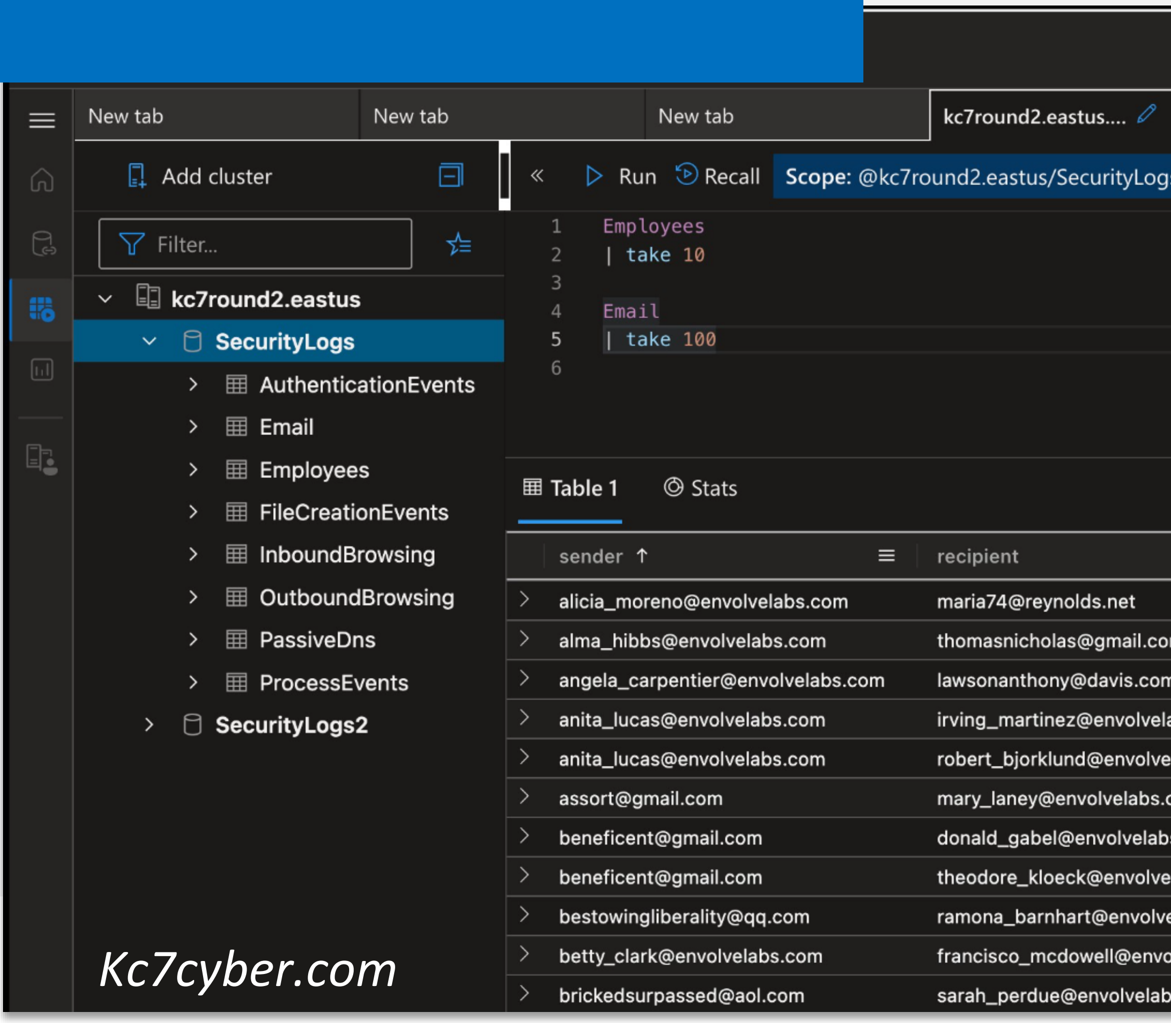
PRACTICE PIVOTING AND ANALYSIS

Simeon Kakpovi
Greg Schloemer
Emily Hacker



```
Employees
| take 10

Email
| take 100
```

sender ↑	recipient
alicia_moreno@envolvelabs.com	maria74@reynolds.net
alma_hibbs@envolvelabs.com	thomasnicholas@gmail.co
angela_carpentier@envolvelabs.com	lawsonanthony@davis.com
anita_lucas@envolvelabs.com	irving_martinez@envolvela
anita_lucas@envolvelabs.com	robert_bjorklund@envolve
assort@gmail.com	mary_laney@envolvelabs.c
beneficent@gmail.com	donald_gabel@envolvelab
beneficent@gmail.com	theodore_kloeck@envolve
bestowingliberality@qq.com	ramona_barnhart@envolve
betty_clark@envolvelabs.com	francisco_mcdowell@envo
brickedsurpassed@aol.com	sarah_perdue@envolvelab

Kc7cyber.com

Introduction: Welcome to The Krusty Krab

Welcome to the Krusty Krab! 🥳 Today is your first day as a Junior Security Operations Center (SOC) Analyst with our company.

