Solvi Systems

Monday, July 28, 2025 7:37 AM

>

As you go through KC7, we're exposing you to **all kinds of real-world threats** — and this one's a big deal. 🏭⚡

Solvi Systems builds software for power and utility companies. A single breach here could ripple through entire nations.

This case takes you into the world of **critical infrastructure attacks** — supply chains, phishing, lateral movement, and high-stakes consequences.

Let's see how quickly a small crack in the system becomes a full-on blackout.

07:37 AM

Objectives

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

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

Legend

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

🤔 Question – "Thinking" emojis represent questions that will enable you to demonstrate mastery of the concepts at hand. You can earn points by entering your responses to questions from section 3 in the scoring portal available at kc7cyber.com/scoreboard.

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

Table Name	Description
AuthenticationEvents	Records successful and failed logins to devices on the company network. This includes logins to the company's mail server.
Email	Records emails sent and received by employees
Employees	Contains information about the company's employees
FileCreationEvents	Records files stored on employee's devices
InboundNetworkEvents	Records inbound network events including browsing activity from the Internet to devices within the company network
NetworkFlow	Records network traffic details for analysis, including source and destination IP addresses, ports, protocols, and packet bytes
OutboundNetworkEvents	Records outbound network events including browsing activity from within the company network out to the Internet
PassiveDns (External)	Records IP-domain resolutions
ProcessEvents	Records processes created on employee's devices
SecurityAlerts	Records security alerts from an employee's device or the company's email security system

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

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

Operator	Description	Case-Sensitive	Example (yields true)
==	Equals	Yes	"aBc" == "aBc"
!=	Not equals	Yes	"abc" != "ABC"
=~	Equals	No	"abc" =~ "ABC"
contains	Right-hand-side (RHS) occurs as a subsequence of left-hand-side (LHS)	No	"FabriKam" contains "BRik"
has	RHS is a whole term in LHS	No	"North America" has "america"
has_all	Same as has but works on all of the elements	No	"North and South America" has_all("south", "north")
has_any	Same as has but works on any of the elements	No	"North America" has_any("south", "north")
in	Equals to any of the elements	Yes	"abc" in ("123", "345", "abc")

Solvi Systems is a software company that plays a pivotal role in shaping the future of the energy sector in South Africa. At the heart of Solvi Systems' operations is its Docks software, a critical component used by major power and utility companies.

Solvi Systems' influence extends beyond national borders. The company plays a crucial role in regional stability, as South Africa exports power to neighboring states like Mozambique, Eswatini, Zimbabwe, and Namibia. This interconnectedness means that any vulnerability or disruption in South Africa's energy infrastructure, and by extension Solvi Systems' software, doesn't just affect one nation but echoes across the region.

Given this key role, Solvi Systems is a prime target for cyber adversaries. You've been hired to identify any intrusions against this company.

To start your investigation, you will need access to the company's pool of data!

1. *Login to Azure Data Explorer (ADX). This is where you will find our TOP SECRET data. You will need a Microsoft account (hotmail, outlook, O365..) We will use ADX to run queries that will help us answer these questions.*

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

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

Now that we have access to the data, we'll need to get a lay of the land. Let's get some more information about Solvi Systems.

How many employees work at Solvi Systems?

```
Employees
| count
```

Copy

500

Solved by 1514 players || Need help?

```
Employees
| count
```

Table 1

Count
500

We can use the **where** operator with the Employees table to find a specific employee.

To learn more about how to use **where**, see the training guide.

training guide

What is the CTO's name?

```
Employees
| where role == "CTO"
```

Copy

Alexis Khoza

Solved by 1484 players || Need help?

```
Employees
| where role == "CTO"
```

Table 1

hire_date	name	user_agent	ip_addr	email_addr
5/24/2021, 12:00:00 AM	Alexis Khoza	Mozilla/5.0 (Windows NT 6.2; rv:50.0) Gecko/20100101 Firefox/5(	10.10.0.7	alexis_khoza@

We can learn more about `Alexis Khoza` using information from other tables. Let's take her email address from the Employees table and use it in a query for the Email table.

