Identifier (et bloquer !) les menaces avec Elastic Security

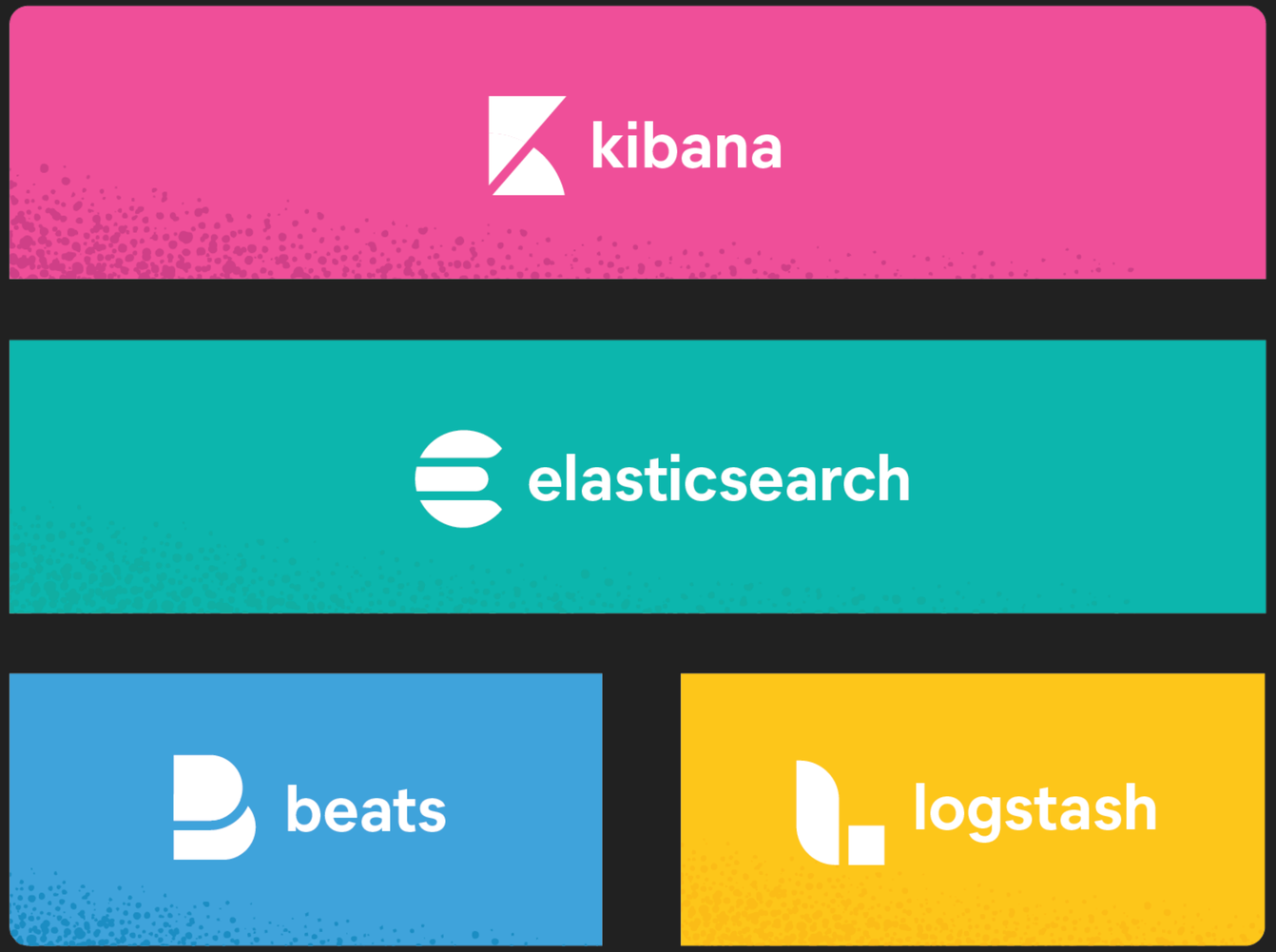
David Pilato @dadoonet
Developer | Evangelist

