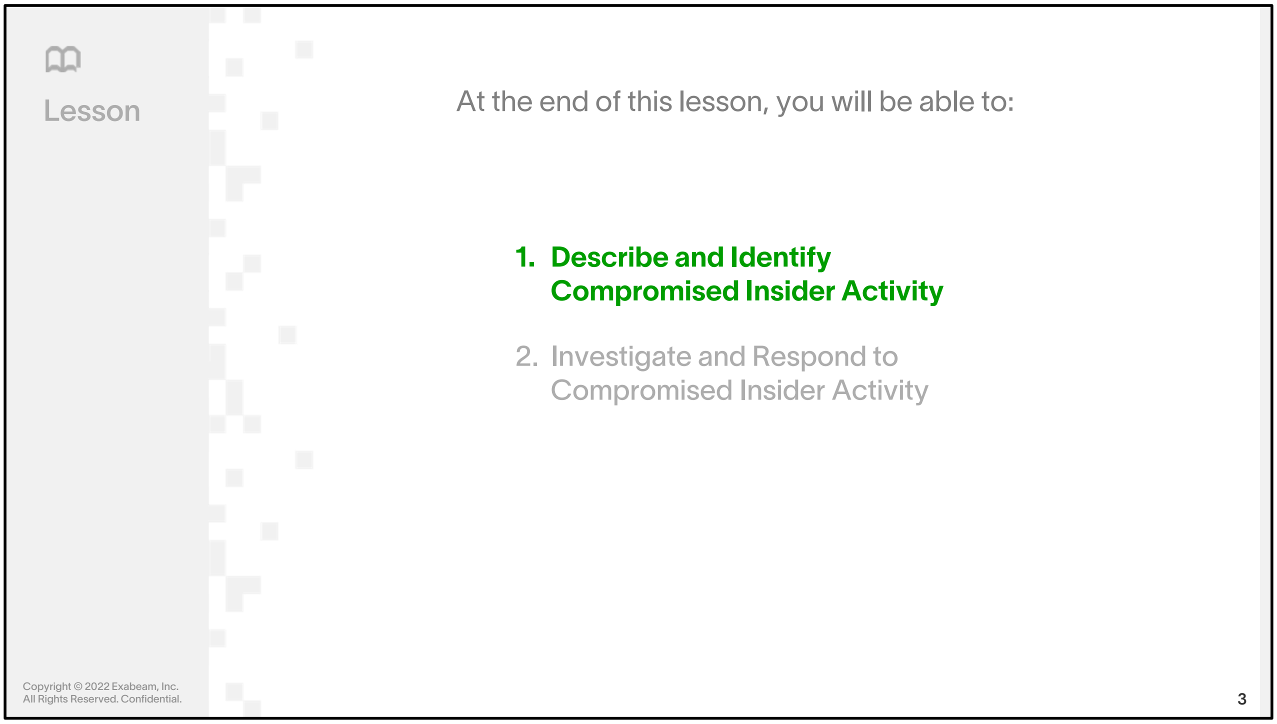
v4.00

Compromised Insiders

EDU-2170 : Module 8

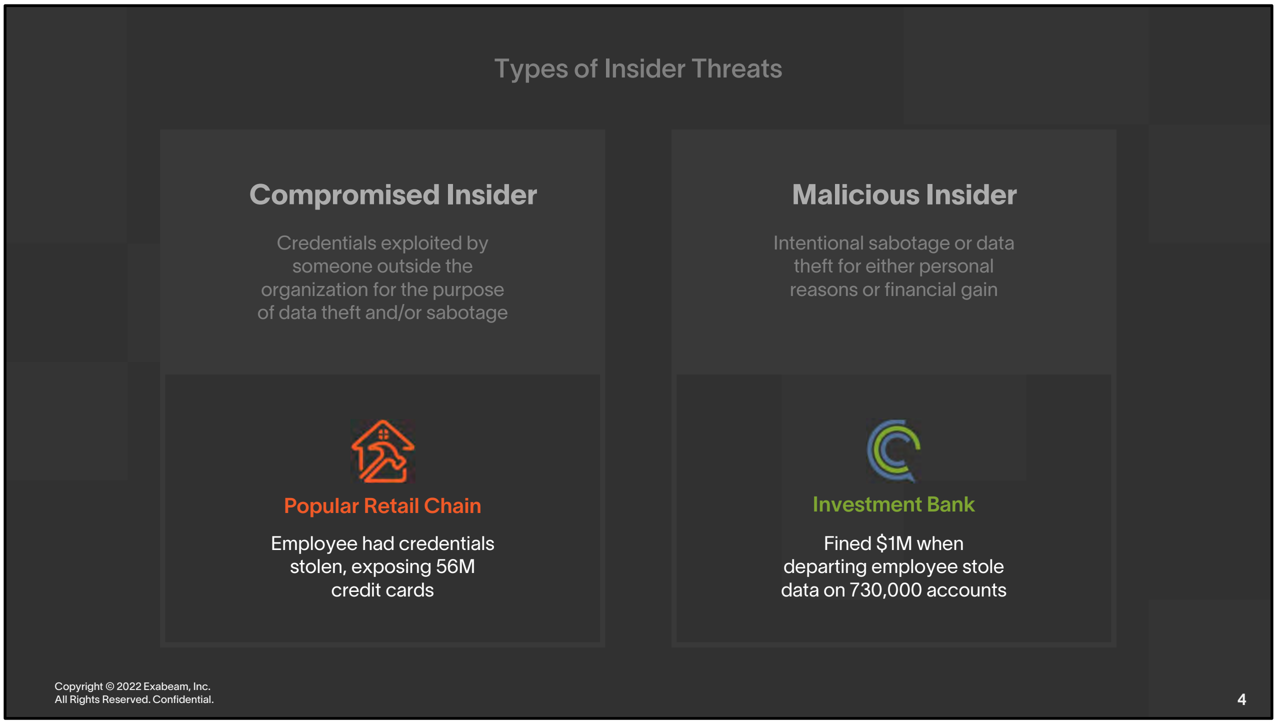
What breach techniques do you most commonly see?



Lesson

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

1. **Describe and Identify Compromised Insider Activity**
2. Investigate and Respond to Compromised Insider Activity



Types of Insider Threats

Compromised Insider

Credentials exploited by someone outside the organization for the purpose of data theft and/or sabotage

Popular Retail Chain

Employee had credentials stolen, exposing 56M credit cards

Malicious Insider

Intentional sabotage or data theft for either personal reasons or financial gain

Investment Bank

Fined $1M when departing employee stole data on 730,000 accounts

Student Notes

- An insider threat is a malicious threat to an organization that comes from people within the organization who have inside information concerning the organization’s security practices, data and computer systems.
- Insider risks can often be attributed to credential theft (both internal and external) or some other form of malicious activity.
- More than 60% of reported insider threat incidents were the result of a careless employee or contractor, and 23% were caused by malicious insiders. A total of 14% of all insider threat incidents involved cyber criminals stealing credentials

Compromised Insider: Monitor and detect ***attackers*** who have compromised the credentials of internal users to exploited typically for purpose of data theft or monetary gain.

Contains both anomaly and fact-based detection; with a relatively ***equal emphasis*** on detecting fact-based attacker techniques and anomalous user/asset behavior.

The use case category **contains** detection rules pertaining to specific advanced persistent attacks (APT) or sophisticated hacking techniques.
Guided investigations and playbooks are tailored to respond to external threat actors.

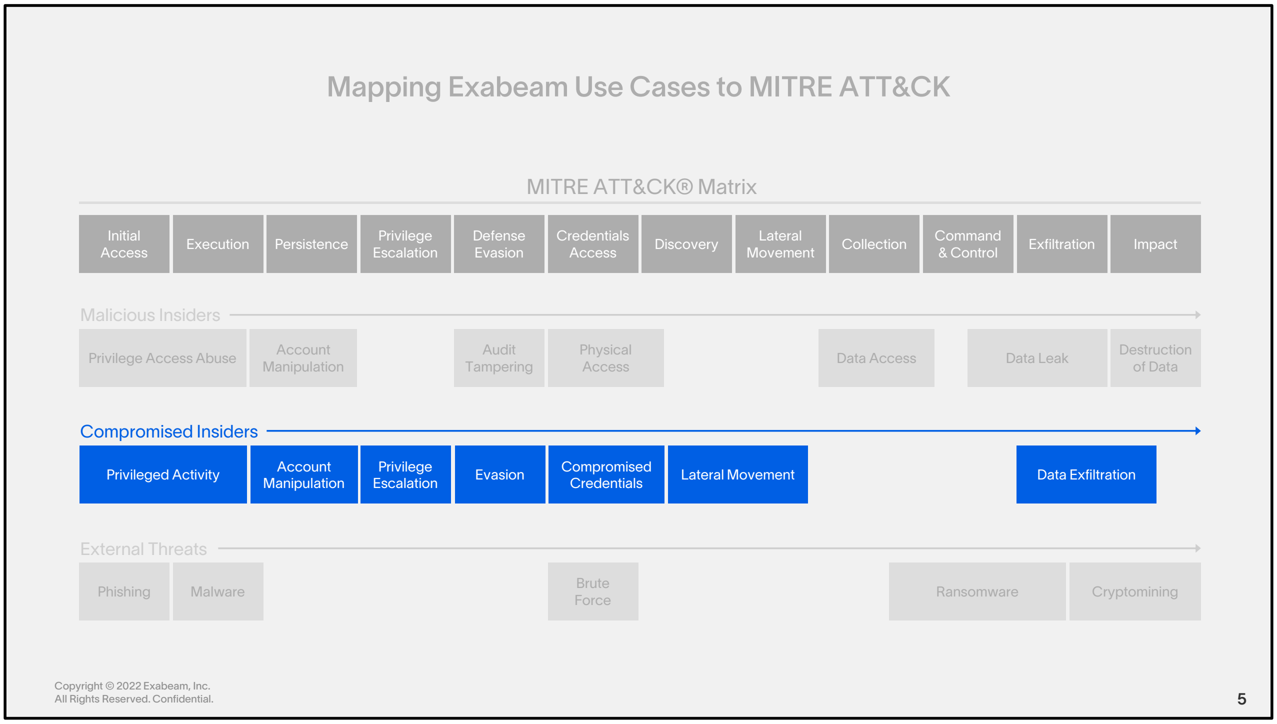
Malicious Insider: Monitor and detect ***internal users*** who are ***deliberately*** causing regulatory, operational, financial, and reputational harm to an organization.

Contains both anomaly and fact-based detection, but with much greater ***emphasis on detecting behavior*** based changes.

The use case category **does not contains** detection rules pertaining to specific advanced persistent attacks (APT) or sophisticated hacking techniques.
Guided investigations and playbooks are tailored to respond to malicious internal users.

References

https://global.techradar.com/en-ae/news/organisations-in-middle-east-spend-more-than-global-average-on-insider-threats
https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/



Mapping Exabeam Use Cases to MITRE ATT&CK

MITRE ATT&CK® Matrix

Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credentials Access | Discovery | Lateral Movement | Collection | Command & Control | Exfiltration | Impact

Malicious Insiders

Privilege Access Abuse | Account Manipulation | Audit Tampering | Physical Access | Data Access | Data Leak | Destruction of Data

Compromised Insiders

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

External Threats

Phishing | Malware | Brute Force | Ransomware | Cryptomining

Student Notes

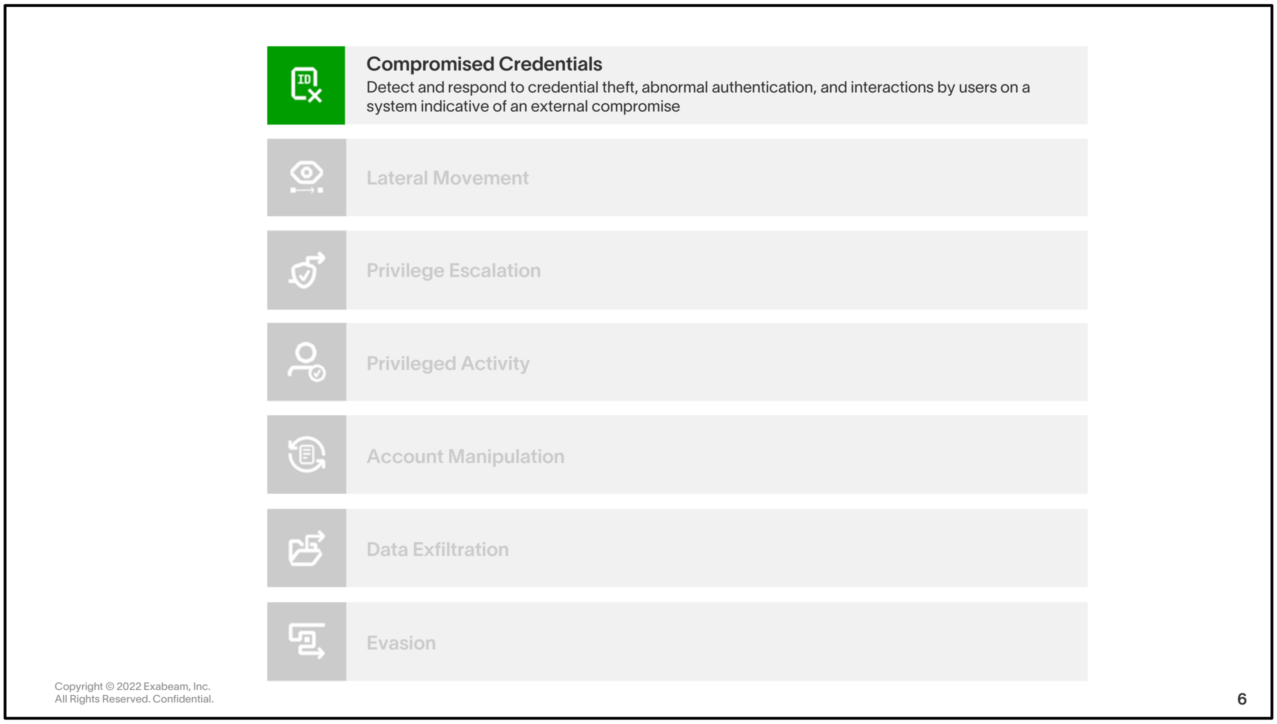
Monitor and detect ***attackers*** who have compromised the credentials of internal users to exploited typically for purpose of data theft or monetary gain.

Contains both anomaly and fact-based detection; with a relatively ***equal emphasis*** on detecting fact-based attacker techniques and anomalous user/asset behavior.

The use case category contains detection rules pertaining to specific advanced persistent attacks (APT) or sophisticated hacking techniques.

Guided investigations and playbooks are tailored to respond to external threat actors.

References
https://www.exabeam.com/ueba/insider-threats/



Compromised Credentials
Detect and respond to credential theft, abnormal authentication, and interactions by users on a system indicative of an external compromise

Lateral Movement

Privilege Escalation

Privileged Activity

Account Manipulation

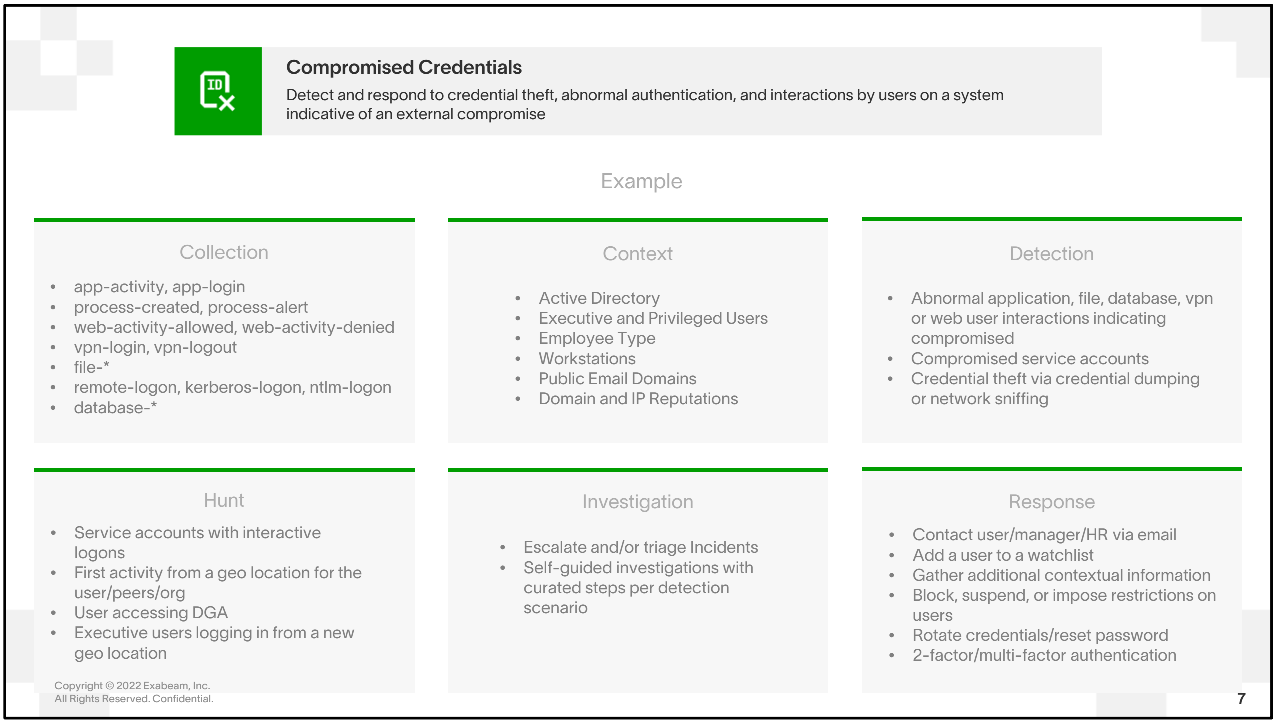
Data Exfiltration

Evasion

Student Notes

The Compromised Insider use case category currently includes the following seven use cases:

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



Compromised Credentials

Detect and respond to credential theft, abnormal authentication, and interactions by users on a system indicative of an external compromise

Example

Collection

- app-activity, app-login
- process-created, process-alert
- web-activity-allowed, web-activity-denied
- vpn-login, vpn-logout
- file-*
- remote-logon, kerberos-logon, ntlm-logon
- database-*

Context

- Active Directory
- Executive and Privileged Users
- Employee Type
- Workstations
- Public Email Domains
- Domain and IP Reputations

Detection

- Abnormal application, file, database, vpn or web user interactions indicating compromised
- Compromised service accounts
- Credential theft via credential dumping or network sniffing

Hunt

- Service accounts with interactive logons
- First activity from a geo location for the user/peers/org
- User accessing DGA
- Executive users logging in from a new geo location

Investigation

- Escalate and/or triage Incidents
- Self-guided investigations with curated steps per detection scenario

Response

- Contact user/manager/HR via email
- Add a user to a watchlist
- Gather additional contextual information
- Block, suspend, or impose restrictions on users
- Rotate credentials/reset password
- 2-factor/multi-factor authentication

Student Notes

The Exabeam SOC platform maps content and tools to the Threat Detection, Investigation, and Response workflow on a per use case basis, providing prescriptive guidance and tooling for end-to-end TDIR.

Collection: these are the event types created from parsed logs for the Compromised Credentials use case. Log sources to include are:

- Application Activity/Cloud Application Activity
- Database Activity Monitoring (DAM)
- Endpoint Security (EPP/EDR)
- File Monitoring
- VPN/Zero Trust Network Access
- Web Security and Monitoring
- Authentication and Access Management
- Privileged Access Management (PAM)
- Network Access, Analysis, and Monitoring

Note that Data Lake supports over 500 data source integrations out of the box, as well as Cloud Connectors.

- Context: we'll highlight more on context for Compromised Credentials on upcoming slides
- Detection: Rule types for detecting Compromised Credentials
- Investigation: note that Data Lake requires Fusion SIEM
- Response: Incidents that are classified in Case Manager will include additional prescriptive investigation and response tasks. Turnkey playbooks provide configureless, out-of-the-box SOAR functionality to automate much of the process.
- Hunt: Threat Hunter queries will be added to the customer's environment by Professional Services (Deployment Services) based on entitlements.

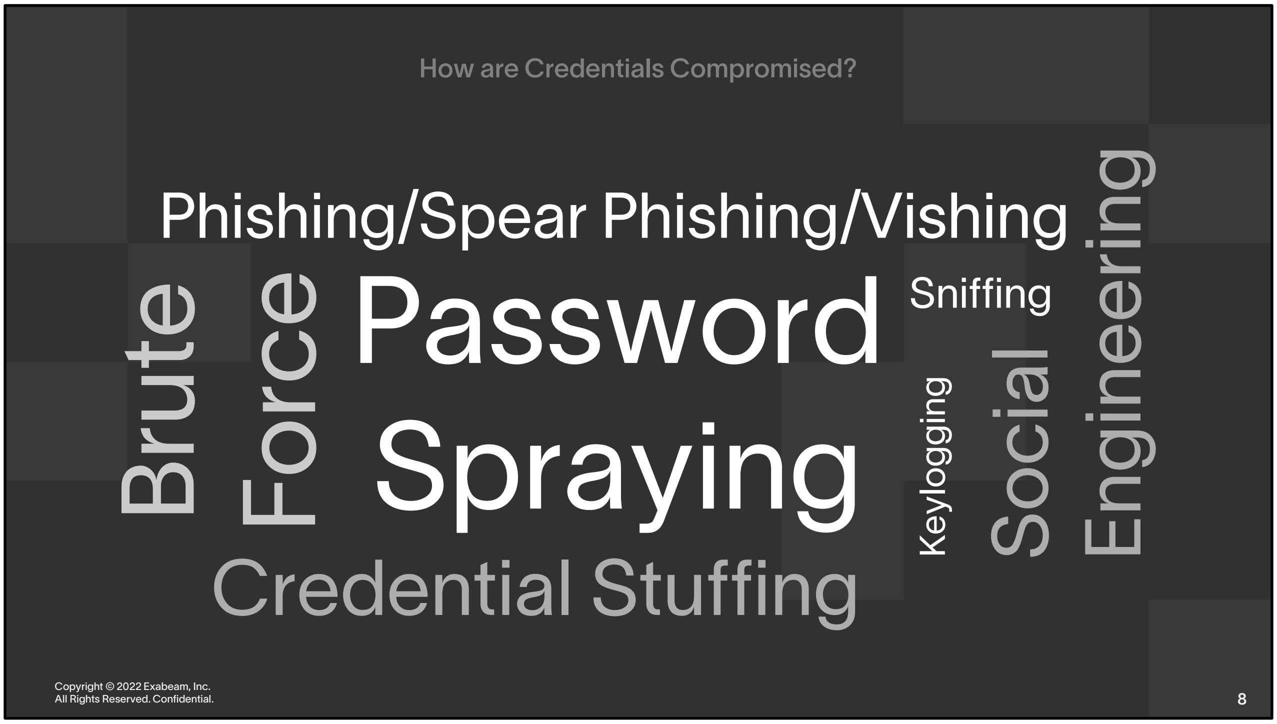
Compromised Credentials data sources may include:

- Application Activity/Cloud Application Activity
- Database Activity Monitoring (DAM)
- Endpoint Security (EPP/EDR)
- File Monitoring
- VPN/Zero Trust Network Access
- Web Security and Monitoring
- Authentication and Access Management
- Privileged Access Management (PAM)
- Network Access, Analysis, and Monitoring

MITRE techniques mapping to the Compromised Credentials use case include:

- T1213: Data from Information Repositories
- T1078: Valid Accounts
- T1133: External Remote Services
- T1071: Application Layer Protocol
- T1102: Web Service
- T1003: OS Credential Dumping
- T1040: Network Sniffing

References
https://community.exabeam.com/s/article/Compromised-Credentials-MITRE-ATT-CK-Framework-Mapping



How are Credentials Compromised?

Phishing/Spear Phishing/Vishing

Brute Force

Password Spraying

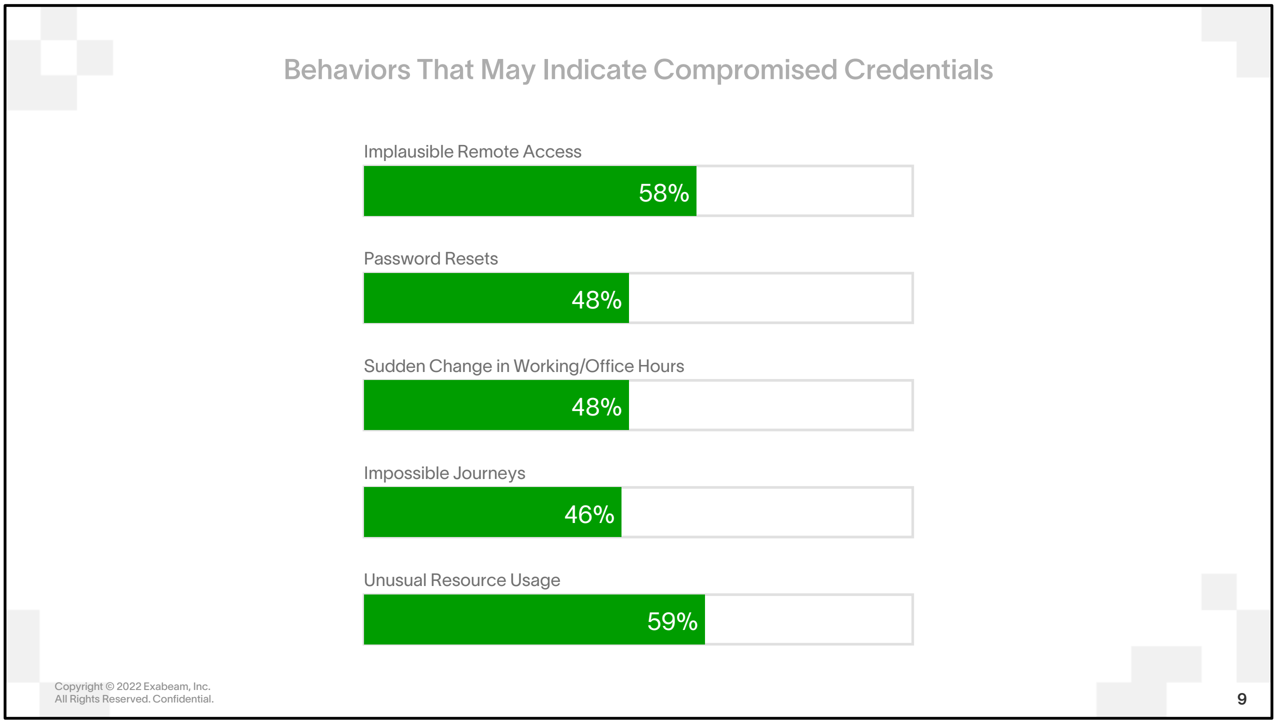
Sniffing

Keylogging

Social Engineering

Credential Stuffing

Student Notes
References:
https://community.exabeam.com/s/article/Compromised-Credentials-Chapter-1



Behaviors That May Indicate Compromised Credentials

Implausible Remote Access
58%

Password Resets
48%

Sudden Change in Working/Office Hours
48%

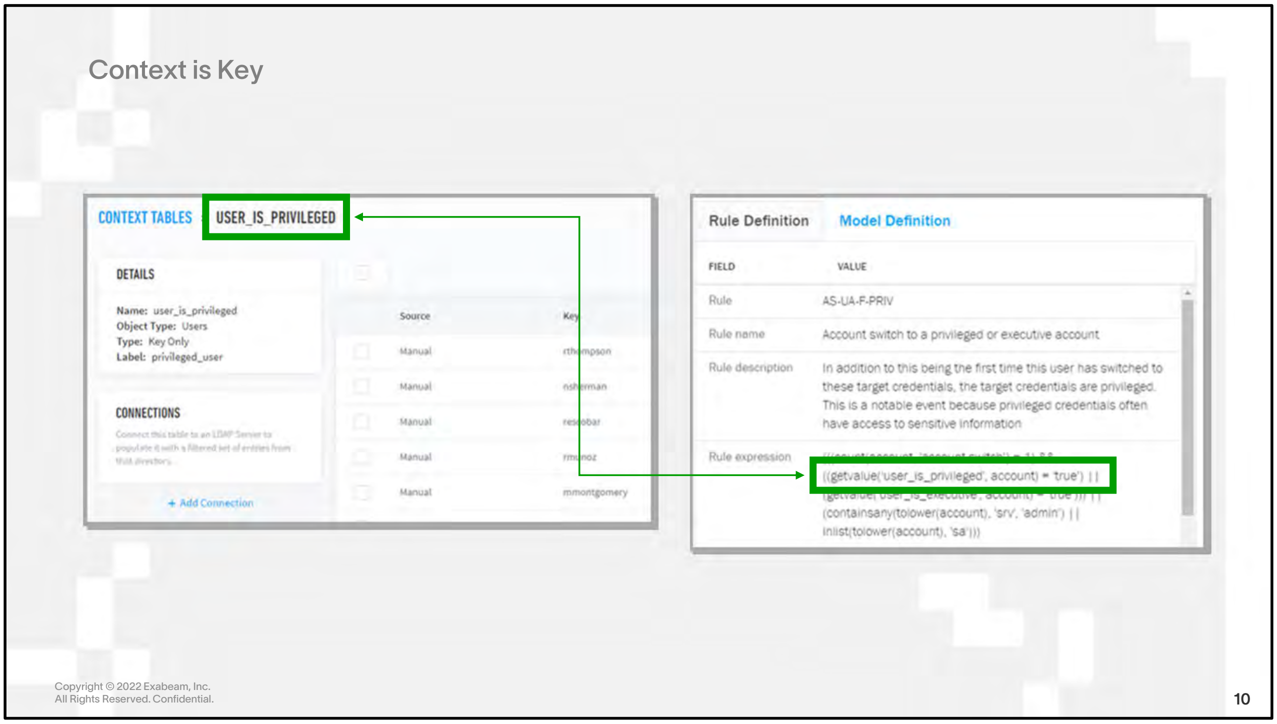
Impossible Journeys
46%

Unusual Resource Usage
59%

Student Notes
When credentials have been compromised, how do you distinguish legitimate user activity from compromised user activity? As one saying goes, not all hackers break in—often, they log in.

References
https://www.isdecisions.com/security-breach-infographic-compromised-login/

Context is Key



DETAILS

Name: user_is_privileged
Object Type: Users
Type: Key Only
Label: privileged_user

CONNECTIONS

Connect this table to an LDAP Server to populate it with a filtered set of entries from that directory.

+ Add Connection

Source	Key
Manual	rthompson
Manual	nsherman
Manual	rescobar
Manual	rmunoz
Manual	mmontgomery

FIELD	VALUE
Rule	AS-UA-F-PRIV
Rule name	Account switch to a privileged or executive account
Rule description	In addition to this being the first time this user has switched to these target credentials, the target credentials are privileged. This is a notable event because privileged credentials often have access to sensitive information
Rule expression	(((count(account, 'account switch') = 1) && ((getvalue('user_is_privileged', account) = 'true') || (getvalue('user_is_executive', account) = 'true'))) || (containsany(tolower(account), 'srv', 'admin') || inlist(tolower(account), 'sa')))

Student Notes

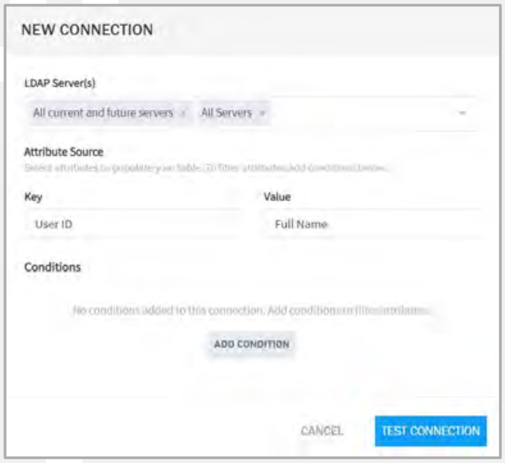
Logs tell Exabeam what the users and entities are doing while context tells us who the users and entities are. Context sources enrich the logs to help with the anomaly detection process and can be also be used directly by the risk engine layer for fact-based rules. Many rules, like the one shown above, use the context tables to allocate additional risk to sensitive accounts. Users with an assigned role that allows them to edit rule scores can customize rule scores directly in the Advanced Analytics user interface to meet their organization's security needs. You can also create custom context and/or custom rules to meet your organization’s unique requirements.

References

https://docs.exabeam.com/en/advanced-analytics/i57/advanced-analytics-administration-guide/127369-advanced-analytics.html

Adjusting a rule’s score: https://community.exabeam.com/s/article/Advanced-Analytics-Top-Tip-Reducing-a-Rule-s-Score

Building and Updating Context Tables



NEW CONNECTION

LDAP Server(s)

All current and future servers × All Servers ×

Attribute Source

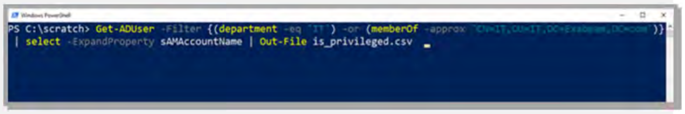
Select attributes to populate your table. To filter attributes, add conditions below.

Key: User ID

Value: Full Name

Conditions

No conditions added to this connection. Add conditions to filter attributes.



```
PS C:\scratch> Get-ADUser -Filter {(department -eq 'IT') -or (memberOf -approx 'CN=IT,OU=IT,DC=Exabeam,DC=com')}
 | select -ExpandProperty sAMAccountName | Out-File is_privileged.csv _
```

Or

Student Notes

As an example, the rule “Account switch to a privileged or executive account” shown previously depends upon the corresponding context tables and their accuracy. The easiest and most automated way to retrieve and update context is via an LDAP query to your identity server(s). For context retrieval in Microsoft Active Directory environments, we recommend pointing to a Global Catalog server. To list Global Catalog servers, enter the following command in a Windows command line: nslookup -querytype=srv gc.tcp.acme.local.

