



INTRODUCTION TO ATTRIBUTION AND CLUSTERING

Simeon Kakpovi
Greg Schloemer
Emily Hacker

Azure Data Explorer

New tab New tab New tab kc7round2.eastus....

Add cluster Filter...

kc7round2.eastus

- SecurityLogs
 - AuthenticationEvents
 - Email
 - Employees
 - FileCreationEvents
 - InboundBrowsing
 - OutboundBrowsing
 - PassiveDns
 - ProcessEvents
 - SecurityLogs2

Run Recall Scope: @kc7round2.eastus/SecurityLog

```
1 Employees
2 | take 10
3
4 Email
5 | take 100
6
```

Table 1 Stats

sender ↑	recipient
> alicia_moreno@envovellabs.com	maria74@reynolds.net
> alma_hibbs@envovellabs.com	thomasnicholas@gmail.com
> angela_carpentier@envovellabs.com	lawsonanthony@davis.com
> anita_lucas@envovellabs.com	irving_martinez@envovellabs.com
> anita_lucas@envovellabs.com	robert_bjorklund@envovellabs.com
> assort@gmail.com	mary_laney@envovellabs.com
> beneficent@gmail.com	donald_gabel@envovellabs.com
> beneficent@gmail.com	theodore_kloeck@envovellabs.com
> bestowingliberality@qq.com	ramona_barnhart@envovellabs.com
> betty_clark@envovellabs.com	francisco_mcdowell@envovellabs.com
> brickedsurpassed@aol.com	sarah_perdue@envovellabs.com

Kc7cyber.com

Introduction: Welcome to Envolve Labs

Welcome to Envolve Labs Corporation! 🎉 Today is your first day as a Junior Security Operations Center (SOC) Analyst with our company. Your primary job responsibility is to defend Envolve Labs and its employees from malicious cyber actors.



Envolve Labs is a med-tech startup based in the United States that was founded in 2012. Our mission is to develop a new type of flexible vaccine technology that covers many different viral strains and offers long-lasting immunity (which means no more boosters!) Our initial research has proven this technology is highly effective – we’re planning to start production in Q1 2023.

EnvolveLabs has a series of key partners who contribute to the success of our business:

Partner Name	Relationship
We Sell Beakers™ (wesellbeakers.com)	A key distributor of medical-grade laboratory equipment, We Sell Beakers™ provides all of the equipment for our world-class research facilities.
PharmaSupplies, Inc. (pharmasupplies.org)	PharmaSupplies provides Envolve Labs with the core ingredients used in our vaccine products.
Vaccine Distributors Worldwide (vaccinedistributors.com):	EnvolveLabs trusts Vaccine Distributors Worldwide to deliver our temperature and time-sensitive vaccine products to customers around the globe.
Research Compliance, PSC (researchcompliance.com)	Research Compliance, PSC is the key legal partner of Envolve Labs who helps ensure compliance with international guidelines and regulations that govern vaccine production.

Until now, we’ve been laser focused on medical research and meeting production goals. But, as our work becomes more important and successful, we’ve realized the need to invest more in cybersecurity efforts. That’s why we’ve hired you!

Like all good companies, Envolve Labs 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 analysing 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.

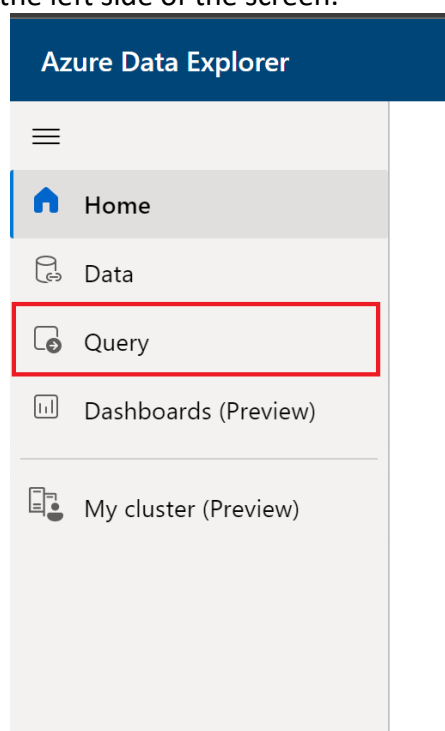
Section 1: The walkthrough

Getting Set Up in Azure Data Explorer (ADX)

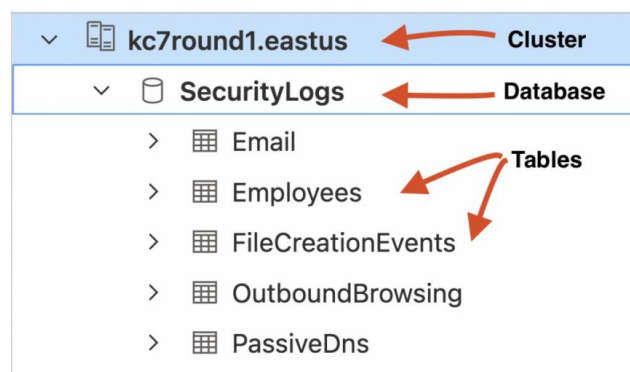
ADX is the primary tool used in the Envolve Labs SOC for data exploration and analysis. The great thing about ADX is that it is used by cyber analysts at many of the smallest and largest organizations in the world.