elastic

Devoxx France

#DevoxxFR

La suite Elastic



3 solutions

Elastic Enterprise Search

Elastic Observability

Elastic Security

Elastic Stack

Live Demo

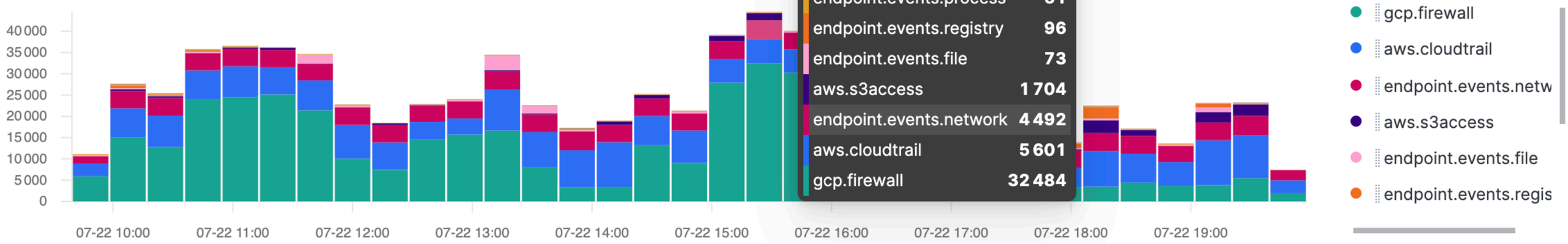
Backup slides

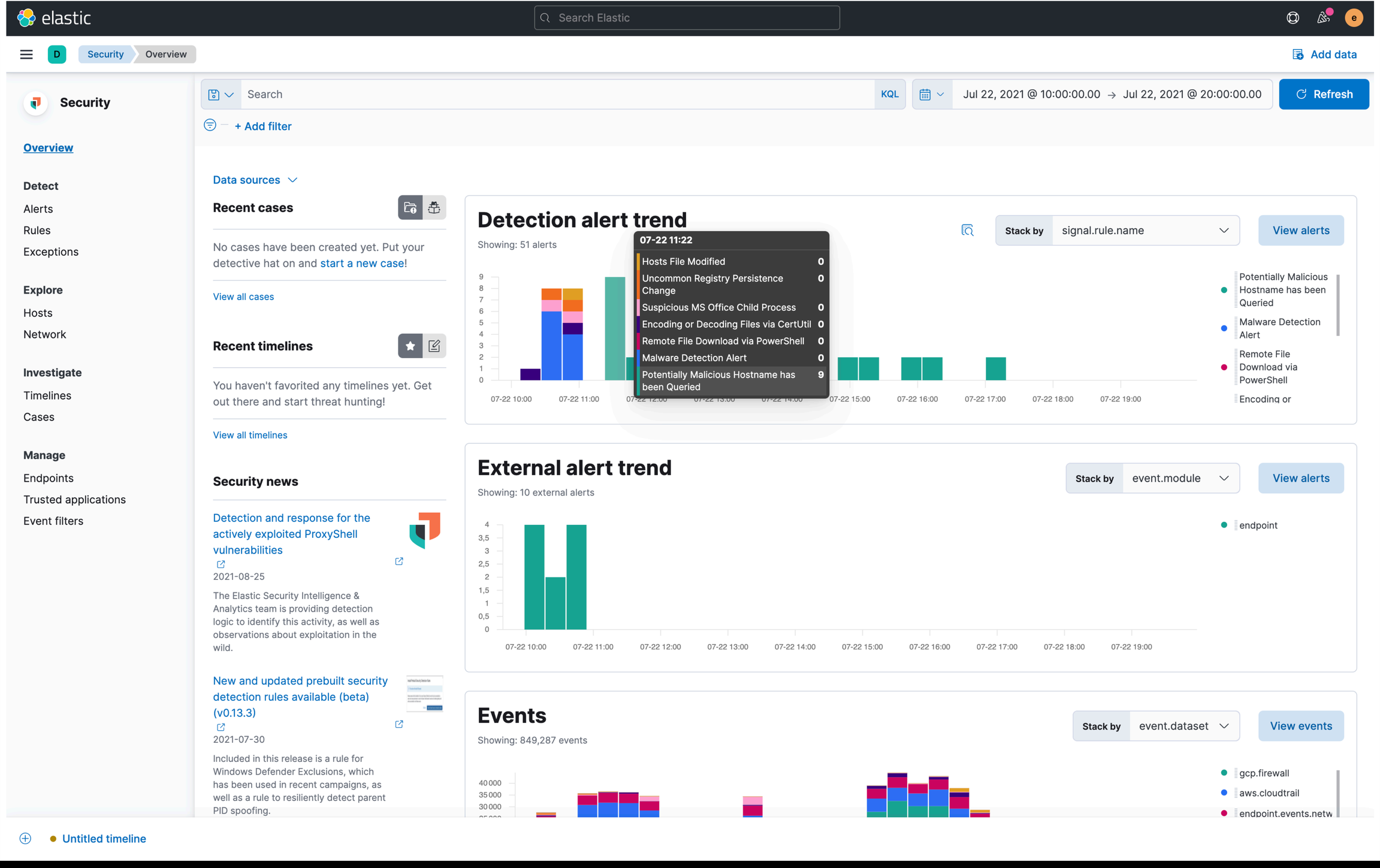
Events

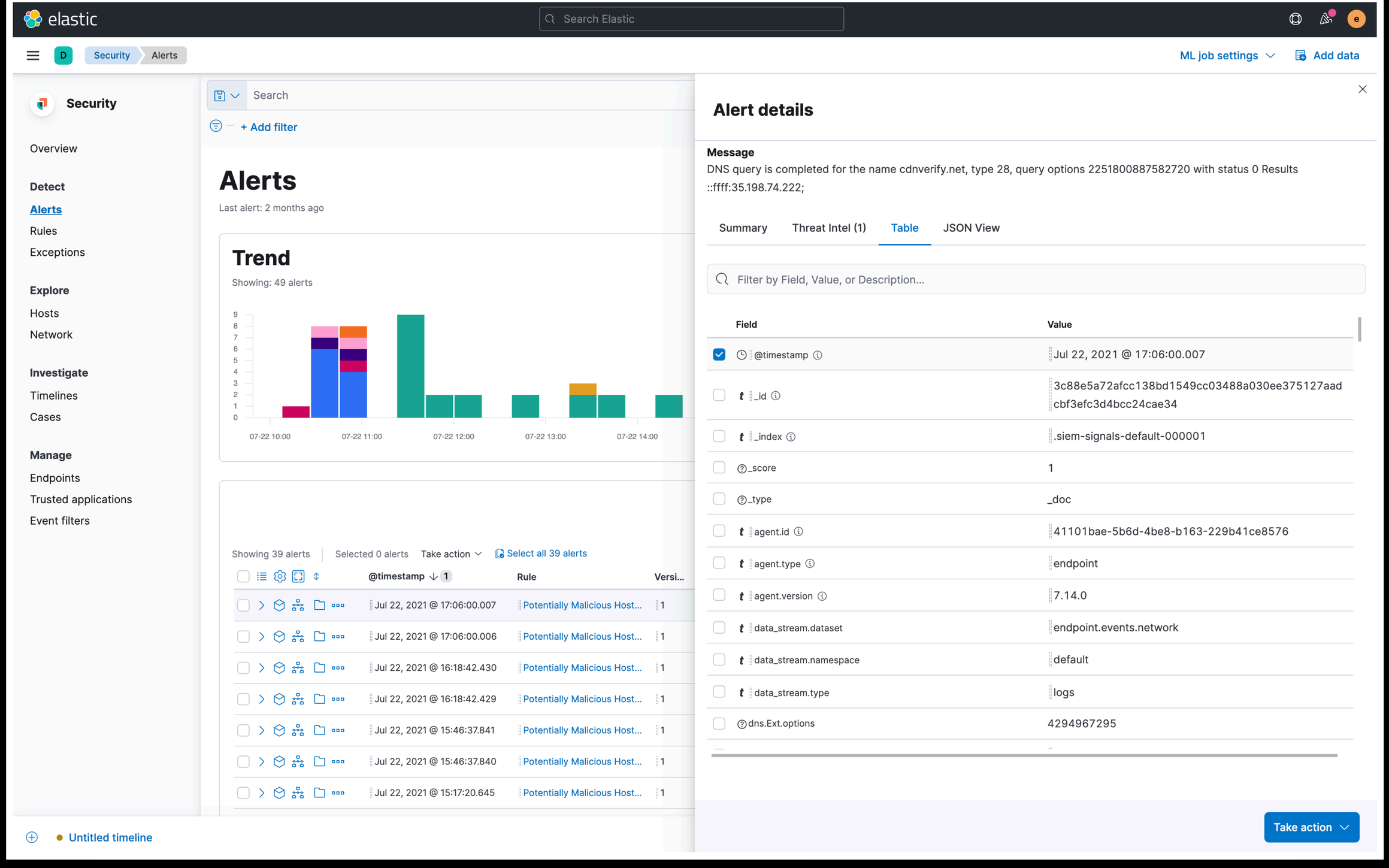
Showing: 849,287 events

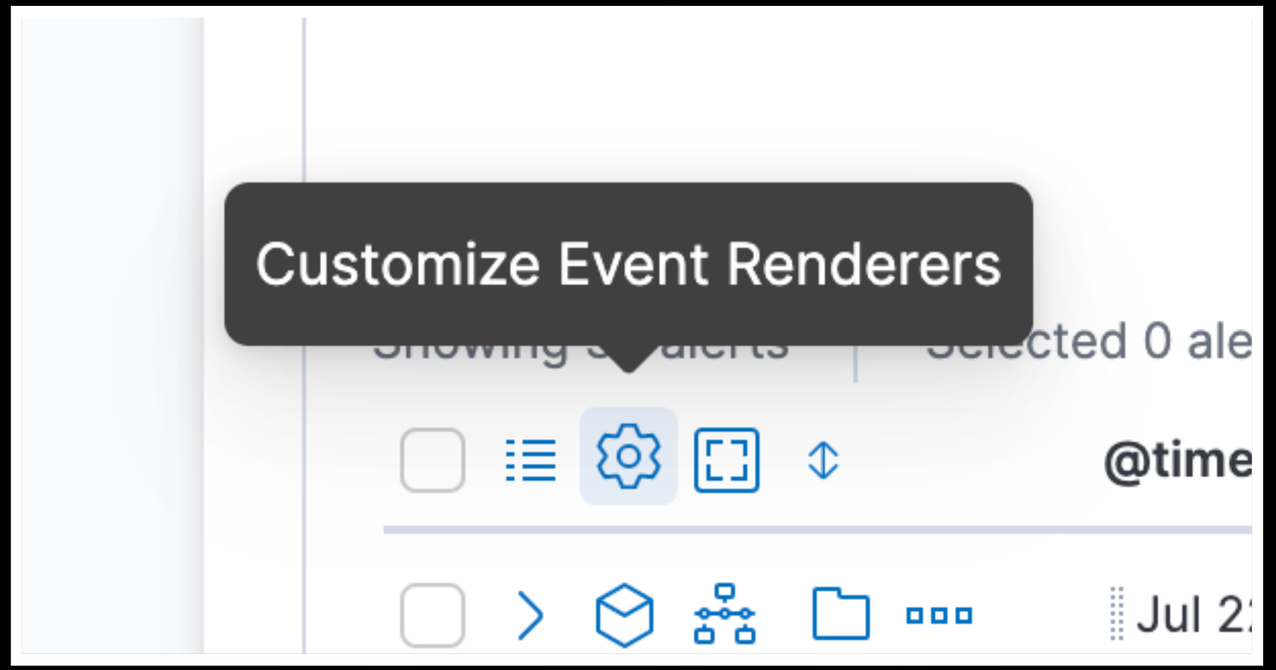
Stack by event.dataset

View events




elastic
Search Elastic
D
Security
Overview
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Search
KQL
Jul 22, 2021 @ 10:00:00.00 → Jul 22, 2021 @ 20:00:00.00
Refresh
+ Add filter
Data sources
Recent cases
No cases have been created yet. Put your detective hat on and start a new case!
View all cases
Recent timelines
You haven't favorited any timelines yet. Get out there and start threat hunting!
View all timelines
Security news
Detection and response for the actively exploited ProxyShell vulnerabilities
2021-08-25
The Elastic Security Intelligence & Analytics team is providing detection logic to identify this activity, as well as observations about exploitation in the wild.
New and updated prebuilt security detection rules available (beta) (v0.13.3)
2021-07-30
Included in this release is a rule for Windows Defender Exclusions, which has been used in recent campaigns, as well as a rule to resiliently detect parent PID spoofing.
Detection alert trend
Showing: 51 alerts
Stack by
signal.rule.name
View alerts
07-22 11:22
Hosts File Modified 0
Uncommon Registry Persistence Change 0
Suspicious MS Office Child Process 0
Encoding or Decoding Files via CertUtil 0
Remote File Download via PowerShell 0