How many emails did Alexis Khoza receive?

```
Email
| where recipient == "<Alexis Khoza's Email Ac
| count
```

Copy

31

Solved by 1439 players || Need help?

```
Email
| where recipient == "alexis_khoza@solvisystems.com"
| count
```

Table 1

Count
31

You can use the **distinct** operator to find unique values in a specific column.

How many distinct senders were seen in the email logs from eskom.co.za?

```
Email
| where sender has "<Domain Name>"
| distinct <field>
| count
```

Copy

745

Solved by 1392 players || Need help?

```
Email
| where sender has "eskom.co.za"
| distinct sender
```

Table 1 745

sender
kathleen_pena@eskom.co.za
danny_ward@eskom.co.za

How many distinct websites did "Alexis Khoza" visit?

```
OutboundNetworkEvents
| where src_ip == "<Alexis Khoza IP>"
| <operator> <field>
| <operator>
```

Copy

72

Solved by 1355 players || Need help?

```
Employees
| where role == "CTO"
```

To find out who is the CTO == Alexis Khoza and to find out the IP of Alexis.

```
OutboundNetworkEvents
| where src_ip == "10.10.0.7"
| distinct url
| count
```

Table 1

Count
72

How many distinct domains in the PassiveDns records contain the word "real"?

```
PassiveDns
| where <field> contains <value>
| <operator> <field>
| <operator>
```

Copy

*You may notice we're using **contains** instead of **has** here. If you are curious about the differences between these, check out this post."*

19

Solved by 1327 players || Need help?

```
PassiveDns
| take 10

PassiveDns
| where domain contains "real"
| distinct domain
| count
```

Table 1

Count
19

What IPs did the domain "bit.ly" resolve to (enter any one of them)?

```
PassiveDns
| where domain == "<domain>"
| distinct <field>
```

Copy

30.99.71.8;179.251.245.106;179.14.26.20

Solved by 1316 players || Need help?

```
PassiveDns
| where domain == "bit.ly"
| distinct ip
```

Table 1 — 10

ip
219.82.23.42

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

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

Copy

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

847

Solved by 1255 players || 🤓 Need help?

```
let mary_ips =
Employees
| where name has "Mary"
| distinct ip_addr;
OutboundNetworkEvents
| where src_ip in (mary_ips)
| distinct url
```

Table 1 — 847

url
https://docs.google.com/document/d/OmdhONi3Bul7gYocv38DeTx09
http://hino.co.jp/public/public/published/share/transpositions.pptx

Congratulations! 🎉 You've passed KQL 101! Let's dive into the investigation! 🔎

Enter "ready" to earn credit for this question.

✅ ready

Solved by 1263 players || 🤓 Need help?

```
let list_variable_name = Employees
| where name has "Mary"
| distinct username;
AuthenticationEvents
| where username in (list_variable_name)
| count
```

Table 1

Count
1,150

Our mission is to identify any intrusion attempts against Solvi Systems. In order to do this, we'll start by reviewing some alerts.

You got an alert from your Web Application Firewall (WAF) appliance that someone may be trying to compromise your Solvi System's website!

What kind of attack does the alert suggest happened?

✅ xss;cross site scripting;cross-site scriptin

Solved by 1199 players || 🤓 Need help?

```
{
    description: "DETECTION RULE TRIGGERED",
    severity: "HIGH",
    rule_description: "SUSPICIOUS TEXT IN HTTP REQUEST",
    data: https://www.solvisystems.com/feedback?message=</script>.
  <script>alert('xss')</script>
}
```

We can actually identify this request in our inbound browsing logs.

