exabeam
Education

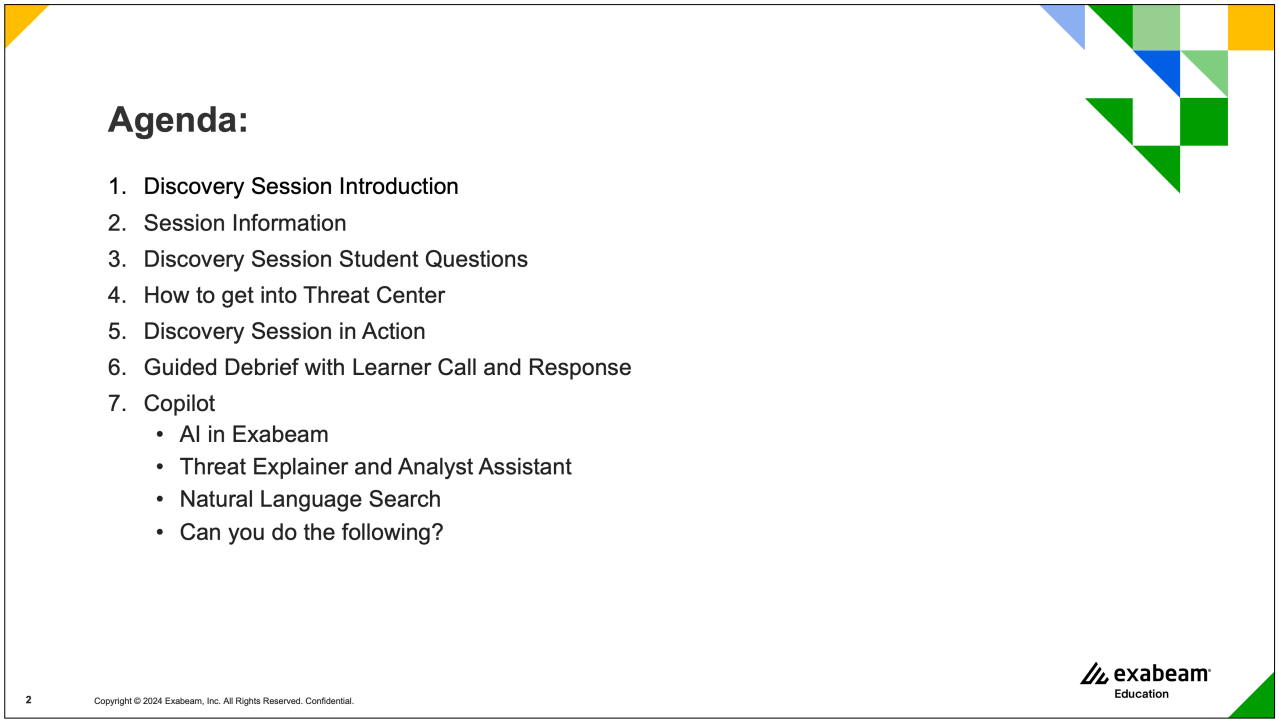
Exabeam Spotlight 24

Table of Contents

Student Notes

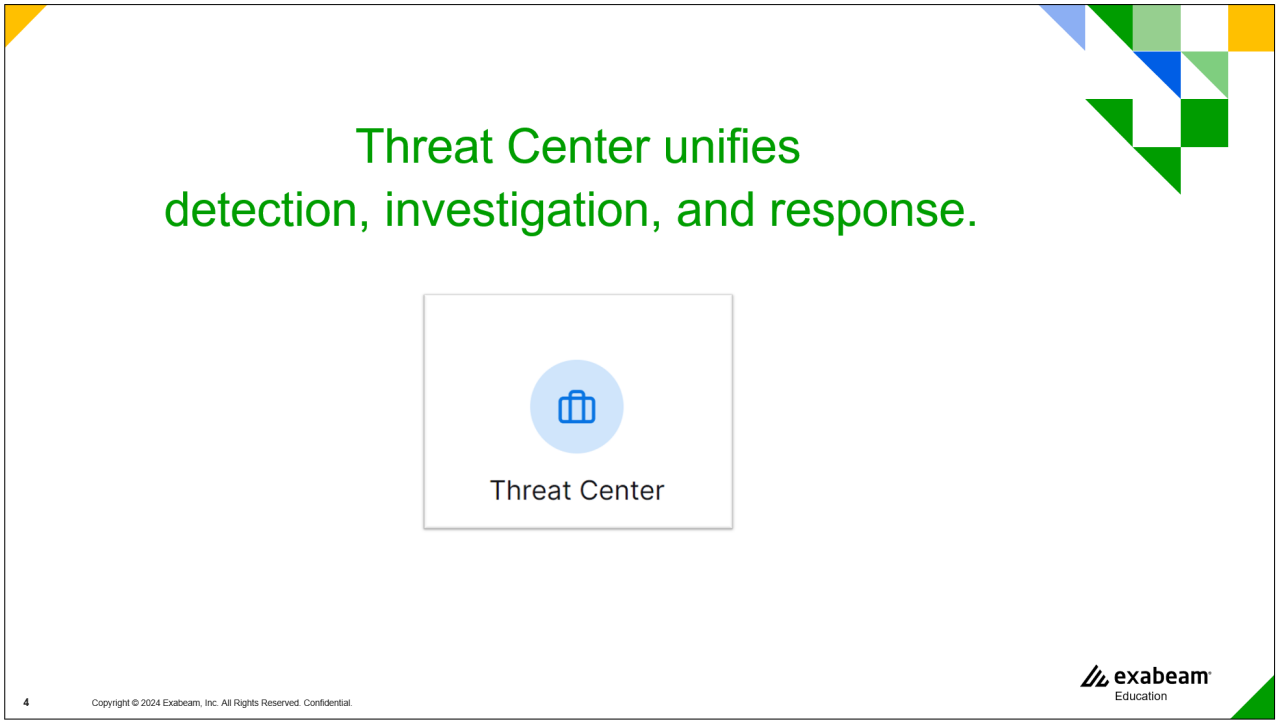
Threat Center, on the Exabeam Security Operations Platform, is like your cybersecurity command center. It centralizes detections, alerts, and cases, streamlining your workflow. When a threat arises, Threat Center summarizes the core information, assesses risk, and lets you act.

Imagine having a central hub where all the action happens—the place where threats are detected, investigated, and responded to. Well, that's Threat Center! It's like the mission control for your cybersecurity team. Let's dive into a few details:

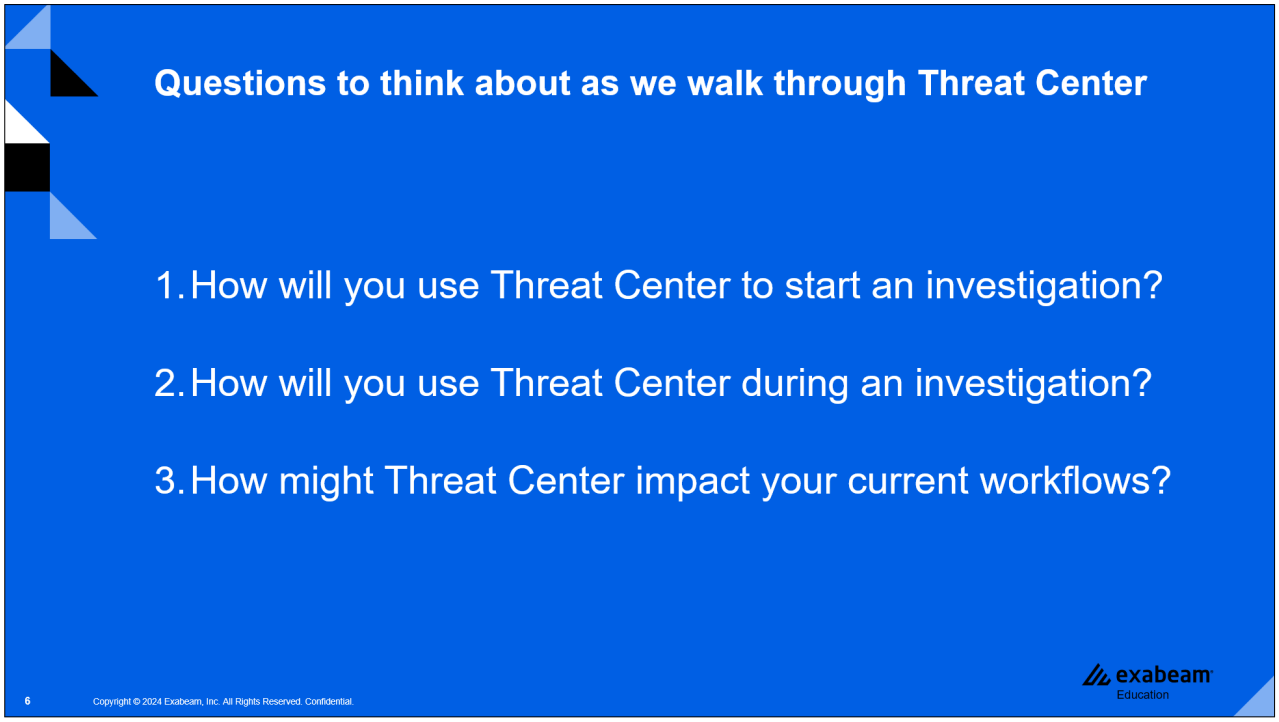


Ok, enough talk! Let's get into the product and see what it's all about. Threat Center is a place where every alert, detection, and case comes together in one streamlined workflow. That’s what you’re about to experience. When a threat looms on the horizon, Threat Center is your lookout point, summarizing key information, assessing the risk, and empowering you to take decisive action. It’s the central hub where all the cybersecurity action takes place—detecting, investigating, and responding to threats efficiently.

Get ready to see how Threat Center transforms your cybersecurity operations. Let’s get started!



