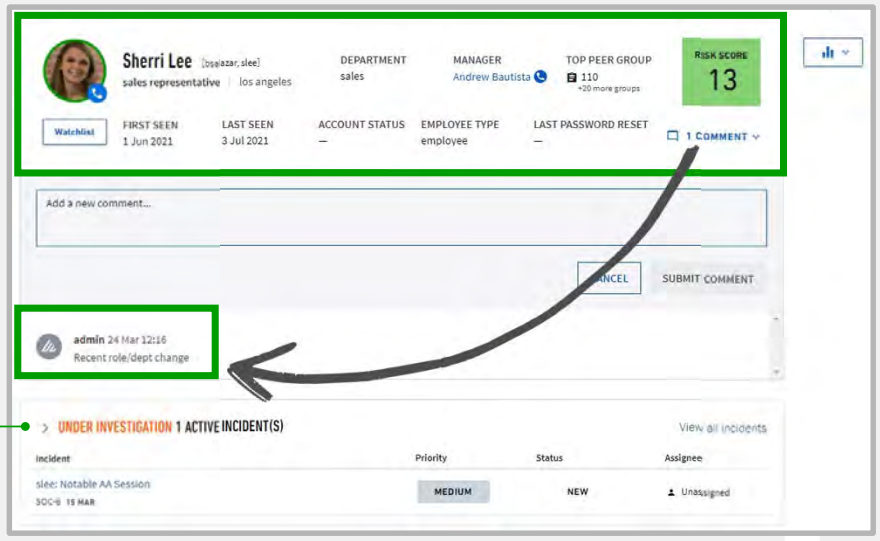
Hover over a task for additional details