What javascript command was the attacker trying to run?

alert;alert();alert('xss')

Solved by 1159 players || Need help?

```
55  InboundNetworkEvents
56  | where url has "script or alert"
57
```

Table 1

timestamp	method	src_ip	user_agent	url	status_code
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x	https://www.solvisystems.c	404

```
1  48:08.000Z,
2
3
4  (11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00,
5  tems.com/feedback%3Fmessage%3D%3C/script%3E%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E,
6
```

Recipe

URL Decode

Treat "+" as space

Input

```
www.solvisystems.com/feedback%3Fmessage%3D%3C/script%3E%3Cscript%3Ealert%28%27xss%27%29
%3C/script%3E
```

Output

```
www.solvisystems.com/feedback?message=</script><script>alert('xss')</script>
```

You would take the body of the URL and use Cyberchef to decode the URL encoding.

What response code did they receive from the website?

404

Solved by 1180 players || Need help?

```
55  InboundNetworkEvents
56  | where url has "script or alert"
57
```

Table 1

timestamp	method	src_ip	user_agent	url	status_code
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x	https://www.solvisystems.c	404

JPath: / url Inline Compact


```
1  "timestamp": 2024-05-03T14:48:08.000Z,
2  "method": GET,
3  "src_ip": 13.201.46.208,
4  "user_agent": Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00,
5  "url": https://www.solvisystems.com/feedback%3Fmessage%3D%3C/script%3E%3Cscript%3Ealert%28%
6  "status_code": 404
```


Let's take some notes on the details of this event. These details may help us find more malicious activity later.

What user agent did the attackers use to make the web requests in this attack? Enter only the initial part of the user agent (XXXXX/N.NN).

Opera/8.64

Solved by 1164 players || Need help?

```
55  InboundNetworkEvents
56  | where url has "script or alert"
57
```

timestamp	method	src_ip	user_agent
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.

JPath: / user_agent Inline Compact


```
1  "timestamp": 2024-05-03T14:48:08.000Z,
2  "method": GET,
3  "src_ip": 13.201.46.208,
4  "user_agent": Opera/8.64.(X11; Linux x86_64; k
5  "url": https://www.solvisystems.com/feedback%3
6  "status_code": 404
7
```


On what day did the attack happen? Give the timestamp in the format YYYY-MM-DD.

2024-05-03

Solved by 1163 players || Need help?

```
55  InboundNetworkEvents
56  | where url has "script or alert"
57
```

timestamp	method	src_ip	user_agent
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.(X1

JPath: / user_agent Inline Compact


```
1  "timestamp": 2024-05-03T14:48:08.000Z,
2  "method": GET,
3  "src_ip": 13.201.46.208,
4  "user_agent": Opera/8.64.(X11; Linux x86_64; kok
5  "url": https://www.solvisystems.com/feedback%3Fm
6  "status_code": 404
7
```


Ok, that first attempt was unsuccessful but it may not have been the only one.

Let's look for other malicious requests the attacker could have made around that time. It looks like the attacker varied the ip addresses they used to make these requests.

Use this query as a template:

How many malicious requests did the attacker make in total?

9

Solved by 1146 players || Need help?

```
58  InboundNetworkEvents
59  | where user_agent has "Opera/8.64"
60  | where timestamp between (datetime("2024-05-03") .. datetime("2024-05-05"))
61
```

Table 1 9

timestamp	method	src_ip	user_agent	url	status_code
5/3/2024, 11:29:08 AM	GET	98.117.26.236	Opera/8.64.(X11; Linux x	https://www.solvisystems.cc	404

Were any of these attacks successful? (yes/no)

no

Solved by 1153 players || Need help?

```
58  InboundNetworkEvents
59  | where user_agent has "Opera/8.64"
60  | where timestamp between (datetime("2024-05-03") .. datetime("2024-05-05"))
61
```

Table 1

timestamp	method	src_ip	user_agent	url	status_code
5/3/2024, 11:29:08 AM	GET	98.117.26.236	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 12:15:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 12:31:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 1:07:08 PM	GET	56.6.30.190	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 1:12:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 1:29:08 PM	GET	56.6.30.190	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 2:00:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 2:11:08 PM	GET	98.117.26.236	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x8	https://www.solvisystems.co	404

What IP addresses did the requests originate from? (Enter any of them.)