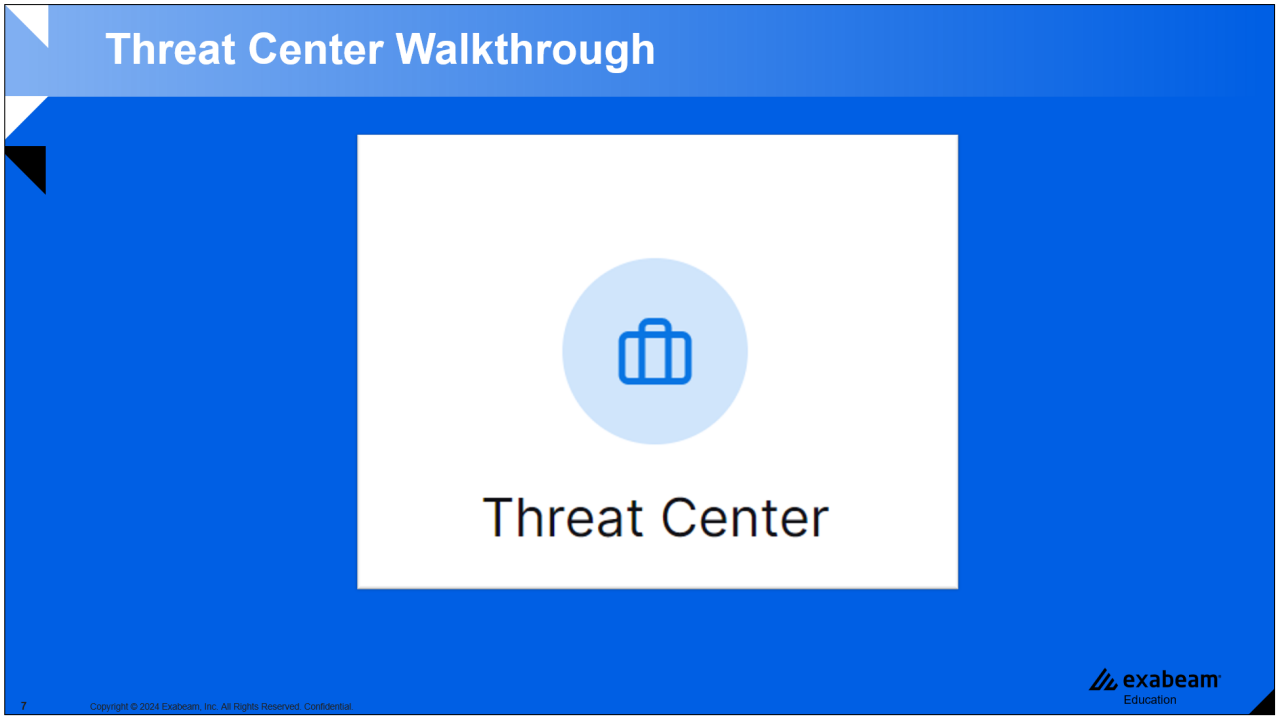
Threat Center is designed to be your unified workbench for threat discovery, investigation, and response. View Threat Center from the perspective of you how can naturally find ways to accomplish your day-to-day tasks and goals with Exabeam quickly and confidently.



When going through Threat Center for this firs time, try to balance your natural curiosity and discovery.

Some questions you might want to seek the answer to are:

How will you use Threat Center to start an investigation?
How will you use Threat Center during an investigation?
How might Threat Center impact your current workflows?



Threat Center is accessed by clicking on the Threat Center tile on the Exabeam home screen.


exabeam
Education
Getting to Know
Exabeam Copilot
Copyright © 2024 Exabeam, Inc. All Rights Reserved. Confidential.

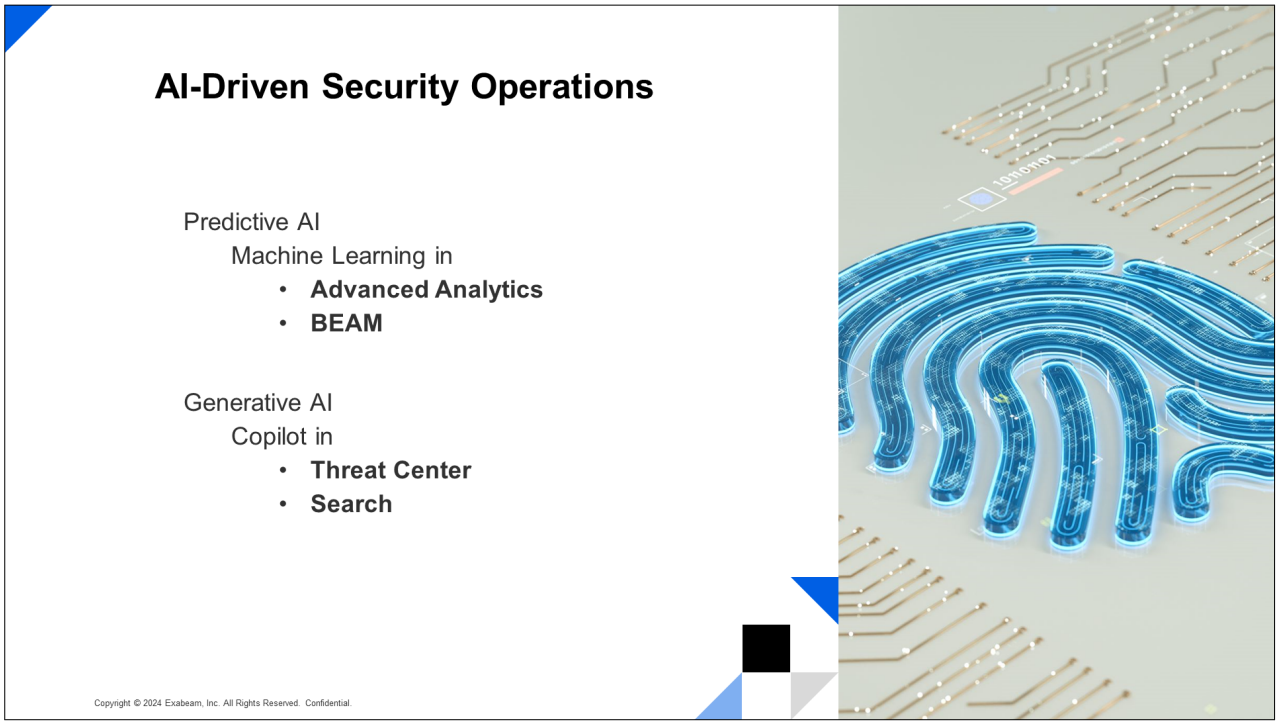
AI in Exabeam

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

1. Describe the core aspects of AI in the Exabeam platform
2. Leverage Copilot Threat Explainer in the analyst workflow and drill down into investigation details using Copilot Analyst Assistant
3. Search and hunt using Copilot Natural Language Search

exabeam Education

AI-Driven Security Operations



Student Notes

From its inception, Exabeam has deeply integrated predictive artificial intelligence into its UEBA platform to better equip cybersecurity professionals. UEBA is a category of cybersecurity tools that focus on detecting network intrusions. Unlike traditional security tools that rely on known attack patterns and signatures, UEBA employs advanced analytics to identify anomalous behavior that may indicate a threat. This allows for the detection of previously unknown attacks and enables organizations to respond more effectively.

UEBA uses various modern technologies to identify abnormal behavior, even without known patterns. These include:

- Supervised machine learning
- Bayesian networks
- Unsupervised learning
- Reinforced/semi-supervised machine learning
- Deep learning

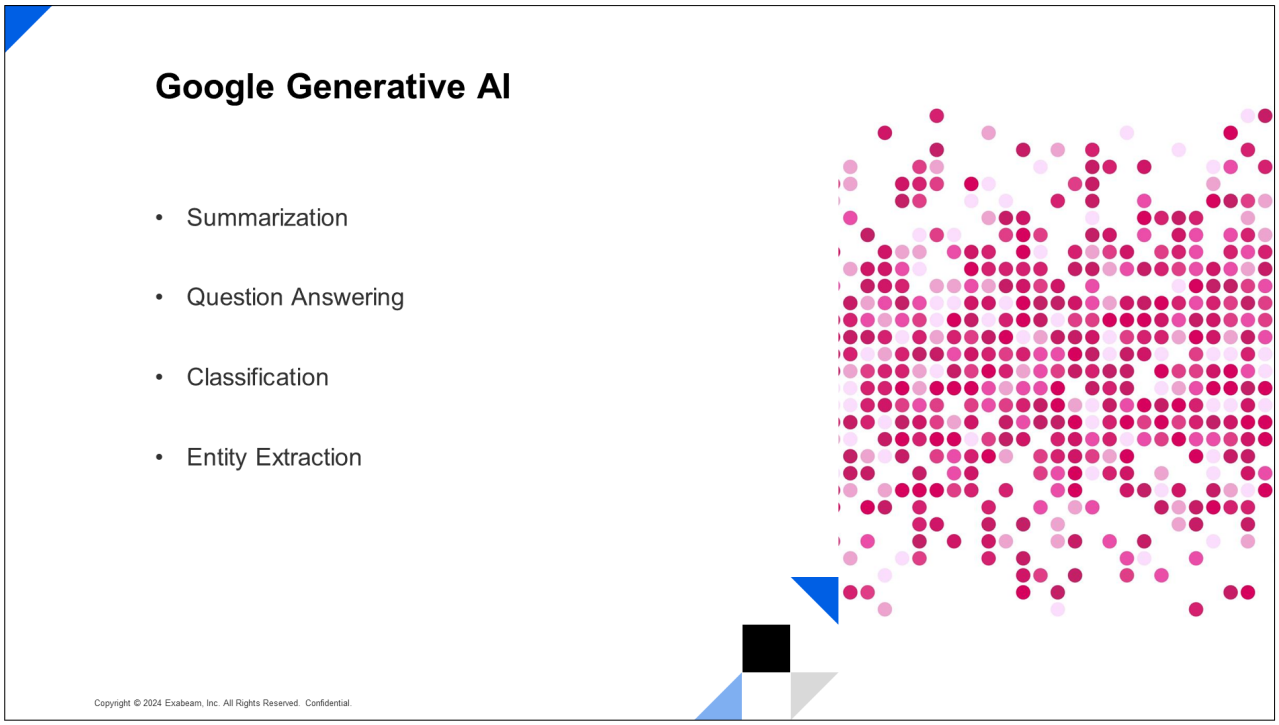
Adding to this existing predictive AI, Exabeam Copilot is the generative AI experience of the Exabeam Security Operations Platform. Copilot encompasses 3 distinct features in the platform:

- Threat Explainer
- Analyst Assistant

- Natural Language Search

Resources
A CISO's Guide to the AI Opportunity in Security Operations

Google Generative AI



Student Notes

Exabeam Copilot leverages Google's Generative AI platform, which provides UI and API-based access to a number of models.