Malware Detection Alert 0
Potentially Malicious Hostname has been Queried 9
Potentially Malicious Hostname has been Queried
Malware Detection Alert
Remote File Download via PowerShell
Encoding or
07-22 10:00
07-22 11:00
07-22 16:00
07-22 17:00
07-22 18:00
07-22 19:00
External alert trend
Showing: 10 external alerts
Stack by
event.module
View alerts
endpoint
07-22 10:00
07-22 11:00
07-22 12:00
07-22 13:00
07-22 14:00
07-22 15:00
07-22 16:00
07-22 17:00
07-22 18:00
07-22 19:00
Events
Showing: 849,287 events
Stack by
event.dataset
View events
gcp.firewall
aws.cloudtrail
Untitled timeline


elastic
Search Elastic
Security
Alerts
ML job settings
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Search
+ Add filter
Alerts
Last alert: 2 months ago
Trend
Showing: 49 alerts
9
8
7
6
5
4
3
2
1
0
07-22 10:00
07-22 11:00
07-22 12:00
07-22 13:00
07-22 14:00
Showing 39 alerts
Selected 0 alerts
Take action
Select all 39 alerts
@timestamp
Rule
Versi...
Jul 22, 2021 @ 17:06:00.007
Potentially Malicious Host...
1
Jul 22, 2021 @ 17:06:00.006
Potentially Malicious Host...
1
Jul 22, 2021 @ 16:18:42.430
Potentially Malicious Host...
1
Jul 22, 2021 @ 16:18:42.429
Potentially Malicious Host...
1
Jul 22, 2021 @ 15:46:37.841
Potentially Malicious Host...
1
Jul 22, 2021 @ 15:46:37.840
Potentially Malicious Host...
1
Jul 22, 2021 @ 15:17:20.645
Potentially Malicious Host...
1
Untitled timeline
Alert details
Message
DNS query is completed for the name cdnverify.net, type 28, query options 2251800887582720 with status 0 Results ::ffff:35.198.74.222;
Summary
Threat Intel (1)
Table
JSON View