98.117.26.236;13.201.46.208;105.78.23.6

Solved by 1138 players || Need help?

```
InboundNetworkEvents
| where user_agent has "Opera/8.64"
| where timestamp between (datetime("2024-05-03") .. datetime("2024-05-05"))
```

Table 1

timestamp	method	src_ip	user_agent	url	status_code
5/3/2024, 11:29:08 AM	GET	98.117.26.236	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 12:15:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 12:31:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 1:07:08 PM	GET	56.6.30.190	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 1:12:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 1:29:08 PM	GET	56.6.30.190	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 2:00:08 PM	GET	105.78.23.64	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 2:11:08 PM	GET	98.117.26.236	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404
5/3/2024, 2:48:08 PM	GET	13.201.46.208	Opera/8.64.(X11; Linux x8	https://www.solvisystems.cc	404

It looks like the threat actor did some reconnaissance prior to the attack. They were seen browsing the company website before sending malicious requests to it.

How many total records do we have of them browsing Solvi Systems?

64

Solved by 1111 players || Need help?

```
InboundNetworkEvents
| where user_agent has "Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00"
| count
```

Table 1

Count
64

Now that we know more about the threat actors' infrastructure, we can pivot out even further and see what else the threat actor may have done.

What is the timestamp of the first web request the threat actor sent to Solvi System's website?

2024-05-01T00:00:00Z

Solved by 1095 players || Need help?

```
InboundNetworkEvents
| where user_agent has "Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00"
| count
```

Table 1

timestamp	method	src_ip	user_agent	ur
5/1/2024, 12:00:00 AM	GET	98.117.26.236	Opera/8.64.(X11; Linux x	ht

JPath: / timestamp Inline Compact

```
1  "timestamp": 2024-05-01T00:00:00.000Z,
2  "method": GET,
```

5/1/2024, 11:20:47 AM	GET	105.78.23.64	Opera/8.64.(X11; Linux x	ht

Looks like the threat actors did some research beforehand. They were interested in one very special software developed by Solvi Systems.

```
InboundNetworkEvents
| where user_agent has "Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00"
| count
```

Which product did the threat actors research before the day that they sent the malicious web requests?

docks-ics;docks ics;docks

Solved by 1087 players || Need help?


```
InboundNetworkEvents
| where user_agent has "Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00"
| count
```


timestamp	method	src_ip	user_agent	url	status_code
5/1/2024, 12:00:00 AM	GET	98.117.26.236	Opera/8.64.(X11; Linux x	https://www.solvisystems	200
5/1/2024, 11:20:47 AM	GET	105.78.23.64	Opera/8.64.(X11; Linux x	https://www.solvisystems	200
5/1/2024, 12:07:47 PM	GET	56.6.30.190	Opera/8.64.(X11; Linux x	https://www.solvisystems	200

JPath: /url Inline Compact


```
"timestamp": 2024-05-01T12:07:47.000Z,
"method": GET,
"src_ip": 56.6.30.190,
"user_agent": Opera/8.64.(X11; Linux x86_64; kok-IN) Presto/2.9.165 Version/10.00,
"url": https://www.solvisystems.com/products/docks-ics,
"status_code": 200
```


So we know the web exploitation attempts failed, but surely that couldn't be the end of it. Based on the reconnaissance we saw, these threat actors were far too interested in Solvi Systems to give up that easily.

Let's try pivoting on the adversary infrastructure to see if they tried to get in some other way.

First we'll look in PassiveDns to see if there are any domains registered by the adversary.

How many distinct domains do the ip addresses used by the threat actor resolve to?