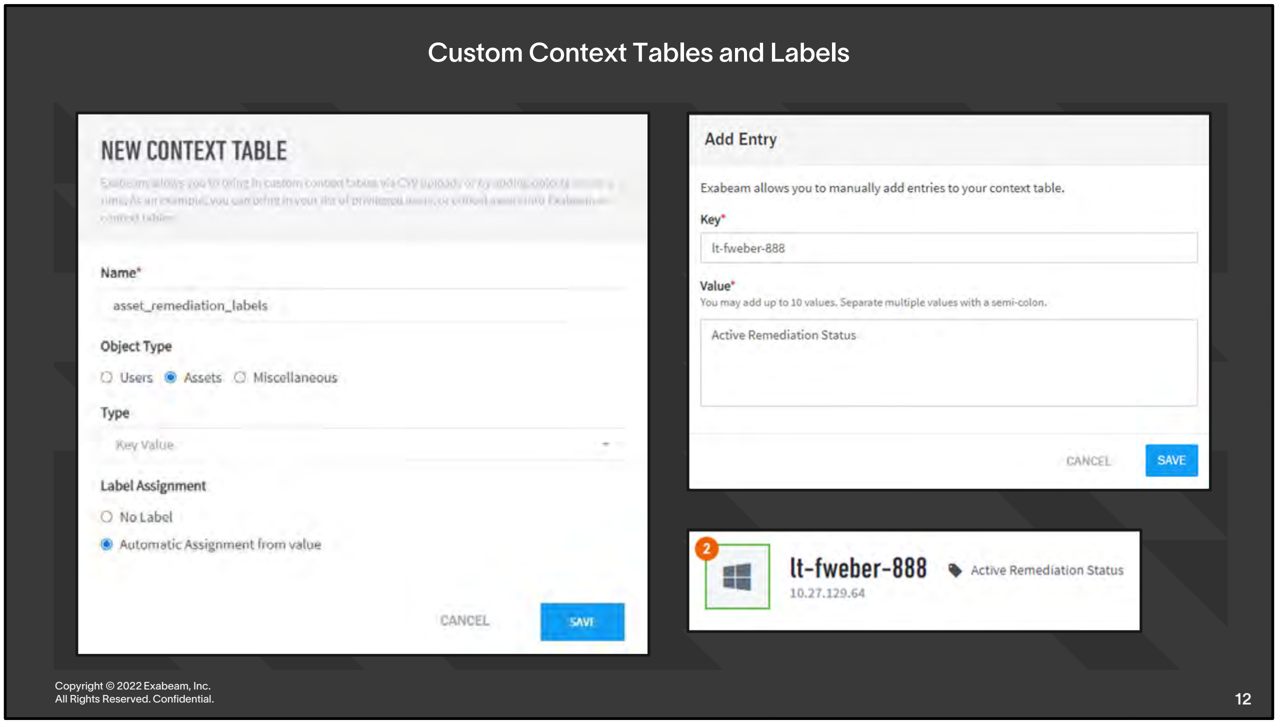
For more sophisticated filtering, you could use command-line tools like PowerShell to build a query and fetch the results to populate a CSV file, as in the example above. When you import a CSV, you have the option of merging the new data with the existing data or replacing it. If a key exists in the current context table, its value will be replaced with the newest uploaded value(s).
Certain events may be more important to highlight within your organization.

References

Adjusting a rule’s score: https://community.exabeam.com/s/article/Advanced-Analytics-Top-Tip-Reducing-a-Rule-s-Score

References

https://docs.exabeam.com/en/advanced-analytics/i57/advanced-analytics-administration-guide/127369-advanced-analytics.html
https://community.exabeam.com/s/article/How-to-Set-up-a-Context-Table-and-Watchlist-for-Privileged-Users



Custom Context Tables and Labels

NEW CONTEXT TABLE

Exabeam allows you to bring in custom context tables via CSV upload, or by adding [illegible] time. As an example, you can bring in your list of privileged users, or critical assets into Exabeam context tables.

Name*: asset_remediation_labels

Object Type: ○ Users ● Assets ○ Miscellaneous

Type: Key Value

Label Assignment:
○ No Label
● Automatic Assignment from value

Add Entry

Exabeam allows you to manually add entries to your context table.

Key*: lt-fweber-888

Value*: Active Remediation Status
You may add up to 10 values. Separate multiple values with a semi-colon.

lt-fweber-888 — Active Remediation Status
10.27.129.64

Student Notes

Custom context tables allow you the flexibility to create watchlists or reference lists for assets, threat intelligence indicators, and users/groups that do not fit in the typical deployment categories. Custom context tables let you put parts of your organization under extra monitoring or special scrutiny, such as financial servers, privileged insiders, and high-level departed employees.

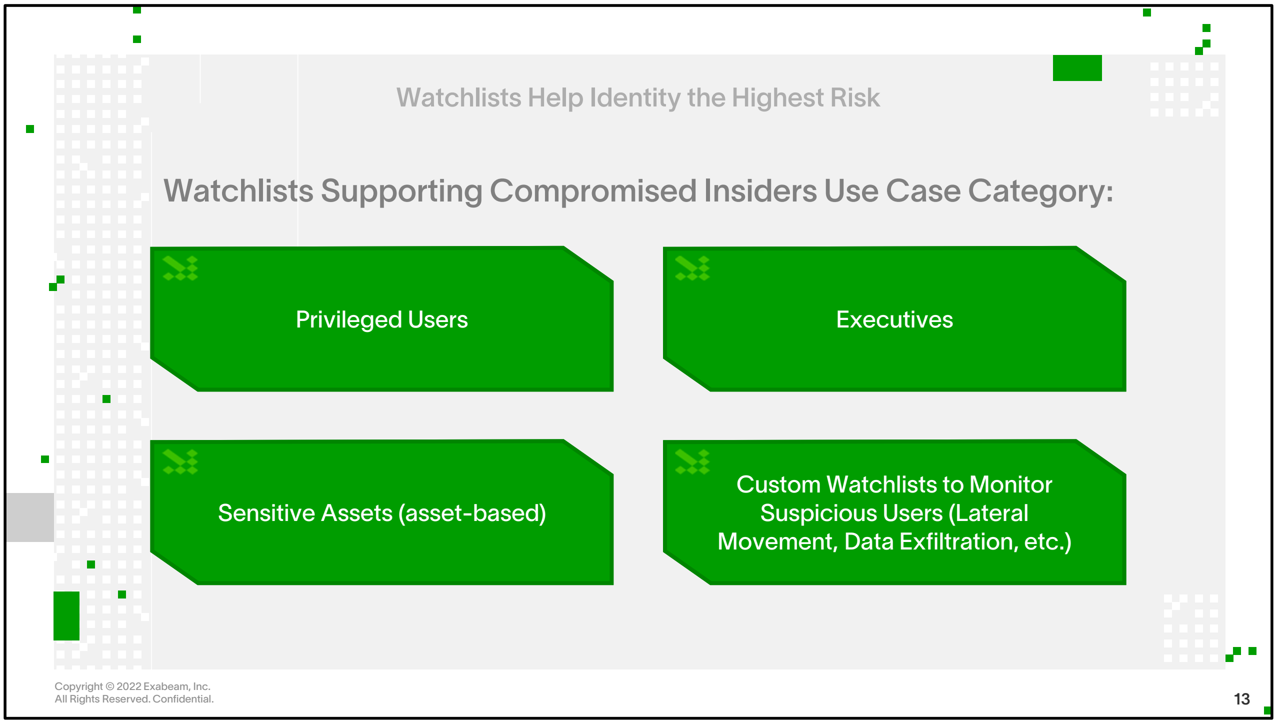
Within Advanced Analytics, you can create watchlists using context tables. When creating the table, the Label attribute allows you to attach tags to records that match entries in your context table. This provides quick access to query your results and/or focus your tracking using a global characteristic.

You can also build rules based on entries in your context tables. Set up alerts, actions, or playbooks to trigger when conditions match records, such as access to devices in a special asset group.

References

https://community.exabeam.com/s/article/Adding-Custom-User-Labels-in-Advanced-Analytics
https://community.exabeam.com/s/article/Exabeam-APIs-Overview-and-Context-Table-Demo

https://community.exabeam.com/s/article/Adding-Custom-User-Labels-in-Advanced-Analytics



Watchlists Help Identity the Highest Risk

Watchlists Supporting Compromised Insiders Use Case Category:

- Privileged Users
- Executives
- Sensitive Assets (asset-based)
- Custom Watchlists to Monitor Suspicious Users (Lateral Movement, Data Exfiltration, etc.)

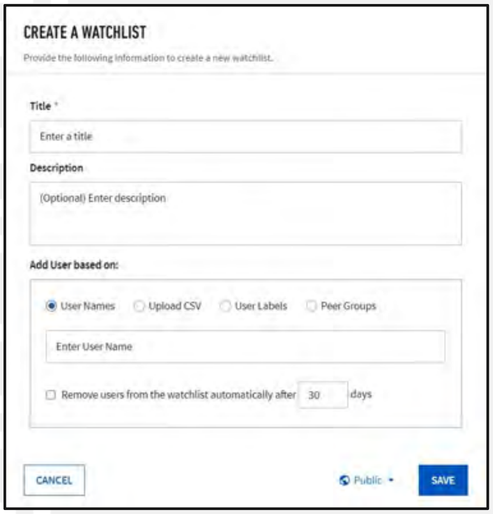
Student Notes
Within Advanced Analytics, you can create watchlists using context tables. When creating the table, the Label attribute allows you to attach tags to records that match entries in your context table. This provides quick access to query your results and/or focus your tracking using a global characteristic.

Users and assets added to a watchlist are prominently surfaced on the Advanced Analytics homepage. Custom context tables allow you the flexibility to create watchlists or reference lists for assets, threat intelligence indicators, and users/groups that do not fit in the typical deployment categories. Custom context tables let you put parts of your organization under extra monitoring or special scrutiny, such as financial servers, privileged insiders, and high-level departed employees.

References
https://community.exabeam.com/s/article/Create-Use-Case-Specific-Watchlists

Demo

Create a Watchlist from a Context Table



CREATE A WATCHLIST

Provide the following information to create a new watchlist.

Title *

Enter a title

Description

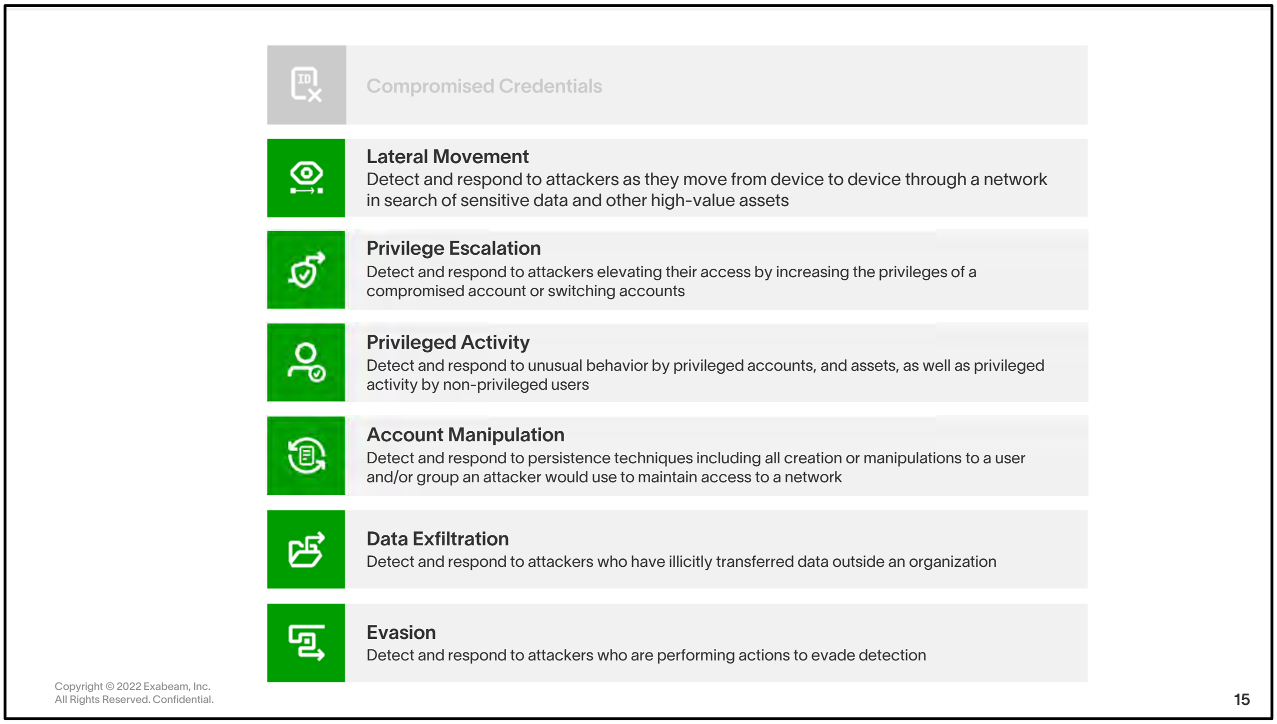
(Optional) Enter description

Add User based on:

● User Names ○ Upload CSV ○ User Labels ○ Peer Groups

Enter User Name

□ Remove users from the watchlist automatically after 30 days



Compromised Credentials

Lateral Movement
Detect and respond to attackers as they move from device to device through a network in search of sensitive data and other high-value assets

Privilege Escalation
Detect and respond to attackers elevating their access by increasing the privileges of a compromised account or switching accounts

Privileged Activity
Detect and respond to unusual behavior by privileged accounts, and assets, as well as privileged activity by non-privileged users

Account Manipulation
Detect and respond to persistence techniques including all creation or manipulations to a user and/or group an attacker would use to maintain access to a network

Data Exfiltration
Detect and respond to attackers who have illicitly transferred data outside an organization

Evasion
Detect and respond to attackers who are performing actions to evade detection

15

Student Notes
Lateral Movement use case

According to the Carbon Black Global Threat Report from 2019, nearly 60% of external attacks involve lateral movement. But what is lateral movement?

Lateral movement is a term that refers to techniques cyber attackers use to progressively move through a network, searching for targeted key data and assets. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, aka, “living off the land,” which may be stealthier. Legacy SIEMs will fire an alert based upon a correlation rule (static rule) for each event, but without context, the system, as well as the analyst, does not know to “tie them together”. This is what leads to inconsistent and incomplete responses and can result in a situation where there is no containment or response, but rather a metric being met that shows two closed attacks. In a day and age of metric-driven “results” it appears to be a win-win but in reality, it’s truly a false sense of security because a threat is not contained and remains present in your organization.
Security teams need smart, data-enriched timelines with contextual insights to surface attacks that involve lateral movement. This is where machine learning shines within the Exabeam Advanced Analytics platform.

Additional resources supporting the lateral movement use case in the Exabeam SOC platform include the following:

- Stateful timeline sessions map IP:Host:User, providing complete east-to-west visibility within the network perimeter despite changes in devices, credentials, or IP addresses.
- Pass-the-Hash and Golden Ticket rules
- Easy identification of account switch activity
- Entity Analytics models asset behavioral changes

Privilege Escalation use case

Privilege escalation can involve an attacker elevating their access either by increasing the level of privileges associated with an already compromised account (vertical escalation) or by switching accounts to gain access to a user with greater privileges (horizontal escalation). Horizontal escalation overlaps with the Lateral Movement use case discussed previously and can be detected by Exabeam through account switching behaviors, among other detection techniques. Exabeam detects vertical privilege escalation by identifying attackers who are bypassing access controls, exploiting access control vulnerabilities, or modifying permissions in order to elevate the privileges of an already compromised user. Note that for all use cases, Exabeam records the complete CLI command when the command line is used.

Privileged Activity use case

The Ponemon Institute states that 14% of incidents involve the abuse of privileged users' credentials and cost organizations an average of $2.79 million annually.

In the Exabeam SOC platform, privileged accounts are identified from contextual data, as discussed earlier. Privilege access abuse represents a greater risk to an organization's data security as privileged access can often lead to exploitation or damage to critical business entities. The Exabeam SOC platform also includes integrated SOAR capabilities in order to automatically terminate user sessions and disrupt a potential attack.

Account Manipulation use case

The Account Manipulation use case identifies users that are performing account management activity outside of their typical behavior patterns. This could indicate threats such as a user has been compromised and the bad actor is attempting to elevate access by modifying group privileges. Or a bad actor may also add and remove a temporary user in order to shield their true identity while performing a malicious activity such as system reconnaissance, or accessing, hoarding, or exfiltrating data. Abnormal account management activity may not be enough to identify if a bad actor has compromised a user, but paired with contextual clues, analysts can start to paint a picture of why this user's behavior has changed.

Data Exfiltration use case

Data Exfiltration is often the ultimate goal of a compromised insider attack, whether for the data itself or to monetize the theft through threat of doxing as is done in many ransomware attacks. Bad actors will often compress and/or encrypt the data they intend to exfiltrate, and they frequently use command and control or alternate network protocol channels, sometimes in small batches, to move the data outside the organization's perimeter. Exabeam has rules to detect these behaviors and many more.

Exabeam detects data exfiltration by analyzing all incoming DLP alerts and quantifying the level of risk. Furthermore, using behavior profiling techniques, Exabeam also detects data exfiltration by baselining normal user activity and monitoring for abnormal usage patterns. We then automatically stitch together the DLP alerts and our own data exfiltration alerts with authentication, access, and contextual data sources into a user-centric timeline to paint a full picture of user activity.
Analysts can leverage user and asset contextual data in conjunction with the abnormal activity to determine if the user is acting with malicious intent or if they have been compromised by an external bad actor. Finally, they are provided with lists of notable accounts, user activity timelines, and customized response plans to support data exfiltration investigations.

Evasion use case

After initial compromise, an adversary seeks to avoid detection to establish persistence within the network. As a result, hackers will leverage a host of tactics to remain undetected. By hiding their activity and evading the organization's detection mechanisms, they are awarded enough time to carry out their true objective, such as deploying malware for exfiltrating data, encrypting files for ransomware, or exploiting resources for crypto-mining.

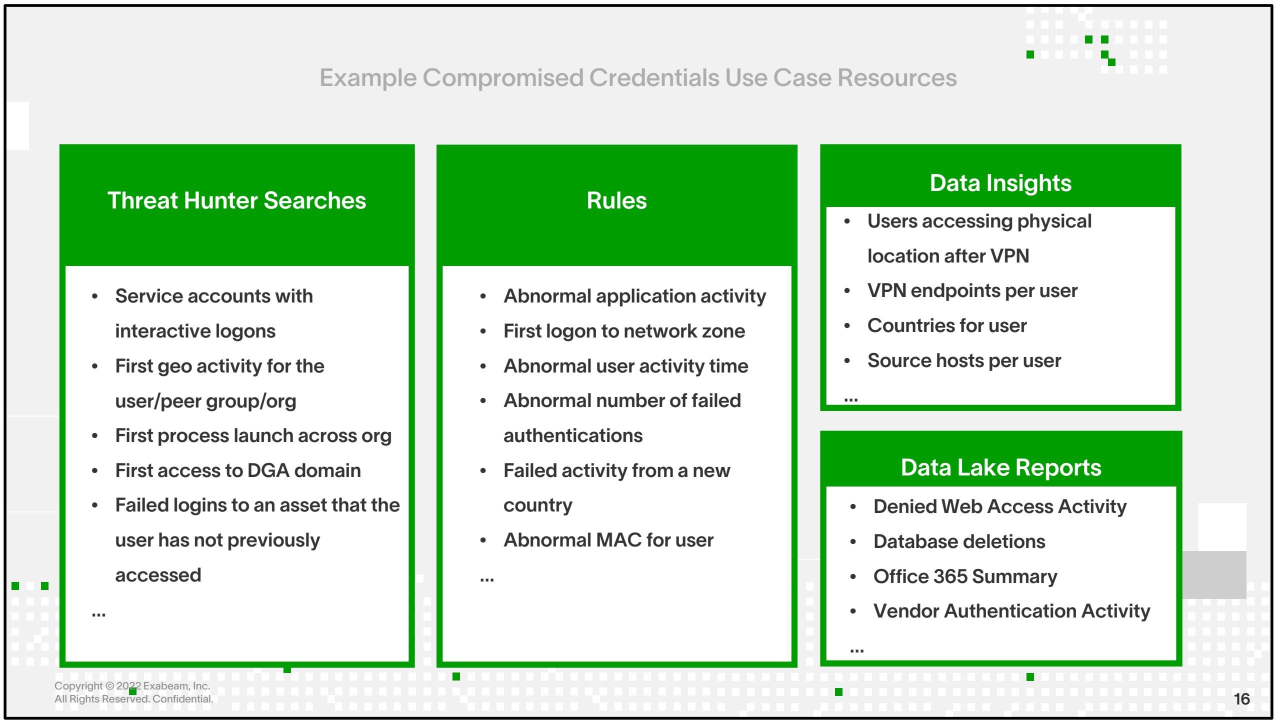
A common evasion technique is audit log clearing and/or tampering. So what do we do if the logs on a system have been cleared? The data used to populate timelines in Exabeam Advanced Analytics provide a historical view of user activity and events prior to any tampering or clearing of the audit log that may have occurred.

Groups such as APT29 make use of the TOR network for, among other things, evading an organization's defenses while exfiltrating data. Potentially dangerous IPs are flagged using Exabeam's is_tor_proxy and is_tor_ip context table enrichment.

Exabeam contributed sub-technique T1553.006: Code Signing Policy Modification to the MITRE ATT&CK framework. The above command line is one example of how a system's code signing policy might be modified, possibly for malicious purposes.

References

https://github.com/ExabeamLabs/Content-Doc/tree/master/UseCases
https://www.exabeam.com/ueba/detecting-lateral-movement-and-credential-switching-human-vs-machine/
https://attack.mitre.org/tactics/TA0008/
https://www.exabeam.com/information-security/lateral-movements/
https://www.exabeam.com/information-security/protecting-your-network-from-lateral-movement/
https://www.exabeam.com/wp-content/uploads/2016/06/Exabeam_BBCN_Case_Study.pdf
https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf



Example Compromised Credentials Use Case Resources

Threat Hunter Searches

- Service accounts with interactive logons
- First geo activity for the user/peer group/org
- First process launch across org
- First access to DGA domain
- Failed logins to an asset that the user has not previously accessed

…

Rules

- Abnormal application activity
- First logon to network zone
- Abnormal user activity time
- Abnormal number of failed authentications
- Failed activity from a new country
- Abnormal MAC for user

…

Data Insights

- Users accessing physical location after VPN
- VPN endpoints per user
- Countries for user
- Source hosts per user

…

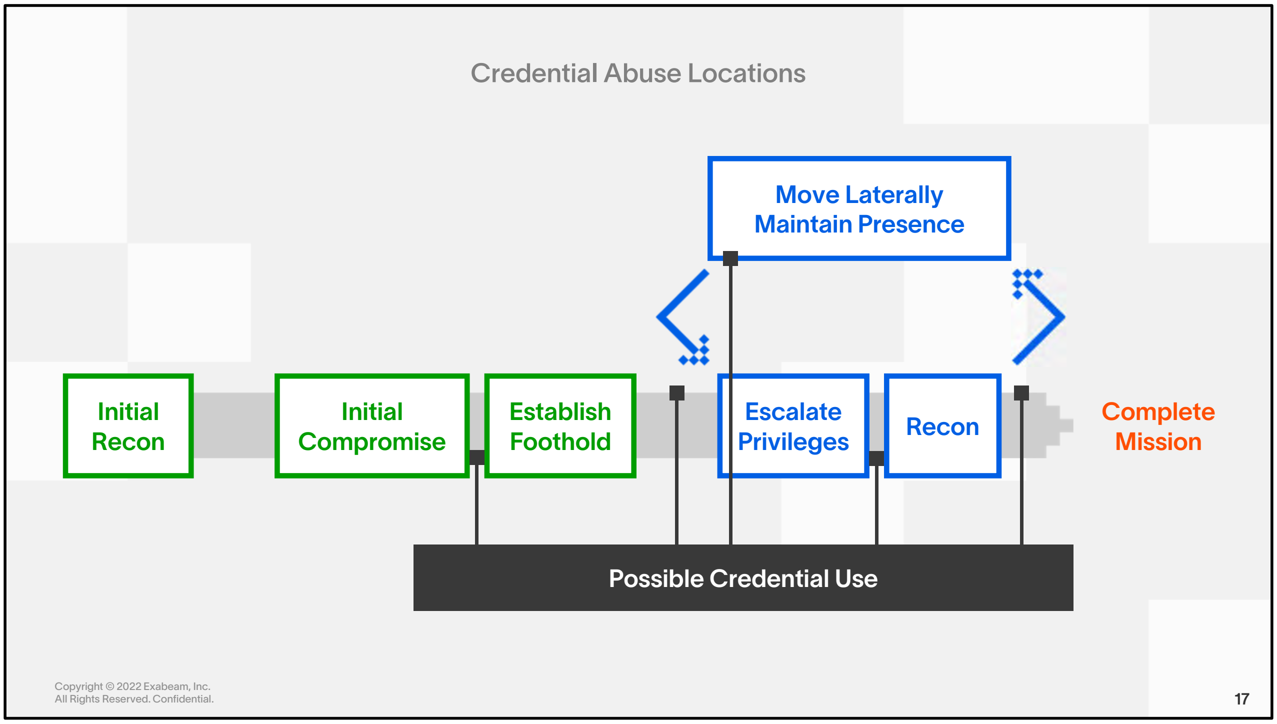
Data Lake Reports

- Denied Web Access Activity
- Database deletions
- Office 365 Summary
- Vendor Authentication Activity

…

Student Notes

Use case 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 compromised credentials use case.



Credential Abuse Locations

Initial Recon

Initial Compromise

Establish Foothold

Move Laterally Maintain Presence

Escalate Privileges

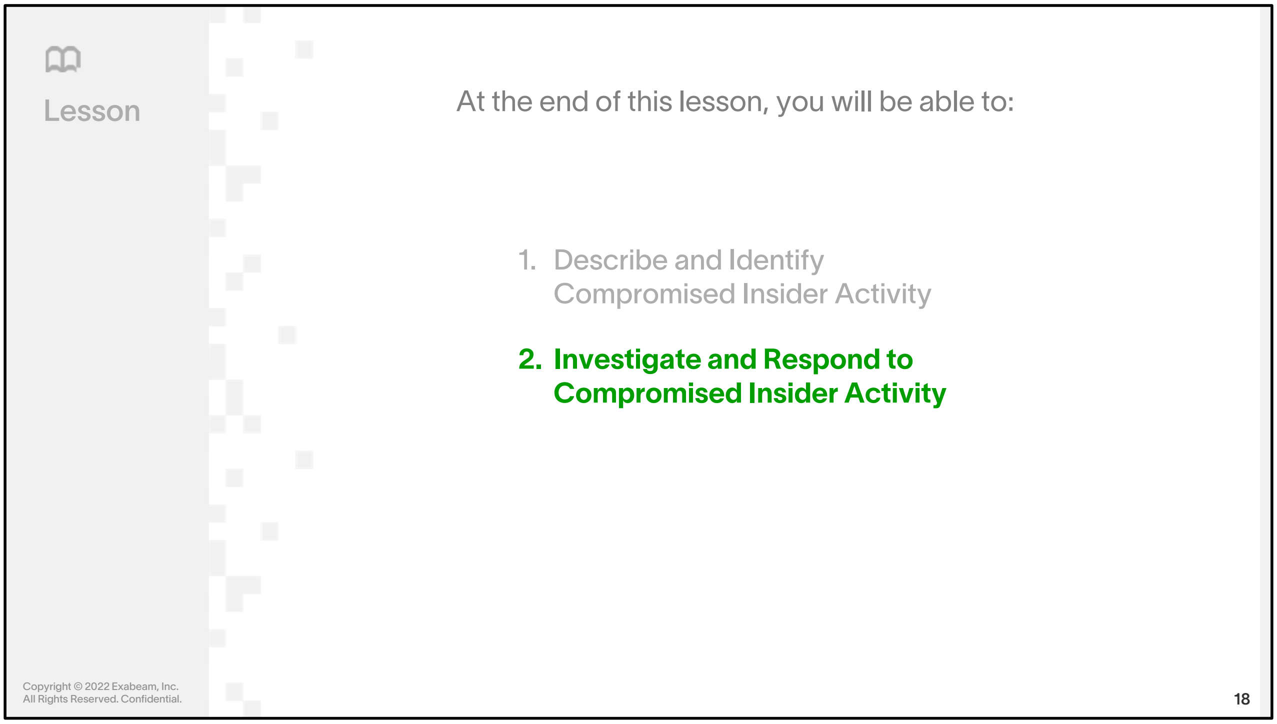
Recon

Complete Mission

Possible Credential Use

Student Notes

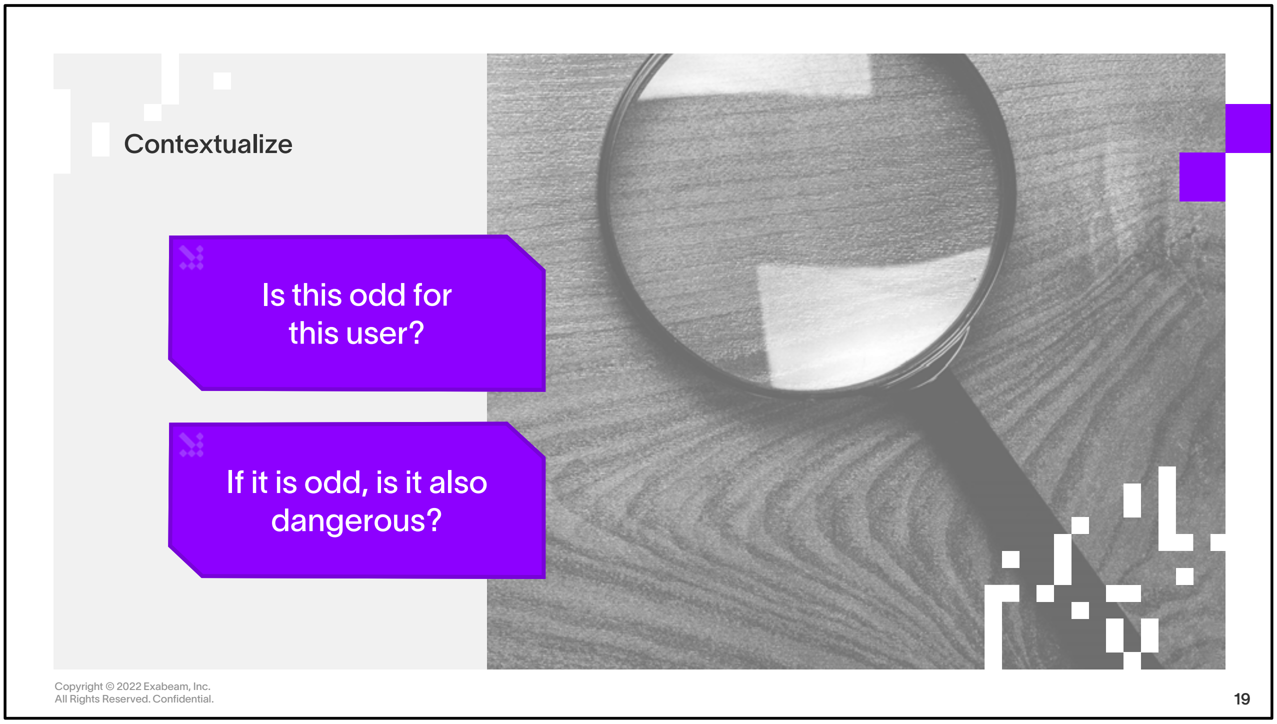
Various techniques can be used in different Attack Chain sequences. It is useful to analyze attacker techniques and tactics on a site like MITRE and to brainstorm various threat hunt searches, watchlists and correlation rules that will help surface suspicious behavior – even if it doesn’t rise to the level of “Notable”.



Lesson

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

1. Describe and Identify Compromised Insider Activity
2. **Investigate and Respond to Compromised Insider Activity**



Contextualize

Is this odd for this user?

If it is odd, is it also dangerous?

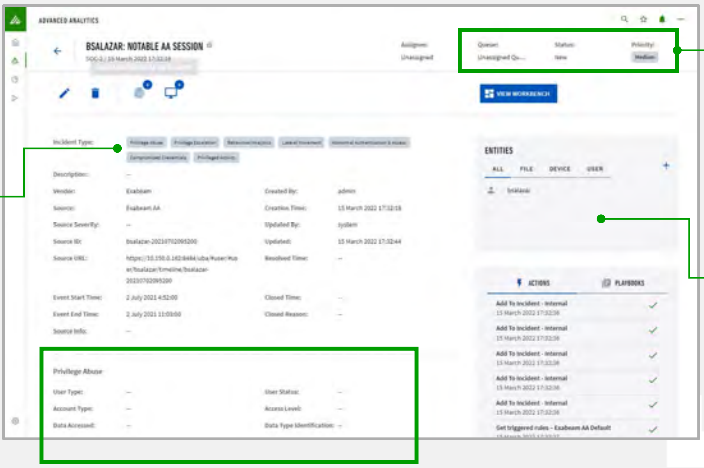
Student Notes

To answer these questions in the Triage and Initial Response phase, we're really going to need solid context.

References

Source: https://community.exabeam.com/s/article/Compromised-Credentials-Use-Case-Chapter-4-Triage#sample_investigation_workflow

Case Manager Incident



ADVANCED ANALYTICS

BSALAZAR: NOTABLE AA SESSION

SOC-2 / 15 March 2022 17:32:18

Assignee:	Queue:	Status:	Priority:
Unassigned	Unassigned Qu...	New	Medium

VIEW WORKBENCH

Incident Type:	Privilege Abuse Privilege Escalation Behavioral Analytics Lateral Movement Abnormal Authentication & Access Compromised Credentials Privileged Activity		
Description:	--		
Vendor:	Exabeam	Created By:	admin
Source:	Exabeam AA	Creation Time:	15 March 2022 17:32:18
Source Severity:	--	Updated By:	system
Source ID:	bsalazar-20210702095200	Updated:	15 March 2022 17:32:44
Source URL:	https://10.150.0.162:8484/uba/#user/#user/bsalazar/timeline/bsalazar-20210702095200	Resolved Time:	--
Event Start Time:	2 July 2021 4:52:00	Closed Time:	--
Event End Time:	2 July 2021 11:03:00	Closed Reason:	--
Source Info:	--		

Privilege Abuse

User Type:	--	User Status:	--
Account Type:	--	Access Level:	--
Data Accessed:	--	Data Type Identification:	--

ENTITIES

ALL FILE DEVICE USER

bsalazar

ACTIONS PLAYBOOKS

- Add To Incident - Internal 15 March 2022 17:32:38 ✓
- Add To Incident - Internal 15 March 2022 17:32:38 ✓
- Add To Incident - Internal 15 March 2022 17:32:38 ✓
- Add To Incident - Internal 15 March 2022 17:32:38 ✓
- Add To Incident - Internal 15 March 2022 17:32:38 ✓
- Get triggered rules - Exabeam AA Default ✓

Status, Assignments, & Priority

Incident Type

Impacted Entities

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

20

Student Notes

We saw in the External Threats module that security alerts for things like phishing, ransomware, malware, and DLP can be processed and prioritized initially through Alert Triage, which potentially includes escalation to the status of “incident.” Other risky activities in your network will surface as notable users and assets in Advanced Analytics. Case Manager will automatically create a corresponding incident for each notable session, populated with details about the event(s) that caused the session to go notable. Triage and initial response

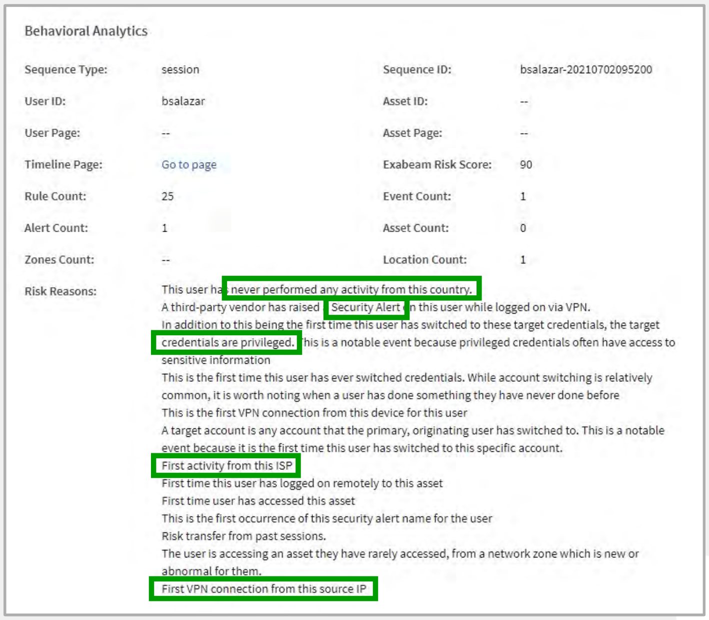
References

Source: https://community.exabeam.com/s/article/Compromised-Credentials-Use-Case-Chapter-5-Investigate

Risk Reasons

Is this odd?