Filter by Field, Value, or Description...
Field
Value
@timestamp
Jul 22, 2021 @ 17:06:00.007
_id
3c88e5a72afcc138bd1549cc03488a030ee375127aadcbf3efc3d4bcc24cae34
_index
.siem-signals-default-000001
_score
1
_type
_doc
agent.id
41101bae-5b6d-4be8-b163-229b41ce8576
agent.type
endpoint
agent.version
7.14.0
data_stream.dataset
endpoint.events.network
data_stream.namespace
default
data_stream.type
logs
dns.Ext.options
4294967295
Take action


Customize Event Renderers
@time
Jul 2


Showing 39 alerts
Selected 0 alerts
Take action
Select all 39 alerts
Additional filters
@timestamp
1
Rule
Versi...
Method
Severity
Risk Score
event.module
event.action
event.category
host
Jul 22, 2021 @ 17:06:00.007
Potentially Malicious Host...
1
threat_match
high
75
endpoint
lookup_result
network
bh
dns.question.name
matched
cdnverify.net
indicator_match_rule

Security

Overview

Detect
Alerts
Rules
Exceptions

Explore
Hosts
Network

Investigate
Timelines
Cases

Manage
Endpoints
Trusted applications
Event filters

Search
KQL
Jul 22, 2021 @ 10:00:00.00 → Jul 22, 2021 @ 20:00:00.00
Refresh
+ Add filter

Rules

Potentially Malicious Hostname has been Queried

Created by: elastic on Jul 22, 2021 @ 11:24:47.806 Updated by: 3612216885 on Jul 28, 2021 @ 16:13:23.990

Last alert: 2 months ago Last response: —

Activated
Edit rule settings

About

This rule matches DNS requests or TLS handshakes against a list of known bad domains.

Author Elastic

Severity High

Risk score 75

License Elastic

MITRE ATT&CK™
- Command and Control (TA0011)
  - Encrypted Channel (T1573)
    - Asymmetric Cryptography (T1573.002)
  - Protocol Tunneling (T1572)