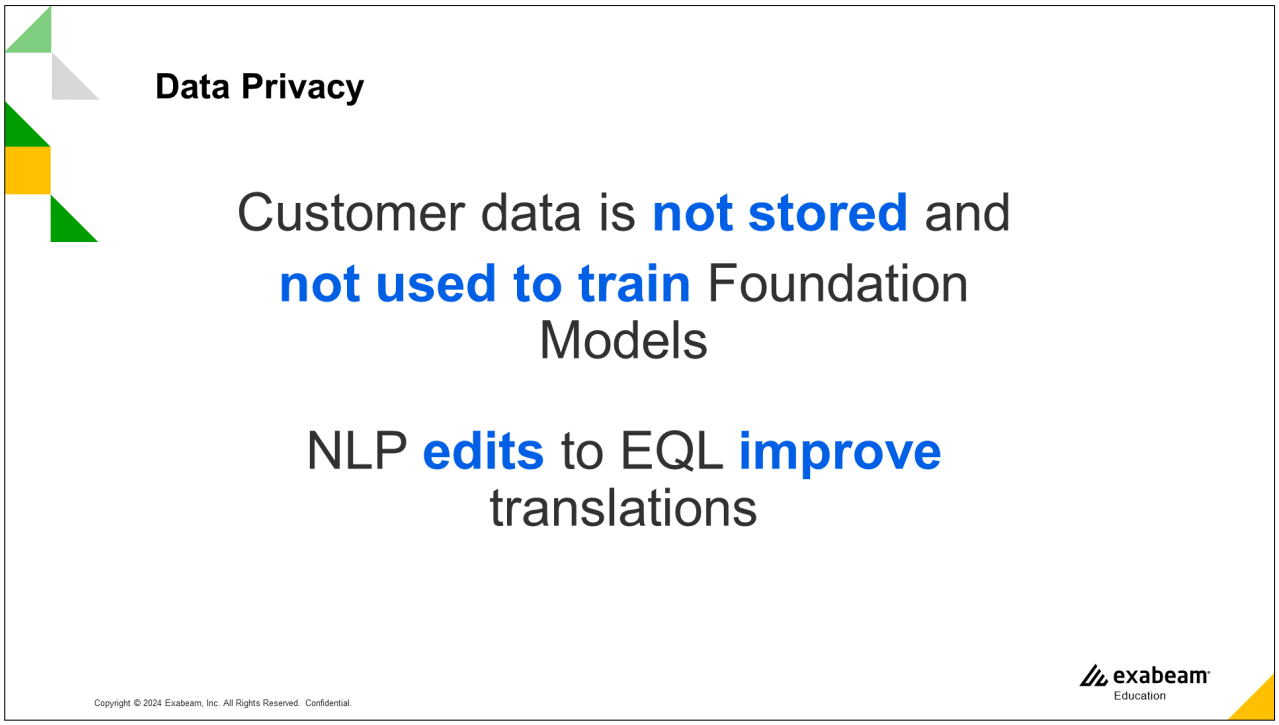
Text Model Use Cases

- **Summarization**: Create a shorter version of a document that incorporates pertinent information from the original text. For example, you might want to summarize a chapter from a textbook. Or, you could create a succinct product description from a long paragraph that describes the product in detail.
- **Question Answering**: Provide answers to questions in text. For example, you might automate the creation of a Frequently Asked Questions (FAQ) document from knowledge base content.
- **Classification**: Assign a label to provided text. For example, a label might be applied to text that describes how grammatically correct it is.
- **Entity Extraction**: Extract a piece of information from text. For example, you can extract the name of a movie from the text of an article.

Resources

Google Generative AI

Privacy



Student Notes

All queries are securely forwarded to Google's Generative API endpoint. Queries are sent with limited supporting case or alert data to a Google Security trained AI for analysis. Google Cloud doesn't use customer data to train its Foundation Models. From Google's AI and Data Governance agreement:

"`Inputs and outputs processed by Foundation Models, Adapter Models, and Safety Classifiers during Prediction are Customer Data. Customer Data isn't stored by Google for longer than necessary to generate a customer's output and isn't used to train Google's Foundation Models.`"

For Natural Language Search, user edits to the Advanced Exabeam Query Language (EQL) are fed back into the system to improve the translation accuracy. This is a technique called *prompt engineering*, which involves training the model on the edits made to the query, but not the data itself.

If customers wish to prevent analysts from using this AI functionality, they can file a support ticket and Exabeam will prevent AI lookups. This can be specific to Threat Explainer, Analyst Assistant queries, or Natural Language Search individually or collectively.

Resources

Generative AI and Data Governance

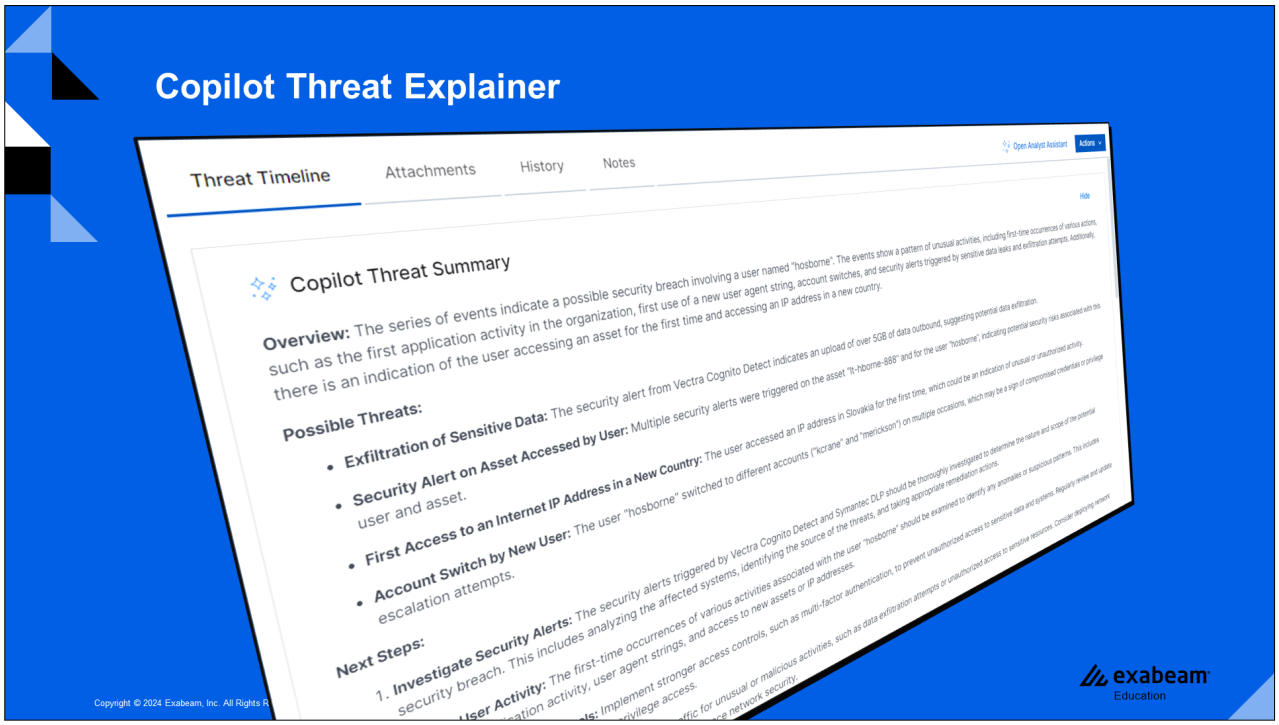
Threat Explainer and Analyst Assistant

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

1. Describe the core aspects of AI in the Exabeam platform
2. Leverage Copilot Threat Explainer in the analyst workflow and drill down into investigation details using Copilot Analyst Assistant
3. Search and hunt using Copilot Natural Language Search

exabeam Education

Copilot Threat Explainer



Student Notes

To help you quickly make sense of a case or alert without reviewing all the details, Threat Explainer gives you an overview of the threat(s) described in a case or alert with an AI-generated summary. In the Threat Timeline tab, Copilot Threat Explainer uses case or alert information to summarize the details, highlight the possible threats, and recommend next steps for addressing the risk.

Some of the Copilot Threat Summary benefits to the analyst include:

- Train security analysts faster and empower "3rd-shift" analysts
- Help prioritize the most concerning threats surfaced in the timeline to accelerate the analyst's response
- Communicate risk with detailed threat explanations to both technical and non-technical stakeholders in understandable terms
- Learn more about general threats

What Should I Do with the Threat Summary?