Is it dangerous?



Behavioral Analytics

Sequence Type:	session	Sequence ID:	bsalazar-20210702095200
User ID:	bsalazar	Asset ID:	--
User Page:	--	Asset Page:	--
Timeline Page:	Go to page	Exabeam Risk Score:	90
Rule Count:	25	Event Count:	1
Alert Count:	1	Asset Count:	0
Zones Count:	--	Location Count:	1

Risk Reasons:

This user has never performed any activity from this country.
A third-party vendor has raised a Security Alert on this user while logged on via VPN.
In addition to this being the first time this user has switched to these target credentials, the target credentials are privileged. This is a notable event because privileged credentials often have access to sensitive information
This is the first time this user has ever switched credentials. While account switching is relatively common, it is worth noting when a user has done something they have never done before
This is the first VPN connection from this device for this user
A target account is any account that the primary, originating user has switched to. This is a notable event because it is the first time this user has switched to this specific account.
First activity from this ISP
First time this user has logged on remotely to this asset
First time user has accessed this asset
This is the first occurrence of this security alert name for the user
Risk transfer from past sessions.
The user is accessing an asset they have rarely accessed, from a network zone which is new or abnormal for them.
First VPN connection from this source IP

Student Notes

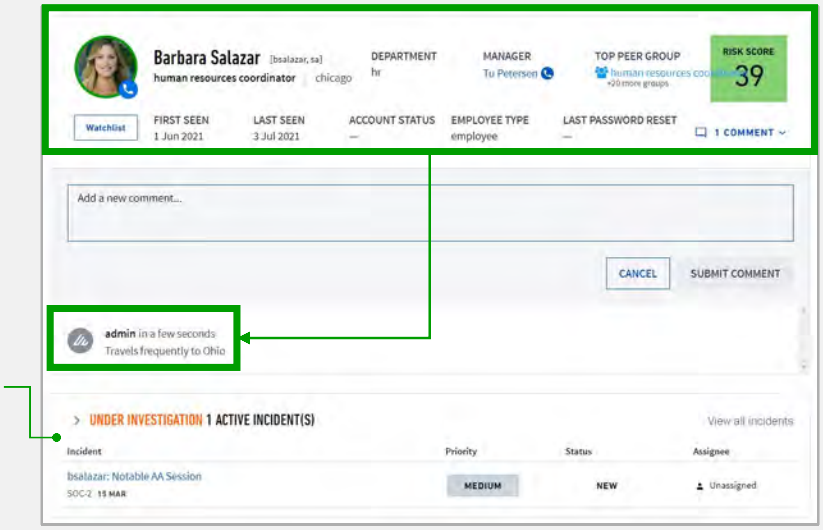
Risk reason inform you with details on *why* a particular event was deemed “risky”. This can lead to faster triage by surfacing at the very least suspicious activity and potentially malicious activity that should be investigated further. Risk reasons can reach a notable or higher status before they even trigger a traditional alert.

References

https://docs.exabeam.com/en/advanced-analytics/i55/advanced-analytics-user-guide/113551-get-to-know-a-user-profile.html#UUID-eb4cb964-5ecd-250a-d911-11fd16f01d9b_section-idm457316332089923166706158037

User Profile Page

Context



Barbara Salazar [bsalazar, sa]
human resources coordinator | chicago

DEPARTMENT: hr

MANAGER: Tu Petersen

TOP PEER GROUP: human resources coo... +20 more groups

RISK SCORE: 39

FIRST SEEN: 1 Jun 2021

LAST SEEN: 3 Jul 2021

ACCOUNT STATUS: —

EMPLOYEE TYPE: employee

LAST PASSWORD RESET: —

admin in a few seconds
Travels frequently to Ohio

UNDER INVESTIGATION 1 ACTIVE INCIDENT(S)

Incident	Priority	Status	Assignee
bsalazar: Notable AA Session SOC-2 15 MAR	MEDIUM	NEW	Unassigned

Active Incidents

Student Notes

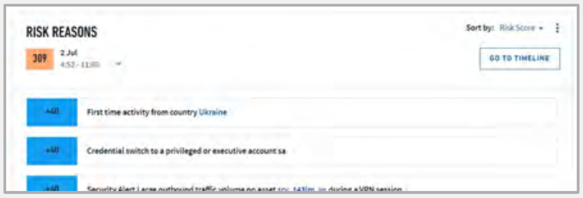
To answer the first question, we need context. Barbara's user profile card tells us that she:

- is a Human Resources Coordinator
- works out of the Chicago office
- reports to Tu Petersen
- has an active account
- is not on any watchlist

Also note the phone icons for both Barbara and her manager, providing quick access to additional contact information like phone numbers and email addresses.

A comment linked to Barbara's account tells us that she "Travels frequently to Ohio," and we see that there is one active incident (the one we began with) associated with her account.

Risk Reasons & Data Insights



RISK REASONS

Sort by: Risk Score

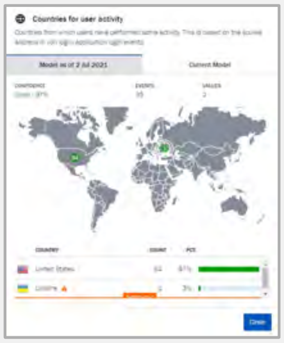
309 2 Jul 4:52 - 11:00

GO TO TIMELINE

+40 First time activity from country Ukraine

+40 Credential switch to a privileged or executive account sa

+40 Security Alert Large outbound traffic volume on asset 143lm during a VPN session



Countries for user activity

Model as of 2 Jul 2021

Current Model

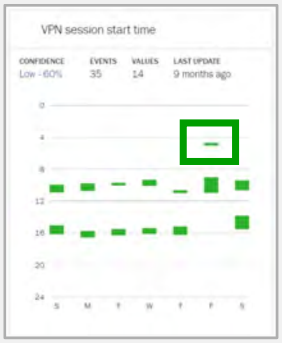
COUNTRY	COUNT	PCT
United States		
Ukraine		3%

Close

Student Notes

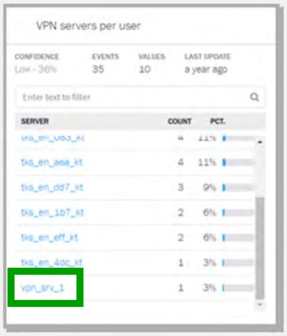
Both Risk Reasons and Data Insights can provide quick context during triage and initial response, and they can be utilized for more detailed investigation when it’s called for. Barbara’s top risk reason in her notable session is “First time activity from country Ukraine.” The VPN Countries histogram for Barbara shows that she has never logged on to the VPN from anywhere but the United States.

More VPN Data Insights



VPN session start time

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Low - 60%	35	14	9 months ago

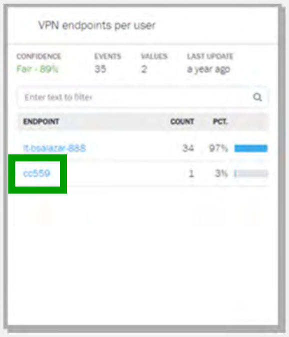


VPN servers per user

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Low - 36%	35	10	a year ago

Enter text to filter

SERVER	COUNT	PCT.
tks_en_[illegible]_kt	4	11%
tks_en_aea_kt	4	11%
tks_en_dd7_kt	3	9%
tks_en_1b7_kt	2	6%
tks_en_eff_kt	2	6%
tks_en_4dc_kt	1	3%
vpn_srv_1	1	3%



VPN endpoints per user

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Fair - 89%	35	2	a year ago

Enter text to filter

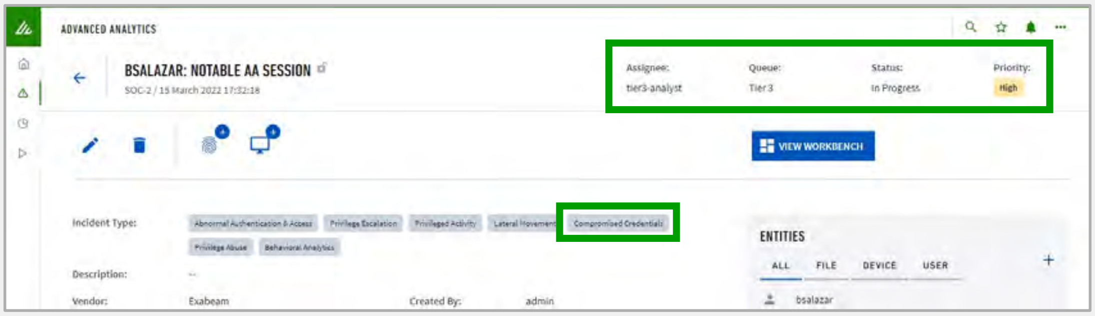
ENDPOINT	COUNT	PCT.
lt-bsalazar-888	34	97%
cc559	1	3%

Student Notes

Looking further at the VPN insights for Barbara’s account, we see an odd logon on a Thursday that doesn’t align with Barbara’s usual session times. Her VPN servers follow a tks_en_…_kt naming protocol. We know this to be the protocol used by our company. There is, however, one variation at the bottom: one logon is from vpn_srv_1 which we don’t recognize. Also worth noting is that Barbara always logs on to the VPN from her laptop, lt-bsalazar-888, except for one time, when her account used a host called cc559.

We’ve established clearly, just from a look at one set of insights, that this is definitely odd behavior from Barbara’s account. We give her manager, Tu Peterson, a quick call to determine whether Barbara might be working on vacation or traveling to some other destination. We can find the contact information listed for Tu by clicking on the phone next to her name in Barbara’s profile. Tu assures us on the phone that Barbara should be in Chicago and that this behavior was indeed very odd.

Update the Incident



BSALAZAR: NOTABLE AA SESSION
SOC-2 / 15 March 2022 17:32:18

Assignee: tier3-analyst
Queue: Tier 3
Status: In Progress
Priority: High

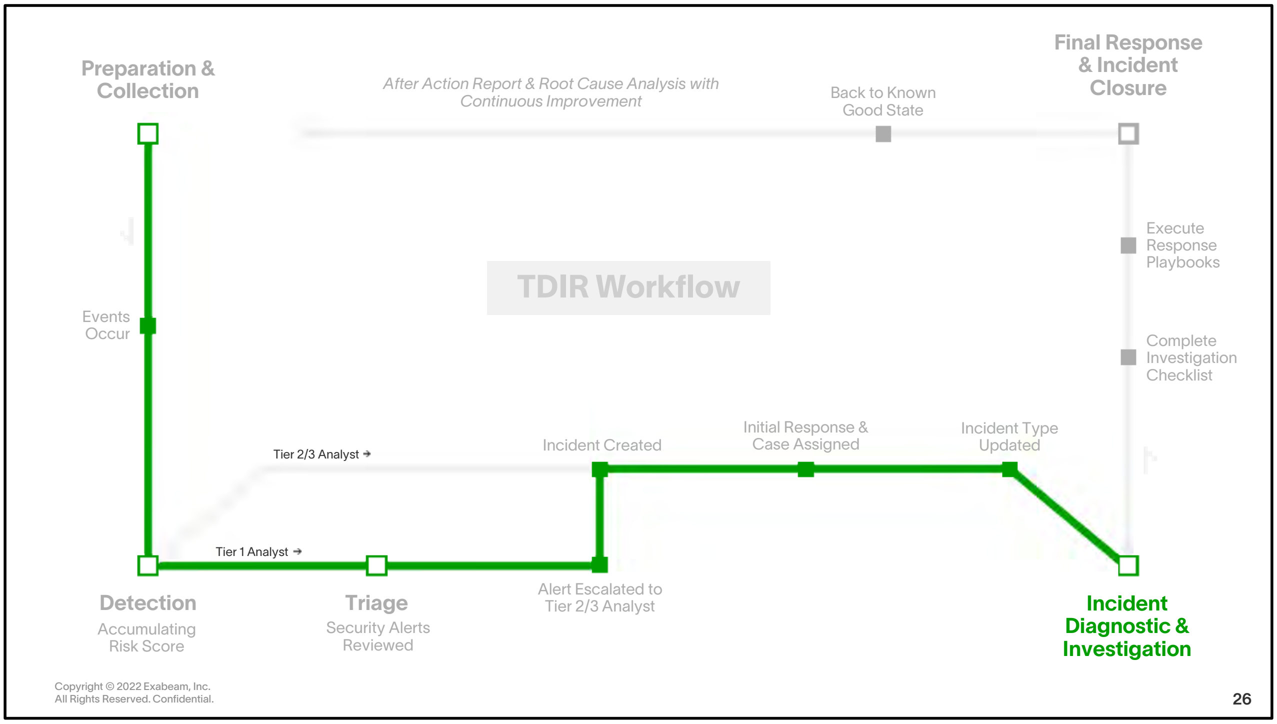
Incident Type: Abnormal Authentication & Access, Privilege Escalation, Privileged Activity, Lateral Movement, Compromised Credentials, Privilege Abuse, Behavioral Analytics
Description: --
Vendor: Exabeam
Created By: admin

bsalazar

Student Notes

At this point we might make a quick call to our Windows Security Team and give them advance notice that an incident that requires a response is likely coming their way and that they should be prepared to lock Barbara’s access down. We may have further accounts to lock down, but Barbara’s is going to be the first. Alternatively, we may make use of an Incident Responder playbook to help automate the process.

Returning to Case Manager, we have enough information to assign and escalate the incident. Assigning the “Compromised Credentials” incident type will add prescribed checklist tasks for the analyst to work through.



TDIR Workflow

Preparation & Collection

After Action Report & Root Cause Analysis with Continuous Improvement

Back to Known Good State

Final Response & Incident Closure

Execute Response Playbooks

Complete Investigation Checklist

Events Occur

Tier 2/3 Analyst →

Incident Created

Initial Response & Case Assigned

Incident Type Updated

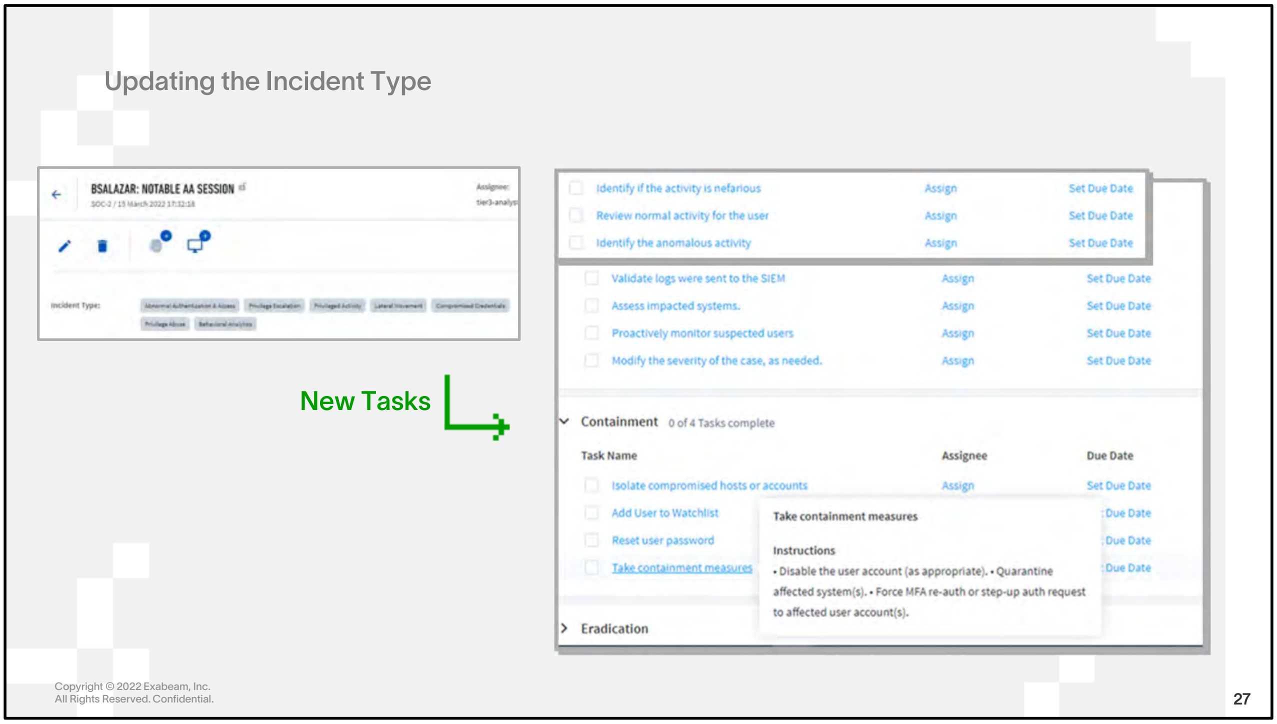
Tier 1 Analyst →

Detection
Accumulating Risk Score

Triage
Security Alerts Reviewed

Alert Escalated to Tier 2/3 Analyst

Incident Diagnostic & Investigation



Updating the Incident Type

BSALAZAR: NOTABLE AA SESSION
SOC-2 / 15 March 2022 17:32:18
Assignee:
tier3-analys

Incident Type: Abnormal Authentication & Access, Privilege Escalation, Privileged Activity, Lateral Movement, Compromised Credentials, Privilege Abuse, Behavioral Analytics

New Tasks

□ Identify if the activity is nefarious	Assign	Set Due Date
□ Review normal activity for the user	Assign	Set Due Date
□ Identify the anomalous activity	Assign	Set Due Date
□ Validate logs were sent to the SIEM	Assign	Set Due Date
□ Assess impacted systems.	Assign	Set Due Date
□ Proactively monitor suspected users	Assign	Set Due Date
□ Modify the severity of the case, as needed.	Assign	Set Due Date

Containment 0 of 4 Tasks complete

Task Name	Assignee	Due Date
□ Isolate compromised hosts or accounts	Assign	Set Due Date
□ Add User to Watchlist		Due Date
□ Reset user password		Due Date
□ Take containment measures		Due Date

Take containment measures

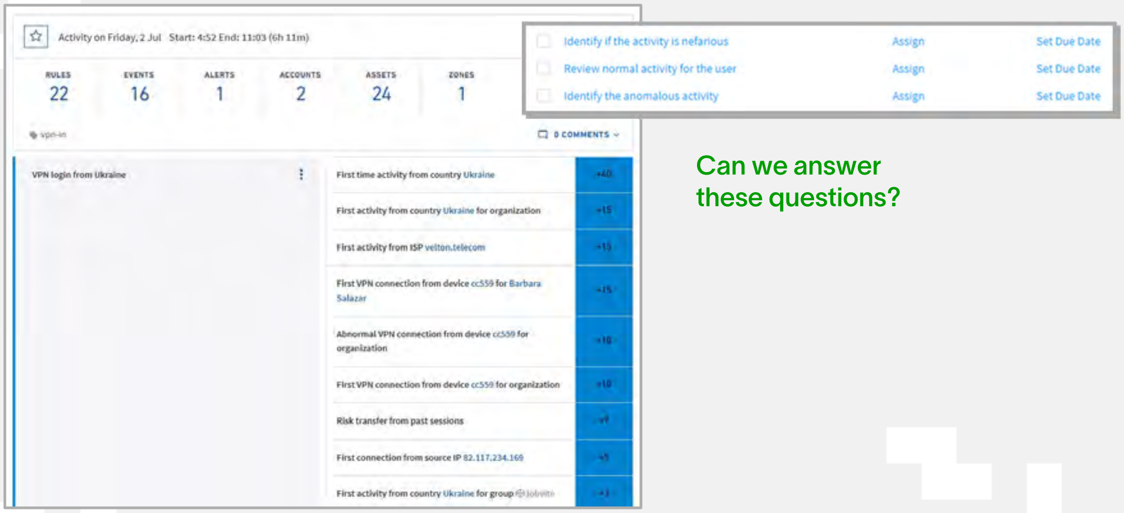
Instructions
• Disable the user account (as appropriate). • Quarantine affected system(s). • Force MFA re-auth or step-up auth request to affected user account(s).

Eradication

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.

Updating the Incident Type



Activity on Friday, 2 Jul Start: 4:52 End: 11:03 (6h 11m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES
22	16	1	2	24	1

vpn-in

0 COMMENTS

VPN login from Ukraine

First time activity from country Ukraine	+40
First activity from country Ukraine for organization	+15
First activity from ISP velton.telecom	+15
First VPN connection from device cc559 for Barbara Salazar	+15
Abnormal VPN connection from device cc559 for organization	+10
First VPN connection from device cc559 for organization	+10
Risk transfer from past sessions	+7
First connection from source IP 82.117.234.169	+5
First activity from country Ukraine for group Jobvite	+3

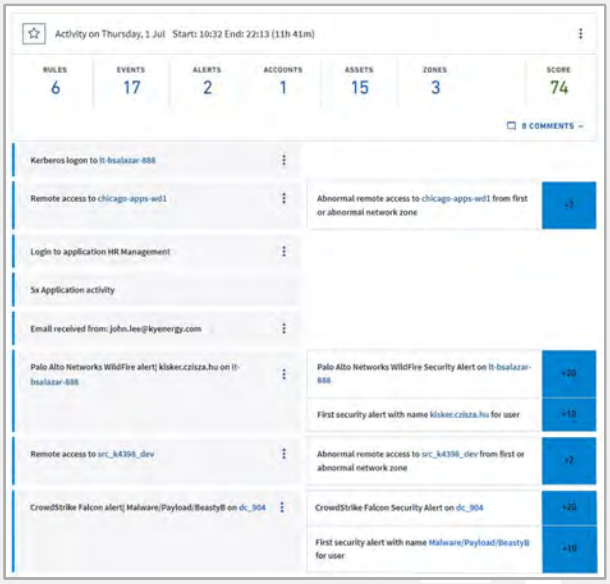
□ Identify if the activity is nefarious	Assign	Set Due Date
□ Review normal activity for the user	Assign	Set Due Date
□ Identify the anomalous activity	Assign	Set Due Date

Can we answer these questions?

Backing Up in the Timeline

Phishing(?)

Compromised Credentials



Activity on Thursday, 1 Jul Start: 10:32 End: 22:13 (11h 41m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
6	17	2	1	15	3	74

0 COMMENTS

Kerberos logon to lt-bsalazar-888		
Remote access to chicago-apps-wd1	Abnormal remote access to chicago-apps-wd1 from first or abnormal network zone	+7
Login to application HR Management		
5x Application activity		
Email received from: john.lee@kyenergy.com		
Palo Alto Networks WildFire alert| kisker.czisza.hu on lt-bsalazar-888	Palo Alto Networks WildFire Security Alert on lt-bsalazar-888	+20
	First security alert with name kisker.czisza.hu for user	+10
Remote access to src_k4398_dev	Abnormal remote access to src_k4398_dev from first or abnormal network zone	+7
CrowdStrike Falcon alert| Malware/Payload/BeastyB on dc_904	CrowdStrike Falcon Security Alert on dc_904	+20
	First security alert with name Malware/Payload/BeastyB for user	+10

Student Notes

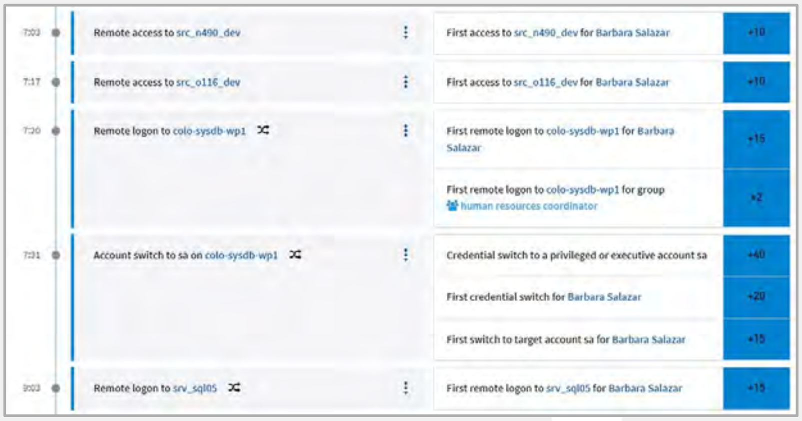
Although Barbara's session the previous day never quite reached notable status, there's some peculiar activity leading up to her notable session. She received an email containing a payroll.zip attachment which, interestingly, didn't get flagged right away. But shortly after, a Palo Alto alert fires on Barbara's laptop, and a Crowdstrike alert is triggered after that.

Further Investigation

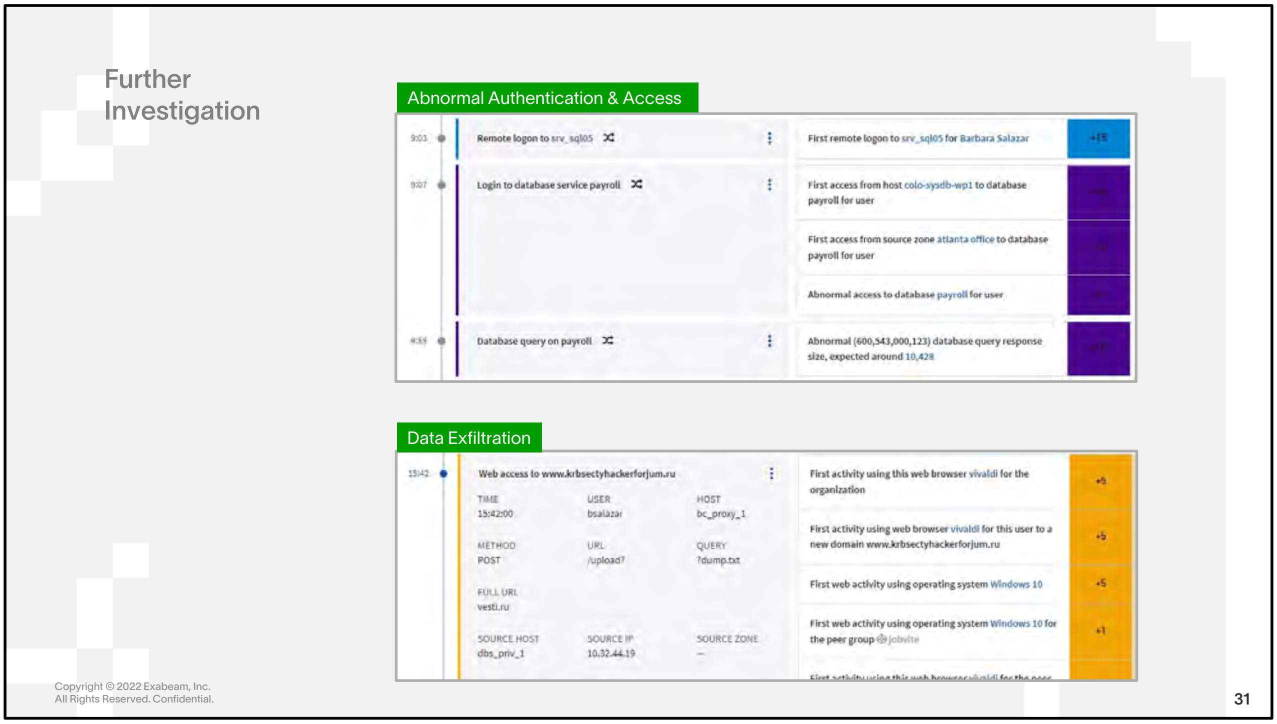
Abnormal Authentication & Access

Privilege Escalation

Lateral Movement



7:03	Remote access to src_n490_dev	First access to src_n490_dev for Barbara Salazar	+10
7:17	Remote access to src_o116_dev	First access to src_o116_dev for Barbara Salazar	+10
7:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+15
		First remote logon to colo-sysdb-wp1 for group human resources coordinator	+2
7:31	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa	+40
		First credential switch for Barbara Salazar	+20
		First switch to target account sa for Barbara Salazar	+15
9:03	Remote logon to srv_sql05	First remote logon to srv_sql05 for Barbara Salazar	+15



Further Investigation

Abnormal Authentication & Access

9:03 Remote logon to srv_sql05

First remote logon to srv_sql05 for Barbara Salazar +15

9:07 Login to database service payroll

First access from host colo-sysdb-wp1 to database payroll for user

First access from source zone atlanta office to database payroll for user

Abnormal access to database payroll for user

9:55 Database query on payroll

Abnormal (600,543,000,123) database query response size, expected around 10,428

Data Exfiltration

15:42 Web access to www.krbsectyhackerforjum.ru

TIME	USER	HOST
15:42:00	bsalazar	bc_proxy_1
METHOD	**URL**	**QUERY**
POST	/upload?	?dump.txt
FULL URL		
vesti.ru		
SOURCE HOST	**SOURCE IP**	**SOURCE ZONE**
dbs_priv_1	10.32.44.19	–

First activity using this web browser vivaldi for the organization +5

First activity using web browser vivaldi for this user to a new domain www.krbsectyhackerforjum.ru +5

First web activity using operating system Windows 10 +5

First web activity using operating system Windows 10 for the peer group jobvite +1

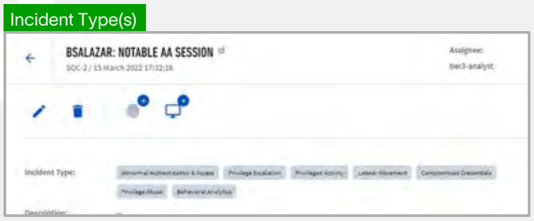
First activity using this web browser vivaldi for the peer

Student Notes

Digging into anomaly details on the user timeline can also reveal more data insights – and lead to ancillary investigations – as well as MITRE tags/rules to build further searches from.

Update Incident

Incident Type(s)



BSALAZAR: NOTABLE AA SESSION

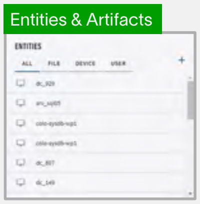
SOC-2 / 15 March 2022 17:32:18

Assignee: tier3-analyst

Incident Type: Abnormal Authentication & Access, Privilege Escalation, Privileged Activity, Lateral Movement, Compromised Credentials, Privilege Abuse, Behavioral Analytics

Description:

Entities & Artifacts

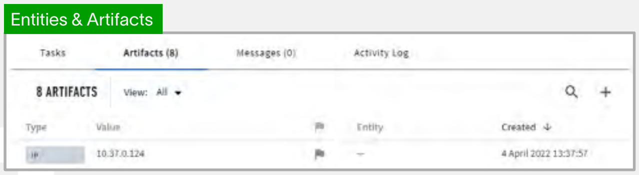


ENTITIES

ALL FILE DEVICE USER

- dc_929
- arc_sql05
- colo-sysdb-sql1
- colo-sysdb-sql1
- dc_807
- dc_149

Entities & Artifacts

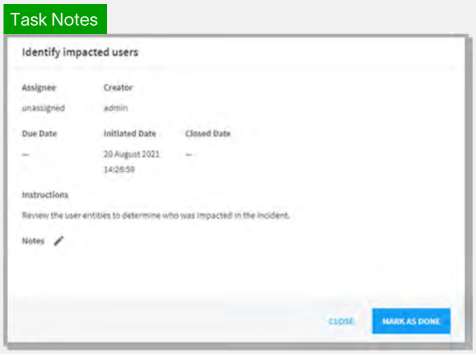


Tasks | Artifacts (8) | Messages (0) | Activity Log

8 ARTIFACTS View: All

Type	Value		Entity	Created
IP	10.37.0.124		--	4 April 2022 13:37:57

Task Notes



Identify impacted users

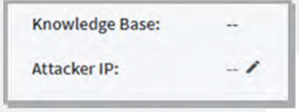
Assignee	Creator	
unassigned	admin	
Due Date	**Initiated Date**	**Closed Date**
--	20 August 2021 14:26:59	--

Instructions

Review the user entities to determine who was impacted in the incident.