3

Solved by 1072 players || Need help?

```
PassiveDns
| where ip has_any ("98.117.26.236", "105.78.23.64", "56.6.30.190", "13.201.46.208")
| distinct domain
```

Table 1 — 3

domain
energy-trends4u.net
news-on-industry.com
eco-awareness-update.net

Hmmm... These domains smell like they were registered for nefarious purposes. Perhaps for... phishing?

Let's check out the email logs to confirm.

How many emails associated with these domains did SolviSystem employees receive?

56

Solved by 1020 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
```

Table 1 — 56

timestamp	sender	reply_to	recipient
5/1/2024, 3:51:41 PM	news@eco-awareness-updates.net	electric_updates@gmail.com	carla_wharton@solvisystems.com
5/1/2024, 3:51:41 PM	news@eco-awareness-updates.net	electric_updates@gmail.com	carolyn_ocampo@solvisystems.com

Before we move on, let's try to get a better scope of the investigation.

You'll answer the following questions about the 56 emails we found earlier that had the adversary domains.

How many distinct email addresses did the threat actor use?

3

Solved by 1011 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct recipient
```

So the distinct email addresses can be deciphered by the three domain names here. If it is not 3 it would be 2 if not two then 1, although the only sus email domains on the SolviSystems email database are these three.

How many distinct filenames were observed in the links in these emails?

3

Solved by 982 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct link
```

Table 1 14

link
http://eco-awareness-update.net/published/online/Recent_Mergers_and_Acquisitions_in_Energy_Industry.docx
https://news-on-industry.com/published/images/Energy_Industry_Trends_2024_4_Solvi.docx
http://energy-trends4u.net/public/share/files/Energy_Industry_Trends_2024_4_Solvi.docx
https://news-on-industry.com/public/Recent_Mergers_and_Acquisitions_in_Energy_Industry.docx

Columns

Out of these 14 records there are only 3 distinct filenames observed associated with the links in these emails.

Let's look into the employee roles that this threat actor was targeting.

How many different roles were targeted with these emails?

5

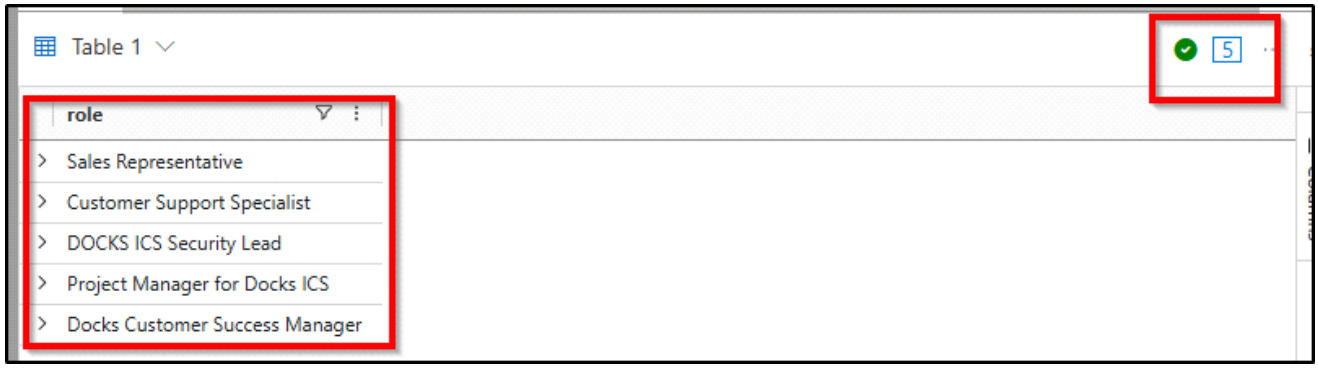
Solved by 950 players || Need help?