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

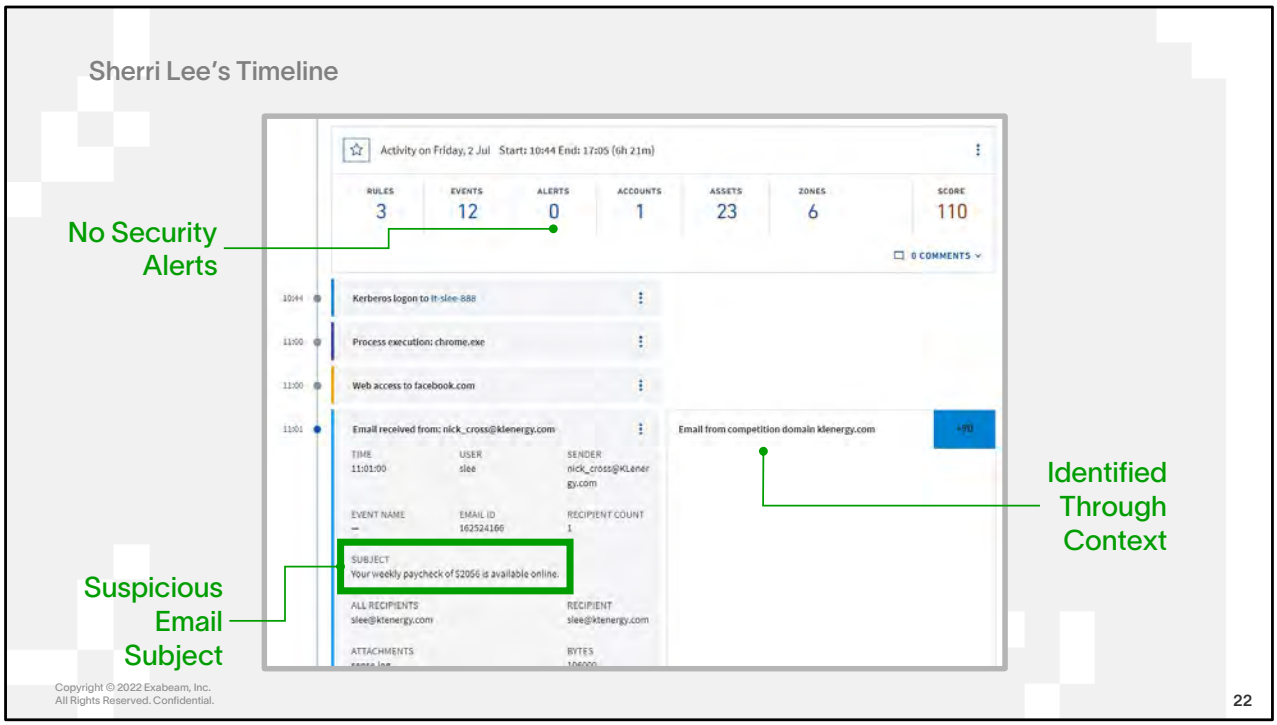


Active Incidents

21

Student Notes

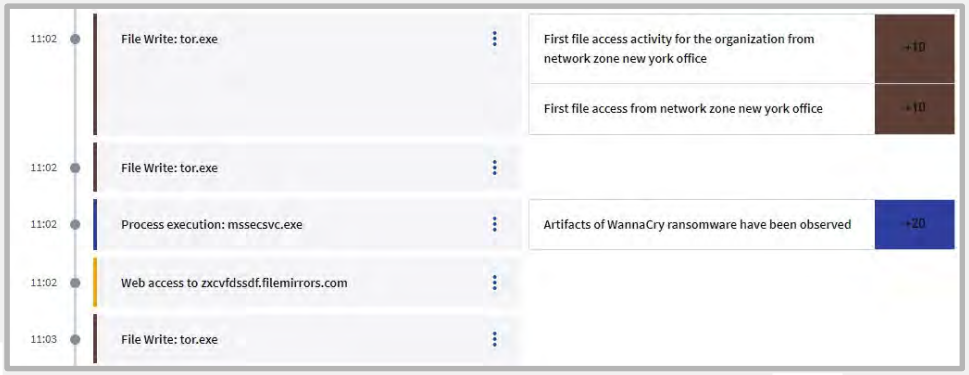
We see from Sherri Lee's profile page that her current risk score is only 13, but there is an active incident tied to her account. The comment on her profile indicates a recent role/department change, a valuable piece of information for the analyst to have when investigating anomalies. Comments can be 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.



Student Notes

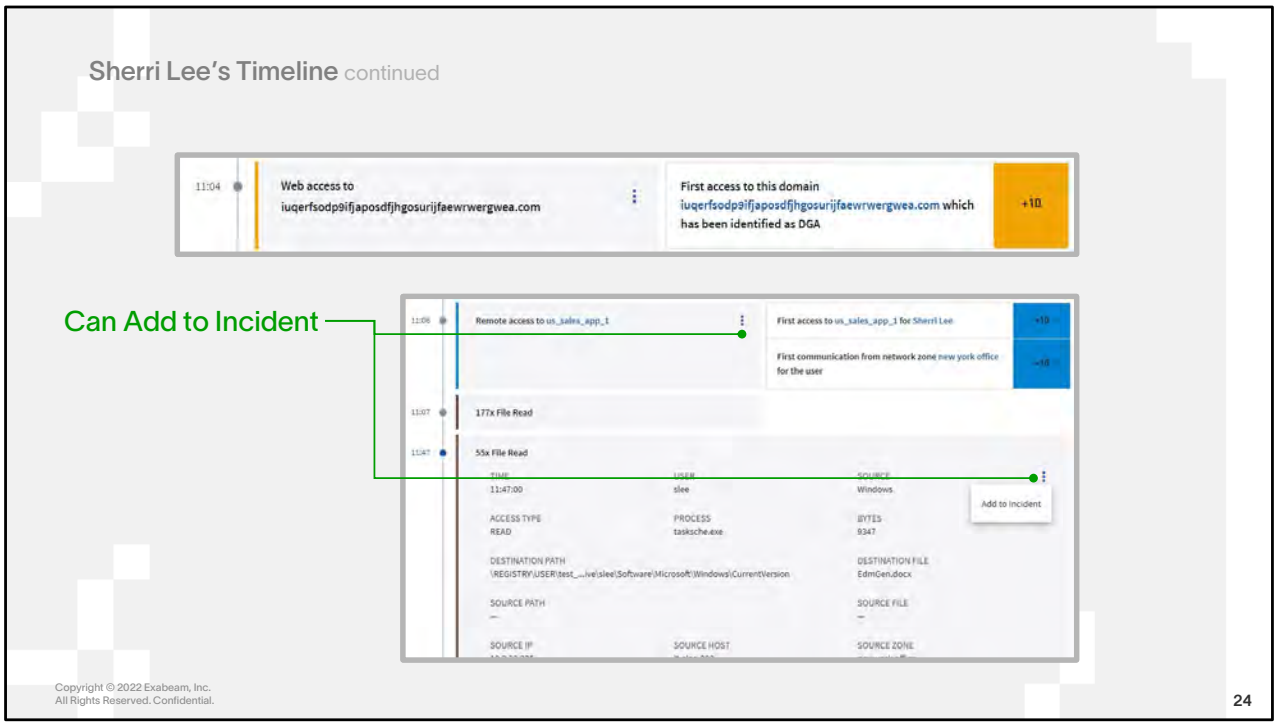
When we pivot to Sherri Lee's timeline for her notable session, we see that it doesn't contain any security alerts (AV, EDR, DLP, etc.), so this activity wouldn't have surfaced in Alert Triage. The first concerning event in Sherri's timeline is the receipt of an email from a "competition domain," which 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



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.