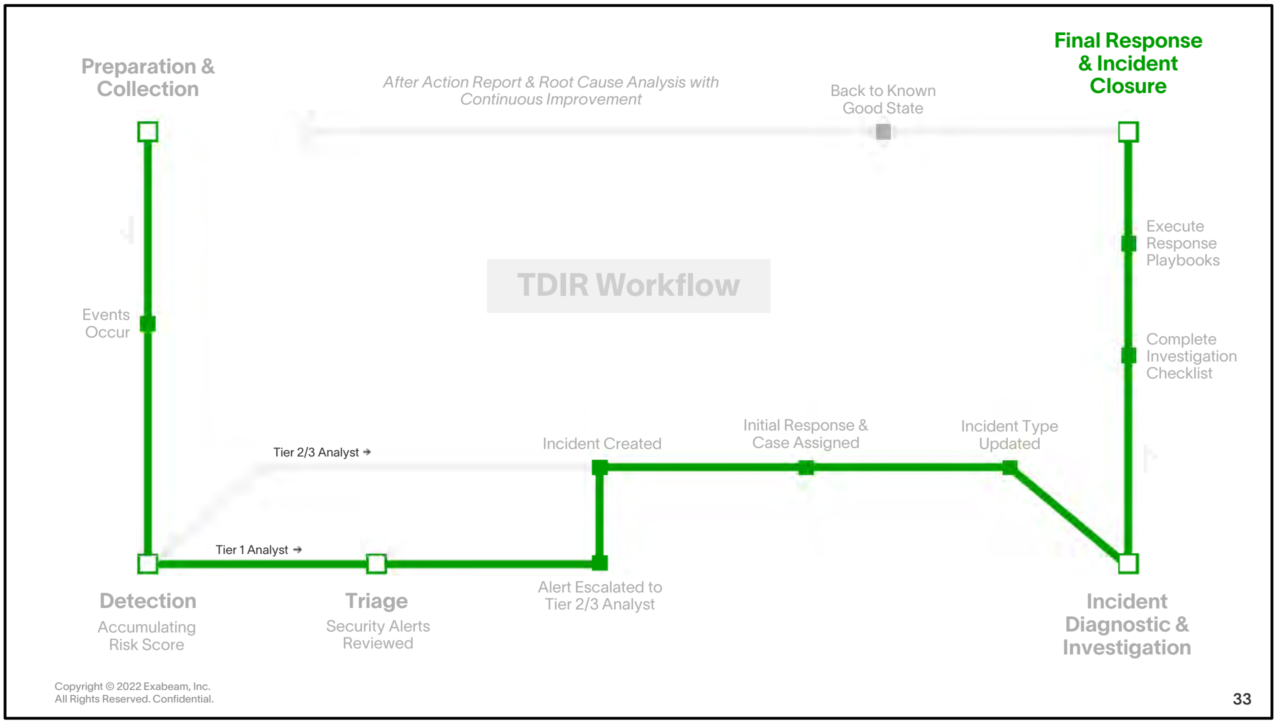
Notes

Incident Fields

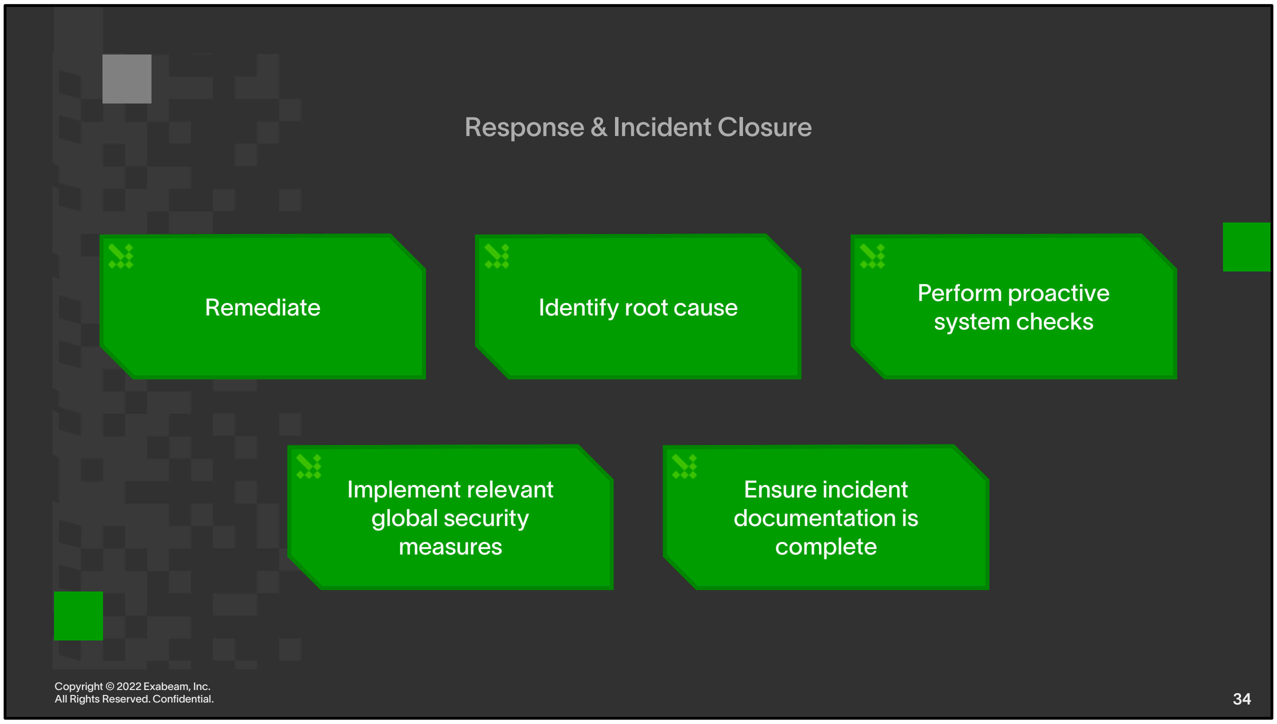


Knowledge Base: --

Attacker IP: --



TDIR Workflow
Preparation & Collection
After Action Report & Root Cause Analysis with Continuous Improvement
Back to Known Good State
Final Response & Incident Closure
Execute Response Playbooks
Complete Investigation Checklist
Events Occur
Tier 2/3 Analyst →
Incident Created
Initial Response & Case Assigned
Incident Type Updated
Tier 1 Analyst →
Detection
Accumulating Risk Score
Triage
Security Alerts Reviewed
Alert Escalated to Tier 2/3 Analyst
Incident Diagnostic & Investigation



Response & Incident Closure

Remediate

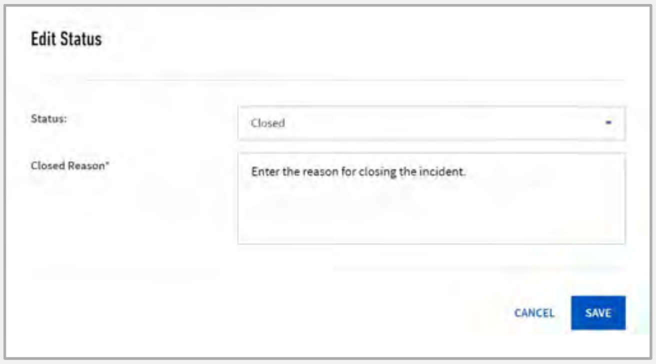
Identify root cause

Perform proactive system checks

Implement relevant global security measures

Ensure incident documentation is complete

Closing the Incident

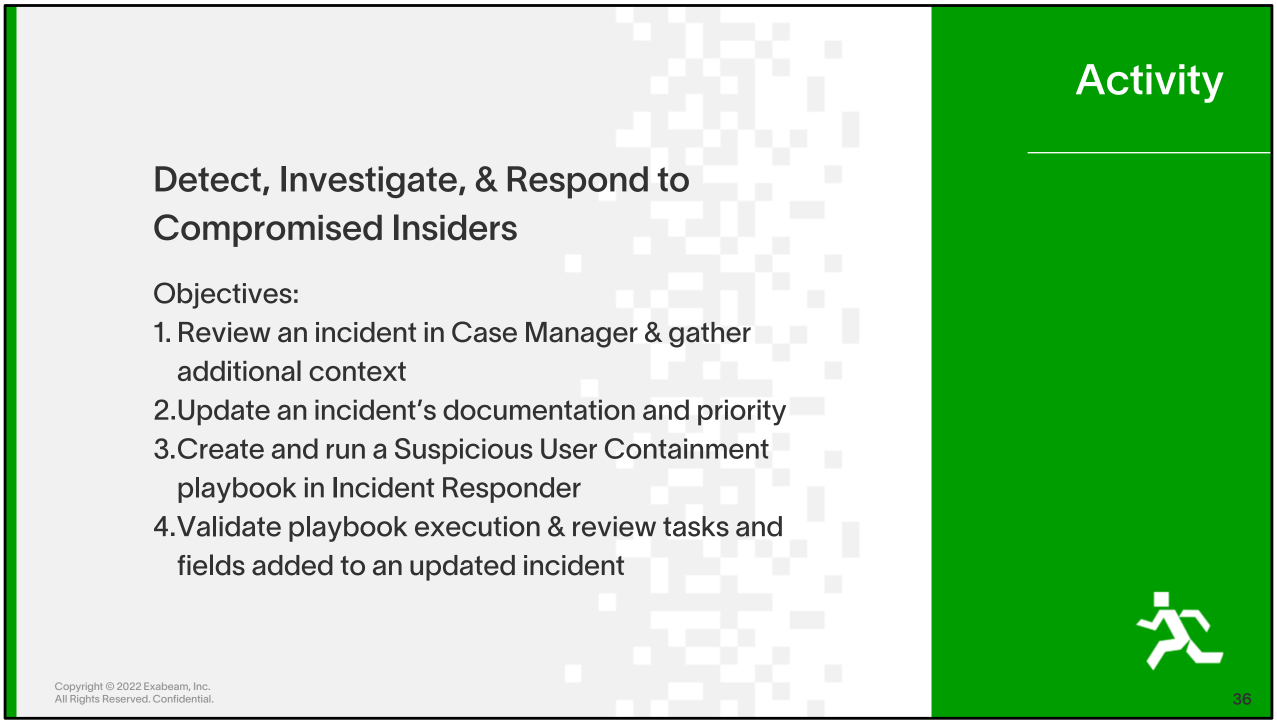


Edit Status

Status: Closed

Closed Reason* Enter the reason for closing the incident.

Student Notes
A closed incident is not deleted from Case Manager, although closed incidents do not appear in the list by default unless you modify the filter to display them. As a best practice, never delete an incident from Case Manager as a means of "closing" the incident. Deleting will remove all incident data, including entities, artifacts, comments, and action/playbook results.



Activity

Detect, Investigate, & Respond to Compromised Insiders

Objectives:

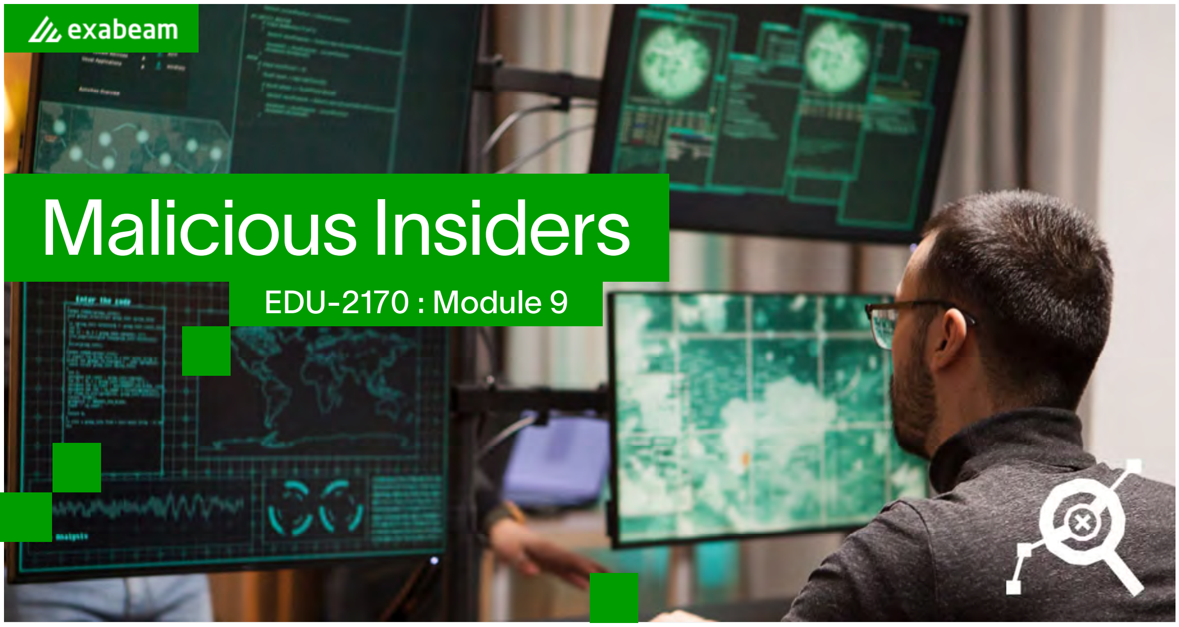
1. Review an incident in Case Manager & gather additional context
2. Update an incident’s documentation and priority
3. Create and run a Suspicious User Containment playbook in Incident Responder
4. Validate playbook execution & review tasks and fields added to an updated incident

Summary

Can You Do the Following?

1. Describe and Identify Compromised Insider Activity
2. Investigate and Respond to Compromised Insider Activity

v4.00



Malicious Insiders

EDU-2170 : Module 9

What motivates a malicious insider?

Student Notes

According to the CERT Insider Threat Center, the four most common types of insider threats, in order of prevalence, are the following:

- Fraud
- Theft of Intellectual Property
- IT Sabotage
- Misuse

CERT defines fraud as “a malicious insider’s use of IT for the unauthorized modification, addition, or deletion of an organization’s data (not programs or systems) for personal gain or the theft of information leading to an identity crime.“ The victim in fraud cases is most often the organization itself, followed by consumers/customers of the company. The information assets most commonly targeted in cases of fraud are, in order:

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Payment Card Information (PCI)
- Federal Tax Information (FTI)

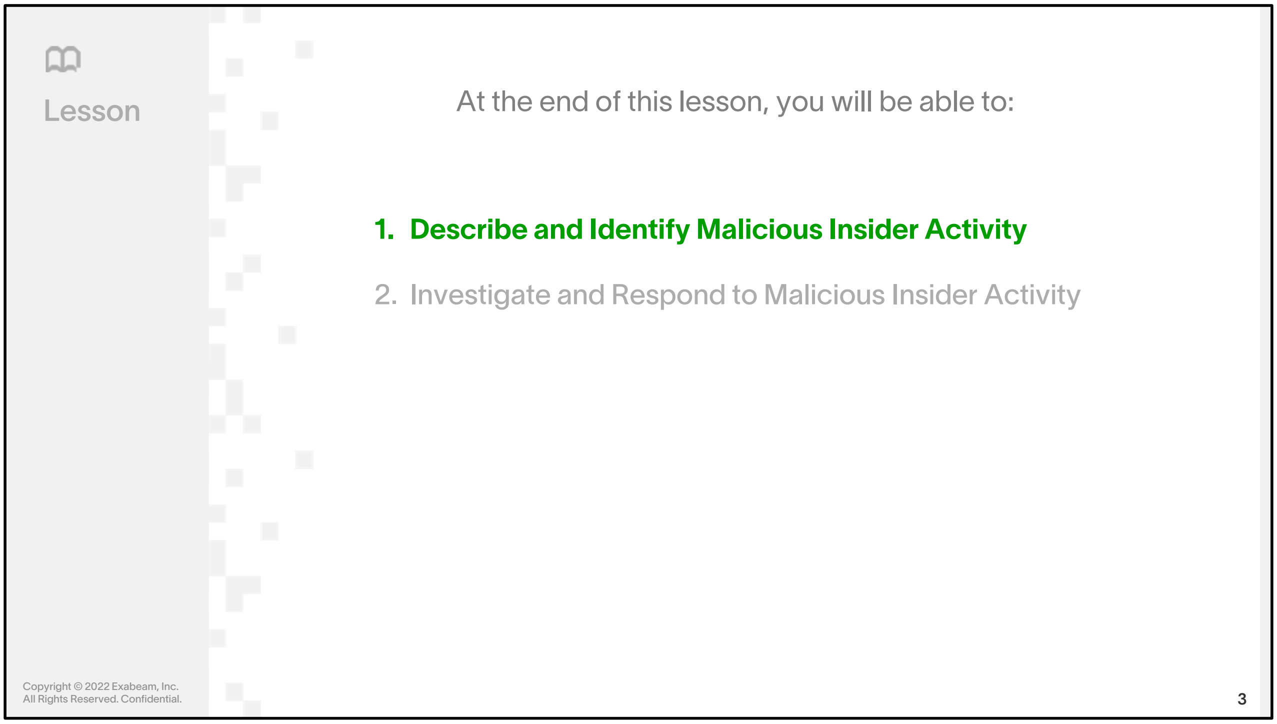
They further define an identity crime as “the misuse of personal or financial identifiers in order to gain something of value and/or facilitate some other criminal activity.”

The most targeted devices for fraud within organizations are, in order:

- Database servers
- Organization desktops
- Other
- File Servers

References

Assets Targeted by Malicious Insiders: https://insights.sei.cmu.edu/blog/insider-threat-incidents-assets-targeted-by-malicious-insiders/
Malicious Insider Fraud: https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf
https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/
https://www.cisa.gov/defining-insider-threats



Lesson

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

1. **Describe and Identify Malicious Insider Activity**
2. Investigate and Respond to Malicious Insider Activity

Malicious Insider

Intentional sabotage or data theft by an employee, contractor or partner for either personal reasons or financial gain

Student Notes

Here’s a sobering statistic: Accenture’s Cost of Cyber Security 2019 Report finds the “cost of malicious insider attacks has increased by 15 percent over the year and is now an average of **US$1.6 million annually for an organization**.”

The Federal Cybersecurity And Infrastructure Security Agency defines Insider Threats thusly:

An **Insider threat** is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. External stakeholders and customers of DHS may find this generic definition better suited and adaptable for their organization’s use.

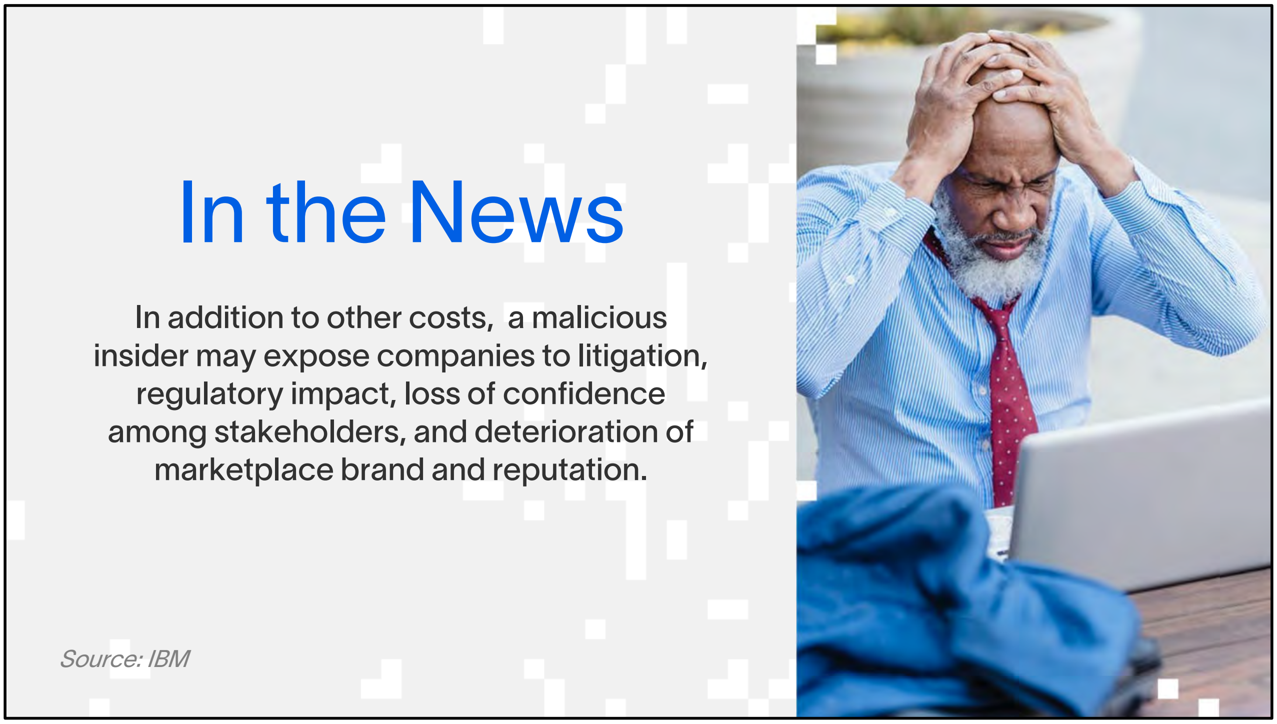
The Cyber and Infrastructure Security Agency (CISA) defines insider threat as the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department’s mission, resources, personnel, facilities, information, equipment, networks, or systems. This threat can manifest as damage to the Department through the following insider behaviors:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Intentional or unintentional loss or degradation of departmental resources or capabilities

References

https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

https://www.cisa.gov/defining-insider-threats



In the News

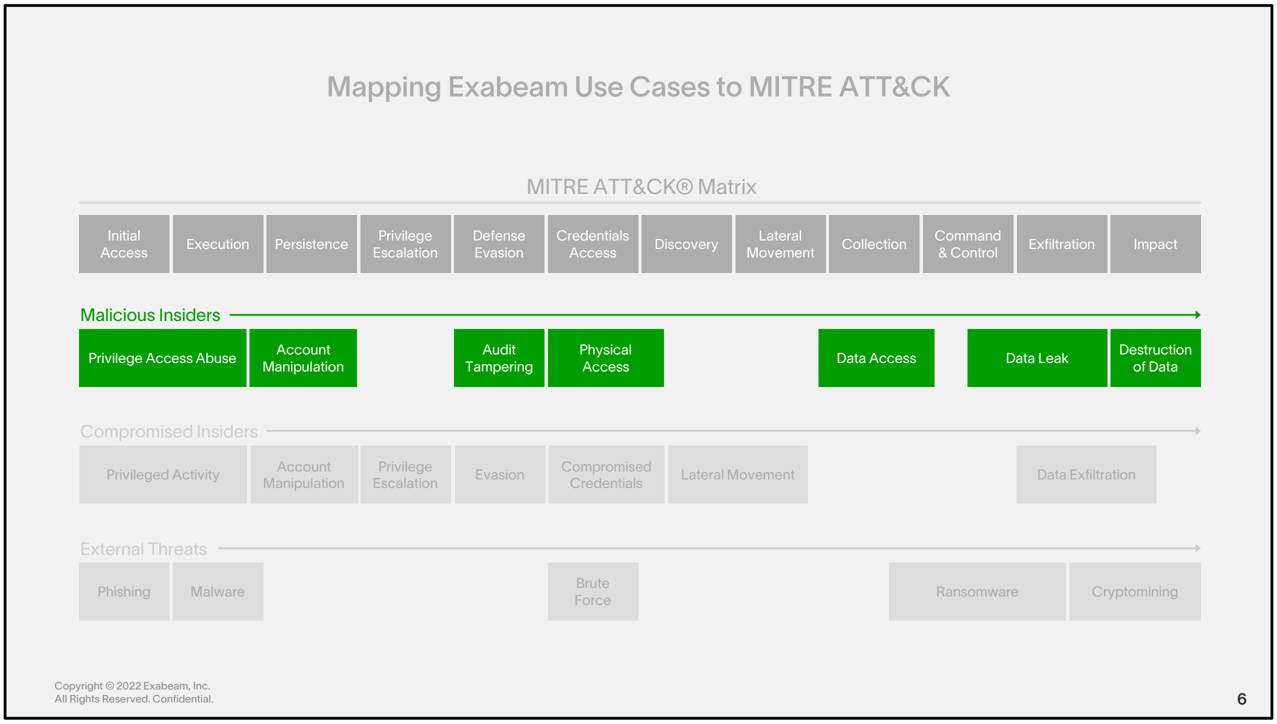
In addition to other costs, a malicious insider may expose companies to litigation, regulatory impact, loss of confidence among stakeholders, and deterioration of marketplace brand and reputation.

Source: IBM

Student Notes
What are some examples of malicious insiders from the news? These types of intrusions can lead to unexpected costs. In addition to other costs, a malicious insider may expose companies to litigation, regulatory impact, loss of confidence among stakeholders, and deterioration of marketplace brand and reputation.

Source
https://www.ibm.com/downloads/cas/LQZ4RONE

Photo by Nicola Barts



Mapping Exabeam Use Cases to MITRE ATT&CK

MITRE ATT&CK® Matrix

Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credentials Access | Discovery | Lateral Movement | Collection | Command & Control | Exfiltration | Impact

Malicious Insiders

Privilege Access Abuse | Account Manipulation | Audit Tampering | Physical Access | Data Access | Data Leak | Destruction of Data

Compromised Insiders

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

External Threats

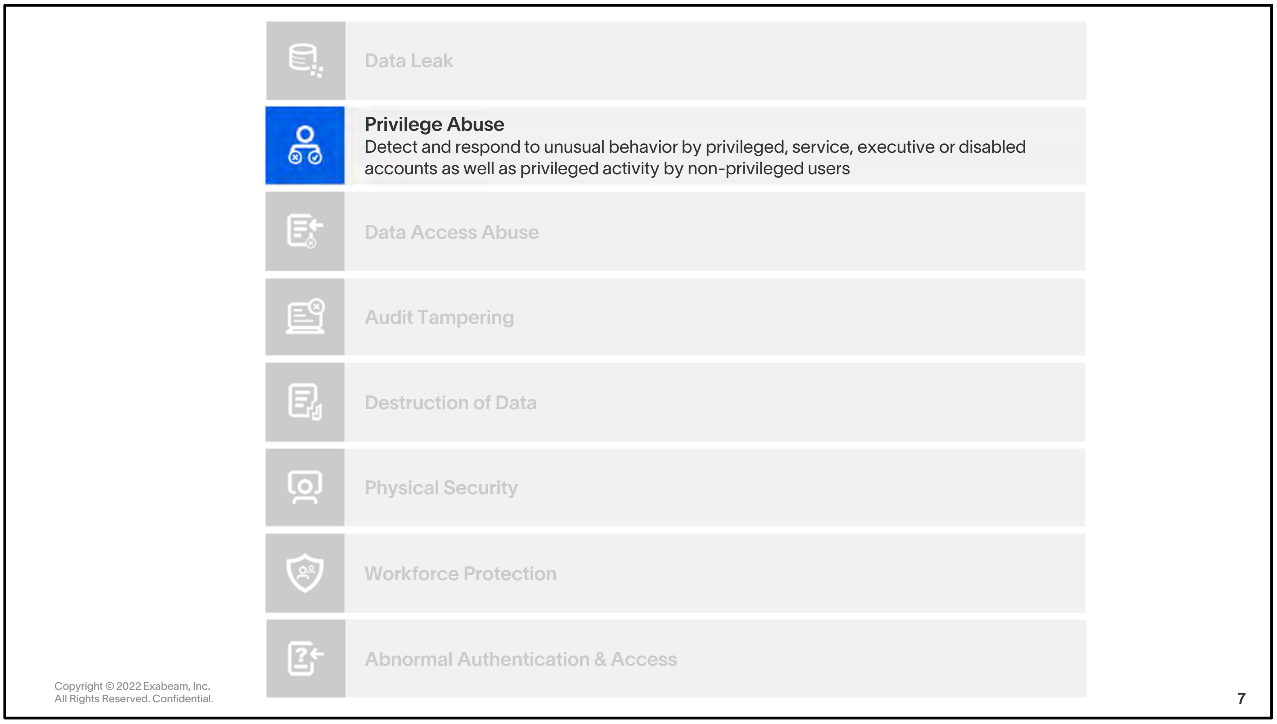
Phishing | Malware | Brute Force | Ransomware | Cryptomining

Student Notes

Exabeam is continually mapping MITRE TTPs to Exabeam Use Cases like Malicious Insiders.

References

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



Data Leak

Privilege Abuse
Detect and respond to unusual behavior by privileged, service, executive or disabled accounts as well as privileged activity by non-privileged users

Data Access Abuse

Audit Tampering

Destruction of Data

Physical Security

Workforce Protection

Abnormal Authentication & Access

Student Notes
The Malicious Insider use case category currently includes the following eight use cases:

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

As an example, the **privilege abuse** use case will be explored in some detail in the next few slides.

This pattern is an uncomfortable one—this is where people we trust betray us.

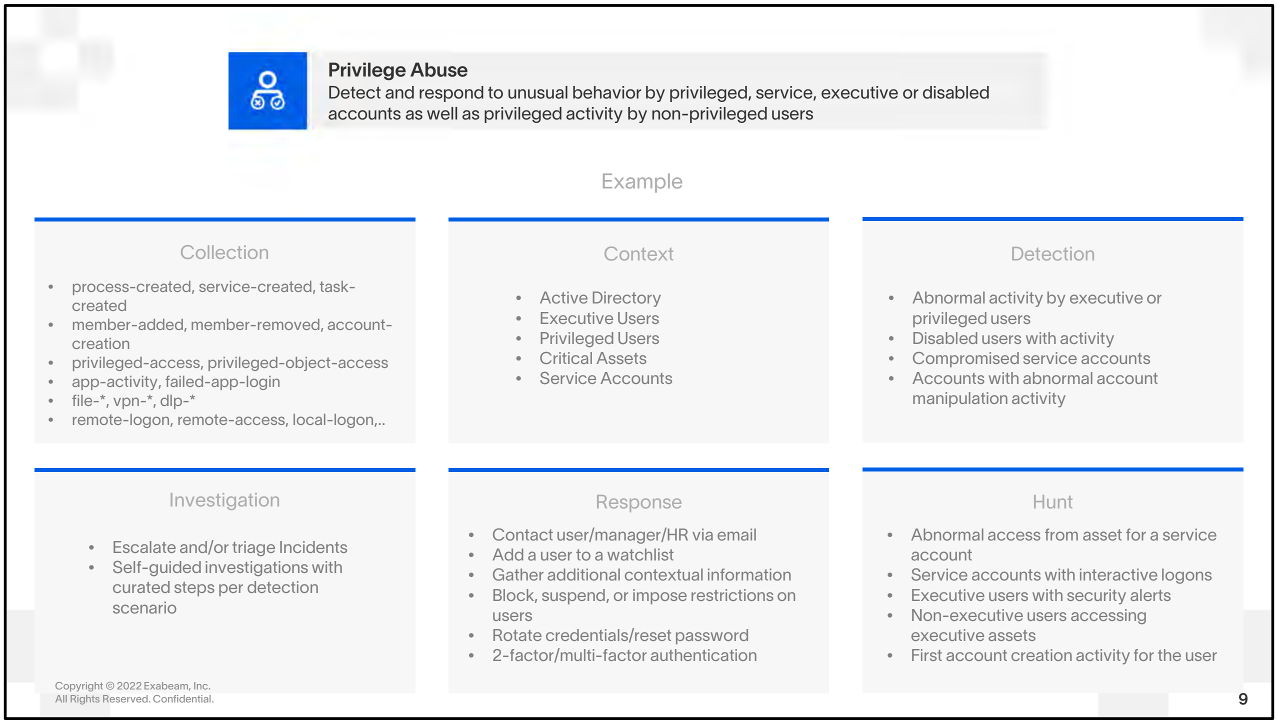
Verizon DBIR 2021

Student Notes

According to Verizon’s 2021 Data Breach Investigations Report, privilege abuse is by far the most common variety of privilege misuse. The majority of threat actors are financially motivated and most commonly target personal information. Attacks are almost exclusively perpetrated by internal actors (as opposed to partners, for example).

References

https://www.verizon.com/business/resources/reports/dbir/
https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50



Privilege Abuse

Detect and respond to unusual behavior by privileged, service, executive or disabled accounts as well as privileged activity by non-privileged users

Example

Collection

- process-created, service-created, task-created
- member-added, member-removed, account-creation
- privileged-access, privileged-object-access
- app-activity, failed-app-login
- file-*, vpn-*, dlp-*
- remote-logon, remote-access, local-logon,..

Context

- Active Directory
- Executive Users
- Privileged Users
- Critical Assets
- Service Accounts

Detection

- Abnormal activity by executive or privileged users
- Disabled users with activity
- Compromised service accounts
- Accounts with abnormal account manipulation activity

Investigation

- Escalate and/or triage Incidents
- Self-guided investigations with curated steps per detection scenario

Response

- Contact user/manager/HR via email
- Add a user to a watchlist
- Gather additional contextual information
- Block, suspend, or impose restrictions on users
- Rotate credentials/reset password
- 2-factor/multi-factor authentication

Hunt

- Abnormal access from asset for a service account
- Service accounts with interactive logons
- Executive users with security alerts
- Non-executive users accessing executive assets
- First account creation activity for the user

Student Notes

The Exabeam SecOps platform maps content and tools to the Threat Detection, Investigation, and Response workflow on a per use case basis, providing prescriptive guidance and tooling for end-to-end TDIR.

Collection: these are the event types created from parsed logs for the Privilege Abuse use case. Log sources to include are:

- Application Activity/Cloud Application Activity
- Database Activity Monitoring (DAM)
- VPN/Zero Trust Network Access
- Authentication and Access Management
- Privileged Access Management (PAM)

Note that Data Lake supports over 500 data source integrations out of the box, as well as Cloud Connectors.

- Context: we'll highlight more on context for Privilege Abuse on an upcoming slide
- Detection: Rule types for detecting Privilege Abuse
- Investigation: note that Data Lake requires Fusion SIEM
- Response: Incidents that are classified in Case Manager will include additional prescriptive investigation and response tasks. Turnkey playbooks provide configureless, out-of-the-box SOAR functionality to automate much of the process.
- Hunt: Threat Hunter queries will be added to the customer's environment by Professional Services (Deployment Services) based on entitlements.

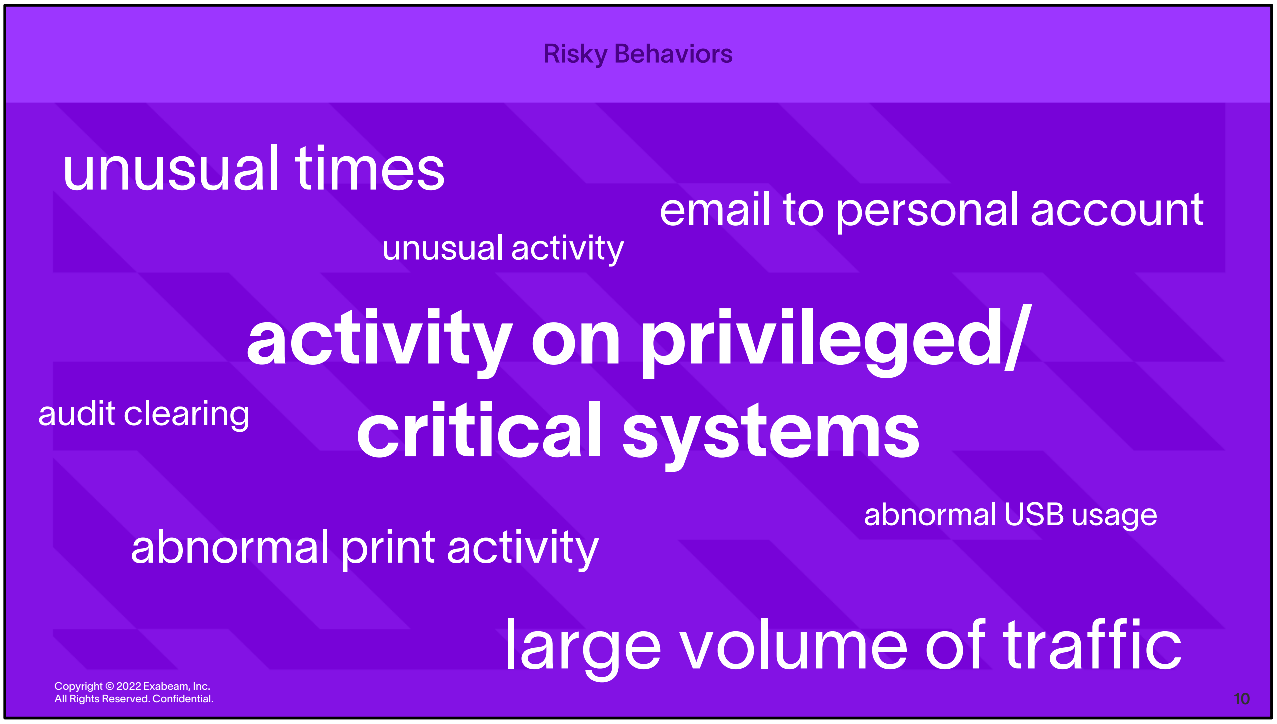
Data sources supporting the Privilege Abuse use case include:

- Application Activity/Cloud Application Activity
- Database Activity Monitoring (DAM)
- VPN/Zero Trust Network Access
- Authentication and Access Management
- Privileged Access Management (PAM)

It’s important to note that not all of these data sources are necessary to train the Privilege Abuse use case models, and many of these sources overlap with other use cases.