```
let threat_actor_ips =
InboundNetworkEvents
| where timestamp between (datetime("2024-05-03") .. datetime("2024-05-05"))
| where user_agent contains "Opera/8.64"
| distinct src_ip;
let threat_actor_domains =
PassiveDns
| where ip in (threat_actor_ips)
| distinct domain;
```

```
let email_recipients =
Email
| where link has_any (threat_actor_domains)
| extend email_recipient = parse_path(recipient).Filename
| distinct tostring(email_recipient);
Employees
| where email_addr in (email_recipients)
| distinct role
```

This query performs **threat intelligence correlation**—tracking threat actor behavior from network events to email recipients and then to their roles in the organization.

- **let threat_actor_ips = ...**: Creates a named subquery called threat_actor_ips to store a set of IP addresses.
- **InboundNetworkEvents**: This is the source table, likely containing firewall or proxy logs.
- **timestamp between (...)**: Filters only network events from **May 3 to May 5, 2024**.
- **user_agent contains "Opera/8.64"**: Looks for traffic from the Opera browser version 8.64—possibly an indicator of malicious behavior (e.g., known threat actor).
- **distinct src_ip**: Returns a **list of unique source IP addresses** (possibly attackers).



You reached level 17!

Reporting from the digital frontiers! Your reconnaissance is exceptional! Your new level title is **Reconnaissance Reporter**.

How many Customer Support Specialist employees received malicious emails?

27

Solved by 918 players || Need help?

```
let threat_actor_ips =
InboundNetworkEvents
| where timestamp between (datetime("2024-05-03") .. datetime("2024-05-05"))
| where user_agent contains "Opera/8.64"
| distinct src_ip;
let threat_actor_domains =
PassiveDns
| where ip in (threat_actor_ips)
| distinct domain;
```

```
let email_recipients =
Email
| where link has_any (threat_actor_domains)
| extend email_recipient = parse_path(recipient).Filename
| distinct tostring(email_recipient);
Employees
| where email_addr in (email_recipients)
| where role == "Customer Support Specialist"
```

Table 1 27

hire_date	name	user_agent	ip_addr	ema
6/20/2021, 12:00:00 AM	Carl Warfield	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; Win64; x64	10.10.0.24	ca

Among these job roles, which word is shared by three of them?

Docks;DOCKS

Solved by 896 players || Need help?

Kinda just guessed on this one as there were two words that is could have been, Docks fit.

We can't investigate all of the emails at once so we'll start by looking in detail at one of the emails.

What was the timestamp of the first email the threat actor sent?

2024-05-01T15:51:41Z

Solved by 889 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct  timestamp, recipient, link, sender, subject, verdict;
```

Table 1 55

timestamp	recipient	link	send
5/1/2024, 3:51:41 PM	carla_wharton@solvisystems.com	http://news-on-industry.com/search/online/files/public/Energy_I	new

JPath: /timestamp Inline Compact


```
"timestamp": 2024-05-01T15:51:41.000Z,
"recipient": carla_wharton@solvisystems.com,
"link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
"sender": news@eco-awareness-updates.net,
"subject": [EXTERNAL] Business Opportunity: Two major energy companies merging,
"verdict": CLEAN
```


What is the recipient's email address?

carla_wharton@solvisystems.com

Solved by 892 players || Need help?


```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct  timestamp, recipient, link, sender, subject, verdict;
```

Table 1 55

timestamp	recipient	link	send
5/1/2024, 3:51:41 PM	carla_wharton@solvisystems.com	http://news-on-industry.com/search/online/files/public/Energy_I	new

JPath: /recipient Inline Compact


```
1  "timestamp": 2024-05-01T15:51:41.000Z,
2  "recipient": carla_wharton@solvisystems.com,
3  "link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
4  "sender": news@eco-awareness-updates.net,
5  "subject": [EXTERNAL] Business Opportunity: Two major energy companies merging,
6  "verdict": CLEAN
7
```


What is that employee's name?