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

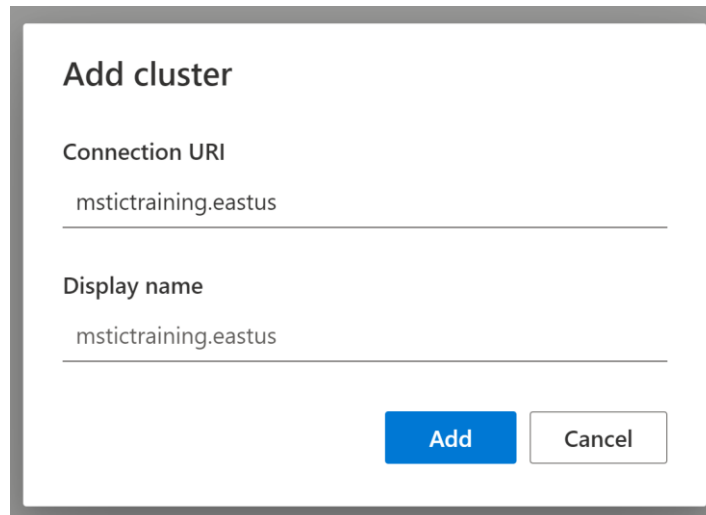
1. Go to <https://dataexplorer.azure.com/> and login with your Microsoft account
2. Click the Query tab on the left side of the screen.



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.

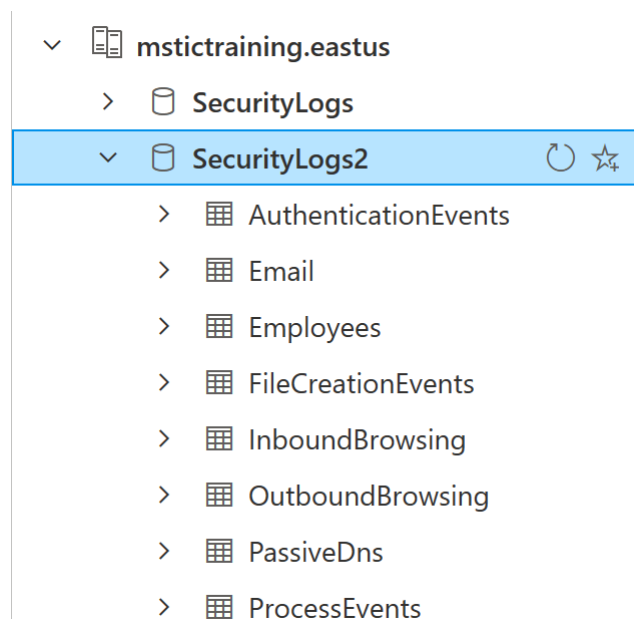


3. Add a new cluster using the cluster URI provided by your instructor
- Click **add cluster**
 - Enter **Connection URI:** **mstictraining.eastus**