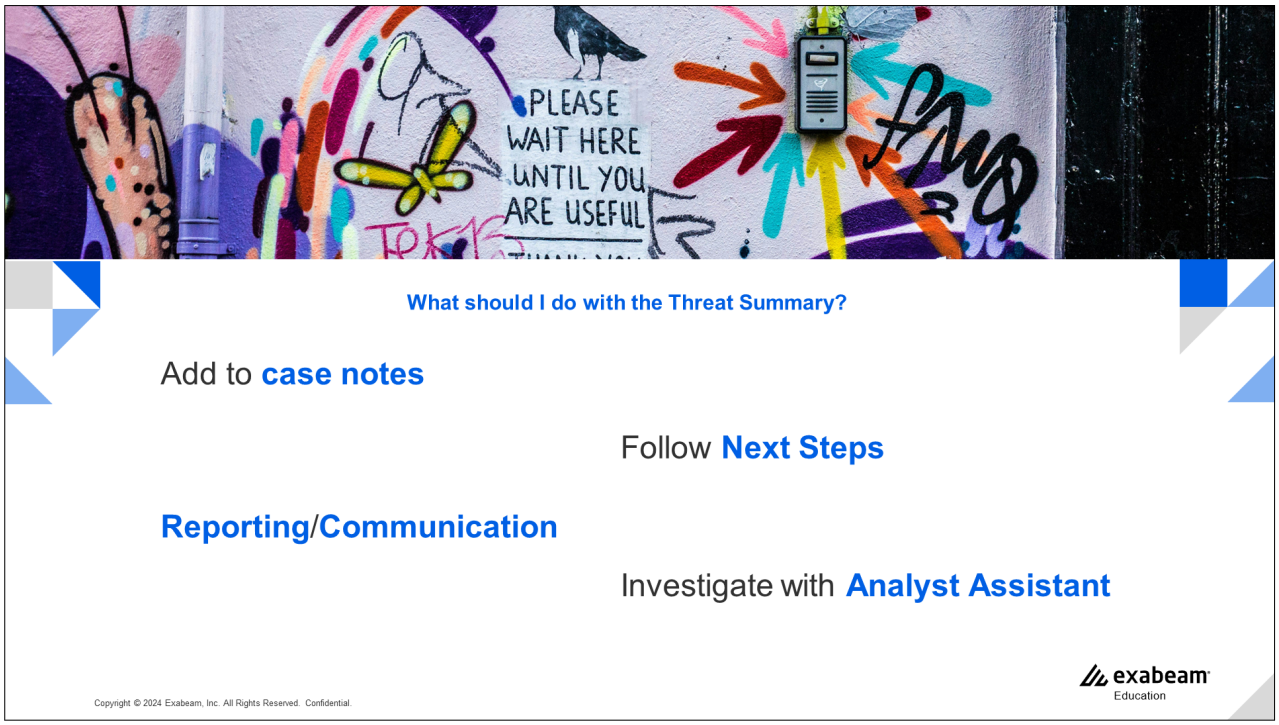


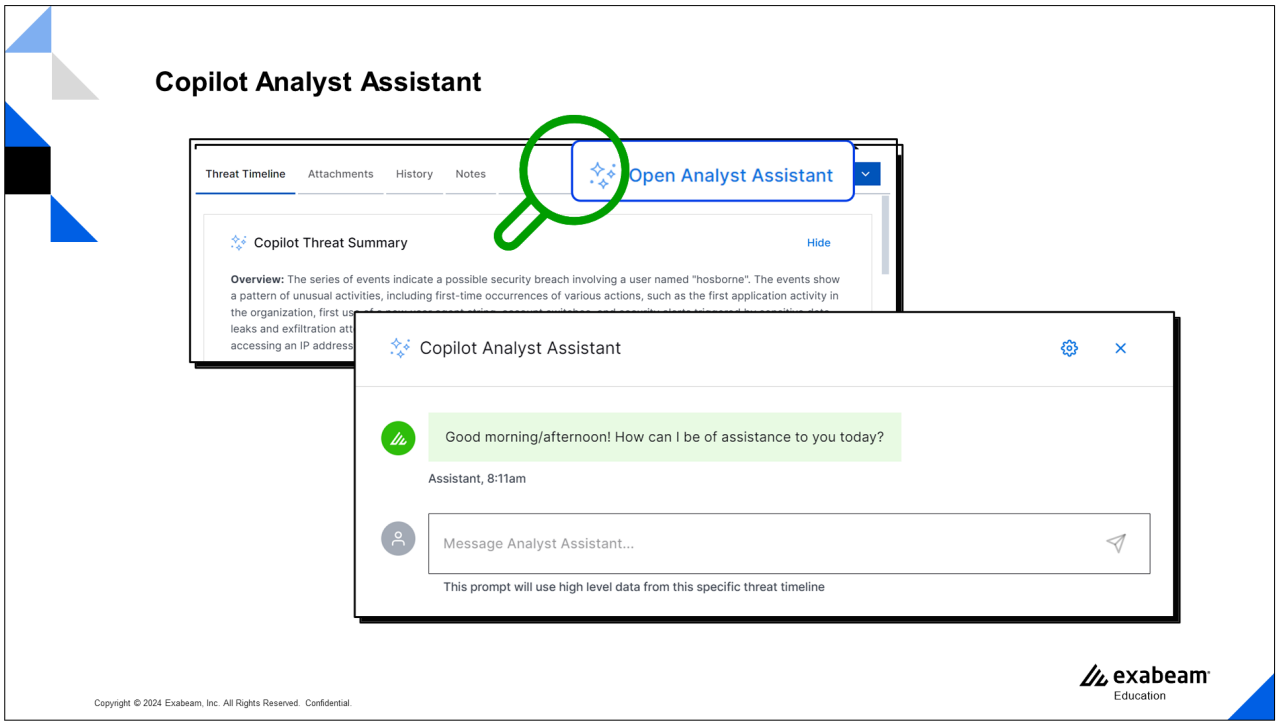
Image courtesy of Ehimetalor Akhere Unuabona on Unsplash

Student Notes

As we saw previously, the Copilot Threat Explainer provides multiple benefits for you as a security analyst. Nonetheless, you'll want to consider specifically how you'll make use of the Threat Summaries provided with each case and alert.

- **Workflow**: You may choose to copy portions of the Threat Summary and paste them into Case notes as a way to document your findings and create an audit trail. Alerts in Threat Center don't include a "Notes" section.
- **Reporting**: The Threat Summary can be a great starting point for building out case reports and for communicating risk, both to your fellow security team members as well as to external groups and stakeholders.
- **Next Steps**: The Next Steps section of the summary provides guidance and best practices for your response. The recommendations you find in this section can be an excellent source of suggestions to continue your investigation using Analyst Assistant and other techniques.
- **Investigate**: Dig deeper using Analyst Assistant prompting. Analyst Assistant is covered in the next topic.

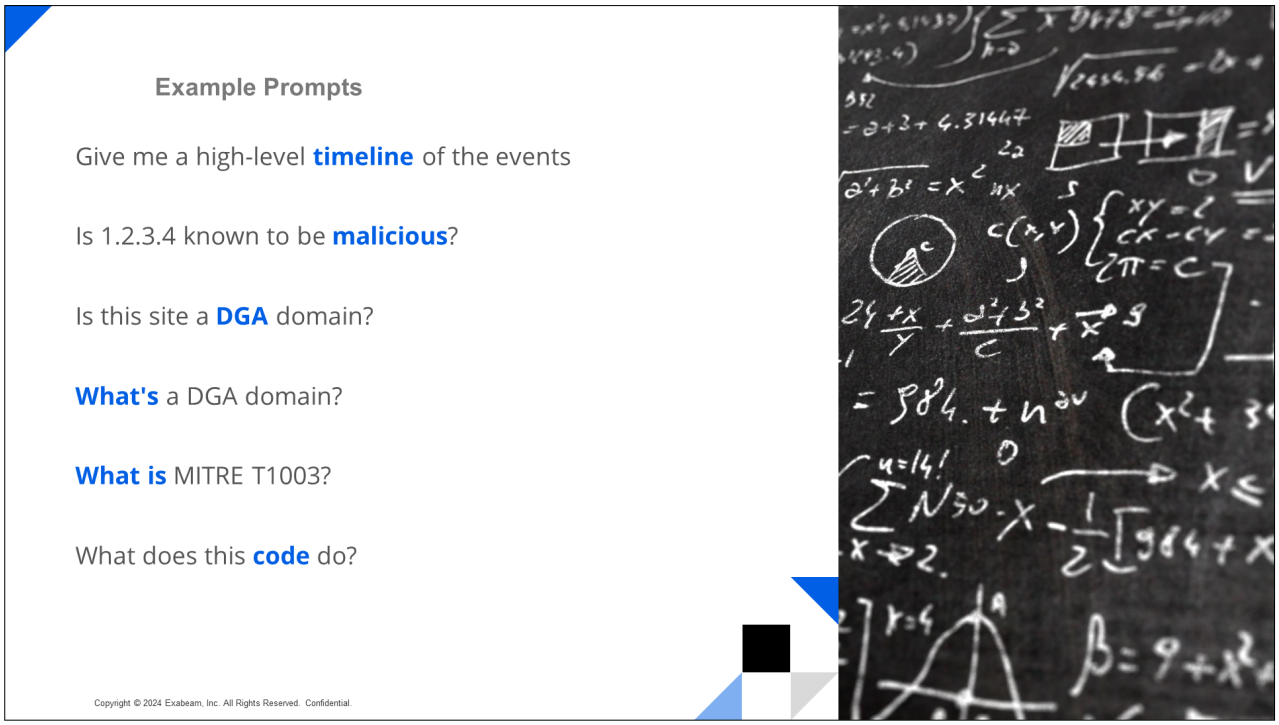
Copilot Analyst Assistant



Student Notes

You can now quickly learn and get answers to questions about a case or alert using an AI assistant. Prompt Copilot Analyst Assistant with a message or query, and it interprets case or alert information to generate a natural language response.