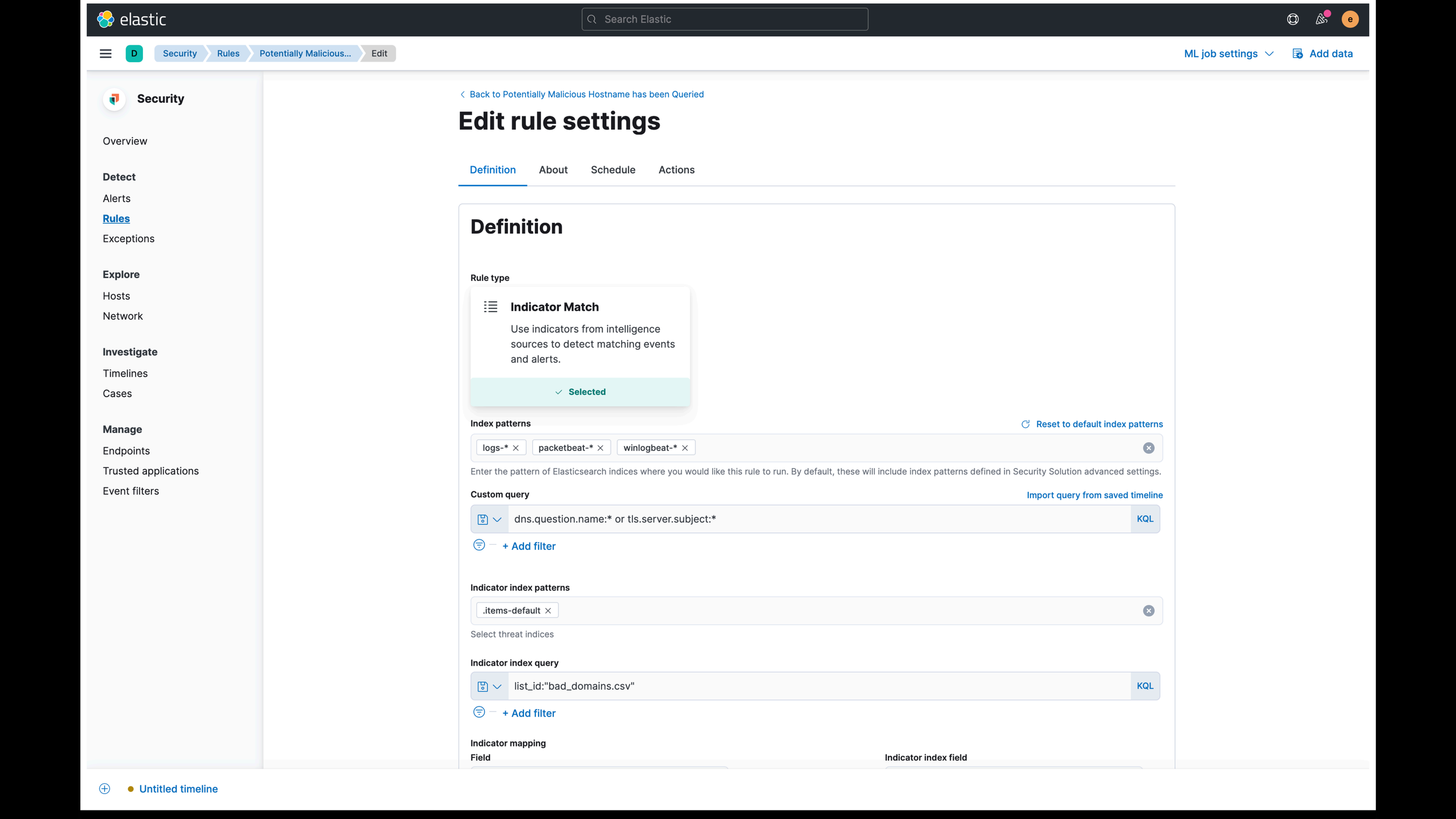
Tags dns, tls, domains

Definition

Index patterns	logs-*, packetbeat-*, winlogbeat-*
Custom query	dns.question.name:* or tls.server.subject:*
Rule type	Indicator Match
Timeline template	None
Indicator index patterns	.items-default
Indicator mapping	(dns.question.name MATCHES keyword) OR (tls.server.subject MATCHES keyword) OR (dns.question.registered_domain MATCHES keyword)
Indicator index query	list_id:"bad_domains.csv"

Schedule

Runs every	1m
Additional look-back time	2h


elastic
Search Elastic
D
Security
Rules
Potentially Malicious...
Edit
ML job settings
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Back to Potentially Malicious Hostname has been Queried
Edit rule settings
Definition
About
Schedule
Actions
Definition
Rule type
Indicator Match
Use indicators from intelligence sources to detect matching events and alerts.
Selected
Index patterns
Reset to default index patterns
logs-*
packetbeat-*
winlogbeat-*
Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.
Custom query
Import query from saved timeline
dns.question.name:* or tls.server.subject:*
KQL
+ Add filter
Indicator index patterns
.items-default
Select threat indices
Indicator index query
list_id:"bad_domains.csv"
KQL
+ Add filter
Indicator mapping
Field
Indicator index field
Untitled timeline