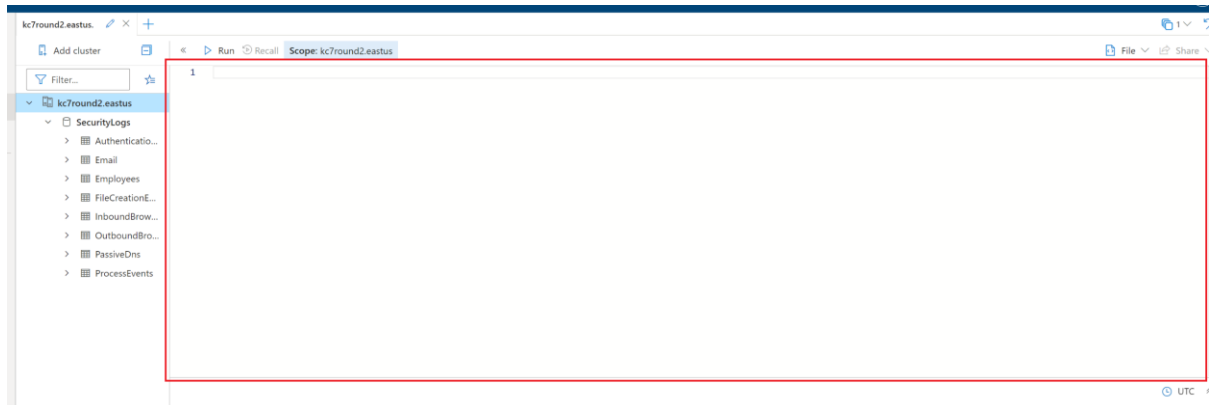


A dialog box titled "Add cluster" with two input fields. The first field is labeled "Connection URI" and contains the text "mstictraining.eastus". The second field is labeled "Display name" and also contains the text "mstictraining.eastus". At the bottom right, there are two buttons: a blue "Add" button and a white "Cancel" button with a grey border.

4. Select your database
- Expand the dropdown arrow next to your cluster. You should then see one database, called **SecurityLogs2** inside it.
 - Expand the dropdown arrow next to the **SecurityLogs2** database.
 - Click on the **SecurityLogs2** 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 **SecurityLogs** 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 **SecurityLogs** 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

Section 1: Introducing the hackers


🔥 Use the database *SecurityLogs2* 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!

A security researcher tweeted that malicious file called "ResearchBibliographyGenerator.zip" was being used by hackers. Apparently, the hackers are sending this file out via phishing emails email.



⚠️ NOTE! This domain and others encountered in this game are fictional and are not representative of actual malicious activity,

 **Key Point – Open Source Intelligence (OSINT):** Security researchers and analysts often use free, publicly available data, like Twitter! We call this public data OSINT, and it can be a great way to get investigative leads. Like all public data sources on the internet, you should follow up any OSINT tip with rigorous analysis, rather than blindly trusting the source.



Use the tipper above to answer the following questions:

You can optionally submit your answers to the scoreboard at <https://kc7cyber.azurewebsites.net/> to get feedback and earn points.

1. Which user has the file named “ResearchBibliographyGenerator.zip” on their machine?
2. When did the user above download “ResearchBibliographyGenerator.zip”?
 - a. What domain did the user download the file from?
3. When did the user above receive an email containing a link to “ResearchBibliographyGenerator.zip”?
 - a. What was the subject of the email in (3)?
 - b. Who was the email in (3) sent by?
 - c. What other domains were delivered via links in emails with the same subjects as the email in (3)?
 - d. What “interview” themed subject was sent by an actor-controlled email address associated with the email in (3)?
 - e. Which “fda” themed email address sent an email with the subject from (3d)?
4. What other “.science” domain is closely associated via Passive DNS to this cluster of activity to the domain used to deliver “ResearchBibliographyGenerator.zip”?
5. Which .dll file was dropped on the victim machine shortly after the user downloaded the zip: ResearchBibliographyGenerator.zip



Hint: Files that are created on employees’ devices are captured in the **FileCreationEvents** log. Try looking there to see which employees downloaded this file.

- a. The dll file is observed on Virustotal under what file name?
- b. Which six letter reconnaissance command was executed on the Machine of the user that loaded the implant above?



Hint: Try narrowing down on one particular device that downloaded the EnvolvLabs_Research_Tool.7z file. Then, look in both the **FileCreationEvents** and **ProcessEvents** logs to find new files and processes created around the time when the file was downloaded.

- c. What IP address does the dll beacon to?
6. What is the domain name of the legitimate service the adversary used to exfiltrate data from the victim machine?

Section 2: Report Analysis

January 31, 2023 • 5 min read

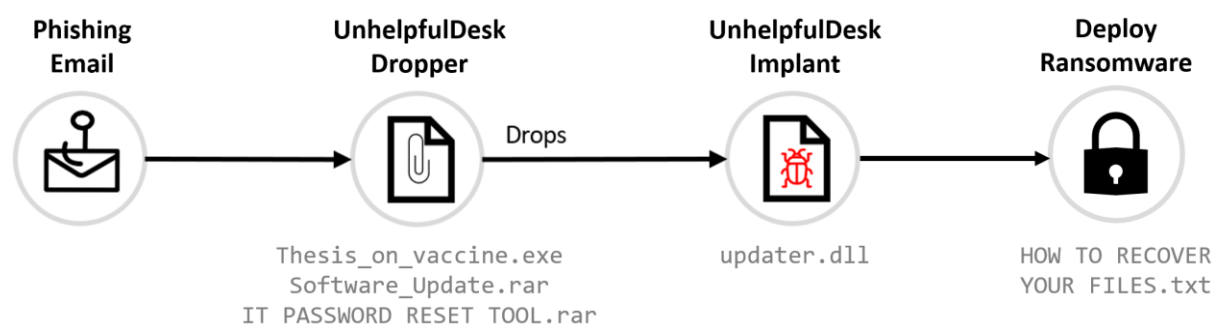
The 10X cyber adversary: ITINIUM APT Group Leverages New 'UnhelpfulDesk' Malware In Ransomware Attacks

VulnerableArray Security Intelligence

VulnerableArray Security Intelligence (VSI) discovered a new APT group named ITINIUM. ITINIUM likely operates from Urzikstan and primarily targets pharmaceutical companies in Europe and North America.