Carla Wharton

Solved by 892 players || Need help?

```
83  Email
84  | where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
85  | distinct  timestamp, recipient, link, sender, subject, verdict;
86
```

Table 1 55

timestamp	recipient	link	send
5/1/2024, 3:51:41 PM	carla_wharton@solvisystems.com	http://news-on-industry.com/search/online/files/public/Energy_I	new

JPath: /recipient Inline Compact


```
1  "timestamp": 2024-05-01T15:51:41.000Z,
2  "recipient": carla_wharton@solvisystems.com,
3  "link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
4  "sender": news@eco-awareness-updates.net,
```


What was the sender address of that email?

news@eco-awareness-updates.net

Solved by 890 players || Need help?

```
83  Email
84  | where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
85  | distinct  timestamp, recipient, link, sender, subject, verdict;
86
```

Table 1 55

sender	subject
news-on-industry.com/search/online/files/public/Energy_I news@eco-awareness-updates.net	[EXTERNAL] Business Opportunity: Two ma

JPath: / sender Inline Compact


```
1  "timestamp": 2024-05-01T15:51:41.000Z,
2  "recipient": carla_wharton@solvisystems.com,
3  "link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
4  "sender": news@eco-awareness-updates.net,
5  "subject": [EXTERNAL] Business Opportunity: Two major energy companies merging,
```


What was the reply to address?

electric_updates@gmail.com

Solved by 892 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct  timestamp, recipient, link, sender, reply_to, subject, verdict;
```

sender	reply_to	subject	verdict
news@eco-awareness-updates.net	electric_updates@gmail.com	[EXTERNAL] Business Opportunity: T	CLEAN
news@eco-awareness-updates.net	electric_updates@gmail.com	[EXTERNAL] Business Opportunity: T	CLEAN
news@eco-awareness-updates.net	electric_updates@gmail.com	[EXTERNAL] Business Opportunity: T	CLEAN
news@eco-awareness-updates.net	electric_updates@gmail.com	[EXTERNAL] Business Opportunity: T	CLEAN

What was the subject of that email?

[EXTERNAL] Business Opportunity: Two

Solved by 890 players || Need help?

```
Email
| where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
| distinct  timestamp, recipient, link, sender, reply_to, subject, verdict;
```

timestamp	recipient	link
5/1/2024, 3:51:41 PM	carla_wharton@solvisystems.com	http://news-on-industry.com/search/online/files/public/Energy_I

JPath: /subject Inline Compact


```
1  "timestamp": 2024-05-01T15:51:41.000Z,
2  "recipient": carla_wharton@solvisystems.com,
3  "link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_20
4  "sender": news@eco-awareness-updates.net,
5  "reply_to": electric_updates@gmail.com,
6  "subject": [EXTERNAL] Business Opportunity: Two major energy companies merging,
7  "verdict": CLEAN
```


What link was observed in the email?

http://news-on-industry.com/search/on

Solved by 887 players || Need help?

```
83  Email
84  | where link has_any ("eco-awareness-update.net", "energy-trends4u.net", "news-on-industry.com")
85  | distinct  timestamp, recipient, link, sender, reply_to, subject, verdict;
86
```

Table 1 55

timestamp	recipient	link	senc
5/1/2024, 3:51:41 PM	carla_wharton@solvisystems.com	http://news-on-industry.com/search/online/files/public/Energy_I	new

JPath: /timestamp Inline Compact


```
1  "timestamp": 2024-05-01T15:51:41.000Z,
2  "recipient": carla_wharton@solvisystems.com,
3  "link": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
4  "sender": news@eco-awareness-updates.net,
5  "reply_to": electric_updates@gmail.com,
6  "subject": [EXTERNAL] Business Opportunity: Two major energy companies merging,
```


```
110  Employees
111  | where name == "Carla Wharton"
112  | distinct ip_addr
113
114
115
```

Table 1

ip_addr
10.10.0.164

Did Carla click on the link in email? If so when?

2024-05-01T15:57:41Z

Solved by 874 players || Need help?