References

https://community.exabeam.com/s/article/Privilege-Escalation-Use-Case-Chapter-1-Introduction
https://community.exabeam.com/s/article/Privileged-Activity-Use-Case-Chapter-1-Introduction



Risky Behaviors

unusual times

email to personal account

unusual activity

activity on privileged/ critical systems

audit clearing

abnormal USB usage

abnormal print activity

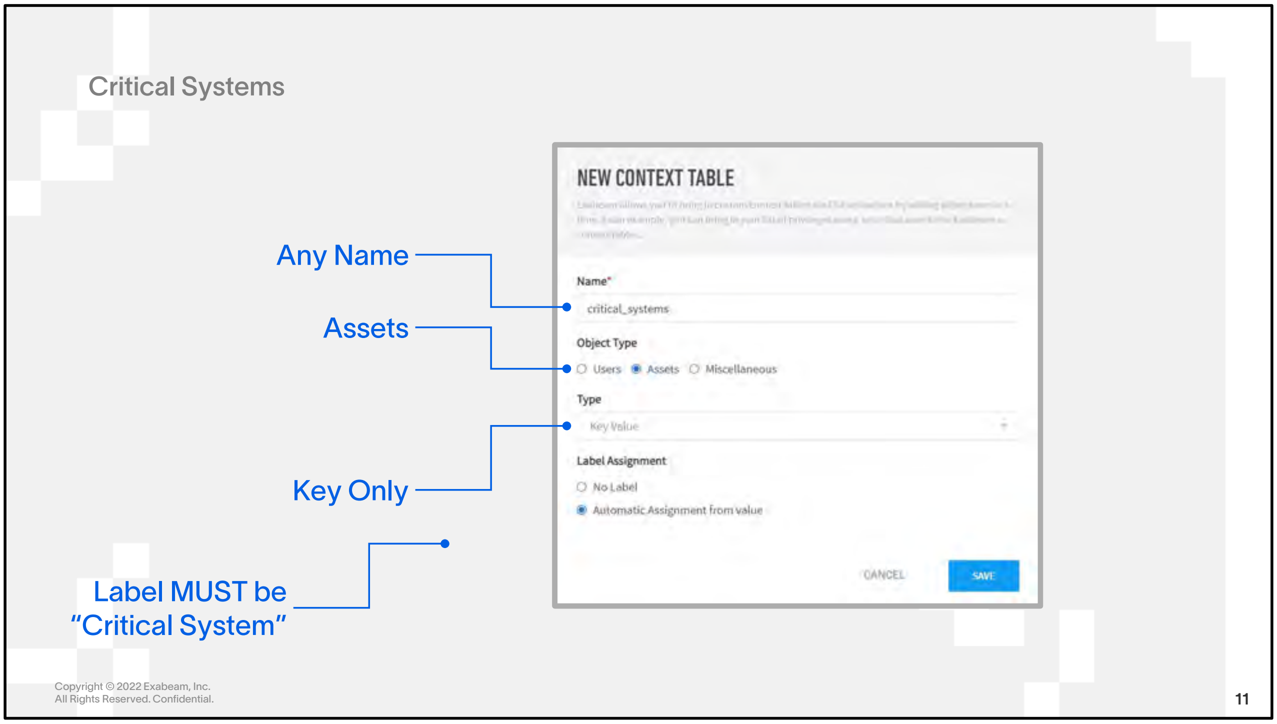
large volume of traffic

Student Notes

Incidents involving privilege abuse tend to take much longer to detect, investigate, and resolve than other incidents. Exabeam reduces the noise and volume of false positives for an analyst to triage by only alerting on abnormal access, rather than flagging each time a user accesses a database or server, for example. The Exabeam SecOps platform provide real-time analysis and reporting on abnormal data access attempts across the environment, allowing insider threat programs to become more proactive by identifying anomalous behavior in the ways users access data they have the permissions to access before exfiltration is attempted.

References

CERT Insider Threat Center: https://www.sei.cmu.edu/our-work/insider-threat/index.cfm
https://www.verizon.com/business/resources/reports/dbir/



Critical Systems

NEW CONTEXT TABLE

[illegible]

Name*

critical_systems

Object Type

○ Users ● Assets ○ Miscellaneous

Type

Key Value

Label Assignment

○ No Label

● Automatic Assignment from value

Any Name

Assets

Key Only

Label MUST be "Critical System"

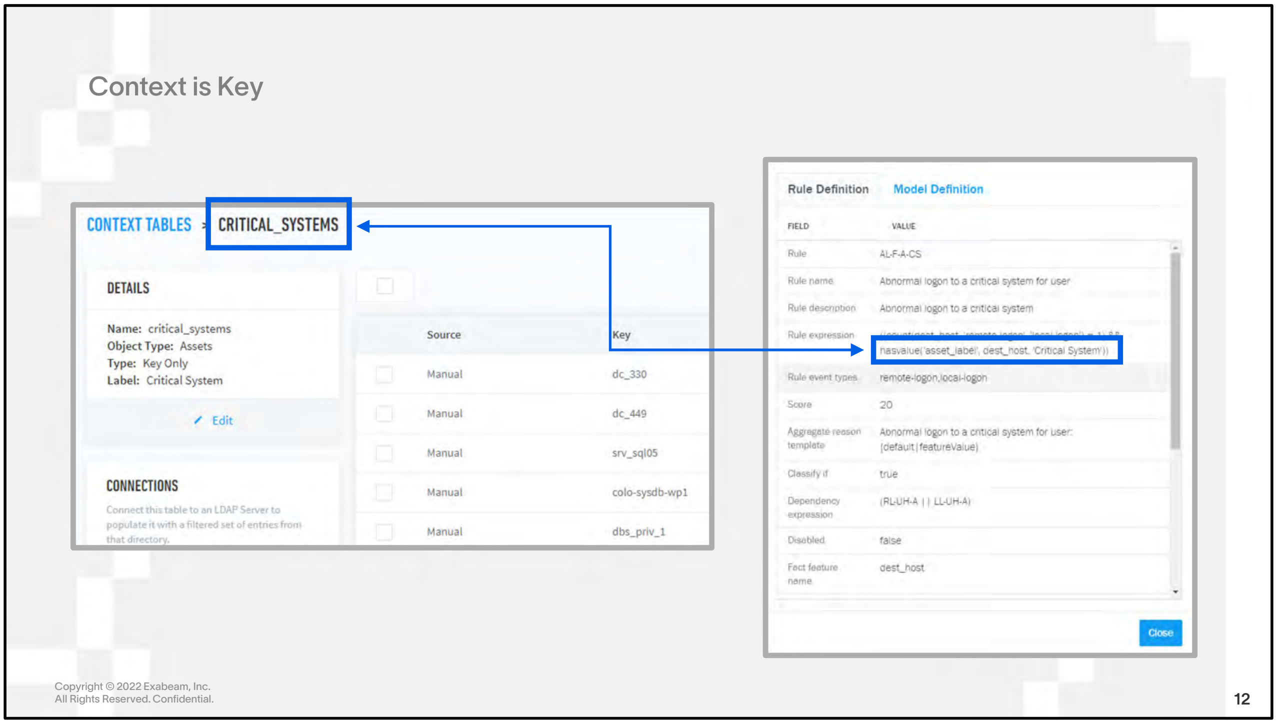
11

Student Notes

The critical systems context table enriches your logs by identifying those assets of most value to your organization, your "crown jewels." Although the critical systems context table should have been created for you, it's not built in, and you should verify that it exists and that it is up to date.

References

https://community.exabeam.com/s/article/Create-a-Context-Table-and-Watchlist-for-Critical-Systems
https://community.exabeam.com/s/article/Exabeam-Directory-Services
https://community.exabeam.com/s/article/Critical-System-Activity-222412731



Context is Key

CONTEXT TABLES > CRITICAL_SYSTEMS

DETAILS

Name: critical_systems
Object Type: Assets
Type: Key Only
Label: Critical System

CONNECTIONS

Connect this table to an LDAP Server to populate it with a filtered set of entries from that directory.

	Source	Key
□	Manual	dc_330
□	Manual	dc_449
□	Manual	srv_sql05
□	Manual	colo-sysdb-wp1
□	Manual	dbs_priv_1

FIELD	VALUE
Rule	AL-F-A-CS
Rule name	Abnormal logon to a critical system for user
Rule description	Abnormal logon to a critical system
Rule expression	((count(dest_host, 'remote-logon', 'local-logon') = 1) && hasvalue('asset_label', dest_host, 'Critical System'))
Rule event types	remote-logon,local-logon
Score	20
Aggregate reason template	Abnormal logon to a critical system for user: {default|featureValue}
Classify if	true
Dependency expression	(RL-UH-A || LL-UH-A)
Disabled	false
Fact feature name	dest_host

Student Notes

Logs tell Exabeam what the users and entities are doing while context tells us who the users and entities are. Context sources enrich the logs to help with the anomaly detection process and can be also be used directly by the risk engine layer for fact-based rules. Many rules, like the one shown above, use the context tables to allocate additional risk to critical systems. Users with an assigned role that allows them to edit rule scores can customize rule scores directly in the Advanced Analytics user interface to meet their organization's security needs. You can also create custom context and/or custom rules to meet your organization’s unique requirements.

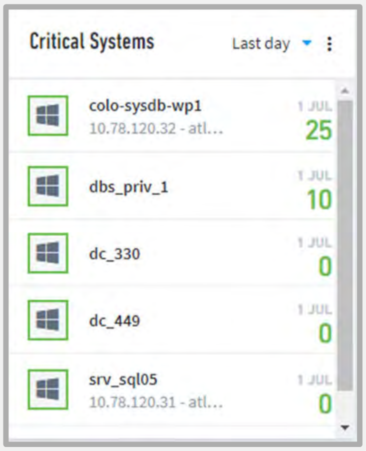
The Privilege Abuse use case leverages the following context tables:

- user_account
- user_is_executive
- Network Zones
- user_is_privileged
- is_ad_user
- Critical Systems (custom)

References

https://docs.exabeam.com/en/advanced-analytics/i57/advanced-analytics-administration-guide/127369-advanced-analytics.html
Adjusting a rule’s score: https://community.exabeam.com/s/article/Advanced-Analytics-Top-Tip-Reducing-a-Rule-s-Score

Watchlists Help Identity the Highest Risk



Critical Systems

Last day

colo-sysdb-wp1 10.78.120.32 - atl…	1 JUL 25
dbs_priv_1	1 JUL 10
dc_330	1 JUL 0
dc_449	1 JUL 0
srv_sql05 10.78.120.31 - atl…	1 JUL 0

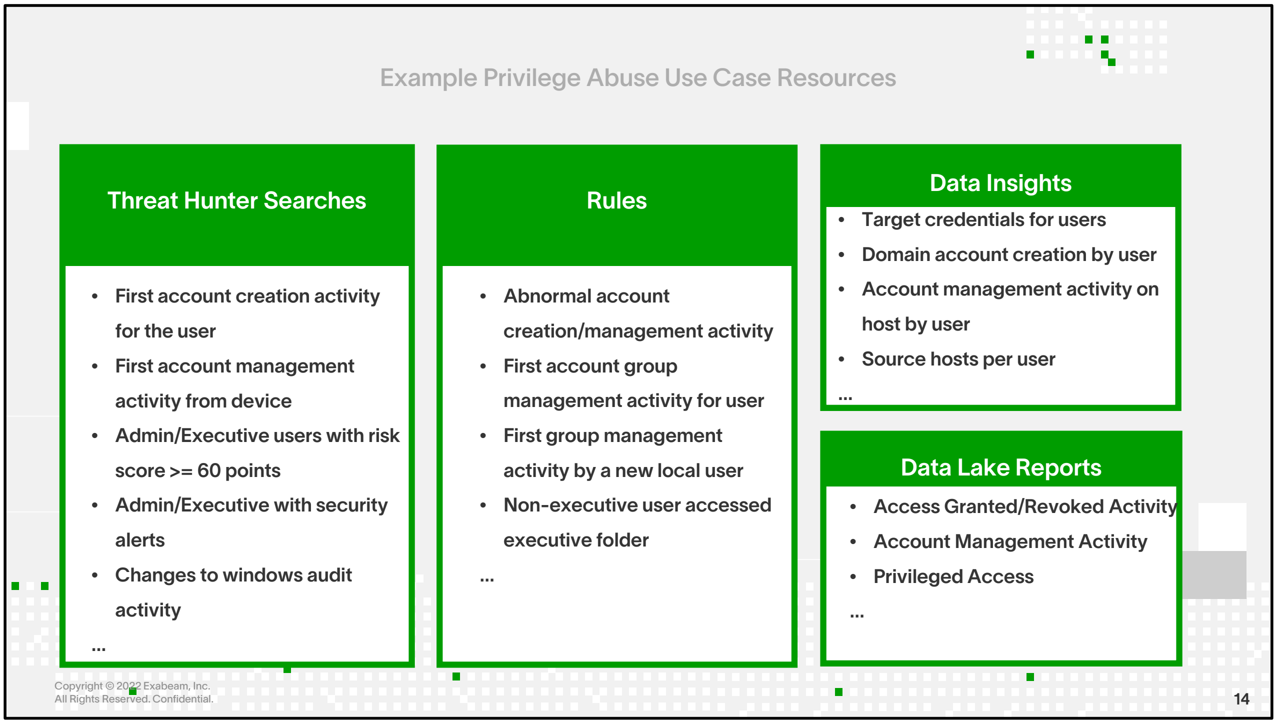
Student Notes

Within Advanced Analytics, you can create watchlists using context tables. When creating the table, the Label attribute allows you to attach tags to records that match entries in your context table. This provides quick access to query your results and/or focus your tracking using a global characteristic.

Users and assets added to a watchlist are prominently surfaced on the Advanced Analytics homepage. Custom context tables allow you the flexibility to create watchlists or reference lists for assets, threat intelligence indicators, and users/groups that do not fit in the typical deployment categories. Custom context tables let you put parts of your organization under extra monitoring or special scrutiny, such as financial servers, privileged insiders, and high-level departed employees.

References

https://community.exabeam.com/s/article/Create-Use-Case-Specific-Watchlists



Example Privilege Abuse Use Case Resources

Threat Hunter Searches

- First account creation activity for the user
- First account management activity from device
- Admin/Executive users with risk score >= 60 points
- Admin/Executive with security alerts
- Changes to windows audit activity

…

Rules

- Abnormal account creation/management activity
- First account group management activity for user
- First group management activity by a new local user
- Non-executive user accessed executive folder

…

Data Insights

- Target credentials for users
- Domain account creation by user
- Account management activity on host by user
- Source hosts per user

…

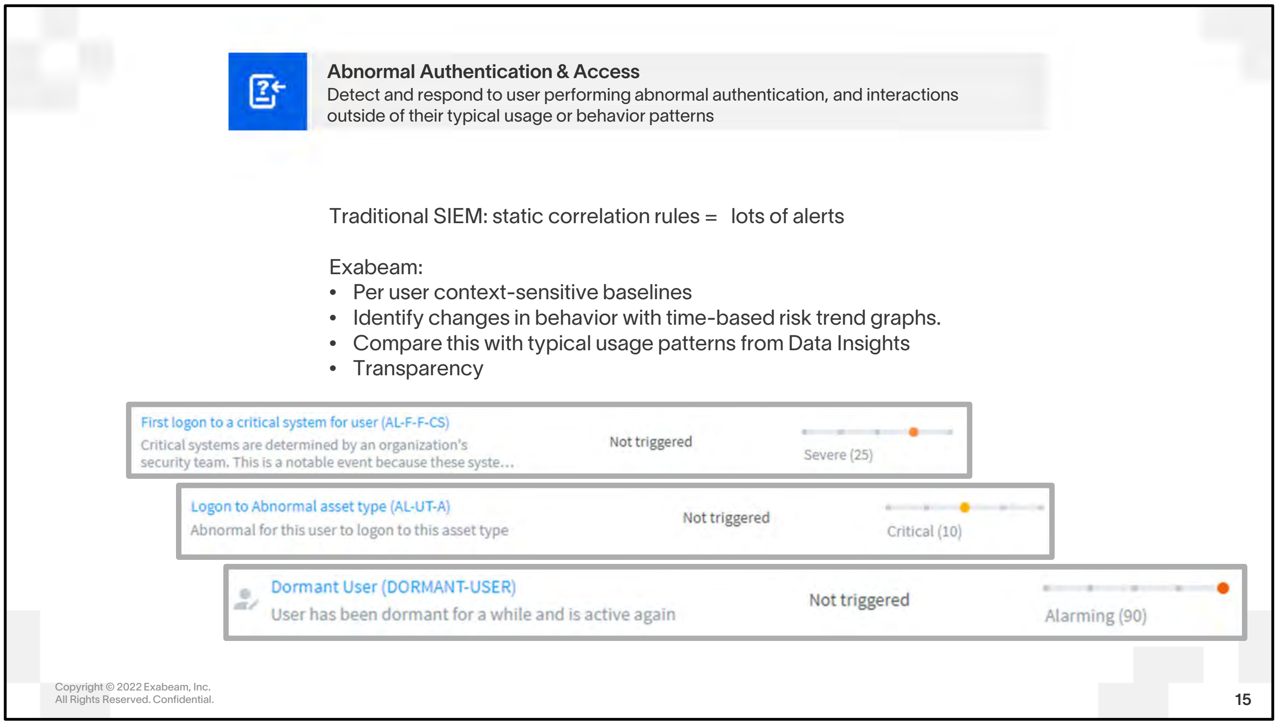
Data Lake Reports

- Access Granted/Revoked Activity
- Account Management Activity
- Privileged Access

…

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 privilege abuse use case.



Abnormal Authentication & Access
Detect and respond to user performing abnormal authentication, and interactions outside of their typical usage or behavior patterns

Traditional SIEM: static correlation rules = lots of alerts

Exabeam:
- Per user context-sensitive baselines
- Identify changes in behavior with time-based risk trend graphs.
- Compare this with typical usage patterns from Data Insights
- Transparency

First logon to a critical system for user (AL-F-F-CS) Critical systems are determined by an organization's security team. This is a notable event because these syste…	Not triggered	Severe (25)
Logon to Abnormal asset type (AL-UT-A) Abnormal for this user to logon to this asset type	Not triggered	Critical (10)
Dormant User (DORMANT-USER) User has been dormant for a while and is active again	Not triggered	Alarming (90)

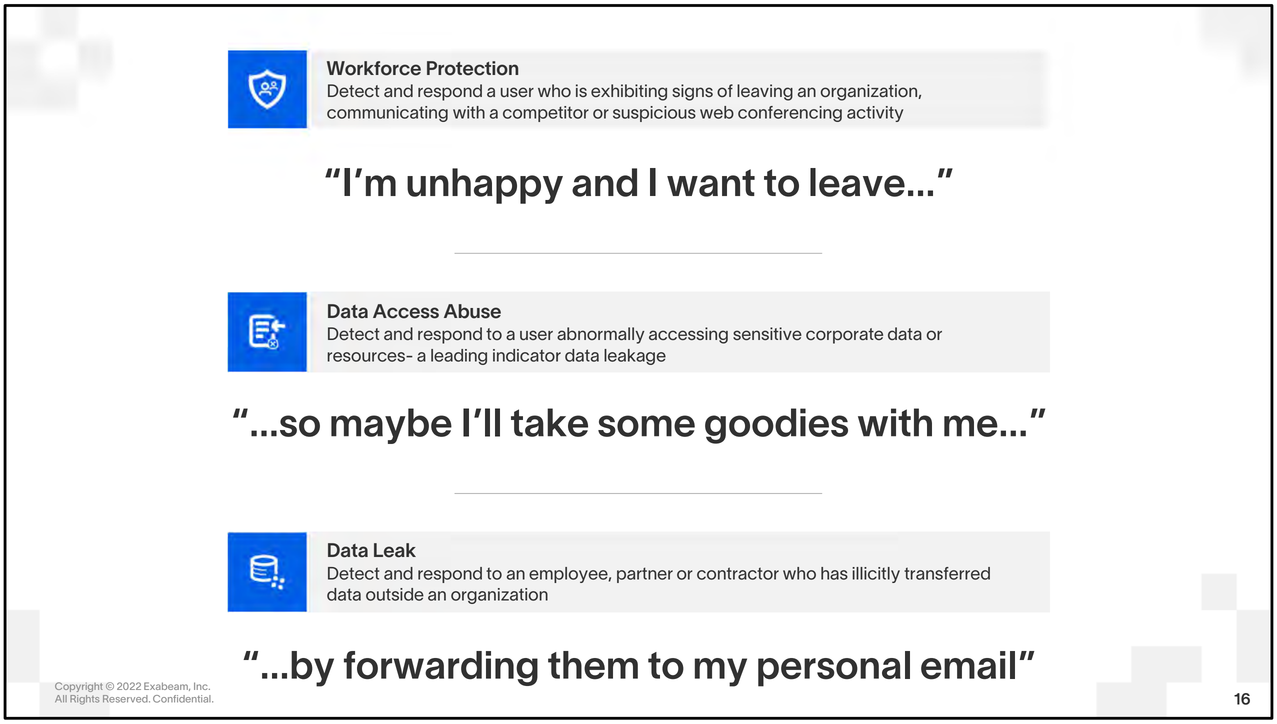
Student Notes
Privilege Abuse, as we noted earlier, is a common aspect of the Malicious Insider threat. But how do we know if an internal user is abusing privileges? Legacy SIEMs have primarily relied on static correlation rules which generate a high volume of alerts, while failing to distinguish between an anomalous and normal user behavior. Traditional correlation rules defined by security administrators may be correct for one set of users, but not for others. For example, if a department starts employing offshore workers, they will start logging in at unusual hours, which would repeatedly trigger a rule-based alert.

These types of static correlation rules create a huge maintenance overhead for the SOC who in turn fail to detect advanced threats due to the large number of false positives generated. Furthermore, the resource-intensive, manual investigations are prone to human error and consume huge amounts of analysts' time.

This is where UEBA really shines. Exabeam reduces the noise and volume of false positives for an analyst to triage by only alerting on abnormal access, rather than flagging each time a user accesses a database or server, for example. The Exabeam SecOps platform provide real-time analysis and reporting on abnormal data access attempts across the environment, allowing insider threat programs to become more proactive by identifying anomalous behavior in the ways users access data they have the permissions to access before exfiltration is attempted.

It's important to note that changes in user activity on their own are not enough to determine the intent of the user but paired with other use cases and contextual clues the analysts can start to paint a picture of why this user's behavior has changed.

Furthermore, Exabeam provides security analysts with the reasoning and analysis behind behavioral models and rules. This takes the guesswork out of behavior-based investigation and provides security analysts with the evidence to feel confident about making a decision to investigate or dismiss an anomalous event at a glance.



Workforce Protection
Detect and respond a user who is exhibiting signs of leaving an organization, communicating with a competitor or suspicious web conferencing activity

"I'm unhappy and I want to leave…"

Data Access Abuse
Detect and respond to a user abnormally accessing sensitive corporate data or resources- a leading indicator data leakage

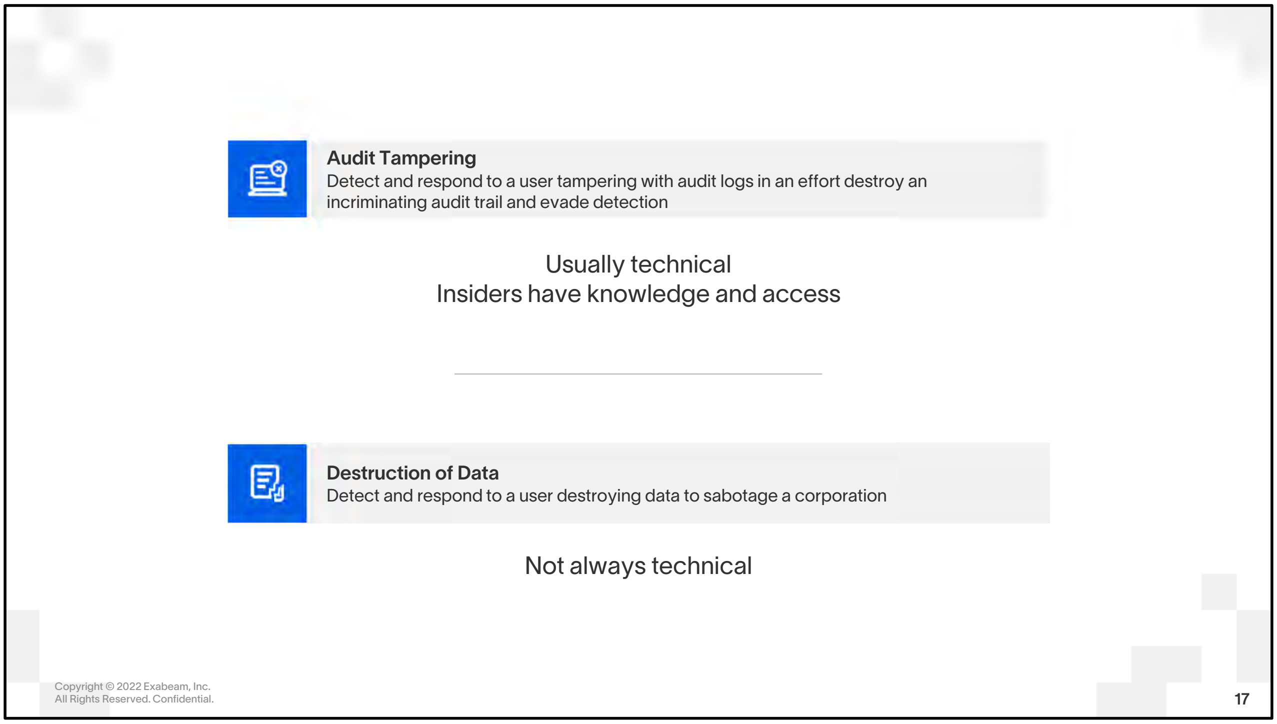
"…so maybe I'll take some goodies with me…"

Data Leak
Detect and respond to an employee, partner or contractor who has illicitly transferred data outside an organization

"…by forwarding them to my personal email"

Student Notes
The **Workforce Protection** use case aids organizations in detecting and responding to a user who is exhibiting signs of leaving, communicating with a competitor, or showing signs of suspicious web conferencing activity.
The **Data Access Abuse** use case helps detect and respond to a user **abnormally** accessing sensitive corporate data or resources--a leading indicator of data leakage.
The **Data Leak** use case supports the detection of and response to an employee, partner or contractor who has illicitly transferred data outside an organization.

References
https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_workforce_protection.md
https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_data_access.md
https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_data_leak.md



Audit Tampering
Detect and respond to a user tampering with audit logs in an effort destroy an incriminating audit trail and evade detection

Usually technical
Insiders have knowledge and access

Destruction of Data
Detect and respond to a user destroying data to sabotage a corporation

Not always technical

Student Notes
Audit Tampering: Insiders have advantages over external actors seeking to circumvent detection: they often enjoy privileged access, as well as knowledge of organizational policies, processes, and procedures. They know when auditing and event logging is enabled to track anomalous events and behavior. These insiders may try to circumvent the detection of malicious activity by tampering or clearing logs

Destruction of Data: Although financial fraud is a more common Malicious Insider threat, disgruntled insiders may seek to harm an organization by disrupting critical business operations. Rather than financial incentive or competitive advantage, their objective may be to simply wreak havoc within an organization by interrupting the availability of systems or services--bringing the organization to a halt. To do this, they may look for ways to delete data and files on critical systems.

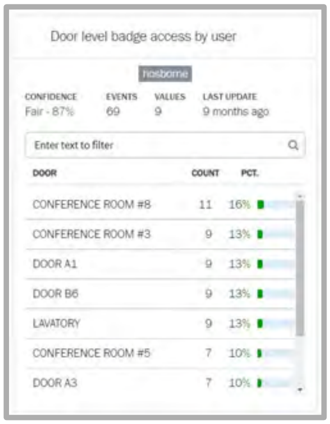
References
https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_audit_tampering.md
https://github.com/ExabeamLabs/Content-Doc/blob/master/UseCases/uc_destruction_of_data.md

Physical Security

Detect and respond to a user accessing physical spaces outside of typical usage patterns

Detection Examples:

- Failed/successful badge access for a **disabled account**
- First/abnormal **badge access**
- Badge access in **multiple cities** within a session
- Abnormal **physical access** in this building for user
- Badge access
    - at **abnormal time**
    - **after VPN** login
    - by **watchlist user**



Door level badge access by user

hosborne

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Fair - 87%	69	9	9 months ago

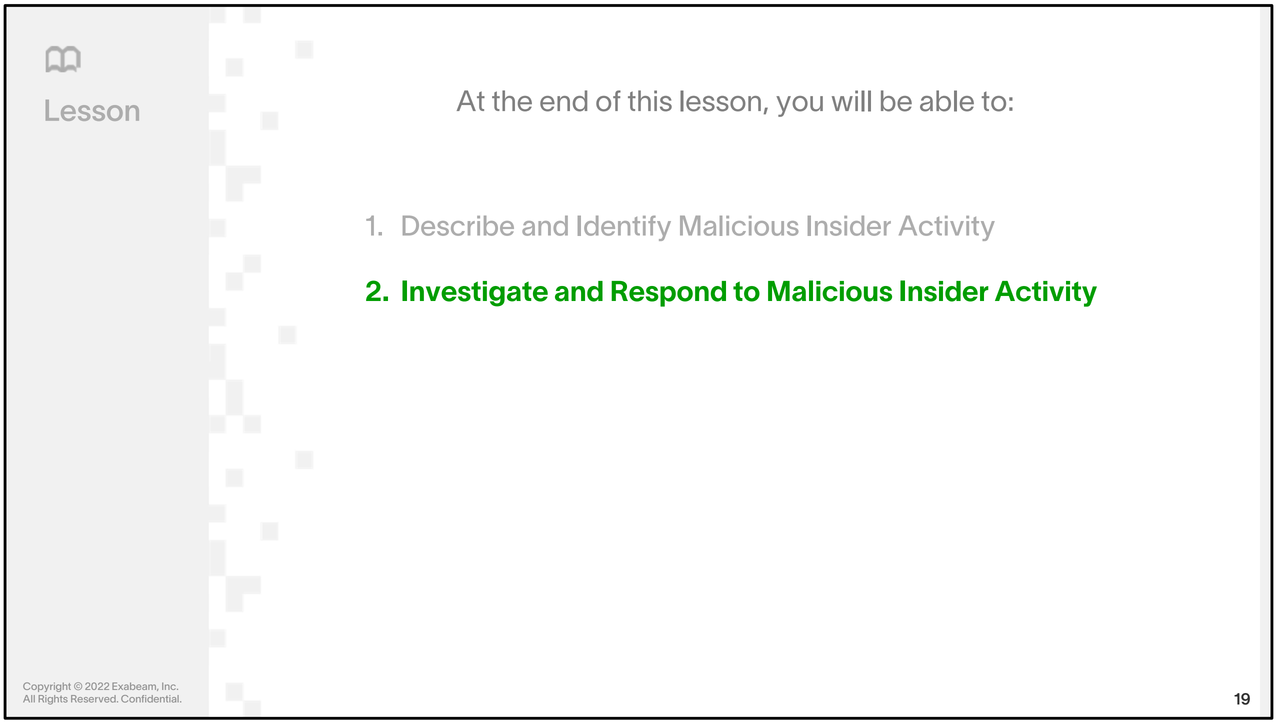
Enter text to filter

DOOR	COUNT	PCT.
CONFERENCE ROOM #8	11	16%
CONFERENCE ROOM #3	9	13%
DOOR A1	9	13%
DOOR B6	9	13%
LAVATORY	9	13%
CONFERENCE ROOM #5	7	10%
DOOR A3	7	10%

Student Notes

The Physical Security use case detects changes in user behavior such as badging into a new building or a user who has traveled an impossible distance between two geographical locations. This could indicate a malicious insider who is attempting to access, manipulate, or destroy critical physical assets. Alternatively, this could also indicate an insider who has shared their badge credentials intentionally giving physical access to another employee, contractor, or partner.

If you create a **Watchlist Users** watchlist, the users on the list will be assigned an additional 5 points of risk once per session when they badge into a door. You can adjust the risk value in the PA-WU rule if necessary.

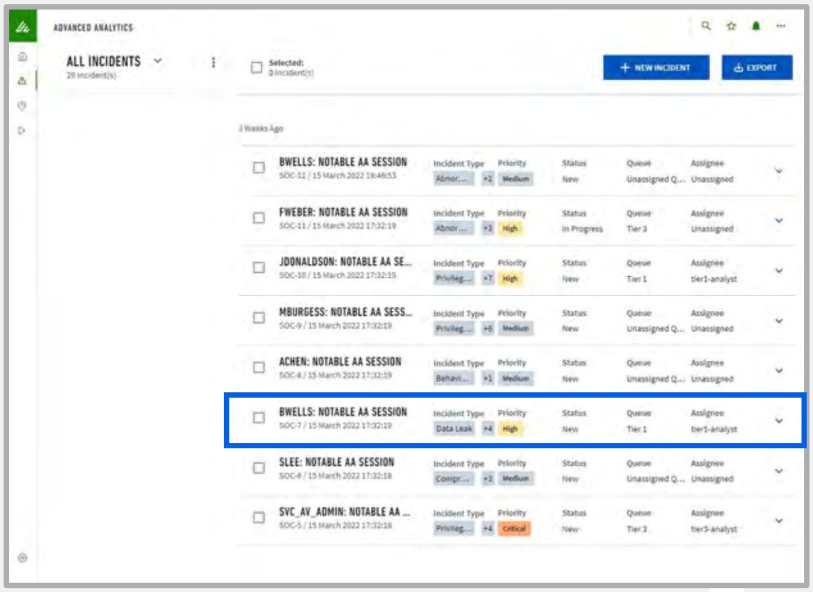


Lesson

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

1. Describe and Identify Malicious Insider Activity
2. **Investigate and Respond to Malicious Insider Activity**

How would you begin working this case?