Beginning in late 2022, ITINIUM launched a targeted phishing campaign in which it delivered emails containing malicious links. The resulting files led to implants from one new malware family that VSI calls UnhelpfulDesk. VulnerableArray Security Intelligence assesses with a high degree of confidence that the UnhelpfulDesk malware is custom-developed and use exclusively by ITINIUM.

ITINIUM uses UnhelpfulDesk in order to gain access to victim systems and encrypt their files.



UnhelpfulDesk

UnhelpfulDesk malware implants are dropped by files with names that resemble legitimate IT functions, such as software updates or password resets, or medical research topics, such as vaccine research. These files are delivered to victims via malicious emails containing links to download the files.

UnhelpfulDesk droppers:

Filename	Sha256
Thesis_on_vaccine.exe	232568cb9c5d1b3698334c504b173e637826d79074fb8fa 23a54981578eb7dc9

ResearchBibliographyGenerator.pptx	6e4a6278077f310e69017dba9a173d9d27eddec9236231e1717a475c26242ae6
Software_Update.rar	2f2e5f20a726e9710b9c5c7c681e66240f854acd48107e5cd193d6133297b72f
IT_PASSWORD_RESET_TOOL.rar	fe04d68b163bbf432196c0d7bb184176a4260630374c93c916cc6b52fc9855f7

Dropped implants

Filename	Sha256
updater.dll	3666cb55d0c4974bfee855ba43d596fc6d10baff5eb45ac8b6432a7d604cb8e9
updater.dll	42a337bcec26df0130a11baf9e60179993851b88f1cabec52973f88774e903fb
updater.dll	ea05ff75fef906a60545129a7c5bea2956bfde63b8e714eb42db3ae50b99dec3
updater.dll	370ce39ba328329ff16b5ede1079f6402e68abceb34e65cb31883a3b3730b530
updater.dll	e3970346ff7fcc3665f027d7f221968087f3c42705f5799fbc1d2811ab1ca4ea

*** Samples of the UnhelpfulDesk implant files detected by VulnerableArray researchers are available on VirusTotal.*

Once successfully deployed, the UnhelpfulDesk implant executes reconnaissance via the following commands:

```
ping 8.8.8.8
whoami
net user Administratr
```

Following this, the malware will encrypt files on the machine and demand a ransom to decrypt the files. The ransom note is pulled down from Pastebin as shown below:

```
curl https://pastebin.com/HOW%20TO%20RECOVER%20YOUR%20FILES.txt
```


Other IOCs

```
214.217.73[.]146
65.69.253[.]41
199.57.49[.]250
install-notice[.]com
remarkablevirus[.]tech
noreply_info[@]hotmail.com
vaccinejournal[@]yahoo.com
```


Now it's up to you...

Our CISO has asked you to evaluate this report from VulnerableArray and determine whether it is accurate. While making your assessment, consider the following questions:


1. Do all the reported indicators belong to the same cluster of activity? How do you know?

 **Hint:** Use the Diamond Model (Adversary, Victim, Infrastructure, Capabilities) to help you think about clustering distinct groups of activity. It Look for similarities and differences in each of the four Diamond Model vertices.


2. The report claims that the UnhelpfulDesk malware is to ultimately deploy ransomware and encrypt files on an infected system. Do you agree with this assessment? Or do you see evidence of alternative actions on objectives?

 **Hint:** Try looking for activity related to the malware-based indicators shared in the blog, then identify a few compromised systems. Do you see post-compromise activity on any of these systems that's different from the ransomware described in the blog?

3. What analytical mistakes, if any, were made by the authors of the blog?


 **Hint:** Some processes are executed automatically by the malware upon execution. Other processes are run manually (hand-on-keyboard) by the operator after the command and control channel is establish.

4. Is the UnhelpfulDesk malware unique to the ITINIUM actor? How do you know?

 **Hint:** The updater.dll implants appear to be dropped from files with two separate themes (IT and research). Think about why that might be the case.

5. Are there multiple actors targeting Envolve Labs? If so, can you describe the Tactics, Techniques, and Procedures (TTPs) of each of them? How are they similar? How are they different?

- 6.

 **Hint:** Compare and contrast the diamond model for each of the observed clusters of activity.

7. How might gaps in visibility have contributed to the conclusions of the blog author(s)? How might they contribute to your own analytical assessments?