Analyst Assistant Example Prompts

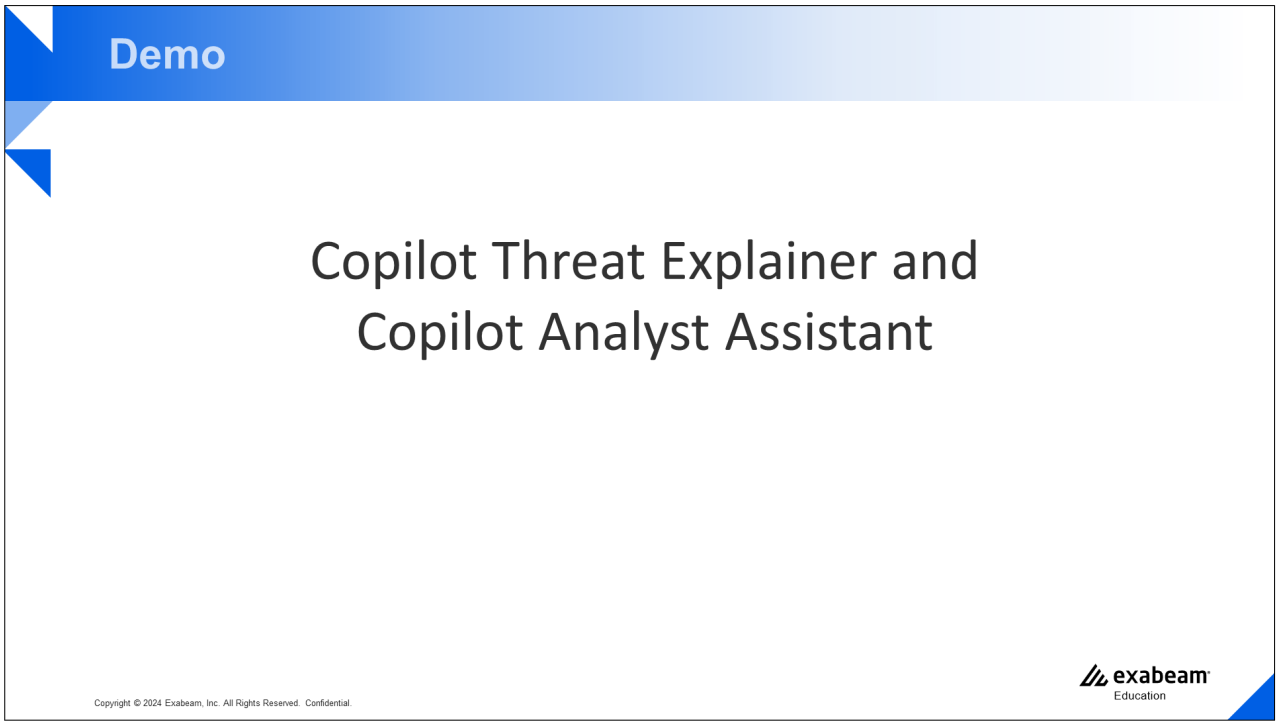


Student Notes

The Copilot Analyst Assistant will process many types of questions and requests, but here are some examples to get you started:

- Give me a high-level timeline of the events
- Define a security term
- Is <host> known to be malicious?
- Is <host> a known TOR exit node?
- Is <site> a DGA domain?
- What's a DGA domain?
- What is CVE-2022-45177?
- What is MITRE T1003?
- What are the landscapes that are included in the threats in this case?
- What does this Python code do?

Threat Explainer and Analyst Assistant Demo



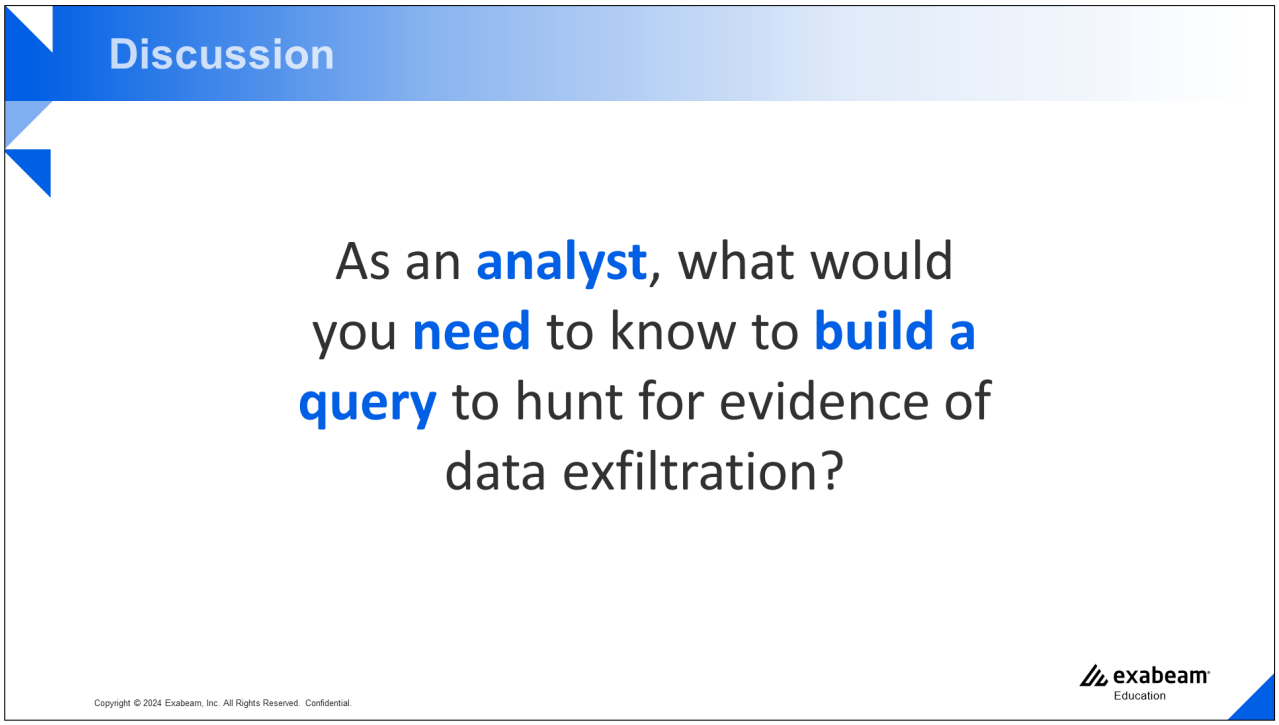
Natural Language Search

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

1. Describe the core aspects of AI in the Exabeam platform
2. Leverage Copilot Threat Explainer in the analyst workflow and drill down into investigation details using Copilot Analyst Assistant
3. Search and hunt using Copilot Natural Language Search

exabeam Education

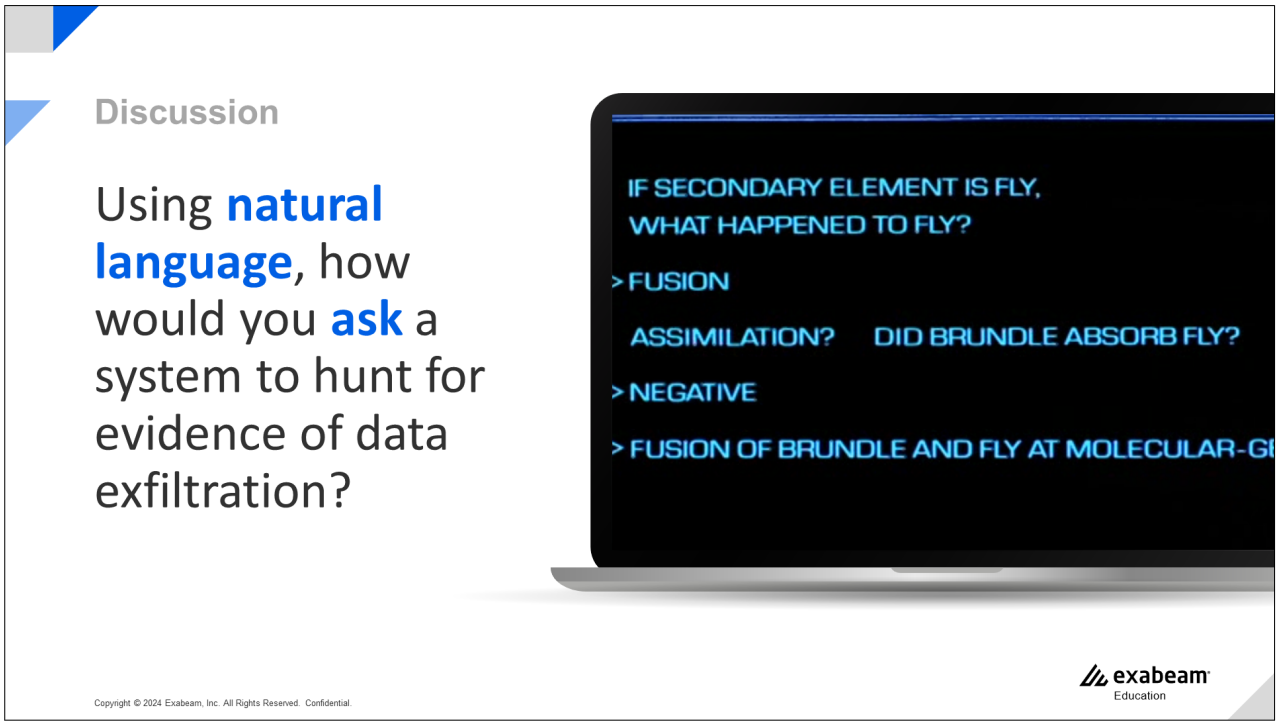
Discussion: What Would You Need to Know...



Student Notes

Your instructor will facilitate a short discussion on the kinds of information and skills a security analyst might need to be effective in querying a SIEM.