Back to Potentially Malicious Hostname has been Queried

Edit rule settings

Definition | About | Schedule | Actions

Schedule

Runs every

1 | Minutes

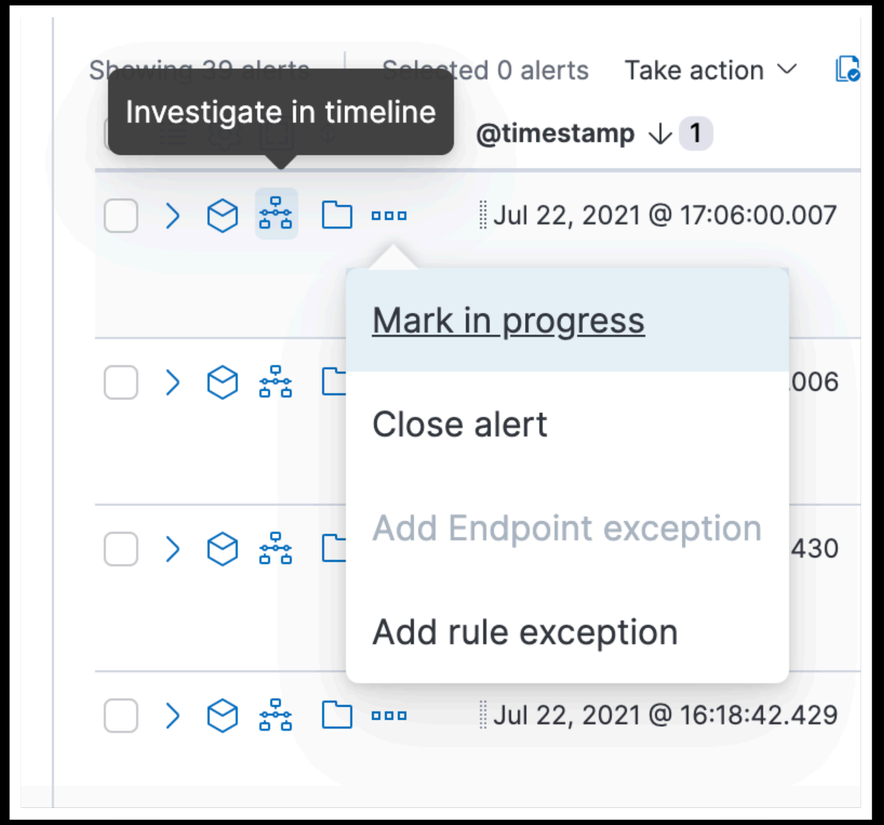
Rules run periodically and detect alerts within the specified time frame.

Additional look-back time Optional

2 | Hours

Adds time to the look-back period to prevent missed alerts.

Cancel | Save changes


Selected 0 alerts
Take action
Investigate in timeline
@timestamp
1
Jul 22, 2021 @ 17:06:00.007
Mark in progress
Close alert
Add Endpoint exception
Add rule exception
Jul 22, 2021 @ 16:18:42.429