ADVANCED ANALYTICS

ALL INCIDENTS
29 incident(s)

□ Selected:
0 incident(s)

+ NEW INCIDENT | EXPORT

3 Weeks Ago

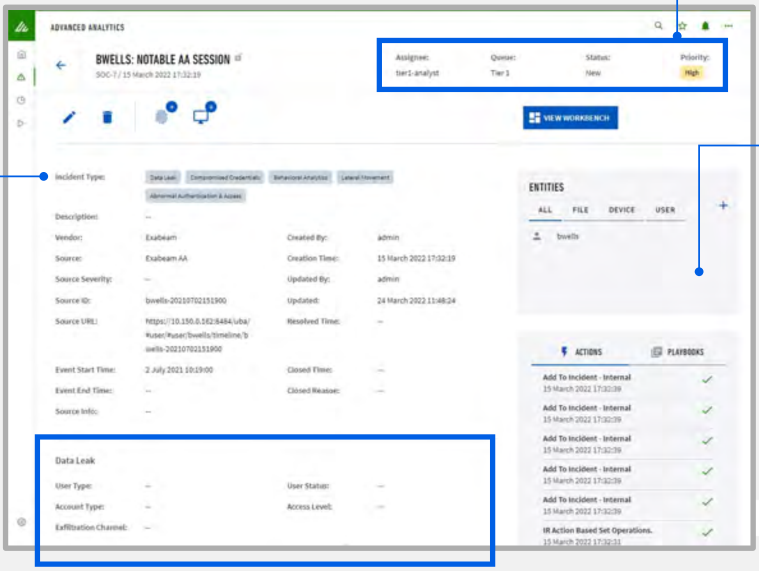
		Incident Type	Priority	Status	Queue	Assignee
□	**BWELLS: NOTABLE AA SESSION** SOC-12 / 15 March 2022 19:46:53	Abnor... +2	Medium	New	Unassigned Q...	Unassigned
□	**FWEBER: NOTABLE AA SESSION** SOC-11 / 15 March 2022 17:32:19	Abnor... +3	High	In Progress	Tier 3	Unassigned
□	**JDONALDSON: NOTABLE AA SE...** SOC-10 / 15 March 2022 17:32:19	Privileg... +7	High	New	Tier 1	tier1-analyst
□	**MBURGESS: NOTABLE AA SESS...** SOC-9 / 15 March 2022 17:32:19	Privileg... +6	Medium	New	Unassigned Q...	Unassigned
□	**ACHEN: NOTABLE AA SESSION** SOC-8 / 15 March 2022 17:32:19	Behavi... +1	Medium	New	Unassigned Q...	Unassigned
□	**BWELLS: NOTABLE AA SESSION** SOC-7 / 15 March 2022 17:32:19	Data Leak +4	High	New	Tier 1	tier1-analyst
□	**SLEE: NOTABLE AA SESSION** SOC-6 / 15 March 2022 17:32:18	Compr... +3	Medium	New	Unassigned Q...	Unassigned
□	**SVC_AV_ADMIN: NOTABLE AA ...** SOC-5 / 15 March 2022 17:32:18	Privileg... +4	Critical	New	Tier 3	tier3-analyst

Triage & Initial Response

Status, Assignments, & Priority

Incident Type

Impacted Entities



BWELLS: NOTABLE AA SESSION

SOC-7 / 15 March 2022 17:32:19

Assignee: tier1-analyst

Queue: Tier 1

Status: New

Priority: High

Incident Type: Data Leak, Compromised Credentials, Behavioral Analytics, Lateral Movement, Abnormal Authentication & Access

Description: --

Vendor:	Exabeam	Created By:	admin
Source:	Exabeam AA	Creation Time:	15 March 2022 17:32:19
Source Severity:	--	Updated By:	admin
Source ID:	bwells-20210702151900	Updated:	24 March 2022 11:48:24
Source URL:	https://10.150.0.162:8484/uba/#user/#user/bwells/timeline/bwells-20210702151900	Resolved Time:	--
Event Start Time:	2 July 2021 10:19:00	Closed Time:	--
Event End Time:	--	Closed Reason:	--
Source Info:	--		

Data Leak

User Type:	--	User Status:	--
Account Type:	--	Access Level:	--
Exfiltration Channel:	--		

ENTITIES

bwells

Add To Incident - Internal
15 March 2022 17:32:39 ✓

Add To Incident - Internal
15 March 2022 17:32:39 ✓

Add To Incident - Internal
15 March 2022 17:32:39 ✓

Add To Incident - Internal
15 March 2022 17:32:39 ✓

Add To Incident - Internal
15 March 2022 17:32:39 ✓

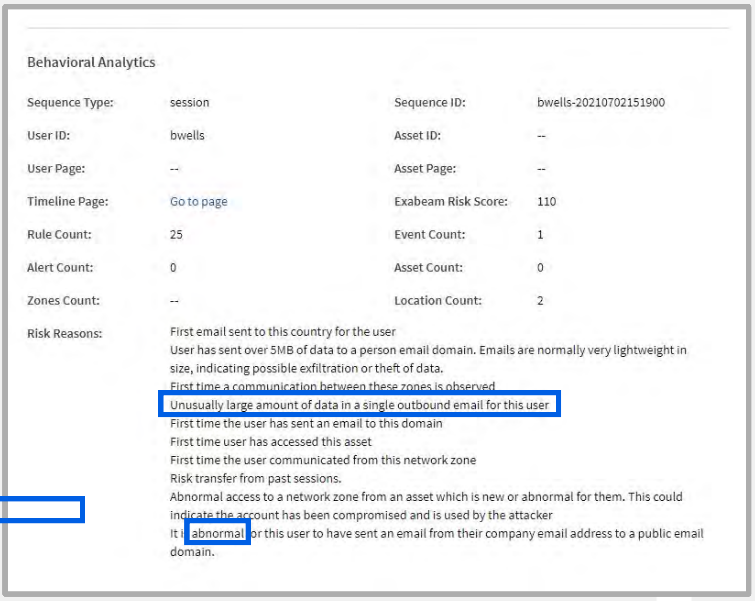
IR Action Based Set Operations.
15 March 2022 17:32:31 ✓

Risk Reasons

What questions should we be asking here?

Is this odd?

Is it dangerous?



Behavioral Analytics

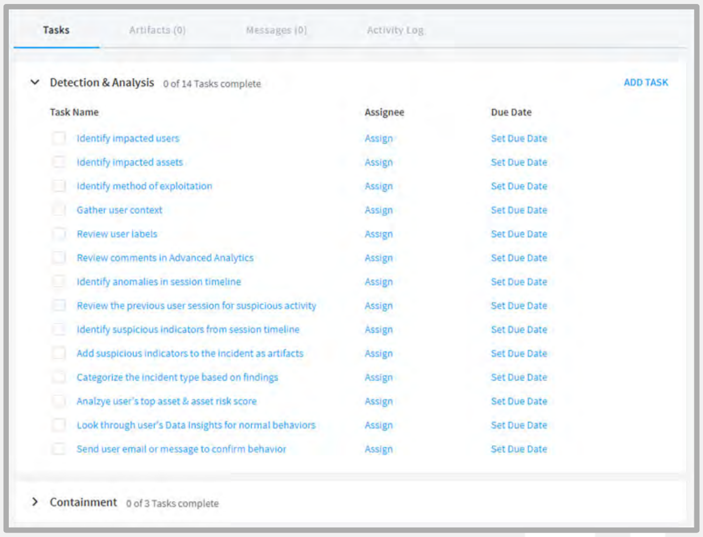
Sequence Type:	session	Sequence ID:	bwells-20210702151900
User ID:	bwells	Asset ID:	--
User Page:	--	Asset Page:	--
Timeline Page:	Go to page	Exabeam Risk Score:	110
Rule Count:	25	Event Count:	1
Alert Count:	0	Asset Count:	0
Zones Count:	--	Location Count:	2

Risk Reasons:

First email sent to this country for the user
User has sent over 5MB of data to a person email domain. Emails are normally very lightweight in size, indicating possible exfiltration or theft of data.
First time a communication between these zones is observed
Unusually large amount of data in a single outbound email for this user
First time the user has sent an email to this domain
First time user has accessed this asset
First time the user communicated from this network zone
Risk transfer from past sessions.
Abnormal access to a network zone from an asset which is new or abnormal for them. This could indicate the account has been compromised and is used by the attacker
It is abnormal for this user to have sent an email from their company email address to a public email domain.

Where can we find prescriptive guidance?

How do we answer these questions?

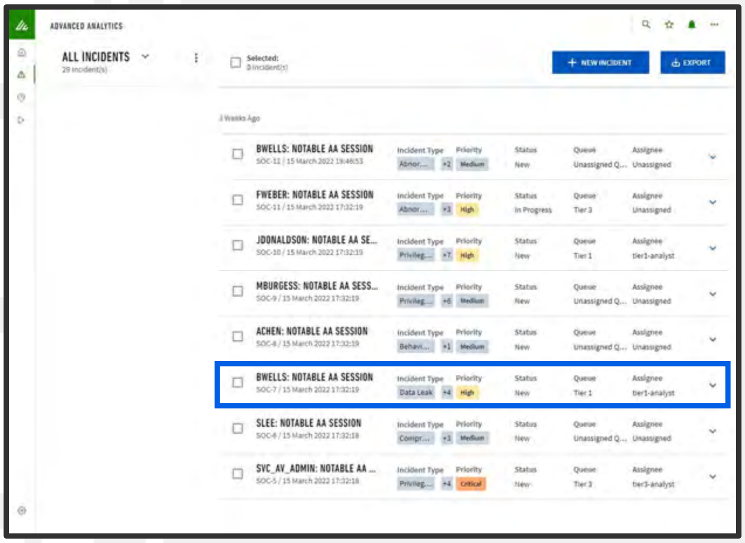


Detection & Analysis 0 of 14 Tasks complete

Task Name	Assignee	Due Date
□ Identify impacted users	Assign	Set Due Date
□ Identify impacted assets	Assign	Set Due Date
□ Identify method of exploitation	Assign	Set Due Date
□ Gather user context	Assign	Set Due Date
□ Review user labels	Assign	Set Due Date
□ Review comments in Advanced Analytics	Assign	Set Due Date
□ Identify anomalies in session timeline	Assign	Set Due Date
□ Review the previous user session for suspicious activity	Assign	Set Due Date
□ Identify suspicious indicators from session timeline	Assign	Set Due Date
□ Add suspicious indicators to the incident as artifacts	Assign	Set Due Date
□ Categorize the incident type based on findings	Assign	Set Due Date
□ Analzye user's top asset & asset risk score	Assign	Set Due Date
□ Look through user's Data Insights for normal behaviors	Assign	Set Due Date
□ Send user email or message to confirm behavior	Assign	Set Due Date

Containment 0 of 3 Tasks complete

Demo



ALL INCIDENTS
29 incident(s)

□ Selected:
0 incident(s)

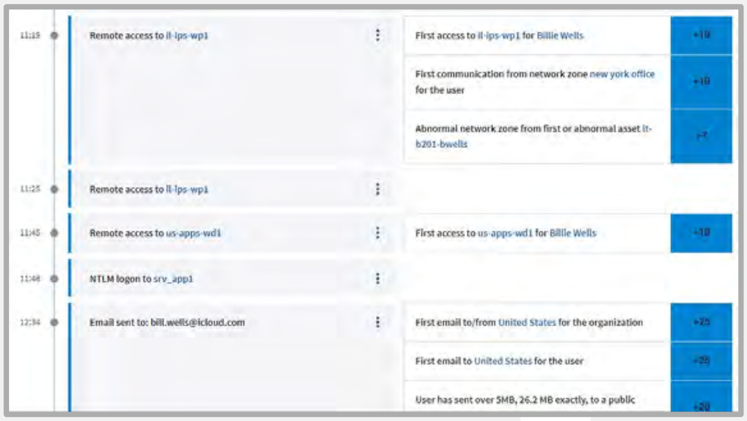
3 Weeks Ago

	Incident	Incident Type	Priority	Status	Queue	Assignee
□	BWELLS: NOTABLE AA SESSION SOC-12 / 15 March 2022 19:46:53	Abnor... +2	Medium	New	Unassigned Q...	Unassigned
□	FWEBER: NOTABLE AA SESSION SOC-11 / 15 March 2022 17:32:19	Abnor... +3	High	In Progress	Tier 3	Unassigned
□	JDONALDSON: NOTABLE AA SE... SOC-10 / 15 March 2022 17:32:19	Privileg... +7	High	New	Tier 1	tier1-analyst
□	MBURGESS: NOTABLE AA SESS... SOC-9 / 15 March 2022 17:32:19	Privileg... +6	Medium	New	Unassigned Q...	Unassigned
□	ACHEN: NOTABLE AA SESSION SOC-8 / 15 March 2022 17:32:19	Behavi... +1	Medium	New	Unassigned Q...	Unassigned
□	BWELLS: NOTABLE AA SESSION SOC-7 / 15 March 2022 17:32:19	Data Leak +4	High	New	Tier 1	tier1-analyst
□	SLEE: NOTABLE AA SESSION SOC-6 / 15 March 2022 17:32:18	Compr... +3	Medium	New	Unassigned Q...	Unassigned
□	SVC_AV_ADMIN: NOTABLE AA ... SOC-5 / 15 March 2022 17:32:18	Privileg... +4	Critical	New	Tier 3	tier3-analyst

Timeline Investigation

Abnormal Authentication & Access

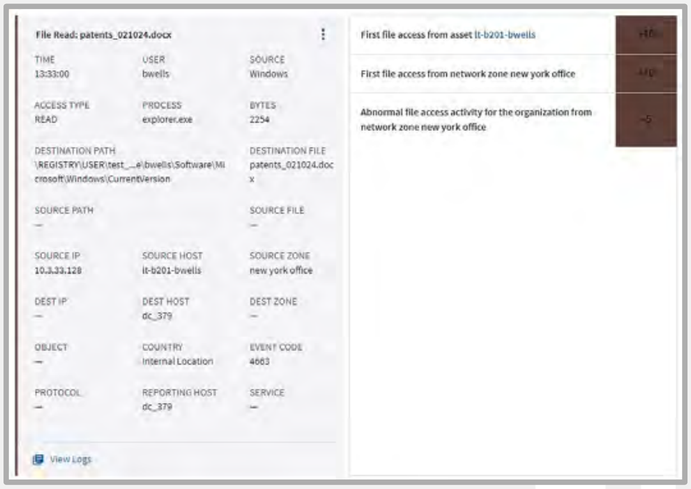
Data Leak



11:19	Remote access to il-ips-wp1	First access to il-ips-wp1 for Billie Wells	+10
		First communication from network zone new york office for the user	+10
		Abnormal network zone from first or abnormal asset lt-b201-bwells	+7
11:25	Remote access to il-ips-wp1		
11:45	Remote access to us-apps-wd1	First access to us-apps-wd1 for Billie Wells	+10
11:48	NTLM logon to srv_app1		
12:34	Email sent to: bill.wells@icloud.com	First email to/from United States for the organization	+25
		First email to United States for the user	+20
		User has sent over 5MB, 26.2 MB exactly, to a public	+20

Timeline Investigation

Data Leak



File Read: patents_021024.docx

TIME
13:33:00

USER
bwells

SOURCE
Windows

ACCESS TYPE
READ

PROCESS
explorer.exe

BYTES
2254

DESTINATION PATH
\REGISTRY\USER\test_...e\bwells\Software\Microsoft\Windows\CurrentVersion

DESTINATION FILE
patents_021024.docx

SOURCE PATH
—

SOURCE FILE
—

SOURCE IP
10.3.33.128

SOURCE HOST
lt-b201-bwells

SOURCE ZONE
new york office

DEST IP
—

DEST HOST
dc_379

DEST ZONE
—

OBJECT
—

COUNTRY
Internal Location

EVENT CODE
4663

PROTOCOL
—

REPORTING HOST
dc_379

SERVICE
—

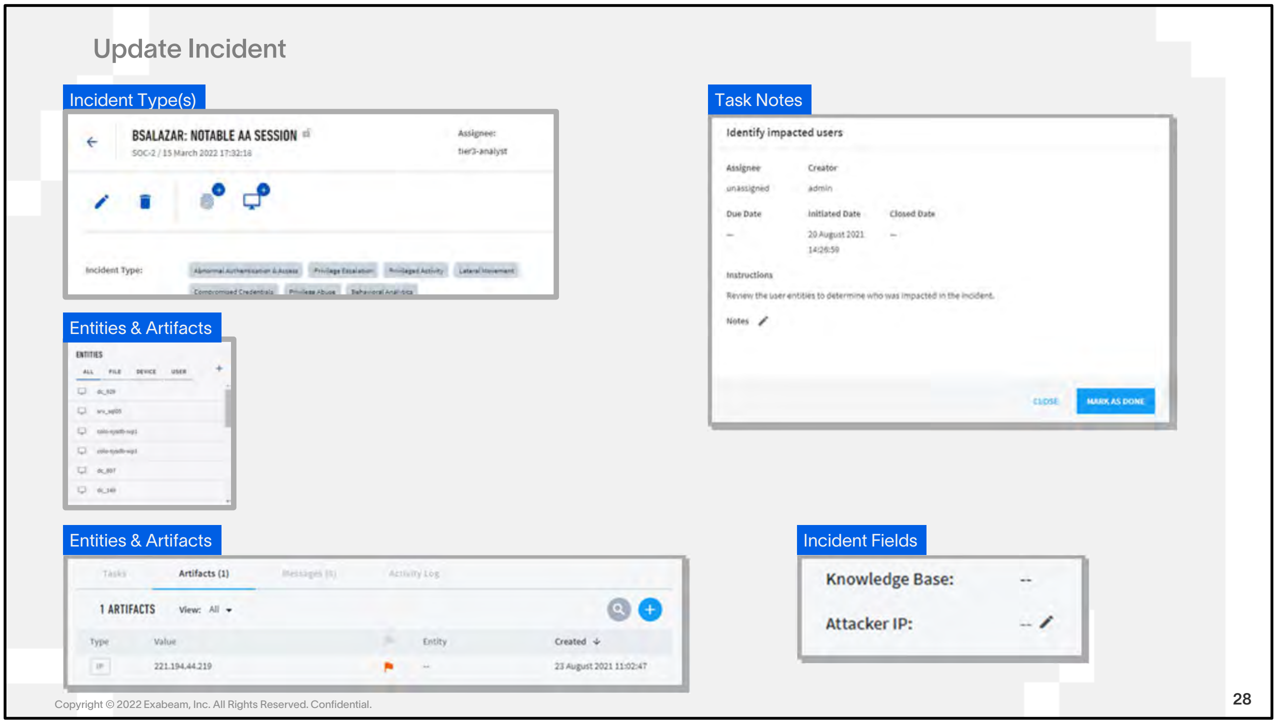
View Logs

First file access from asset lt-b201-bwells +10

First file access from network zone new york office +10

Abnormal file access activity for the organization from network zone new york office +5

How do you **track and document** your findings?



Update Incident

Incident Type(s)

BSALAZAR: NOTABLE AA SESSION

SOC-2 / 15 March 2022 17:32:18

Assignee:
tier3-analyst

Incident Type: Abnormal Authentication & Access | Privilege Escalation | Privileged Activity | Lateral Movement | Compromised Credentials | Privilege Abuse | Behavioral Analytics

Entities & Artifacts

ENTITIES

- dc_929
- srv_sql05
- colo-sysdb-sql1
- colo-sysdb-sql1
- dc_807
- dc_149

Entities & Artifacts

1 ARTIFACTS View: All

Type	Value		Entity	Created
IP	221.194.44.219	🚩	--	23 August 2021 11:02:47

Task Notes

Identify impacted users

Assignee	Creator	
unassigned	admin	
Due Date	**Initiated Date**	**Closed Date**
—	20 August 2021 14:26:59	—

Instructions

Review the user entities to determine who was impacted in the incident.

Notes

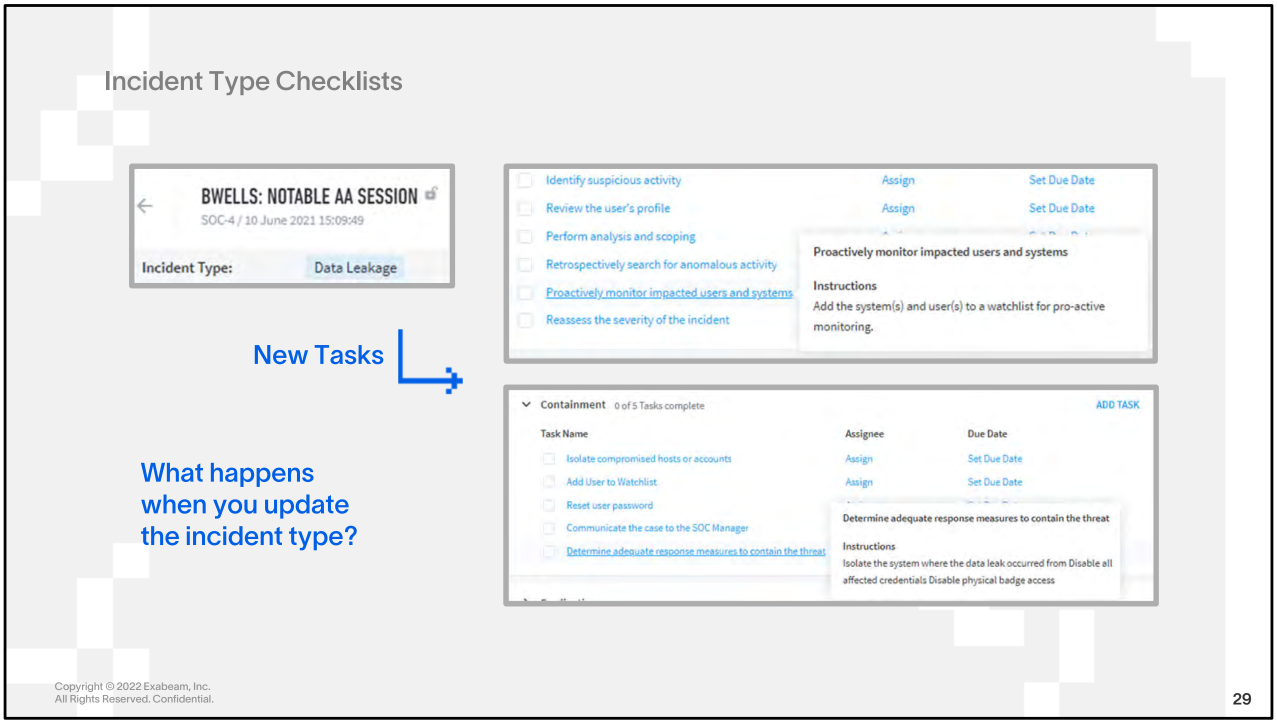
Incident Fields

Knowledge Base: --

Attacker IP: --

Student Notes

Incidents can be updated in several ways - adding more classifications, entities and artifacts, notes on individual tasks, and adding detail to fields.



Incident Type Checklists

BWELLS: NOTABLE AA SESSION

SOC-4 / 10 June 2021 15:09:49

Incident Type: Data Leakage

□ Identify suspicious activity	Assign	Set Due Date
□ Review the user's profile	Assign	Set Due Date
□ Perform analysis and scoping		
□ Retrospectively search for anomalous activity		
□ Proactively monitor impacted users and systems		
□ Reassess the severity of the incident		

Proactively monitor impacted users and systems

Instructions

Add the system(s) and user(s) to a watchlist for pro-active monitoring.

New Tasks

Containment 0 of 5 Tasks complete ADD TASK

Task Name	Assignee	Due Date
□ Isolate compromised hosts or accounts	Assign	Set Due Date
□ Add User to Watchlist	Assign	Set Due Date
□ Reset user password		
□ Communicate the case to the SOC Manager		
□ Determine adequate response measures to contain the threat		

Determine adequate response measures to contain the threat

Instructions

Isolate the system where the data leak occurred from Disable all affected credentials Disable physical badge access

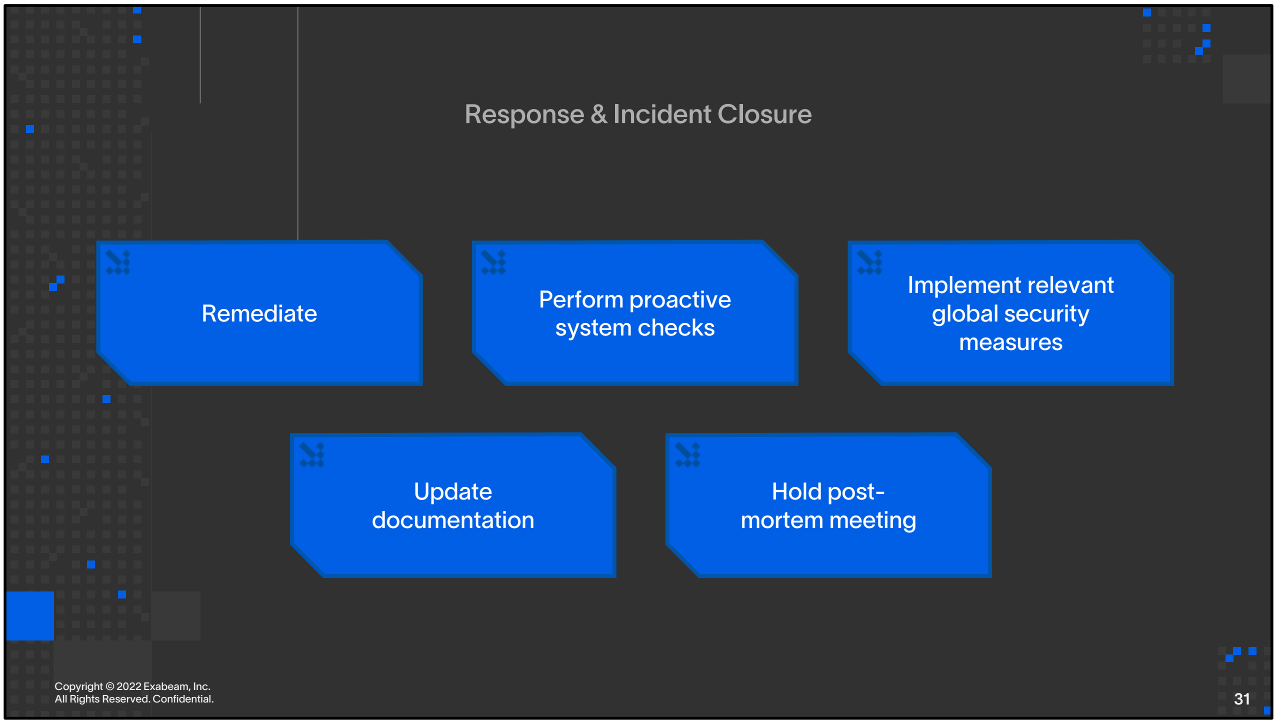
What happens when you update the incident type?

Student Notes

Recall that 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.

What are the next steps?



Response & Incident Closure

Remediate

Perform proactive system checks

Implement relevant global security measures

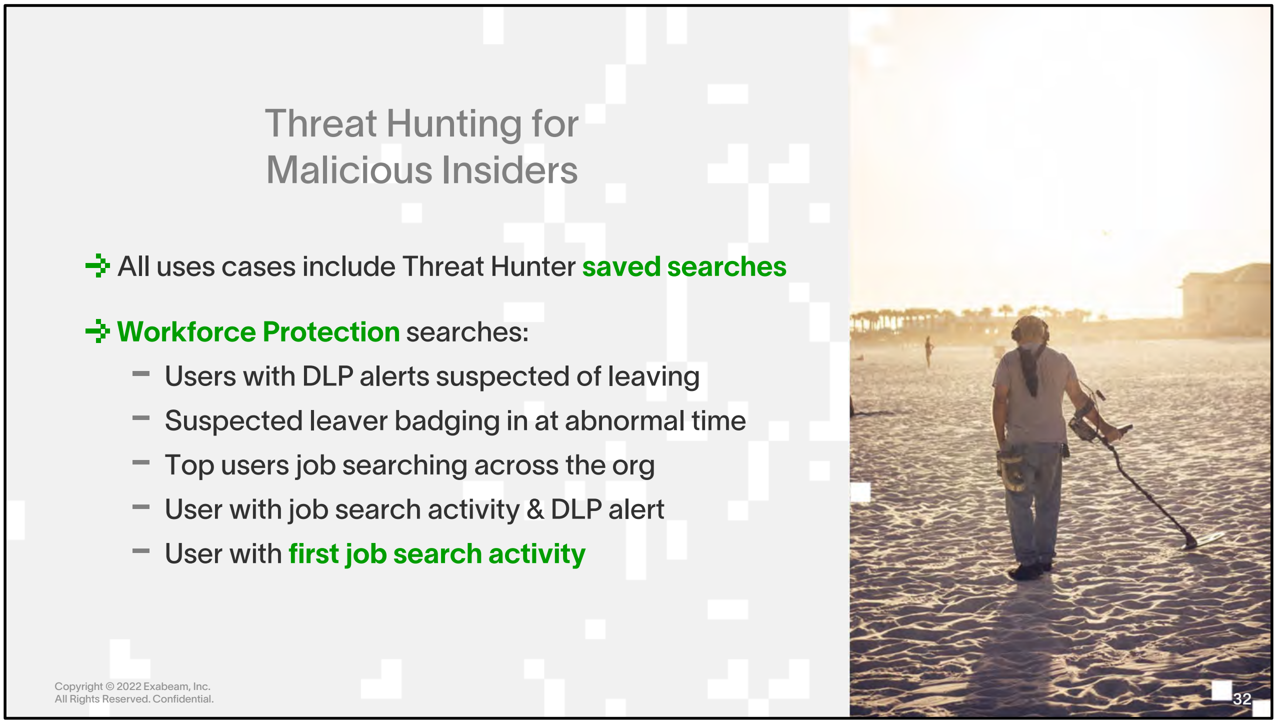
Update documentation

Hold post-mortem meeting

Student Notes

Some recommended responses include:

- Remediation: may include reducing network access by blocking ports, restricting web and email access, etc.
- Perform proactive system checks: Reset all affected credentials, and restore disabled credentials as applicable
- Implement relevant global security measures: Change permissions and access levels as appropriate; Implement new DLP security rules, as needed
- Update documentation: Ensure the case contains documentation of all relevant events and actions taken; Identify methods to improve the team's response to future incidents.
- Hold post-mortem meeting: Hold a meeting with the team to review the incident along with lessons learned. Document and track administrative and technical gaps identified during the incident.



Threat Hunting for Malicious Insiders

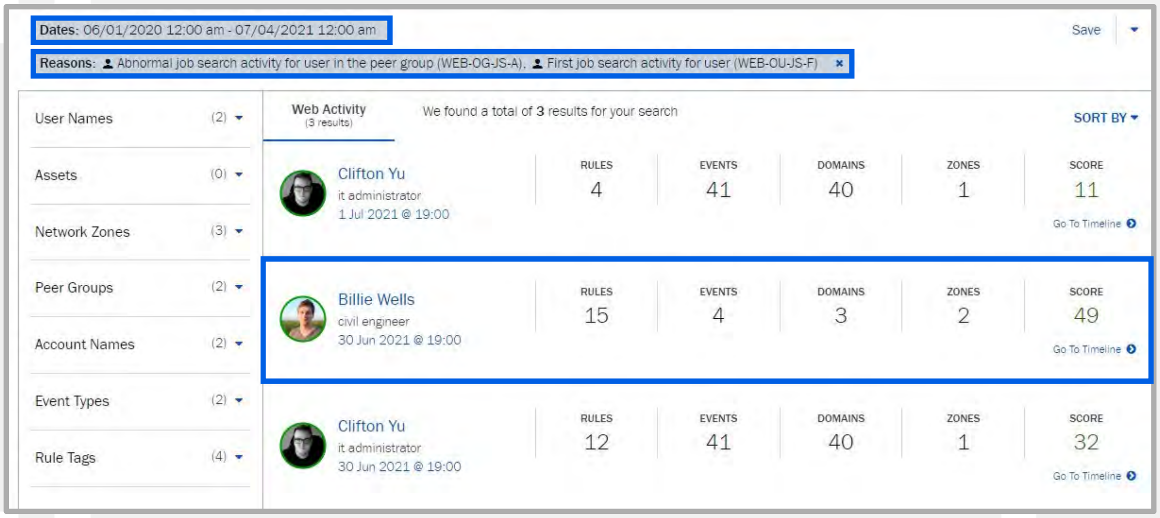
- All uses cases include Threat Hunter **saved searches**
- **Workforce Protection** searches:
  - Users with DLP alerts suspected of leaving
  - Suspected leaver badging in at abnormal time
  - Top users job searching across the org
  - User with job search activity & DLP alert
  - User with **first job search activity**

Student Notes

While threat hunting can be a proactive part of any security program, it's particularly powerful as a part of an insider threat program. All Exabeam use case categories include pre-created Threat Hunter queries. The Data Access Abuse and Data Leak use cases, for example, allow insider threat programs to become more proactive by identifying anomalous data access behaviors before exfiltration is attempted.

{Photo by NICO BHLR on Unsplash}

User with First Job Search Activity



Dates: 06/01/2020 12:00 am - 07/04/2021 12:00 am

Reasons: Abnormal job search activity for user in the peer group (WEB-OG-JS-A), First job search activity for user (WEB-OU-JS-F) ×

Filter	Count
User Names	(2)
Assets	(0)
Network Zones	(3)
Peer Groups	(2)
Account Names	(2)
Event Types	(2)
Rule Tags	(4)

Web Activity (3 results)

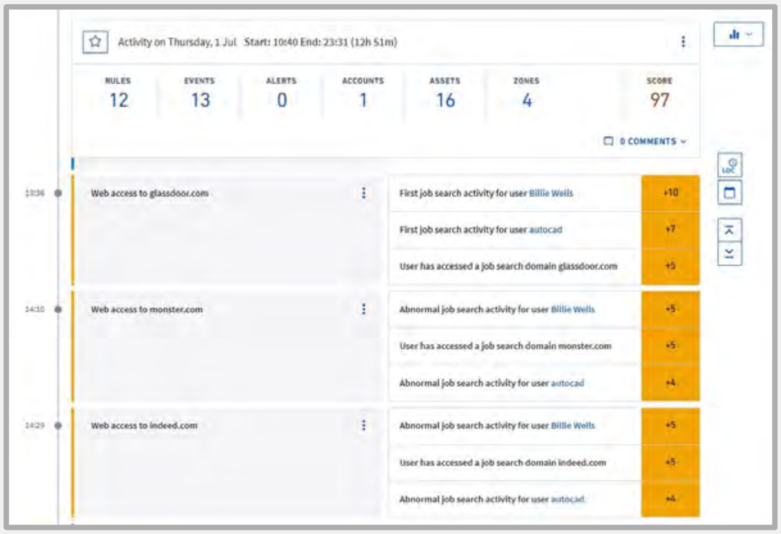
We found a total of **3** results for your search

	RULES	EVENTS	DOMAINS	ZONES	SCORE
Clifton Yu it administrator 1 Jul 2021 @ 19:00	4	41	40	1	11
Billie Wells civil engineer 30 Jun 2021 @ 19:00	15	4	3	2	49
Clifton Yu it administrator 30 Jun 2021 @ 19:00	12	41	40	1	32

Student Notes

The **Workforce Protection: User with first job search activity** Threat Hunter search returns a few hits, including a sub-notable (risk score less than 90) session for Billie Wells. When we pivot to Billie Wells' timeline…

Workforce Protection



Activity on Thursday, 1 Jul Start: 10:40 End: 23:31 (12h 51m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
12	13	0	1	16	4	97

13:36 Web access to glassdoor.com

First job search activity for user Billie Wells	+10
First job search activity for user autocad	+7
User has accessed a job search domain glassdoor.com	+5

14:10 Web access to monster.com

Abnormal job search activity for user Billie Wells	+5
User has accessed a job search domain monster.com	+5
Abnormal job search activity for user autocad	+4

14:29 Web access to indeed.com

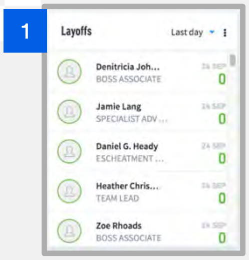
Abnormal job search activity for user Billie Wells	+5
User has accessed a job search domain indeed.com	+5
Abnormal job search activity for user autocad	+4

Student Notes

…we see job search activity **the day before** the activity in his notable session. Because this session never reached the notable threshold score of 90 or greater, the job searches may have gone unnoticed. With proactive threat hunting, a SOC may be able to uncover potential risks before they become much bigger security threats.