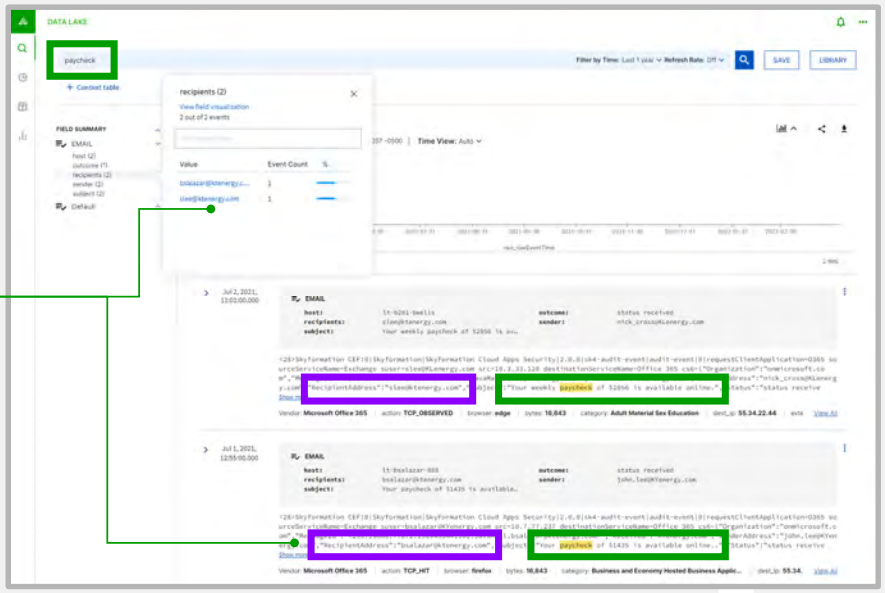


Student Notes

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."