elastic

Search Elastic

Security / Alerts

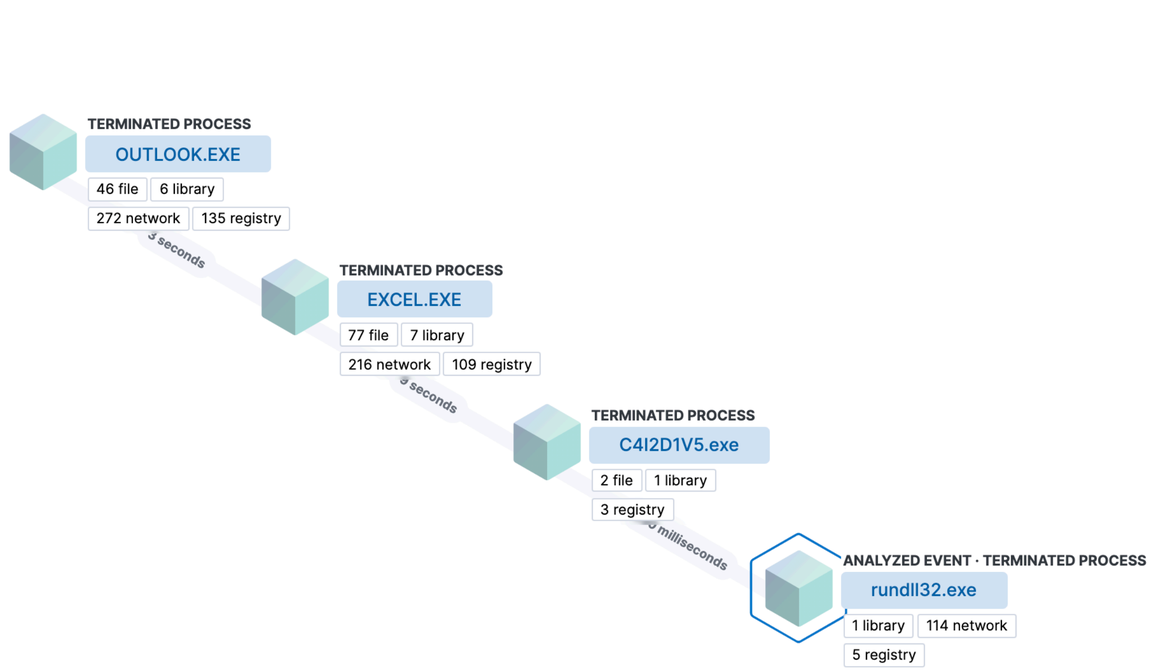
ML job settings | Add data

Exit full screen

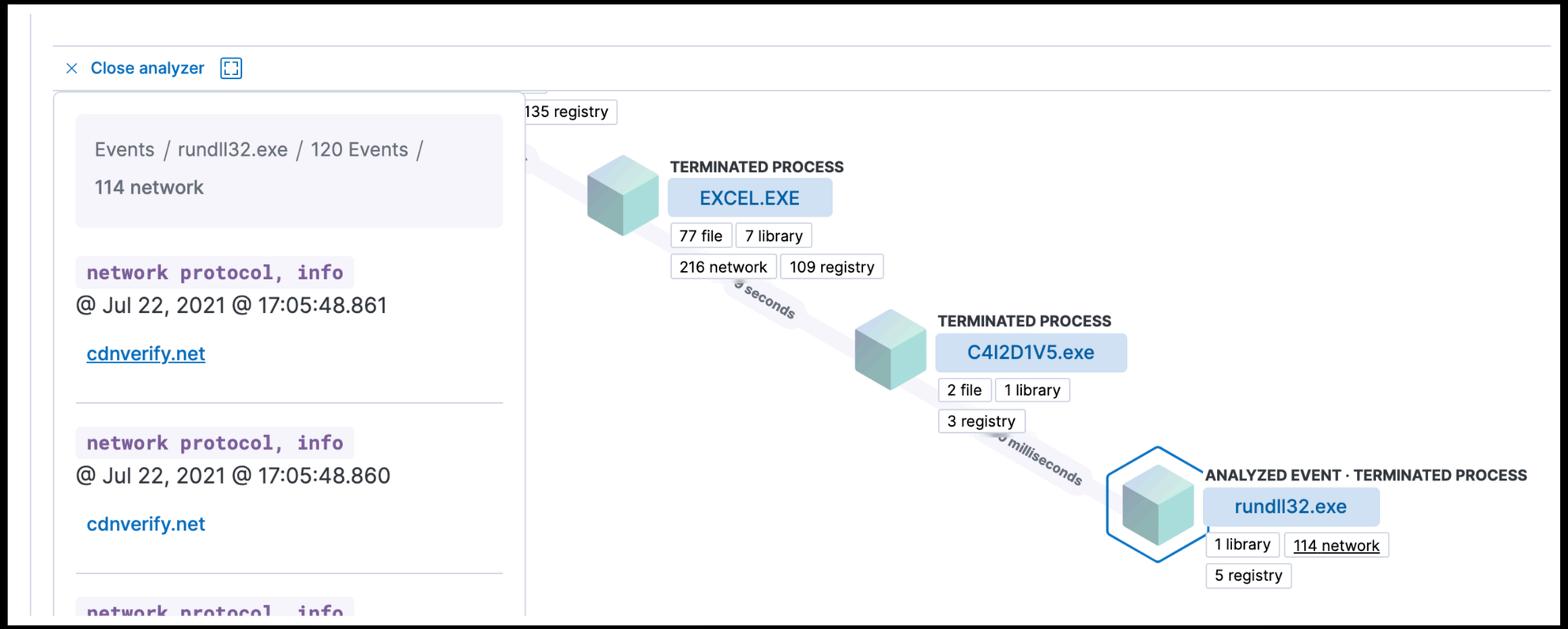
Close analyzer

All Process Events

Process Name	Timestamp
OUTLOOK.E...	Jul 22, 2021 @ 10:46:08.290
EXCEL.EXE	Jul 22, 2021 @ 10:46:11.451
C4I2D1V5.e...	Jul 22, 2021 @ 10:46:20.892
ANALYZED EVE... rundll32.exe	Jul 22, 2021 @ 10:46:21.222



Untitled timeline


Close analyzer
Events / rundll32.exe / 120 Events / 114 network
network protocol, info
@ Jul 22, 2021 @ 17:05:48.861
cdnverify.net
network protocol, info
@ Jul 22, 2021 @ 17:05:48.860
cdnverify.net
135 registry
TERMINATED PROCESS
EXCEL.EXE
77 file
7 library
216 network
109 registry
3 seconds
TERMINATED PROCESS
C4I2D1V5.exe
2 file
1 library
3 registry
3 milliseconds
ANALYZED EVENT · TERMINATED PROCESS
rundll32.exe
1 library
114 network
5 registry