The Krusty Krab is a mid-size fast food chain serving the greater Bikini Bottom metropolitan area. The Krusty Krab is best known for its delectable Krabby Patties™, kelp shakes, and sea dogs. Because of its wild success, some of the Krusty Krab's competitors would benefit from stealing its secret formula and reproducing it themselves. Of note, the Chum bucket - a minor competitor - has been less than ethical in its attempts to infiltrate the Bikini Bottom patty market.

Your job is to defend the Krusty Krab and its employees from malicious cyber actors looking to steal the secret formula.

Like all good companies, The Krusty Krab collects log data about the activity its employees perform on the corporate network. These security audit logs are stored in Azure Data Explorer (ADX) - a data storage service in Azure (Microsoft's cloud). You will use the Kusto Query Language (KQL) to parse through various types of security logs. By analyzing these logs, you can help us determine whether we're being targeted by malicious actors.

You can find full documentation on ADX here: https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/tutorial?pivots=azuredataexplorer

Objectives

🧠 **By the end of your first day on the job, you should be able to:**

- ✓ Use the Azure Data Explorer
- ✓ Use multiple data sets to answer targeted questions
- ✓ Find cyber activity in logs including: email, web traffic, and server logs
- ✓ Use multiple techniques to track the activity of APTs (Advanced Persistent Threats)
- ✓ Use third party data sets to discover things about your attackers
- ✓ Build a threat intelligence report
- ✓ Make recommendations on what actions a company can take to protect themselves

The attackers have gotten a head start, so let's not waste any more time… time to get to work!

Some important links:

- The scoreboard: https://kc7cyber.azurewebsites.net/
- Azure Data Explorer: https://dataexplorer.azure.com

Legend

🎯 **Key Point –** Occasionally, you will see a dart emoji with a "key point." These signal explanations of certain concepts that may enhance your understand of key cybersecurity ideas that are demonstrated in the game.

🤔 **Question –** "Thinking" emojis represent questions that will enable you to demonstrate mastery of the concepts at hand. You can earn points by entering your responses to questions from section 3 in the scoring portal.

🤫 **Hint –** "Whisper" emojis represent in-game hints. These hints will guide you in the right direction in answering some of the questions.

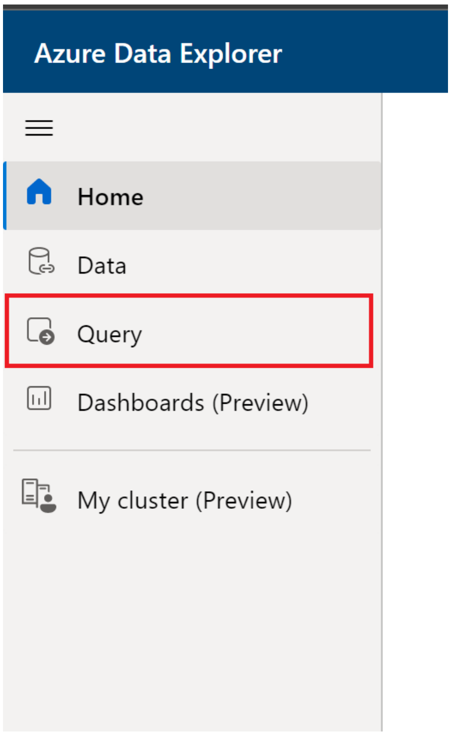
Section 1: The walkthrough

Getting Set Up in Azure Data Explorer (ADX)

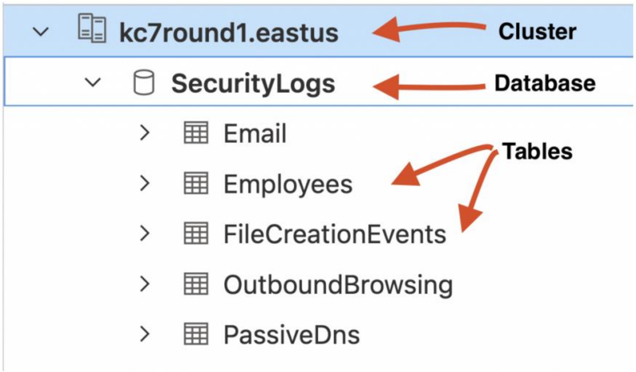
ADX is the primary tool used in the Envolve Labs SOC for data exploration and analysis. The great thing about ADX is that it is used by cyber analysts at many of the smallest and largest organizations in the world.