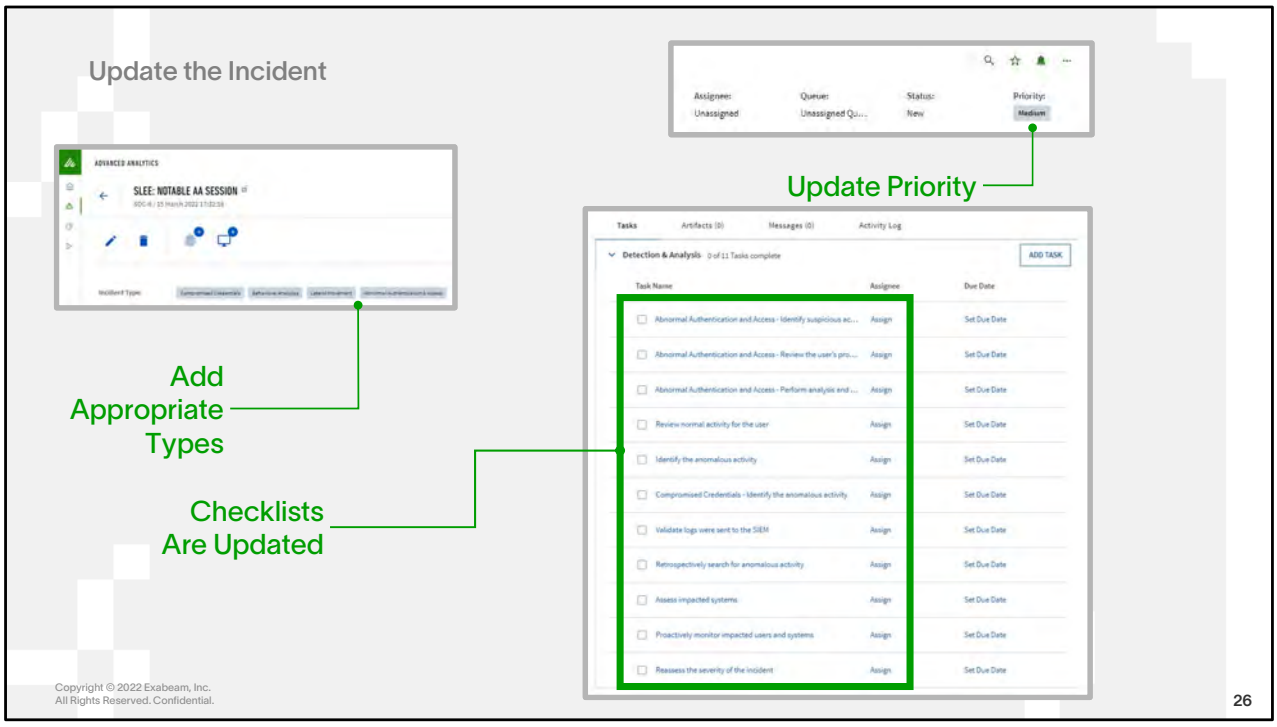
Additional SIEM Research



25

Student Notes

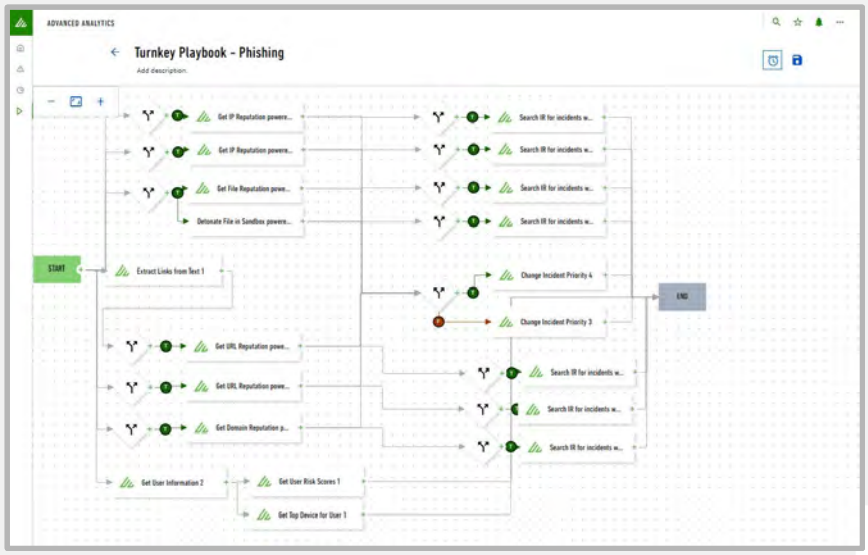
Recall that the suspicious email Sherri Lee received that prompted this investigation did not trigger an EPP/EDR alert. Pivoting to Data Lake and performing a simple, unstructured text search on the string “paycheck” reveals that a similar email was sent to Barbara Salazar (bsalazar@ktenergy.com). The 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.