Workforce Protection

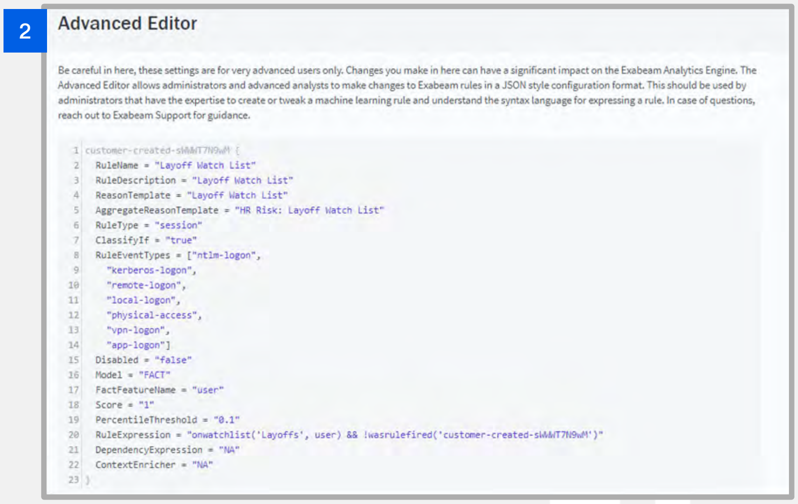
1



Layoffs — Last day

- Denitricia Joh... BOSS ASSOCIATE — 24 SEP 0
- Jamie Lang SPECIALIST ADV ... — 24 SEP 0
- Daniel G. Heady ESCHEATMENT ... — 24 SEP 0
- Heather Chris... TEAM LEAD — 24 SEP 0
- Zoe Rhoads BOSS ASSOCIATE — 24 SEP 0

2

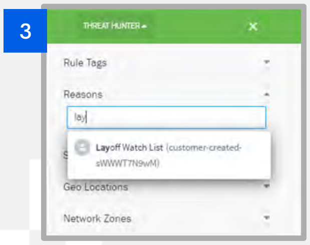


Advanced Editor

Be careful in here, these settings are for very advanced users only. Changes you make in here can have a significant impact on the Exabeam Analytics Engine. The Advanced Editor allows administrators and advanced analysts to make changes to Exabeam rules in a JSON style configuration format. This should be used by administrators that have the expertise to create or tweak a machine learning rule and understand the syntax language for expressing a rule. In case of questions, reach out to Exabeam Support for guidance.

```
customer-created-sWWT7N9wM {
  RuleName = "Layoff Watch List"
  RuleDescription = "Layoff Watch List"
  ReasonTemplate = "Layoff Watch List"
  AggregateReasonTemplate = "HR Risk: Layoff Watch List"
  RuleType = "session"
  ClassifyIf = "true"
  RuleEventTypes = ["ntlm-logon",
    "kerberos-logon",
    "remote-logon",
    "local-logon",
    "physical-access",
    "vpn-logon",
    "app-logon"]
  Disabled = "false"
  Model = "FACT"
  FactFeatureName = "user"
  Score = "1"
  PercentileThreshold = "0.1"
  RuleExpression = "onwatchlist('Layoffs', user) && !wasrulefired('customer-created-sWWT7N9wM')"
  DependencyExpression = "NA"
  ContextEnricher = "NA"
}
```

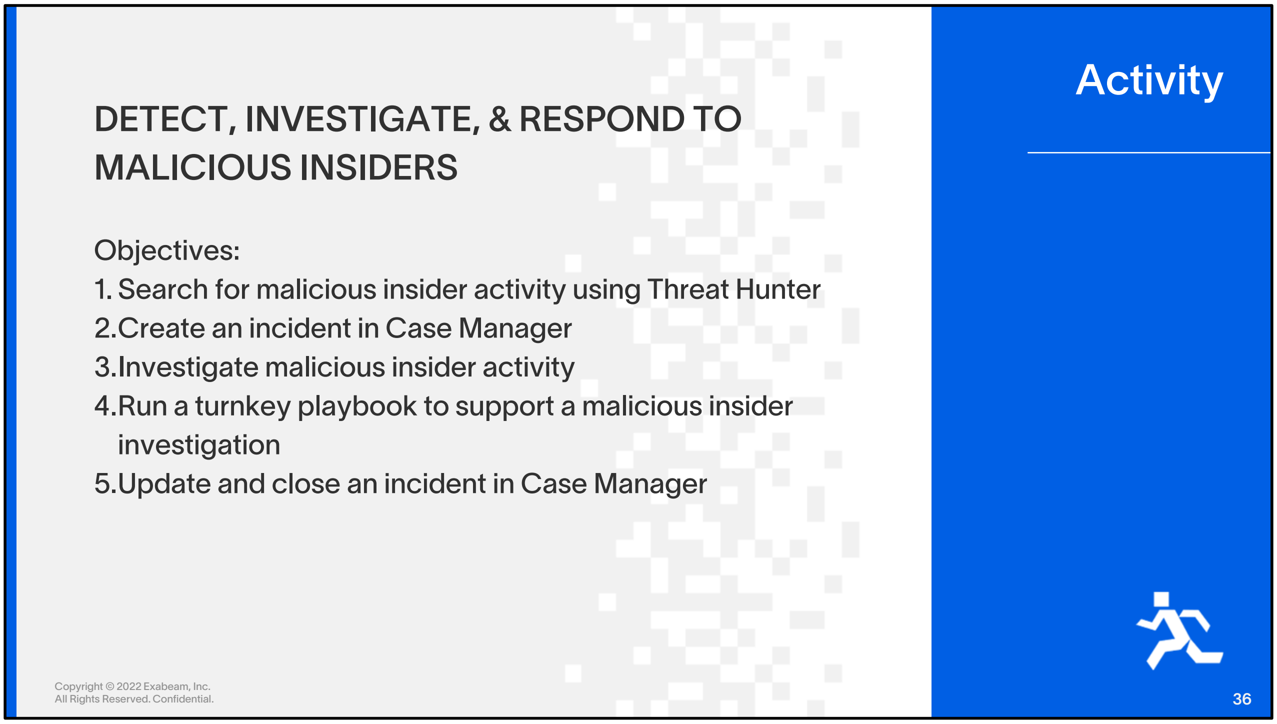
3



Student Notes

In some situations, it may be useful to be able to search in Threat Hunter for users on a watchlist, regardless of whether anomalous behaviors have been detected for that user. In the example above, a **Layoffs** watchlist has been created to surface employees who represent a potential insider threat. The next step is to clone an existing rule—in this case, rule PA_WU—and modify the rule to include updated events types that will fire for normal logon activity.

The RuleExpression also needs to be modified to make use of the **OnWatchlist()** function. A small score has been assigned to the rule because the goal is not to add undue risk to a session for a user on the Layoffs watchlist simply because the user has logged on. The goal is simply to fire a rule when a user on the Layoffs watchlist starts a session, making the event searchable in a Threat Hunter query (step 3 above). Other hunting queries can then be added to the search—for example, hunting for users on the Layoffs watchlist that have also shown signs of Privilege Abuse, Data Access Abuse, Data Leak, and so on.

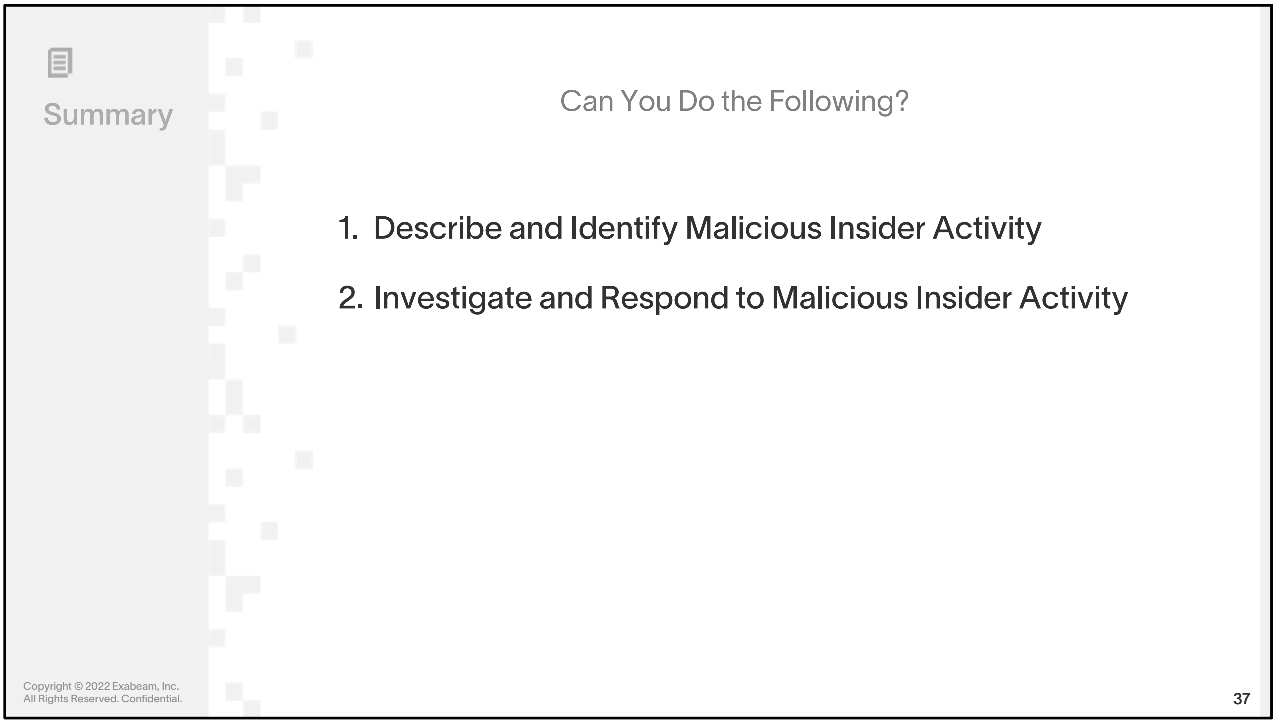


DETECT, INVESTIGATE, & RESPOND TO MALICIOUS INSIDERS

Objectives:

1. Search for malicious insider activity using Threat Hunter
2. Create an incident in Case Manager
3. Investigate malicious insider activity
4. Run a turnkey playbook to support a malicious insider investigation
5. Update and close an incident in Case Manager

Activity



Summary

Can You Do the Following?

1. Describe and Identify Malicious Insider Activity
2. Investigate and Respond to Malicious Insider Activity

v4.00

exabeam

Integrate Exabeam into Your Security Organization

EDU-2170: Module 10

Operationalizing Exabeam requires use, review and enrichment

Remember H.A.B.I.T.S.

Student Notes

According to the CERT Insider Threat Center, the four most common types of insider threats, in order of prevalence, are the following:

- Fraud
- Theft of Intellectual Property
- IT Sabotage
- Misuse

CERT defines fraud as “a malicious insider’s use of IT for the unauthorized modification, addition, or deletion of an organization’s data (not programs or systems) for personal gain or the theft of information leading to an identity crime.“ The victim in fraud cases is most often the organization itself, followed by consumers/customers of the company. The information assets most commonly targeted in cases of fraud are, in order:

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Payment Card Information (PCI)
- Federal Tax Information (FTI)

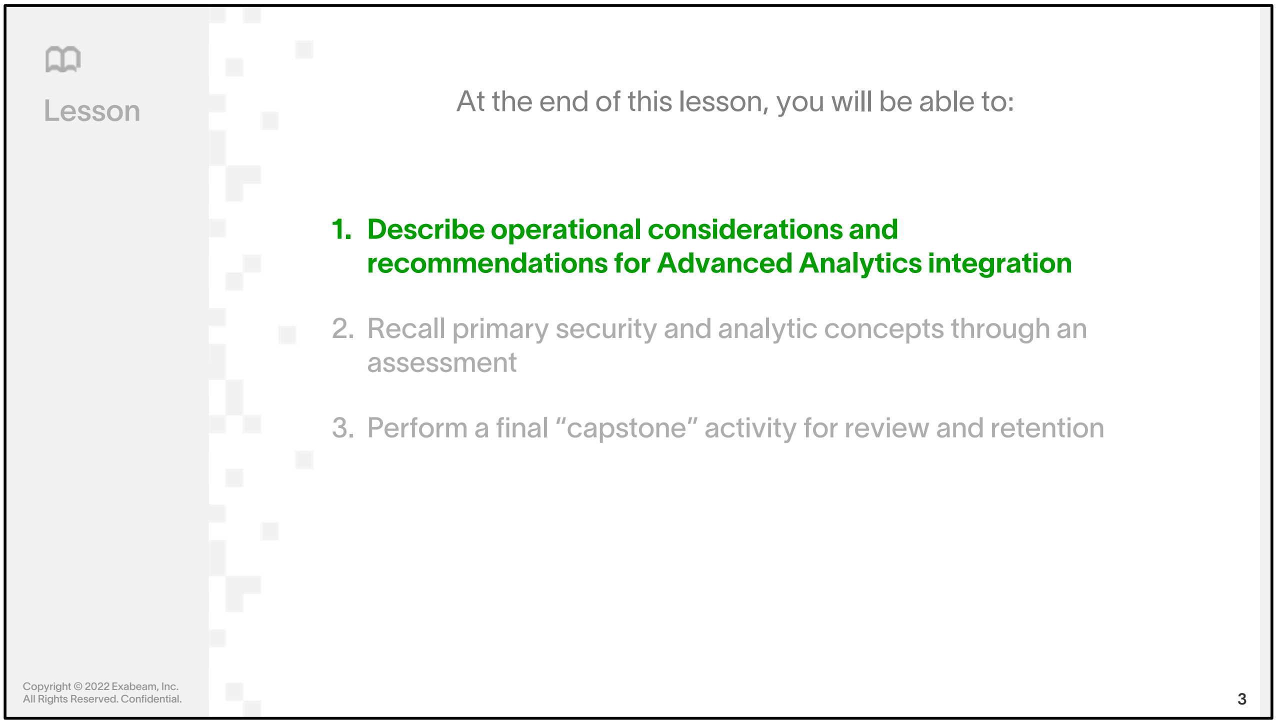
They further define an identity crime as “the misuse of personal or financial identifiers in order to gain something of value and/or facilitate some other criminal activity.”

The most targeted devices for fraud within organizations are, in order:

- Database servers
- Organization desktops
- Other
- File Servers

References

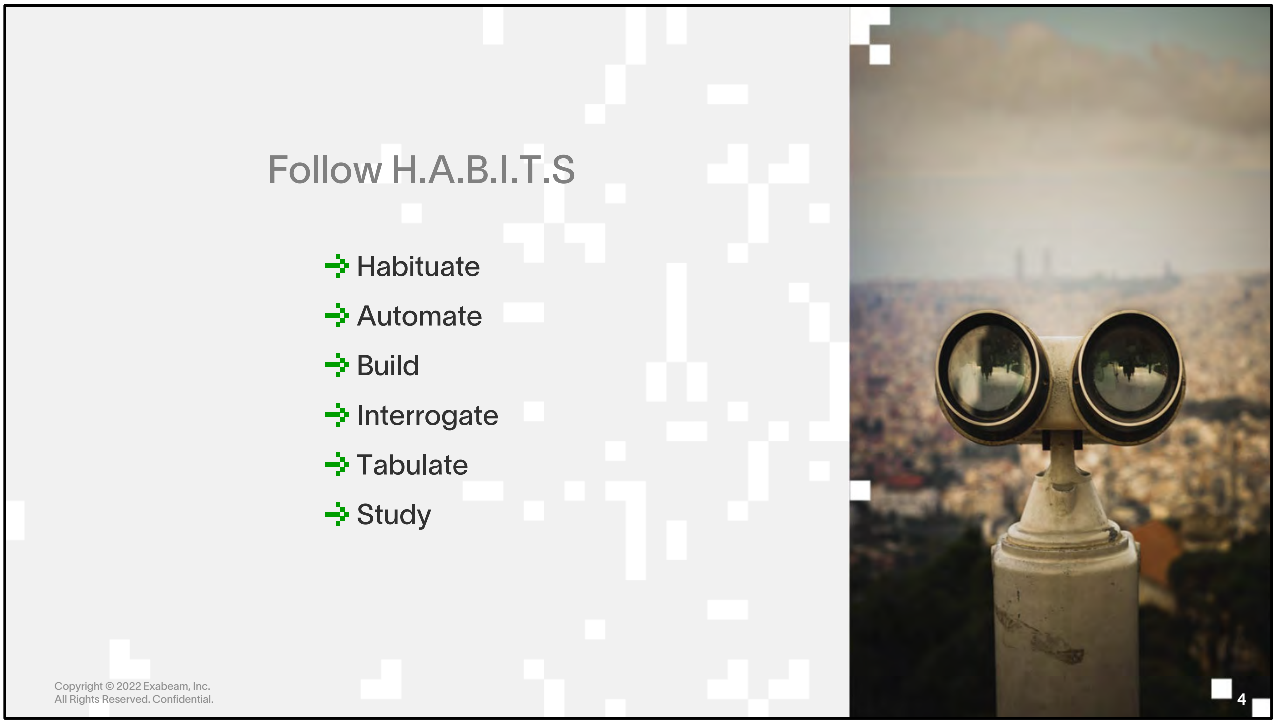
Assets Targeted by Malicious Insiders: https://insights.sei.cmu.edu/blog/insider-threat-incidents-assets-targeted-by-malicious-insiders/
Malicious Insider Fraud: https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf



Lesson

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

1. **Describe operational considerations and recommendations for Advanced Analytics integration**
2. Recall primary security and analytic concepts through an assessment
3. Perform a final "capstone" activity for review and retention



Follow H.A.B.I.T.S

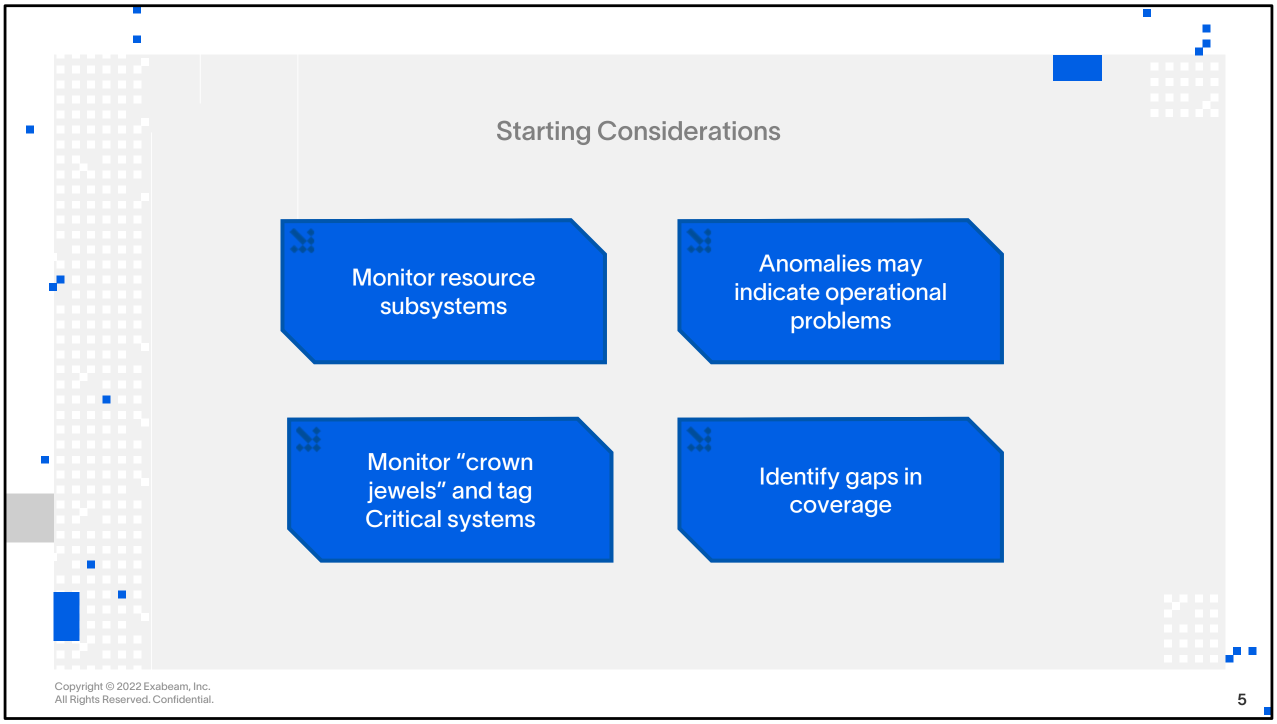
- Habituate
- Automate
- Build
- Interrogate
- Tabulate
- Study

Student Notes

This is a mnemonic to help identify important tasks around security operations and the Exabeam SecOps platform:

- **H**abituate –Create operational habits around Advanced Analytics (and Case Management) for daily triage and weekly investigations. Create daily/weekly/monthly cadences. Use Threat Hunter. This should include infrastructure and subsystem monitoring. Also, find ways to get additional value from it by allowing HR to use the platform with reduced privileges. This way, business policy use cases can be offloaded to HR rather than burden the security team.
- **A**utomate –Identify use cases for automation to improve response times and consider a SOAR solution. Consider starting with case management. Remember, Exabeam provides Case Management and Incident Responder which integrate with Advanced Analytics.
- **B**uild - Improve the efficiency of Advanced Analytics in your organization through building new workflows, log sources, context, custom models and more. Consider building use cases and playbooks for Advanced Analytics. Leverage Entity Analytics. Enrich your context with new data sources.
- **I**nterrogate - Ask the hard questions about processes and solutions such as, How do security operations affect the business? Are we measuring the right things? Where do you want to be?
- **T**abulate - Measure the impact of Advanced Analytics on the business and measure the impact on security operations.
- **S**tudy - Grow your team and your own capacity through extended training and learning.

{Photo by Jose Ros Photo on Unsplash}



Starting Considerations

- Monitor resource subsystems
- Anomalies may indicate operational problems
- Monitor “crown jewels” and tag Critical systems
- Identify gaps in coverage

Student Notes

Here are some starting considerations:

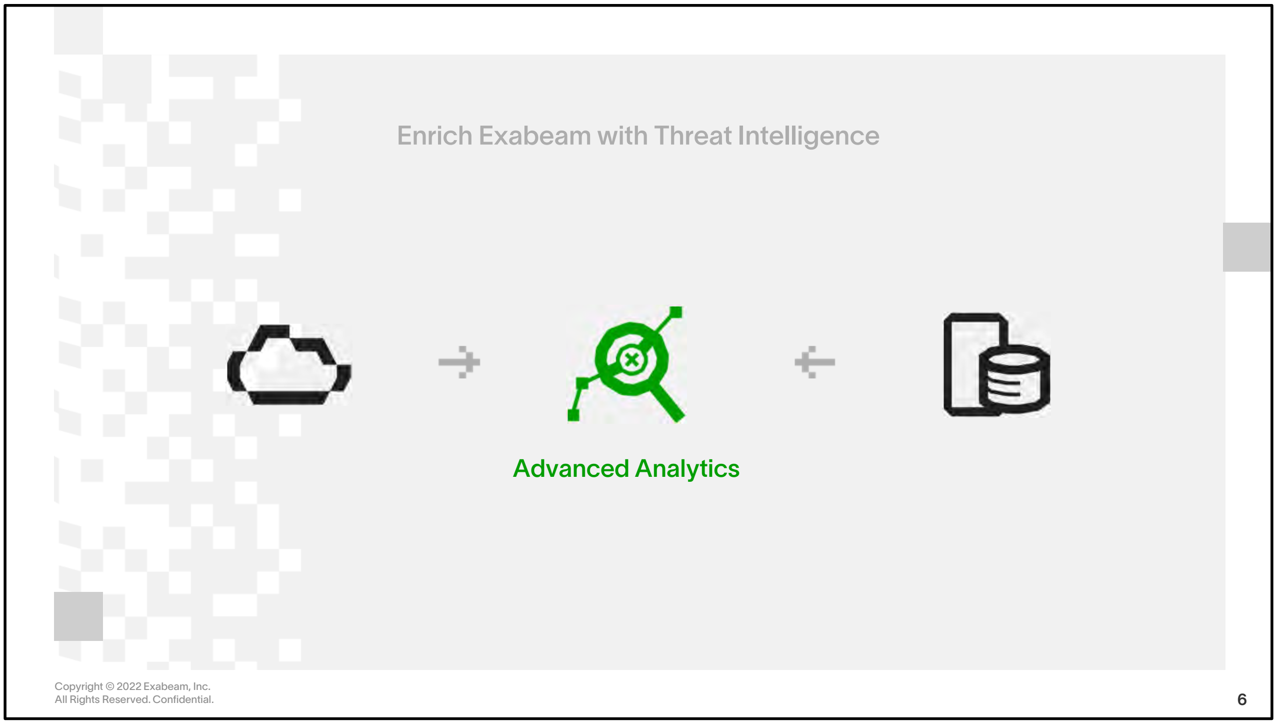
- Monitor resource subsystems – actively monitor the health of Advanced Analytics components and subsystems as well as the health of log sources.
- Monitor “crown jewels” – actively monitor critical, high-priority systems. Tagging those systems results in higher risk scores.
- Anomalies may indicate operational problems – If a service goes down or is misconfigured, it may appear as an anomaly.
- Identify gaps in coverage – Consider any data sources you may be missing that could be beneficial to Advanced Analytics. For example, you may find analysts asking the same set of questions repeatedly. These questions may indicate an opportunity for automation and Advanced Analytics.

One expert’s recommendation is to create a log source library. Identify the logs in your organization. List what those logs provide and then prioritize them based on content and ease of ingestion. Finally, create a plan to include those additional logs based on those priorities and execute.

References

https://community.exabeam.com/s/article/Spotlight19-Best-Practices-to-Integrate-Exabeam-into-Your-Security-Operations

https://docs.exabeam.com/en/advanced-analytics/i57/advanced-analytics-administration-guide/127369-advanced-analytics.html



Enrich Exabeam with Threat Intelligence

Student Notes

Consider enhancing Advanced Analytics or Data Lake with external threat intelligence sources. This is called the Exabeam Threat Intelligence Service (TIS) which delivers a constant stream of up-to-date threat indicators to Advanced Analytics deployments.

The categories of indicators affected are the following:

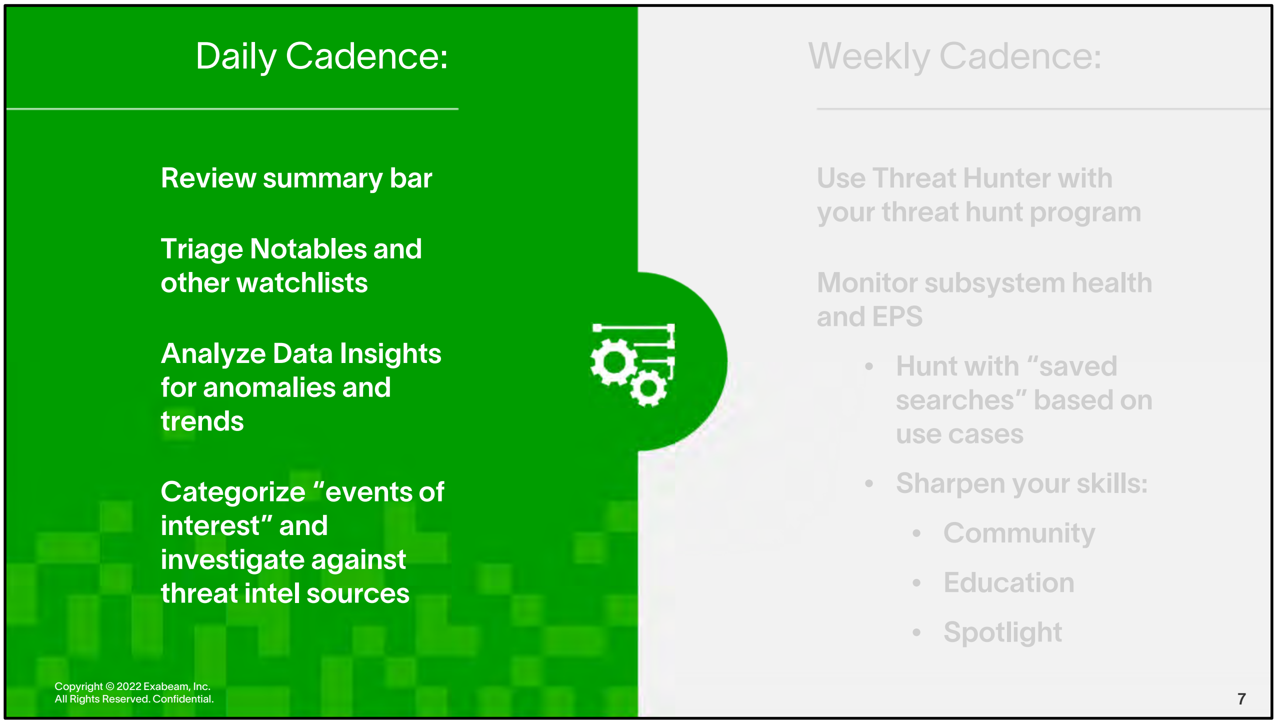
- IP addresses associated with Ransomware or Malware attacks
- IP addresses associated with the TOR network
- Domain names associated with Ransomware, Phishing or Malware attacks

Indicators are downloaded by SaaS and on premises deployments from TIS on a daily basis.

More information is available in the latest Administration Guide.

References

https://community.exabeam.com/s/article/Threat-Intelligence-Service-Overview-3173254
https://community.exabeam.com/s/article/Threat-Intelligence-Service-FAQs



Daily Cadence:

Review summary bar

Triage Notables and other watchlists

Analyze Data Insights for anomalies and trends

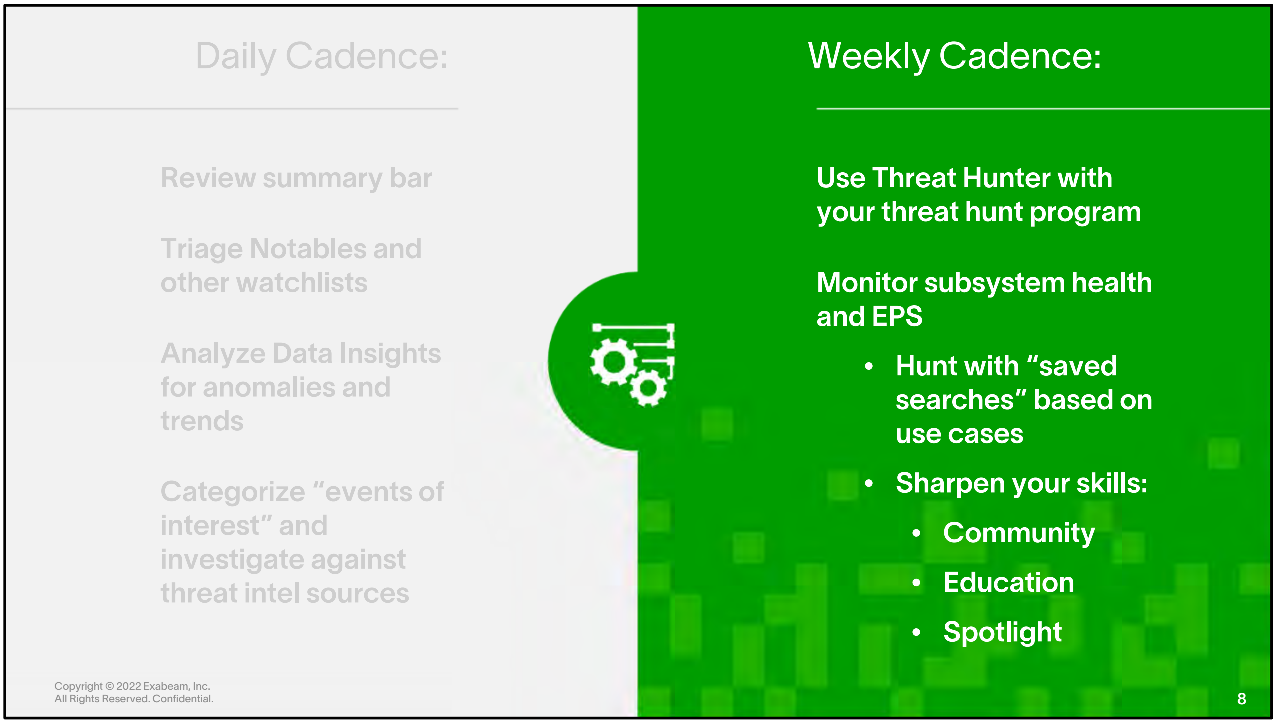
Categorize “events of interest” and investigate against threat intel sources

Weekly Cadence:

Use Threat Hunter with your threat hunt program

Monitor subsystem health and EPS

- Hunt with “saved searches” based on use cases
- Sharpen your skills:
  - Community
  - Education
  - Spotlight



Daily Cadence:

Review summary bar

Triage Notables and other watchlists

Analyze Data Insights for anomalies and trends

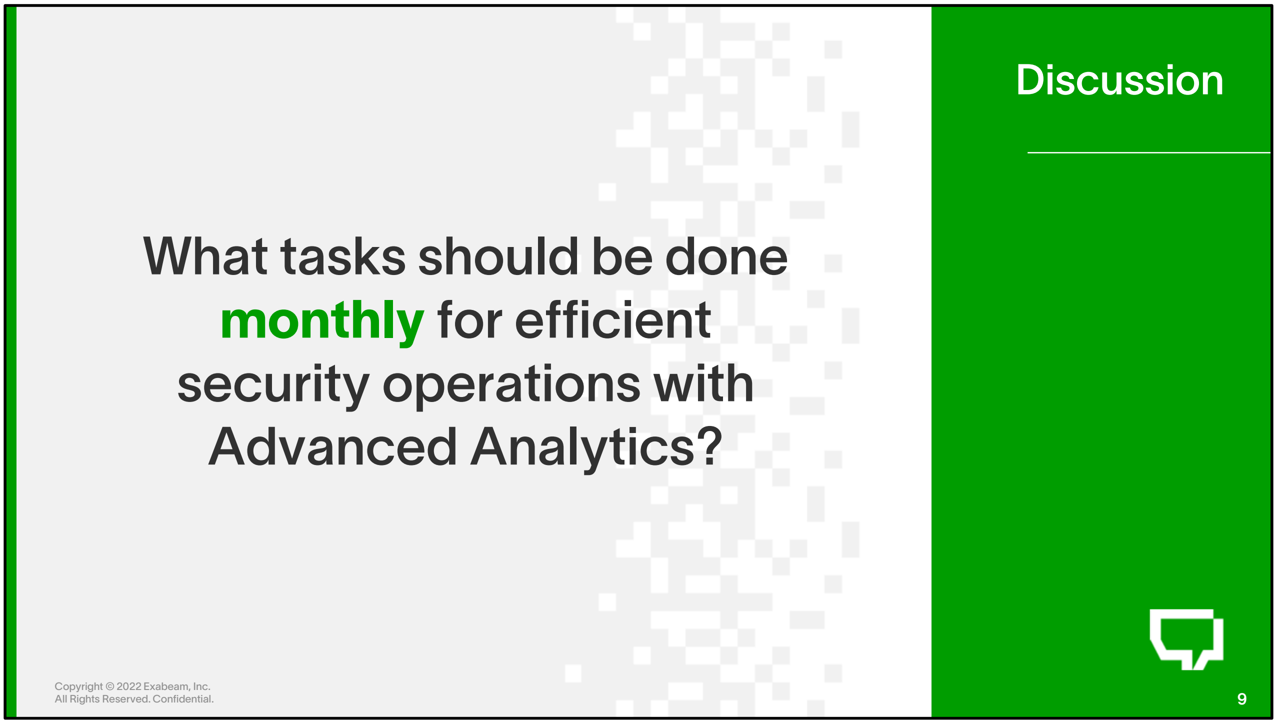
Categorize “events of interest” and investigate against threat intel sources

Weekly Cadence:

Use Threat Hunter with your threat hunt program

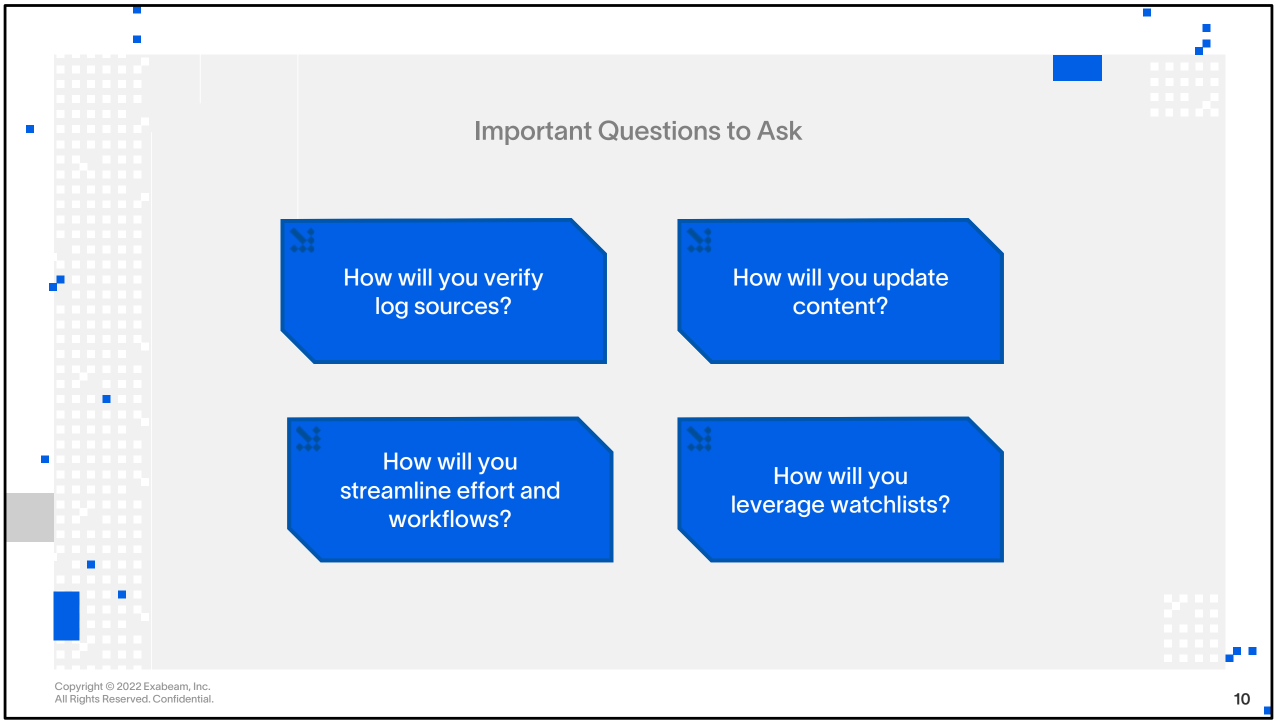
Monitor subsystem health and EPS

- Hunt with “saved searches” based on use cases
- Sharpen your skills:
  - Community
  - Education
  - Spotlight



Discussion

What tasks should be done **monthly** for efficient security operations with Advanced Analytics?