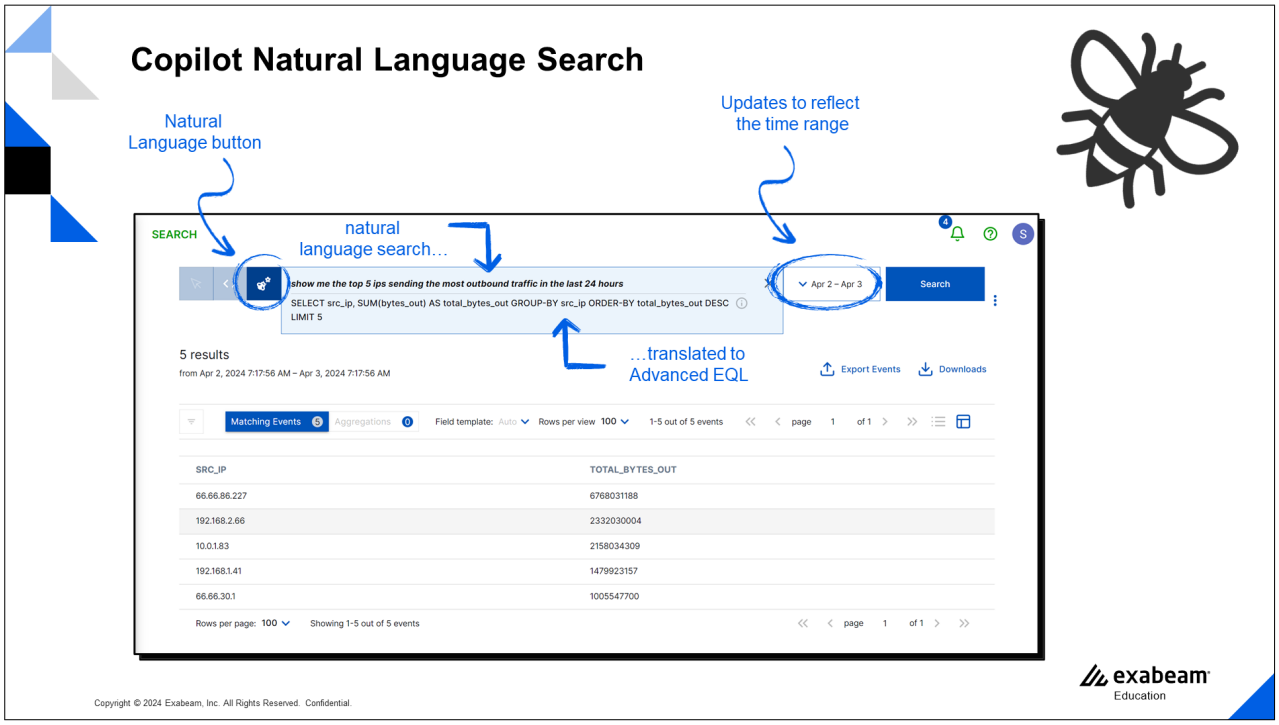
Discussion: Natural Language



Student Notes

Continuing from the previous discussion, think about the ways you might phrase a natural language query to discover evidence of data exfiltration in your environment. What non-technical terms might you use? What terms specific to the platform might you still need to include? What challenges can you imagine that might create friction using natural language queries?

Copilot Natural Language Search



Student Notes

Natural Language Search

The Natural Language Search feature translates a query prompt, entered using natural language, into Exabeam Query Language. This feature is part of Exabeam Copilot and its set of AI-driven capabilities.

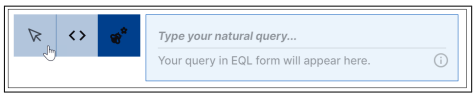
Natural Language Search provides the following benefits:

- You can build complex queries without the need for expert knowledge of complicated query syntax.
- You build day-to-day queries quickly in order to focus efficiently on potential threats.
- You can modify the query either by editing the natural language prompt or by editing the generated query syntax.
- You can modify queries to zero in easily on specific aspects of the results.

Natural language functionality benefits from exposure to use. Our team is working on extending the supported use cases. If you have a specific example, feedback is appreciated.

To use the Natural Language Search feature:

1. Click the ( ) icon to the left of the Search bar, to switch to the Natural Language Search feature. (Make sure the icon is highlighted.) The Search bar changes to present a double line.



2. In the **Type your natural query** line, enter your prompt in natural language. After a few seconds, the prompt is converted into query syntax and displayed in the **Your query in EQL form will appear here** line.
   Example:
   - Natural Language Prompt: `top 50 users filtered by vendor Microsoft`
   - Exabeam Query Language: `SELECT user, count(*) AS user_count WHERE vendor:"Microsoft" GROUP-BY user ORDER-BY user_count desc LIMIT 50`

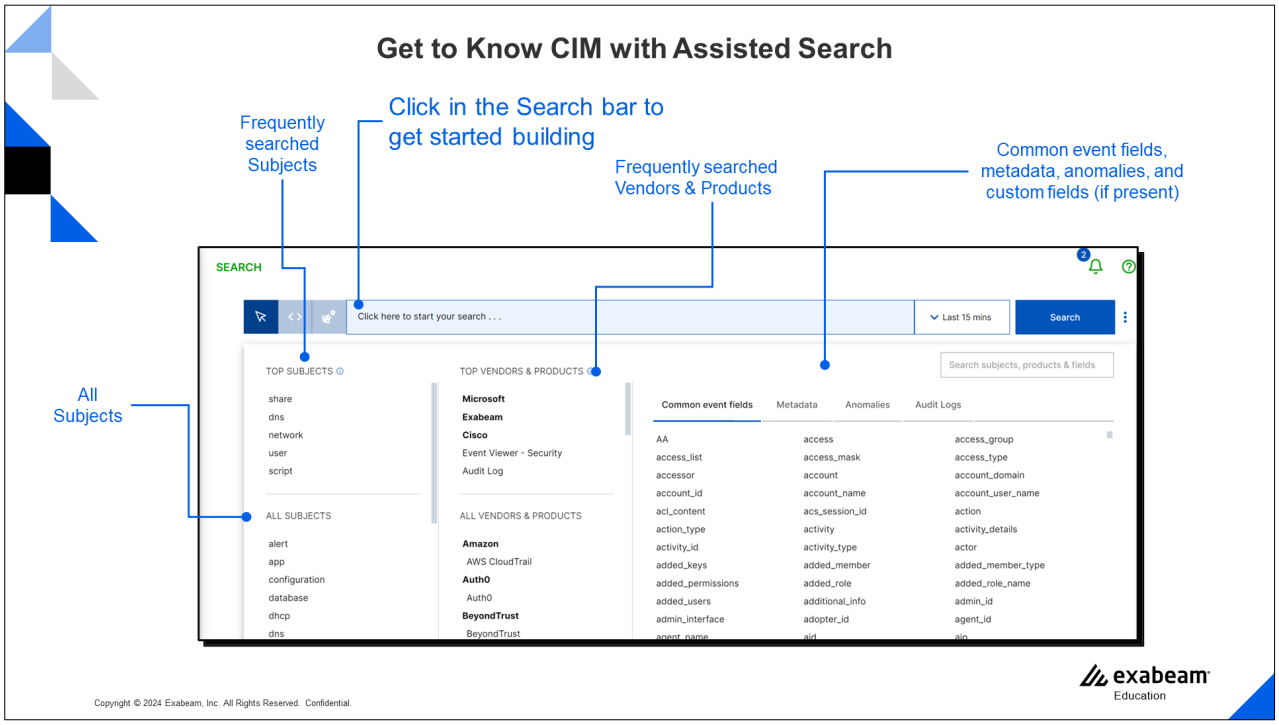
3. After your query has been built, you can still edit either the natural language prompt or the query syntax.
4. Select a time range using the the drop-down time filter ( ) to the right of the search bar to filter logs based on various relative and absolute time ranges.

> If you use a time range in your natural language prompt, such as `last 24 hours`, `last week`, or `last month`, the processing engine recognizes it and enters the time range automatically.

5. Click **Search** to launch your query.

> Your natural language query can optionally include a time window for the search. If you don't include a time range, whatever range is currently configured at the end of the search bar will be used. If you include a time window in your natural language query, the time range button will update to reflect the range.

CIM and Assisted Search



Student Notes

Assisted Search is a great way to get acclimated to the nuances of the Common Information Model in Exabeam. Understanding the field names and data types defined by the CIM will greatly improve your ability to build both natural language and Advanced EQL queries in the platform.

Use the Assisted Search feature to select from prebuilt lists of:

- **subjects,vendors, and products** — these are specific to the customer environment. TOP 5 being used will appear in the list, above ALL. The complete list of subjects, vendors, and products will vary from customer to customer, depending on the logs that they are ingesting.
- **common event fields** — this is a list of all default CIM fields and are not environment or customer specific.
- **custom fields** — these are customer specific, and are a result of a custom parser applied to the ingested logs. These fields start with a c_ and can be used in searches the same way any CIM field would be used.
- **anomalies** — search by Exabeam generated events. For Fusion and analytics customers.

As you make your selections, the query will appear in the search bar, already formatted using proper syntax. After your query has been built, it can still be edited. A panel will also appear, allowing you to enter a value.

Some fields have been changed, either in name or definition, to conform to the Common Information Model structure. If you've been using Exabeam products prior to the introduction of the Common Information Model, the transition to using it does not require any migration effort on your part. You will, however, want to familiarize yourself with the shift that the CIM model represents in the way data is categorized and events are classified. See the resources below for more information.