```
let carla_ip =
Employees
| where email_addr == 'carla_wharton@solvisystems.com'
| project ip_addr;
OutboundNetworkEvents
| where src_ip in (carla_ip)
| where url contains "Energy_Industry_Trends_2024_4_Solvi.docx"
```

timestamp	method	src_ip	user_agent	url
5/1/2024, 3:57:41 PM	GET	10.10.0.164	Mozilla/5.0 (compatible; MSIE 10.0;	http://news-on-industry.com/search/onl

JPath: /timestamp Inline Compact

```
"timestamp": 2024-05-01T15:57:41.000Z,
"method": GET,
"src_ip": 10.10.0.164,
"user_agent": Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; Trident/6.0),
"url": http://news-on-industry.com/search/online/files/public/Energy_Industry_Trends_2024_
```

What file was observed on Carla's machine shortly after she executed the docx file?

ecobug.exe

Solved by 876 players || Need help?

```
let carla =
Employees
| where email_addr == 'carla_wharton@solvisystems.com'
| project username;
FileCreationEvents
| where username in (carla)
| where timestamp between (datetime(2024-05-01T15:58:29Z) .. datetime(2024-05-01T16:58:29Z))
```

Table 1

timestamp	hostname	username	sha256	path
5/1/2024, 3:58:29 PM	JUSP-LAPTOP	cawharton	eb7f26f65e8a0a8ae4c74b94cdd7ae89ebb61e61caa6578c322920	C:\Use
5/1/2024, 3:59:25 PM	JUSP-LAPTOP	cawharton	1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669	C:\Pro

JPath: /filename Inline Compact

```
1  "timestamp": 2024-05-01T15:59:25.000Z,
2  "hostname": JUSP-LAPTOP,
3  "username": cawharton,
4  "sha256": 1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669f92413252,
5  "path": C:\ProgramData\ecobug.exe,
6  "filename": ecobug.exe,
```

What was the hash of the file?

1c3ef0407d5714037504c52f7abfa86c08

Solved by 876 players || Need help?

```
let carla =
Employees
| where email_addr == 'carla_wharton@solvisystems.com'
| project username;
FileCreationEvents
| where username in (carla)
| where timestamp between (datetime(2024-05-01T15:58:29Z) .. datetime(2024-05-01T16:58:29Z))
```

Table 1

timestamp	hostname	username	sha256	path
5/1/2024, 3:58:29 PM	JUSP-LAPTOP	cawharton	eb7f26f65e8a0a8ae4c74b94cdd7ae89ebb61e61caa6578c322920	C:\Use
5/1/2024, 3:59:25 PM	JUSP-LAPTOP	cawharton	1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669	C:\Pro

JPath: /sha256 Inline Compact

```
1  "timestamp": 2024-05-01T15:59:25.000Z,
2  "hostname": JUSP-LAPTOP,
3  "username": cawharton,
4  "sha256": 1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669f92413252,
5  "path": C:\ProgramData\ecobug.exe,
6  "filename": ecobug.exe,
```

How many records do we have of this file being created on Solvi Systems computers?

39

Solved by 867 players || Need help?

```
FileCreationEvents
| where filename == "ecobug.exe"
```

Table 39

timestamp	hostname	username	sha256	path
5/1/2024, 3:58:59 PM	MQQY-MACHINE	makertzman	4c199019661ef7ef79023e2c960617ec9a2f275ad578b1b1a027adl	C:\Pro
5/1/2024, 3:59:25 PM	JUSP-LAPTOP	cawharton	1c3ef0407d5714037504c52f7abfa86c081fd7a021b52e2abe8a669	C:\Pro

Let's go back and look at the process events on Carla's machine to see what happens after ecobug.exe is created.

What IP address does ecobug.exe connect to in order to establish persistence?

98.117.26.236

Solved by 858 players || Need help?

```
InboundNetworkEvents
| where src_ip has_any ("98.117.26.236", "105.78.23.64", "56.6.30.190", "13.201.46.208")
| distinct timestamp, src_ip
```

These are the malicious src_Ips used with the malware C2.

Order confirmation

Thank you for your order!

Order Number: NA1378372