Let’s get you logged in and started with ADX:

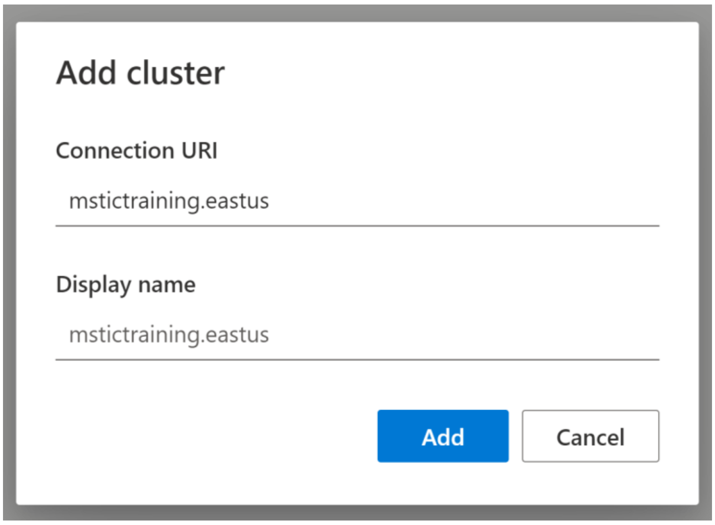
1. Go to https://dataexplorer.azure.com/ and login with your Microsoft account
2. Click the Query tab on the left side of the screen.



Data in ADX is organized in a hierarchical structure which consists of **clusters**, **databases**, and **tables**. All of Envolve Labs’s security logs are stored in a single cluster. You’ll need to add this cluster to your ADX interface so you can start looking at the log data.



3. Add a new cluster using the cluster URI provided by your instructor
    - **Click add cluster**
    - **Enter Connection URI:** mstictraining.eastus