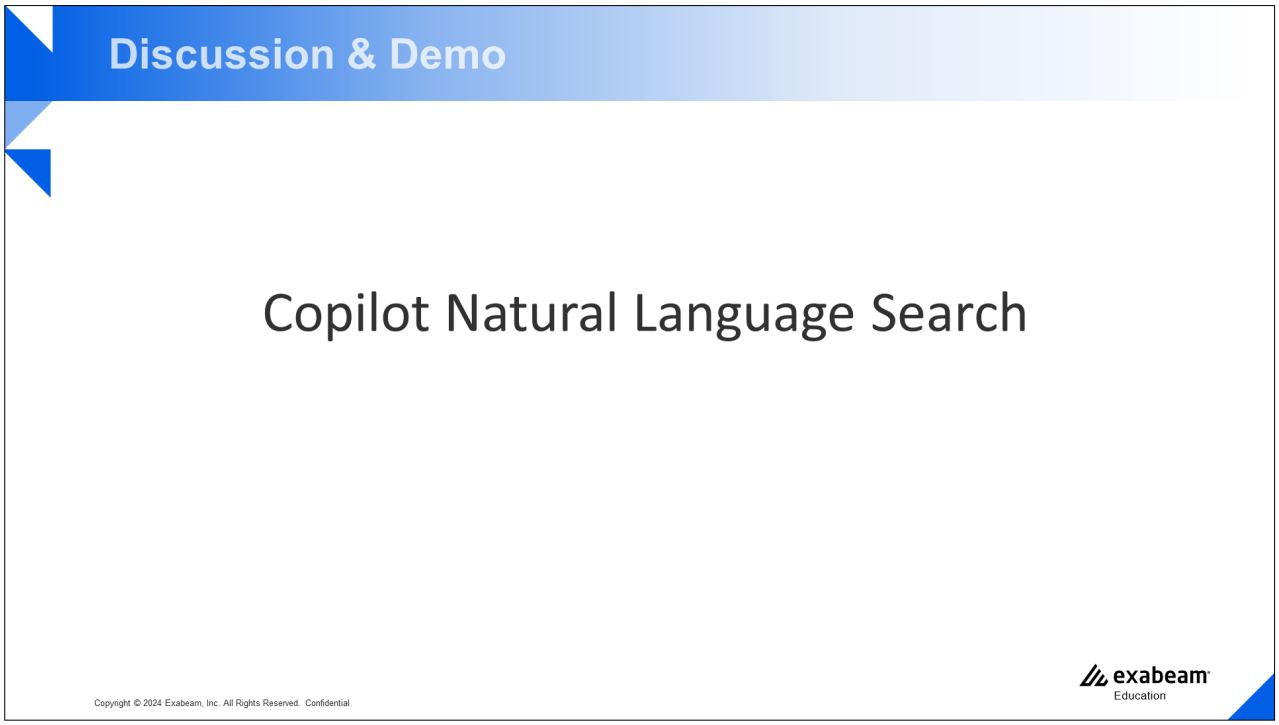
Resources

CIM Documentation

CIM eLearning

Assisted Search

Discussion & Demo

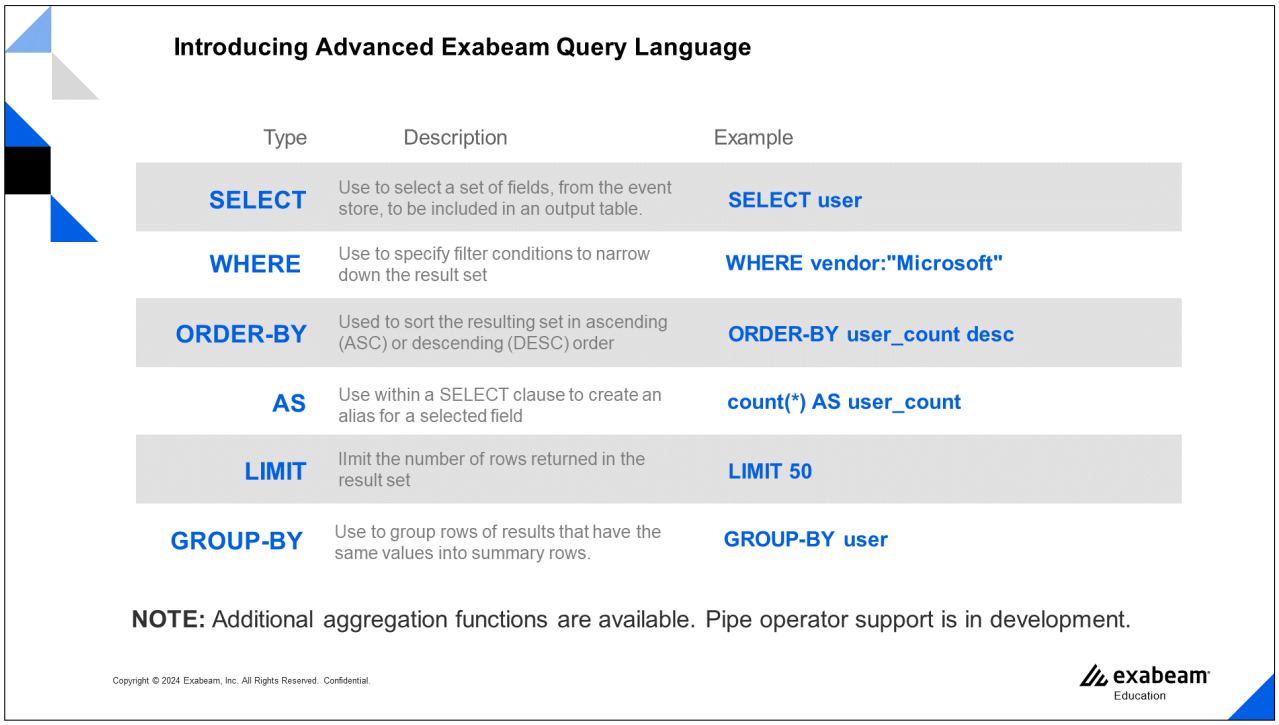


Student Notes

Your instructor will lead an interactive discussion as you collaboratively build natural language queries to do the following:

- List destination IPs associated with Command-and-Control behavior?
- List the names of dangerous websites visited by users in the last week? Bonus if you can filter out domains beginning with "HOST".
- Identify attempts at brute forcing passwords on endpoints?

Advanced EQL



Student Notes

Exabeam Copilot translates your natural language queries into Advanced Exabeam Query Language. The details of EQL are beyond this course. See the resources section below for more information.

In Exabeam advanced query language, a number of operators are available for creating complex queries that can be used in the Search service. A search using advanced operators must contain at least one SELECT or one WHERE clause. Other operators and clauses are optional, but when used they must be placed in a specific order:

```
[SELECT clause] [WHERE clause] [GROUP-BY clause] [ORDER-BY clause]
[LIMIT clause]
```

Example: **SELECT** user, **count**(*) **AS** user_count **WHERE** vendor:"Microsoft" **GROUP-BY** user **ORDER-BY** user_count desc **LIMIT** 50

In specific cases, when a SELECT clause is used, search results are output in a format that is not compatible with the standard results list view. They cannot be displayed in the list view and are instead displayed in a table view. Specifically, when an asterisk (*) is not used in the SELECT clause, it indicates that only the specified fields are of interest and the results are returned in a table view. However, if an asterisk (*) is used in the SELECT clause, it indicates that all the fields should be returned and the results are displayed in the standard list view. The list view is also disabled for any query that includes aggregation functions.

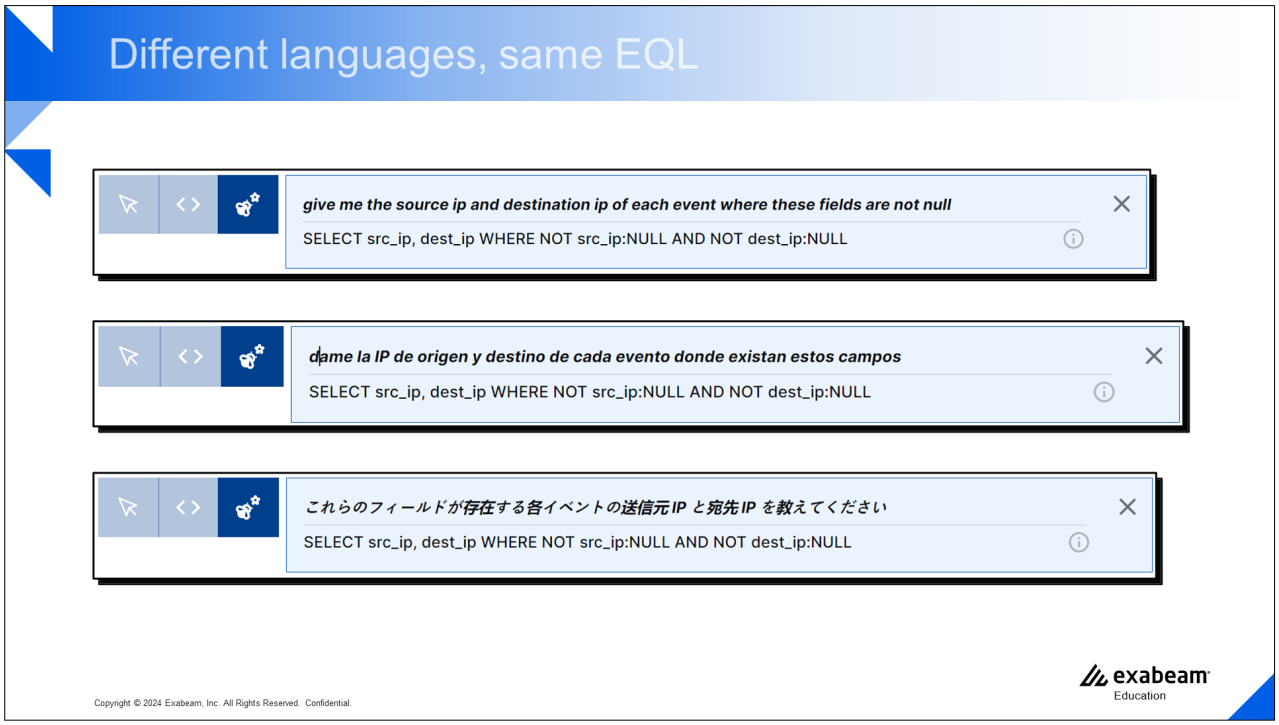
SELECT vendor	Results display in a table view
SELECT subject, COUNT(vendor) GROUP-BY subject	Results display in a table view
SELECT *,vendor	Results display in a list view
SELECT *, RGX_EXTRACT("Status:\s*(0x[0-9a-fA-F]+)") AS extracted_login_status WHERE vendor ="Microsoft" AND outcome="fail" AND activity_type="login"	Results display in a list view