Important Questions to Ask

How will you verify log sources?

How will you update content?

How will you streamline effort and workflows?

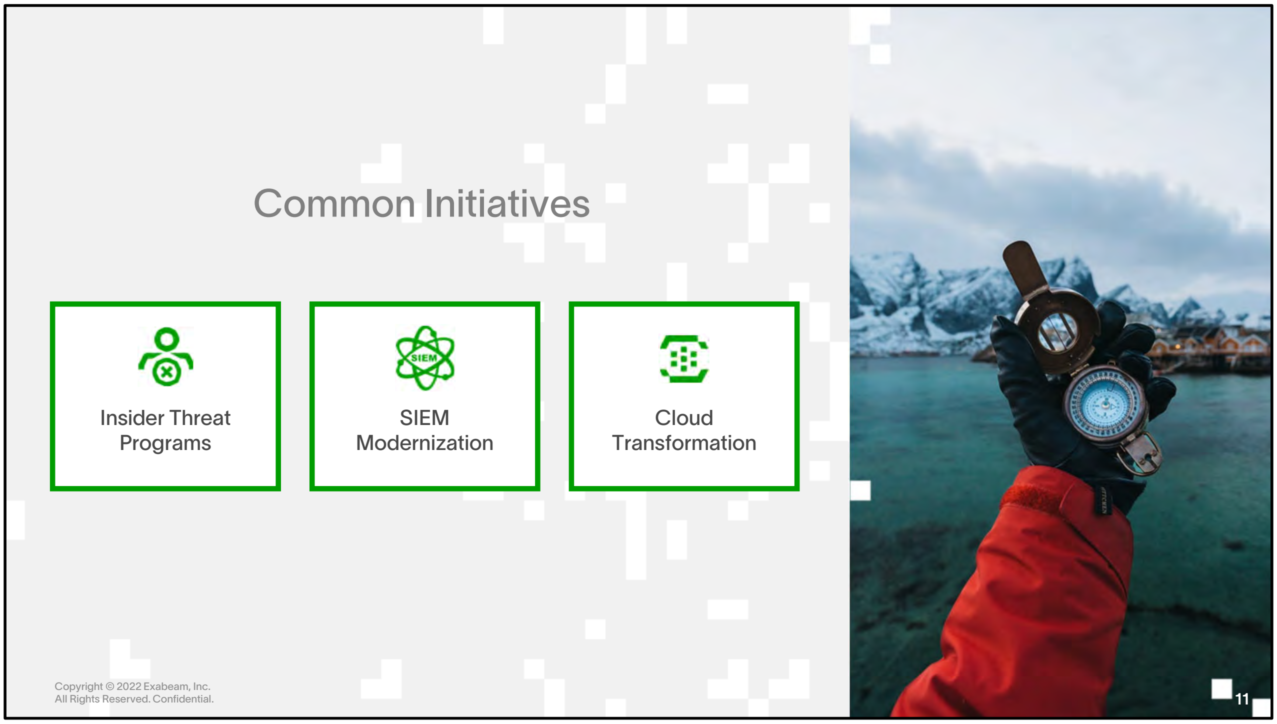
How will you leverage watchlists?

10

Student Notes

Here are some other things to consider:

- If you just onboarded a new log source, have a plan to verify data from that source is moving through our processing systems (i.e., Log > Message > Event > flow to Mongo DB). Develop a strong relationship with your Advanced Analytics Admin/Engineer or Service Delivery Partner
- Ensure Advanced Analytics is updated when new instances are released to the community
- Know & work the content (models, rules, context & enrichment sources, etc.)
- Leverage Advanced Analytics to identify, streamline, and reduce unnecessary duplication regarding threat hunting, incident monitoring, detection, and response capabilities, including toolsets and competencies.
- Match critical business security risk issues with watchlists (for example, HR identified, merger & acquisition network risks, traveling employees within high cyber risk countries, etc.)



Common Initiatives

Insider Threat Programs

SIEM Modernization

Cloud Transformation

Student Notes

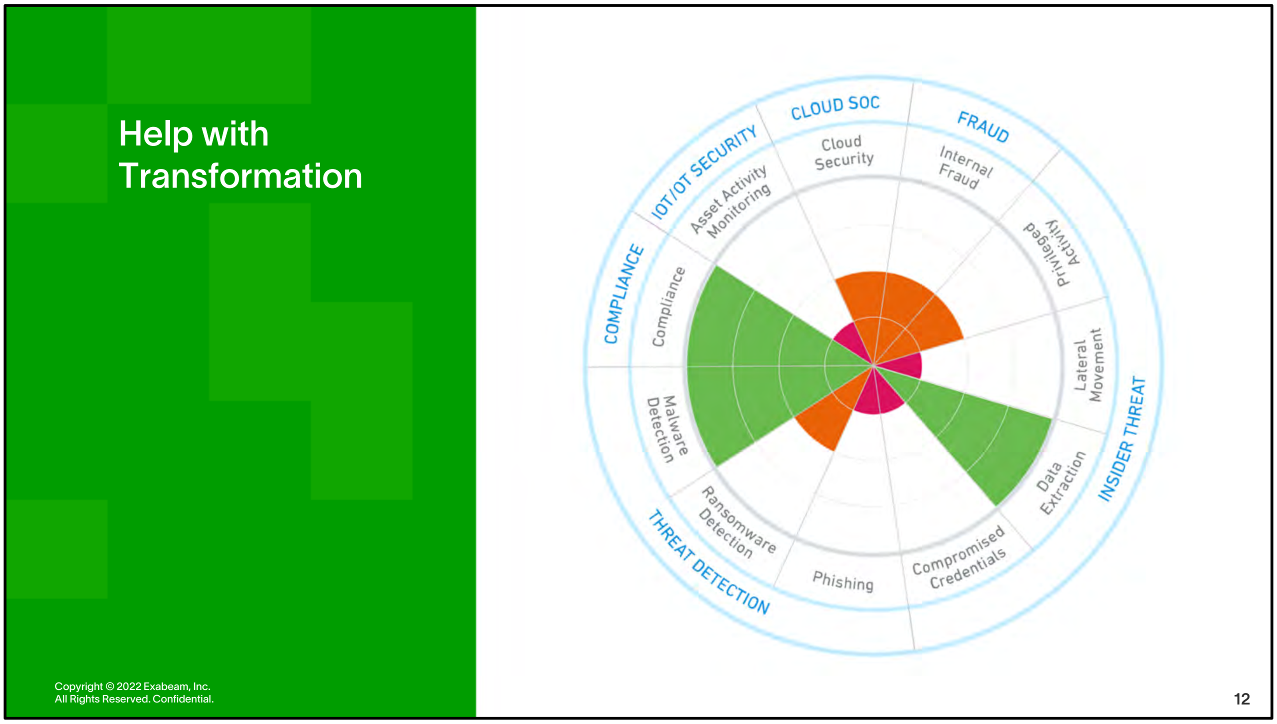
Exabeam helps CISOs with transformational initiatives such as these:

Insider Threat Program – many organizations are adding a new team specifically to help hunt for malicious or compromised insiders.

SIEM Modernization – many organizations are using outdated SIEM tech that pre-dates many of their endpoint, application and network security controls. It likely does not use modern big data tech, machine learning, and may not include UEBA or SOAR. It may also have a pricing model that is prohibitive.

Cloud Transformation – most organizations are moving applications to the cloud. Some are considering moving their security tools to the cloud.

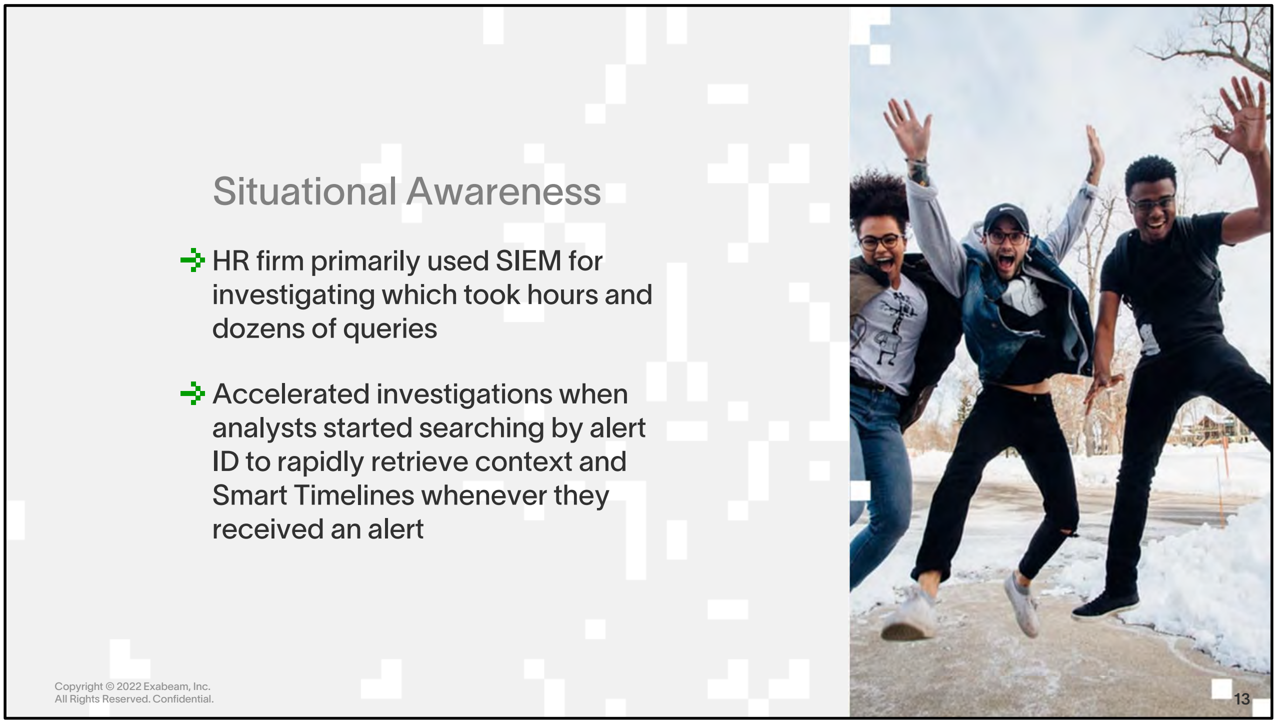
{Photo by Simon Migaj on Unsplash}



Help with Transformation

Student Notes

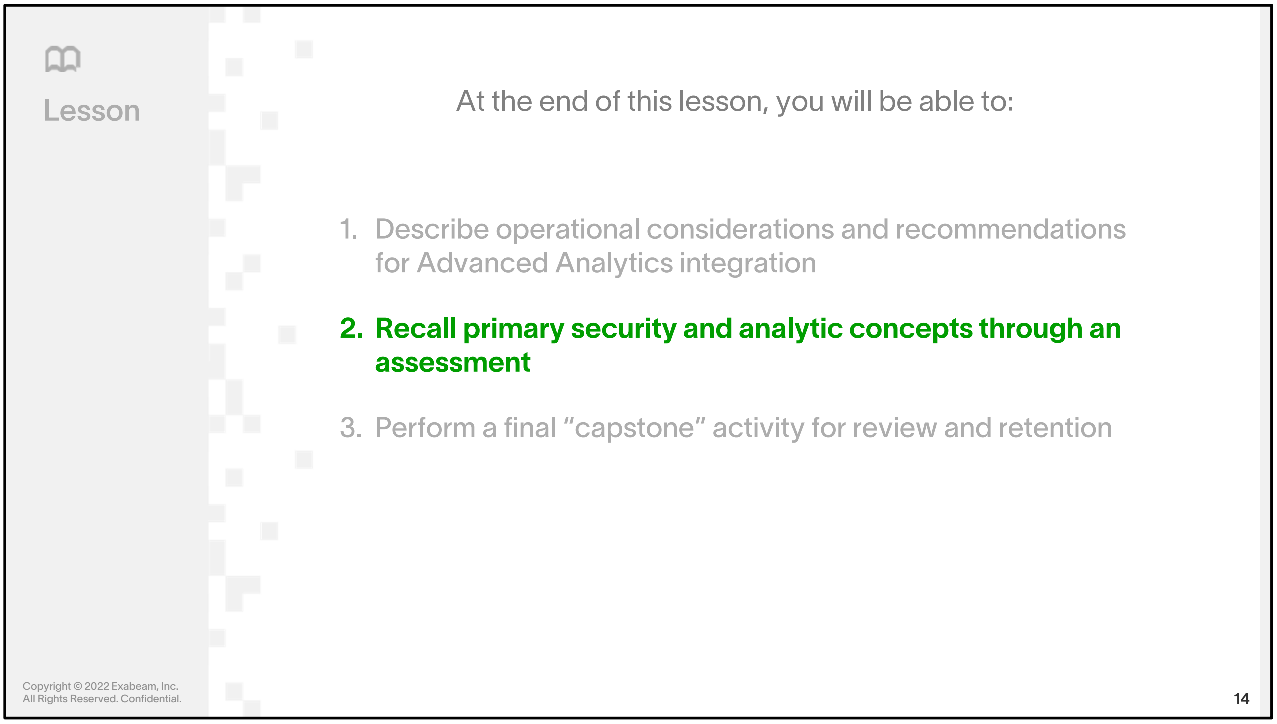
Exabeam helps organizations with maturing their security solutions. Around the outside of the circle are the six main solution areas where Exabeam can help. Grouped inside are the use cases, like compliance and phishing. The ’radar’ diagram is how we depict maturity across those use cases with our clients.



Situational Awareness

- HR firm primarily used SIEM for investigating which took hours and dozens of queries
- Accelerated investigations when analysts started searching by alert ID to rapidly retrieve context and Smart Timelines whenever they received an alert

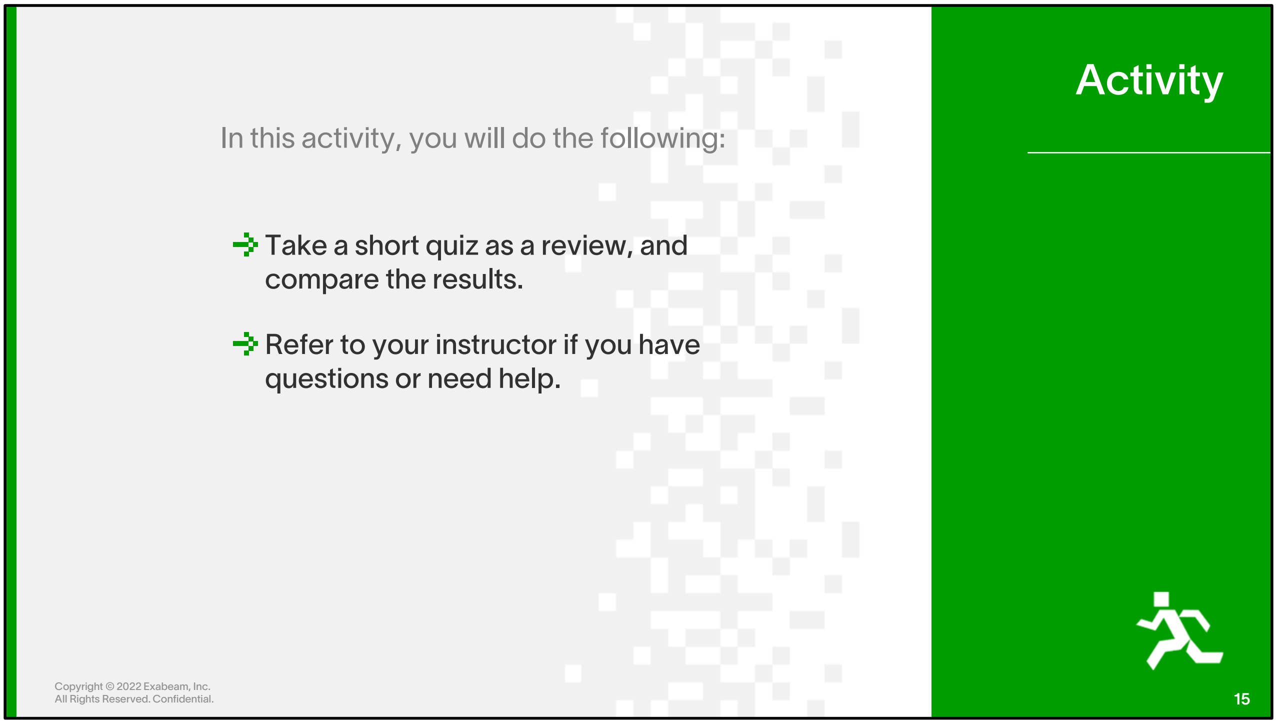
Photo by Lukas Juhas on Unsplash



Lesson

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

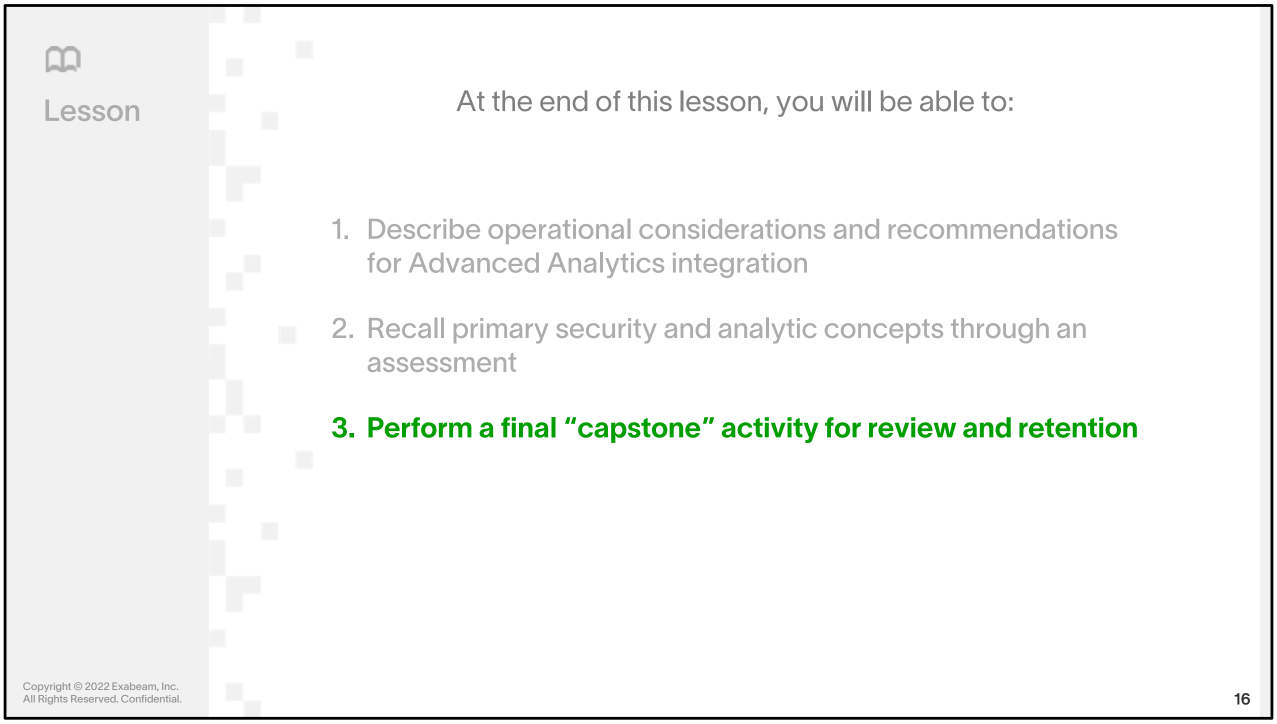
1. Describe operational considerations and recommendations for Advanced Analytics integration
2. **Recall primary security and analytic concepts through an assessment**
3. Perform a final "capstone" activity for review and retention



Activity

In this activity, you will do the following:

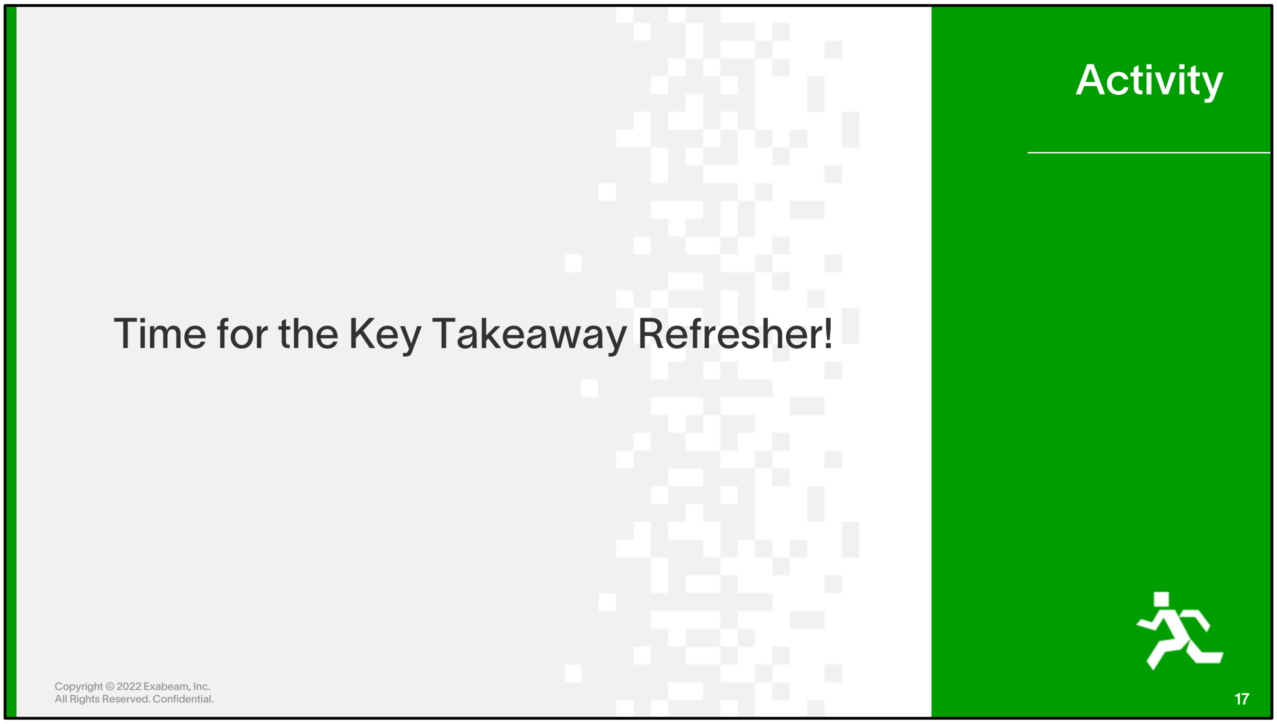
- Take a short quiz as a review, and compare the results.
- Refer to your instructor if you have questions or need help.



Lesson

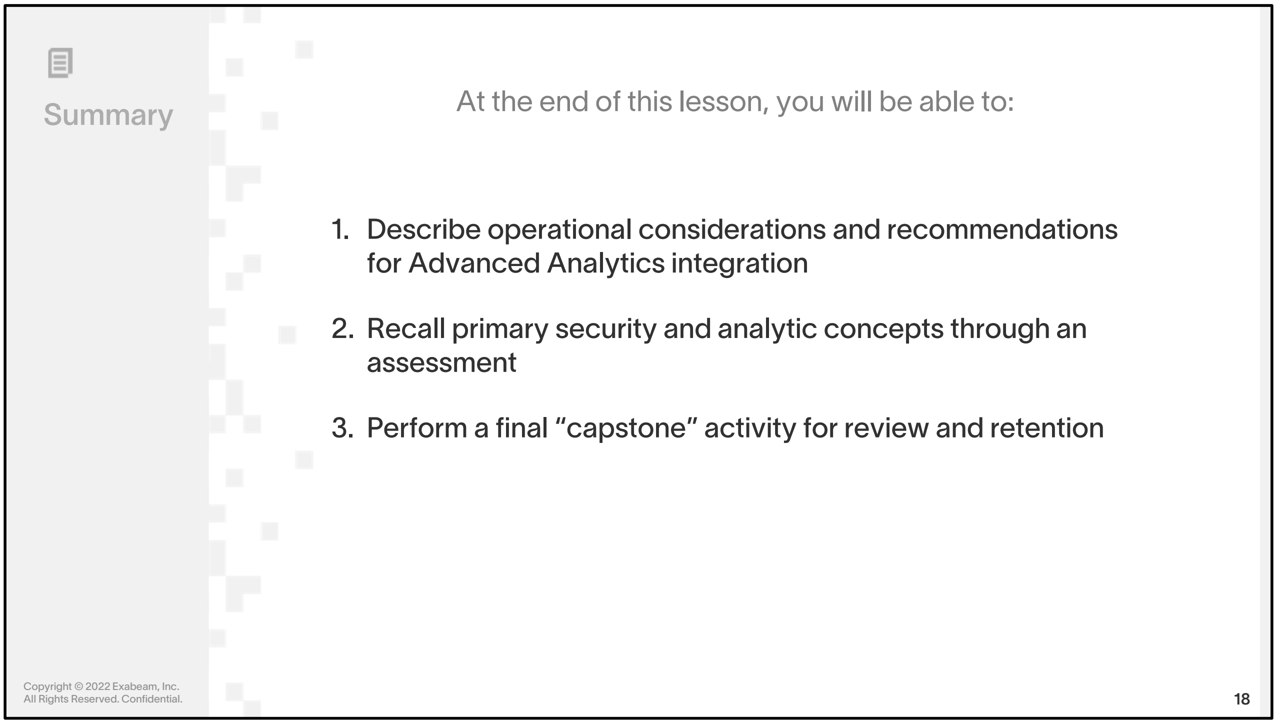
At the end of this lesson, you will be able to:

1. Describe operational considerations and recommendations for Advanced Analytics integration
2. Recall primary security and analytic concepts through an assessment
3. **Perform a final “capstone” activity for review and retention**



Activity

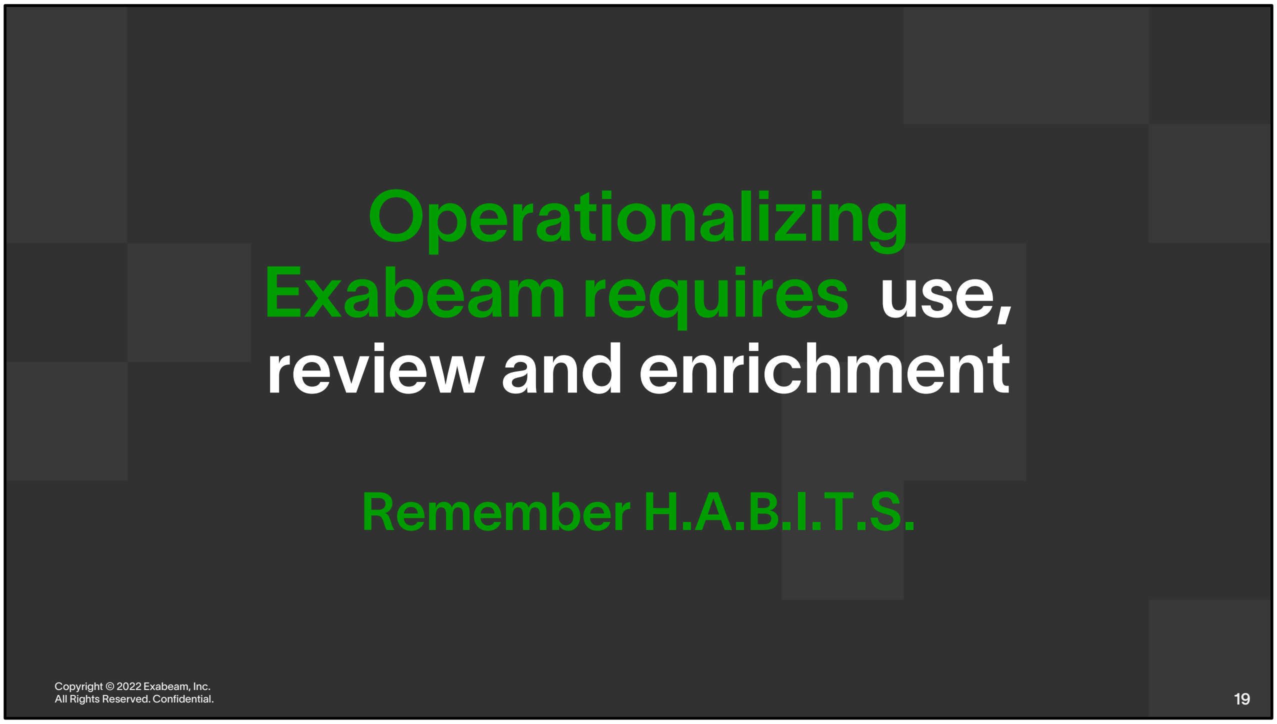
Time for the Key Takeaway Refresher!



Summary

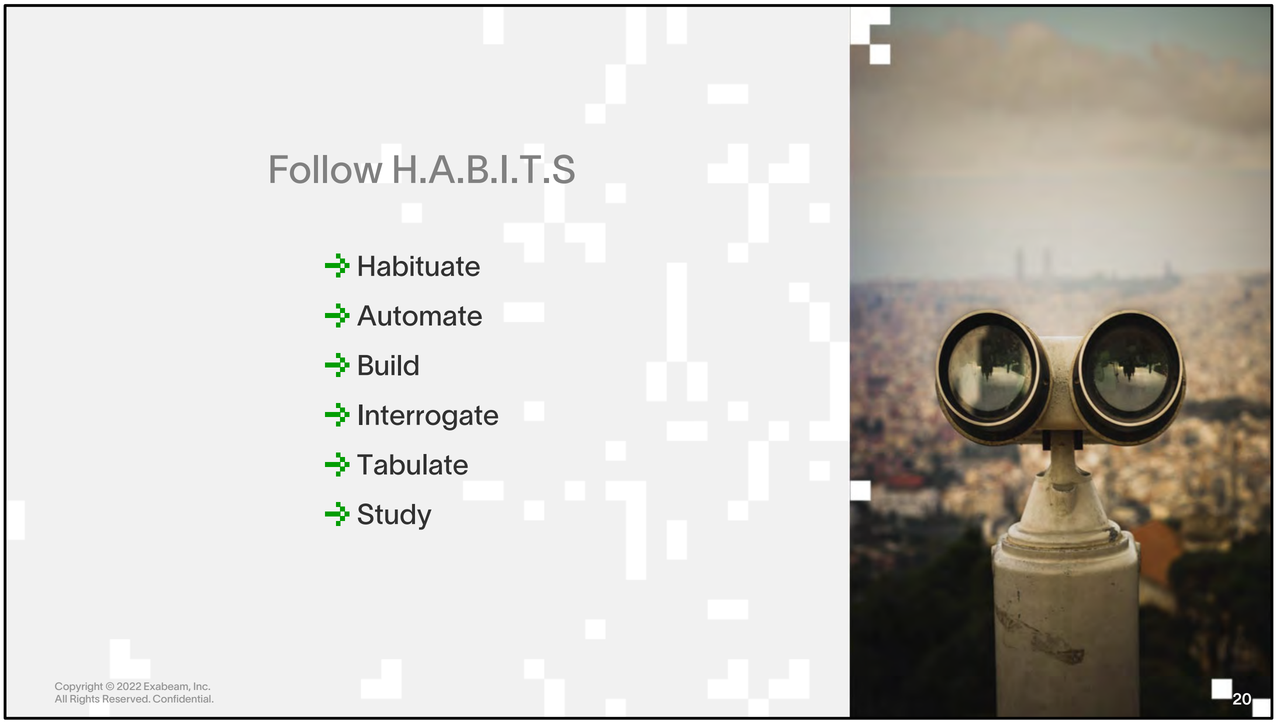
At the end of this lesson, you will be able to:

1. Describe operational considerations and recommendations for Advanced Analytics integration
2. Recall primary security and analytic concepts through an assessment
3. Perform a final “capstone” activity for review and retention



Operationalizing Exabeam requires use, review and enrichment

Remember H.A.B.I.T.S.



Follow H.A.B.I.T.S

- Habituate
- Automate
- Build
- Interrogate
- Tabulate
- Study

Student Notes

- **H**abituate –Create operational habits around Advanced Analytics for daily triage and weekly investigations. Create daily/weekly/monthly cadences. Use Threat Hunter. This should include infrastructure and subsystem monitoring. Also, find ways to get additional value from it by allowing HR to use the platform with reduced privileges. This way, business policy use cases can be offloaded to HR rather than burden the security team
- **A**utomate –Identify use cases for automation to improve response times and consider a SOAR solution.
- **B**uild - Improve the efficiency of Advanced Analytics in your organization through building new workflows, log sources, context, custom models and more. Consider building use cases and playbooks for Advanced Analytics. Consider Entity Analytics. Enrich your context with new data sources.
- **I**nterrogate - Ask the hard questions about processes and solutions such as, How do security operations affect the business? Are we measuring the right things?
- **T**abulate - Measure the impact of Advanced Analytics on the business and measure the impact on security operations.
- **S**tudy - Grow your team and your own capacity through extended training and learning

{Photo by Jose Ros Photo on Unsplash}

Final Thought

What are your **operational Priorities** for Advanced Analytics?