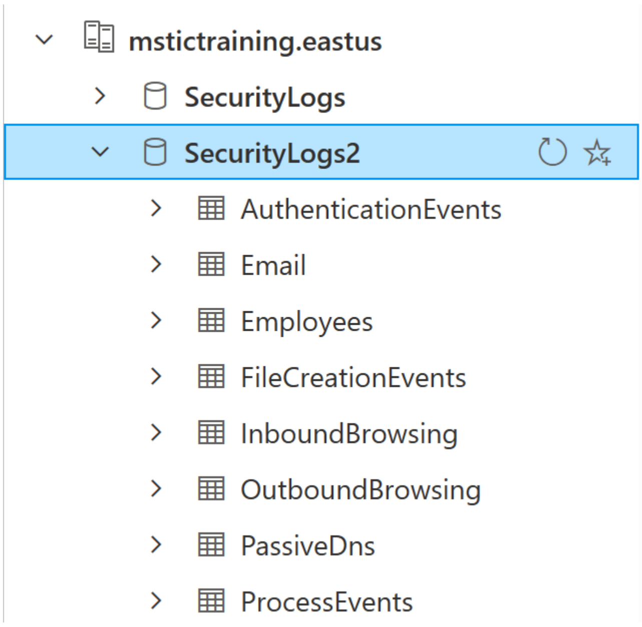


Add cluster

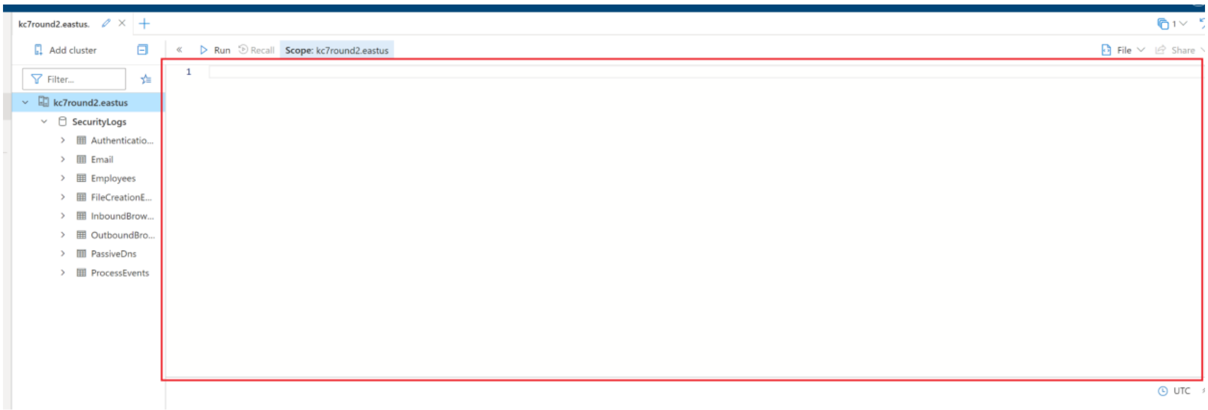
Connection URI: mstictraining.eastus

Display name: mstictraining.eastus

4. Select your database
    - Expand the dropdown arrow next to your cluster. You should then see one database, called **SecurityLogs3** inside it.
    - Expend the dropdown arrow next to the **SecurityLogs3** database.
    - Click on the **SecurityLogs3** database. Once you've done this, you should see the database highlighted- this means you've selected the database and are ready to query the tables inside.



The big blank space to the right of your cluster list is the *query workspace.* That’s where you will write the queries used to interact with our log data.



Okay, enough introductions… let’s get your hands on the data.

First look at the data…

The **SecurityLogs2** database contains eight tables. Tables contain many rows of similar data. For security logs, a single row typically represents a single thing done by an employee or a device on the network at a particular time.

We currently have eight types of log data. As you'll see in ADX, each log type corresponds to a table that exists in the **SecurityLogs3** database:

Table Name	**Description**
Employees	Contains information about the company's employees
Email	Records emails sent and received by employees
InboundBrowsing	Records browsing activity from the Internet to devices within the company network
OutboundBrowsing	Records browsing activity from within the company network out to the Internet
AuthenticationEvents	Records successful and failed logins to devices on the company network. This includes logins to the company's mail server.
FileCreationEvents	Records files stored on employee's devices
ProcessEvents	Records processes created on employee's devices
PassiveDns (External)	Records IP-domain resolutions

🎯 **Key Point – Over the Horizon (OTH) data**: One of the tables listed above is not like the others – **PassiveDns.** Rather than being an internal security log, PassiveDns is a data source that we've purchased from a 3rd party vendor. Not all malicious cyber activity happens within our company network, so sometimes we depend on data from other sources to complete our investigations.

You'll learn more about how to use each of these datasets in just a minute. First, let's just run some queries so you can practice using KQL and ADX.

Section 1: Introducing the hackers

🚨 ***Use the database SecurityLogs3 for this section of the exercise*** 🚨

Now that you’ve completed your initial round of training, you are ready to work your first case in the SOC!

Answer the following questions related to this tip:

1. How many users in our organization were sent emails containing the domain chum.net?
2. One of the employees who was targeted has a 'y' in their name. Who is this employee?
3. How many of the emails containing chum.net were blocked? (hint: the “accepted” field in the Email table tells you whether or not the email was blocked. Blocked emails will show as false).
4. How many unique IP addresses does chum.org resolve to?
5. How many unique IP addresses does fun.com resolve to?
6. How many unique IP addresses does genius.org resolve to?
7. How many unique domains does IP 43.243.201.76 host?
8. How many unique domains does IP 101.143.139.17 host?
9. How many “.net” domains resolve to IP 192.224.255.208? (hint: you can use the in operator to check for multiple values in a field. E.g. | where field in (“x”, “y”, “z”)
10. How many ".com" domains resolve to IP 43.243.201.76?
11. Which ".pizza" domain resolved to the same IP as fun.com
12. Which ".net" domain resolved to the same IP as chum-fun.food
13. How many email addresses did the hackers use to send these domains (the .net domains you found in question #23)?
14. How many of these emails had mismatched sender and reply-to addresses? (You can use the != operators to check if two things are not the same)
15. How many users clicked on a link containing the domain "fun.com"?
16. What was the timestamp of the first employee that clicked on a phishing link containing the domain "fun.com"?

17. What was the first domain sent by "krabbs@yandex.com"? (Hint: You can click on the event_time column header to sort the rows by time. Then, find the link for the email that was sent first.)
18. What was the first email address used to send an email containing a link to "picket.pizza"?
19. Which email address was used to send a link to "bucketdomination.com"?
20. Based on the data you've seen (email addresses, domains, and subject lines), which SpongeBob character do you believe is responsible for the malicious activity targeting the Krusty Krab?