Table 1. Advanced EQL output format examples

Resources

Advanced Exabeam Query Language

NLP Language Support



Student Notes

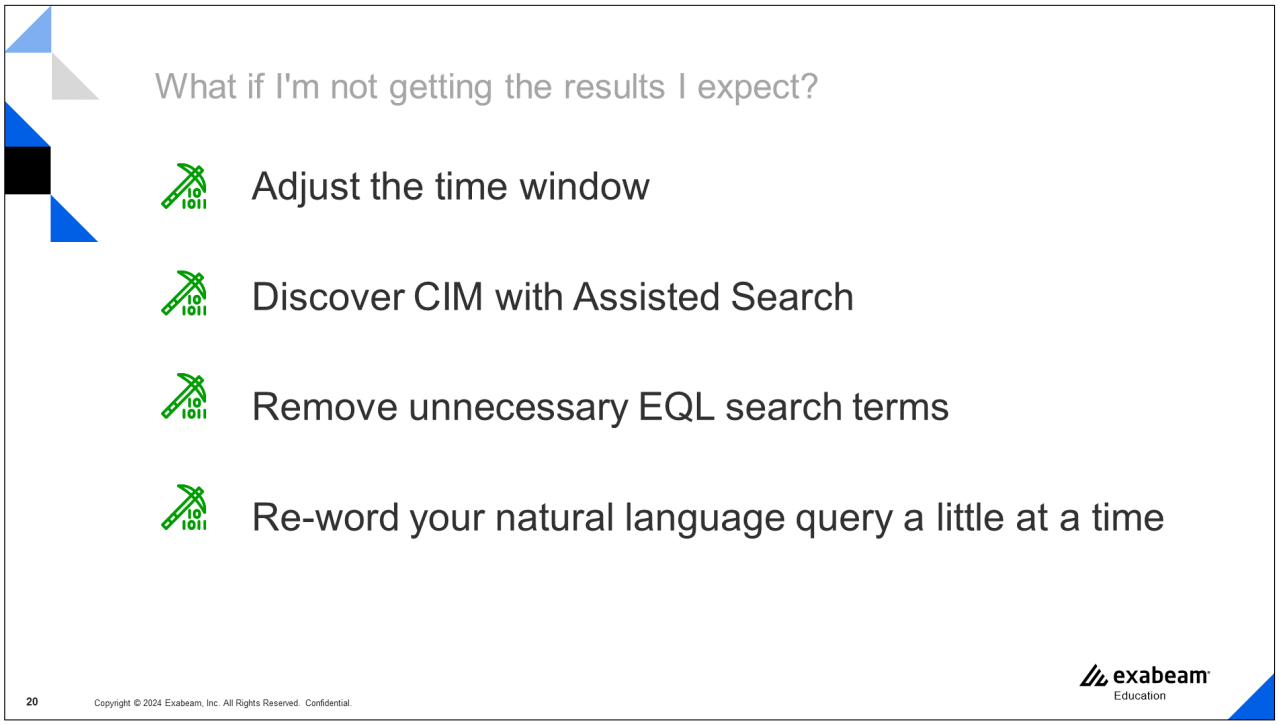
The PaLM 2 language model upon which Sec-PaLM 2 is based has been trained on the nuances of multilingual text spanning more than 100 languages. As of March 2024, Exabeam has over 350 customers worldwide running natural language queries in 15 languages.

The above graphic depicts the same natural langague query written in English, French, and Japanese. Each query translates to the same Advanced Exabeam Query Language:

```
SELECT src_ip, dest_ip WHERE NOT src_ip:NULL AND NOT dest_ip:NULL
```

Resources
PaLM 2 Language Support

What if I'm not getting the results I expect?



Student Notes

Remember, as useful as Copilot Natural Language Search is, it won't always translate your vernacular into the Advanced EQL necessary to return the results you're after. Here are some tips to help you troubleshoot:

Pay attention to the time window

If you don't include a time window in your natural language query, Search will use the existing time window defined at the right of the search bar. This time window may have rolled over from the previous search, so be sure to make sure it aligns with the range you're interested in.

Use Assisted Search to discover CIM field names and values

Search in Exabeam relies on the Common Information Model to describe the fields and types of values that describe the data in your logs. Copilot Natural Language Search doesn't always know what underlying CIM field(s) to use to translate your natural language into Advanced EQL. Assisted Search allows you to select from prebuilt lists of common event fields, as well as custom and metadata fields, making discovery of the correct CIM field names less ambiguous.

Remove unnecessary EQL search terms

Occasionally the Advanced EQL translation adds unnecessary terms to your query, resulting in inaccurate results. Remember, you can edit the query syntax at any time. Carefully scan the EQL and remove (or adjust) any conditions that aren't clearly benefitting your search.

Reword your natural language query a bit at a time

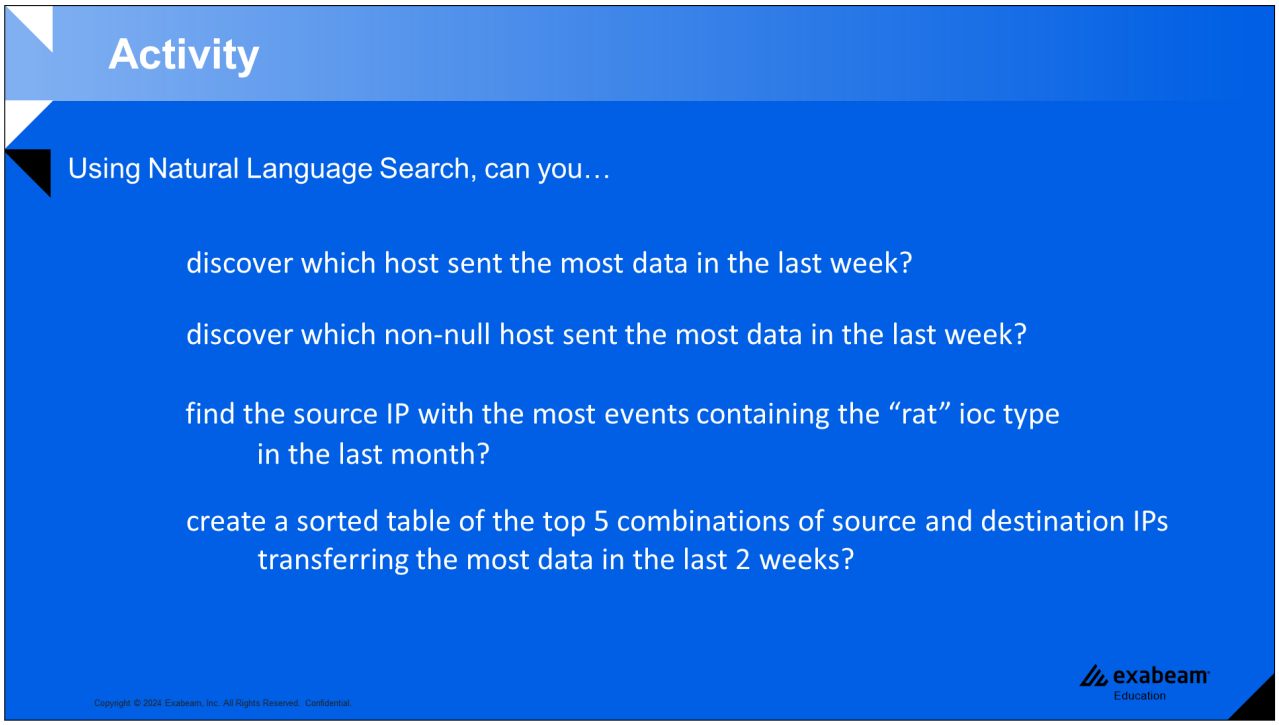
One of the more challenging error messages to overcome in Copilot Natural Language Search is "Sorry, not sure what your query means. Visit our help center to explore what I can do." This means that something in your language is ambiguous or unclear to the underlying generative AI.

Often removing a single term or phrase, or rephrasing slightly, will be enough to nudge the AI into a response.

Natural language query	Problematic translated EQL	Notes & Suggestions
vpn logs	SELECT * WHERE app_protocol:"vpn"	The translation interprets "vpn" as app_protocol and not as a subject
Which host sent the most data in the last week?	Sorry, not sure what your query means. Visit our help center to explore what I can do.	The system sometimes has difficulty with translating time ranges such as "in the last week." You can simply remove the time window from the query and add it as part of the drop-down time filter instead.
show me logs with email attachments in the last week that include an IOC	SELECT * WHERE NOT email_attachments:NULL AND NOT ioc:NULL	Syntax is correct, but **ioc** is not a CIM field; the translation doesn't realize that "include an IOC" should become "**NOT is_ioc:true**"
show me the top 10 users with failed interactive login requests	SELECT user, count(*) AS failed_login_count WHERE activity_type:"app-login" AND outcome:"fail" AND app_protocol:"interactive" GROUP-BY user ORDER-BY failed_login_count desc LIMIT 10	The term "interactive" is interpreted as a protocol

Table 2. Examples of problematic queries with suggestions

Activity



Student Notes

Now's your chance to try Copilot Natural Language Search on your own! Using the credentials provided by your instructor, log on to the Exabeam platform *here*. In Search, try to write natural language queries to accomplish the following tasks:

- Discover which host sent the most data in the last week
- Bonus: Discover which non-null host sent the most data in the last week
- Find the source IP with the most events containing the "rat" IoC type in the last month
- Create a sorted table of the top 5 combinations of source and destination IPs transferring the most data in the last 2 weeks

The actual search results returned are irrelevant for this exercise. The most important takeaway is to practice crafting natural language queries that can be translated for you into the more complex Advanced Exabeam Query Language.

Can you do the following?