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

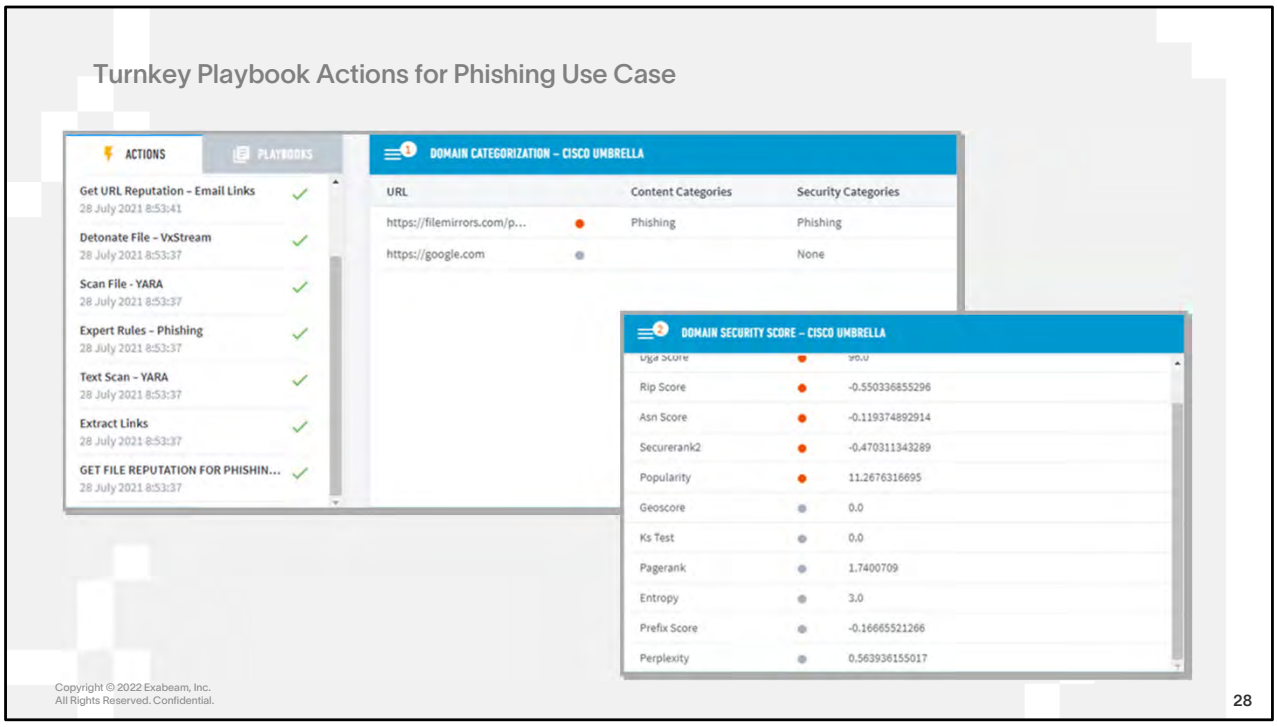


Student Notes

Playbooks in incident responder provide automated ways of gathering data points from 3rd 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



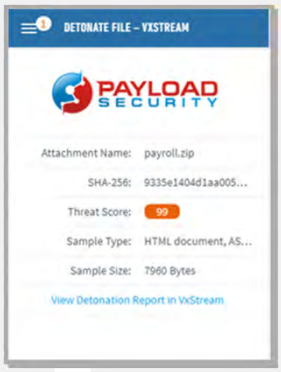
Student Notes

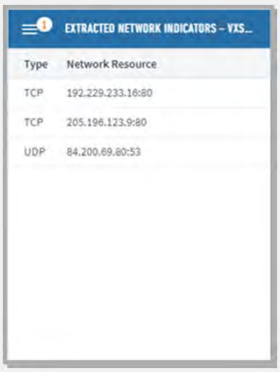
The Exabeam security platform provides turnkey playbook actions for phishing incidents to provide you with out of the box response for this type of attack.

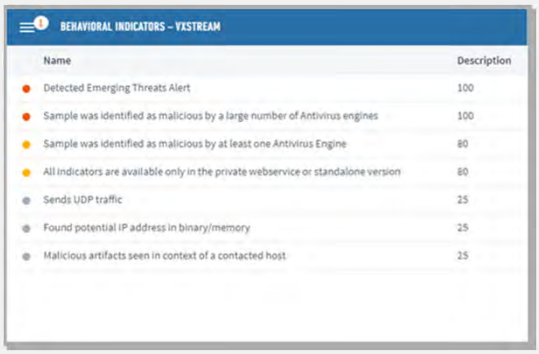
References

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

Turnkey Playbook Actions for Phishing Use Case continued







Turnkey Playbook Actions for Phishing Use Case continued

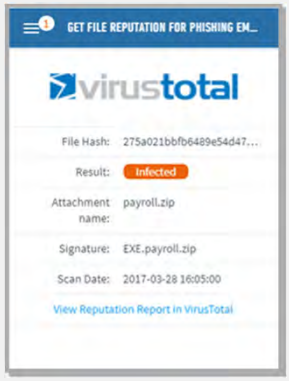
SCAN FILE - YARA

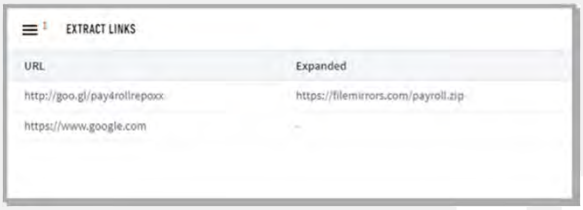
Rule Name	Rule Description
Network vulnerability	Found queries for sensitive IE security settings
URL binary match	Found potential URL in binary/memory
POS_FastPOS	Used to detect FastPOS keylogger + scraper
Additional scripts in payload	Found additional scripts within payload to install hooks/patches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

Turnkey Playbook Actions for Phishing Use Case continued





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

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