Close analyzer

135

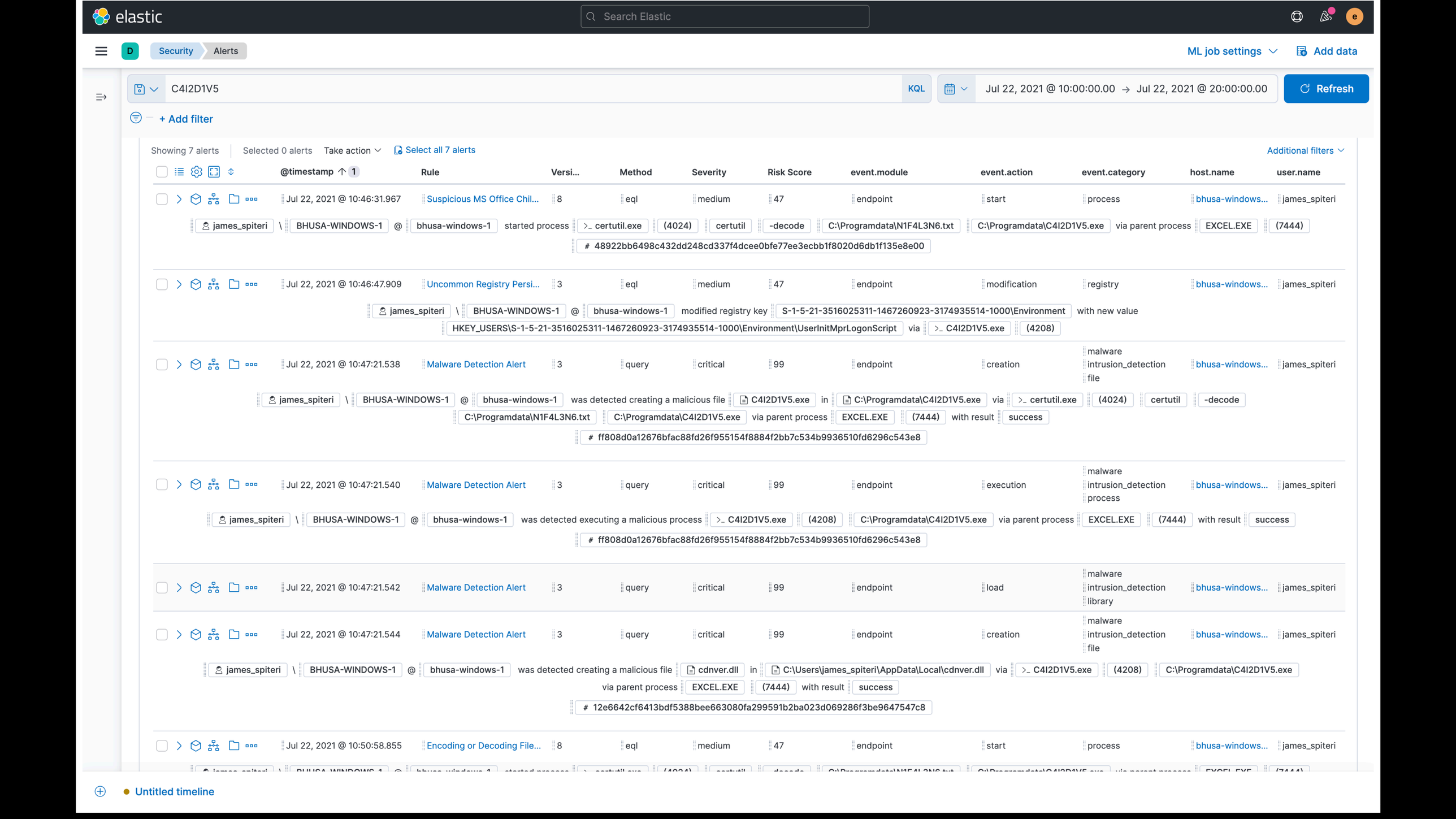
dns

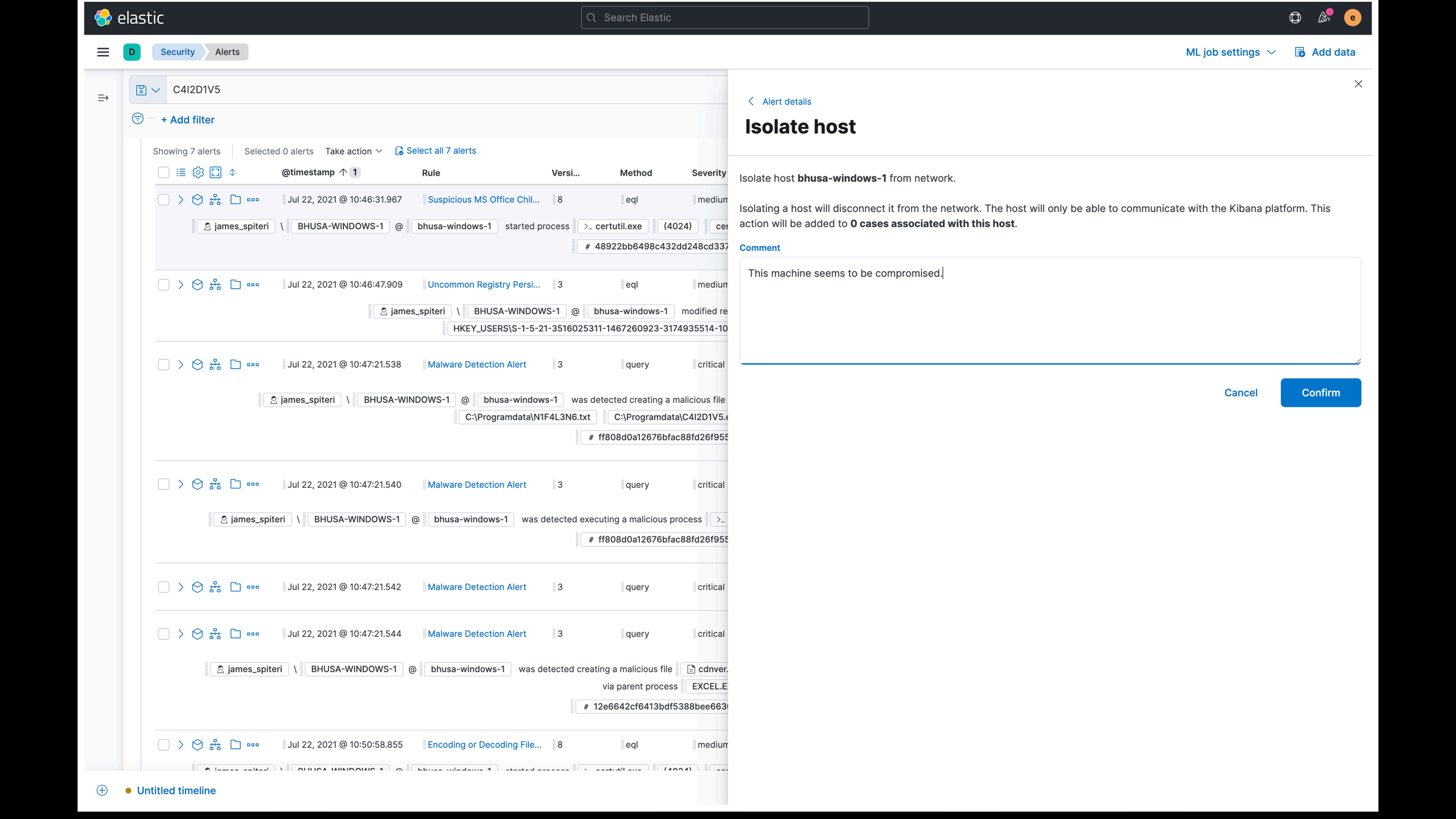
dns.Ext. options	4294967295
dns.question. name	cdnverify.net
dns.question. type	AAAA

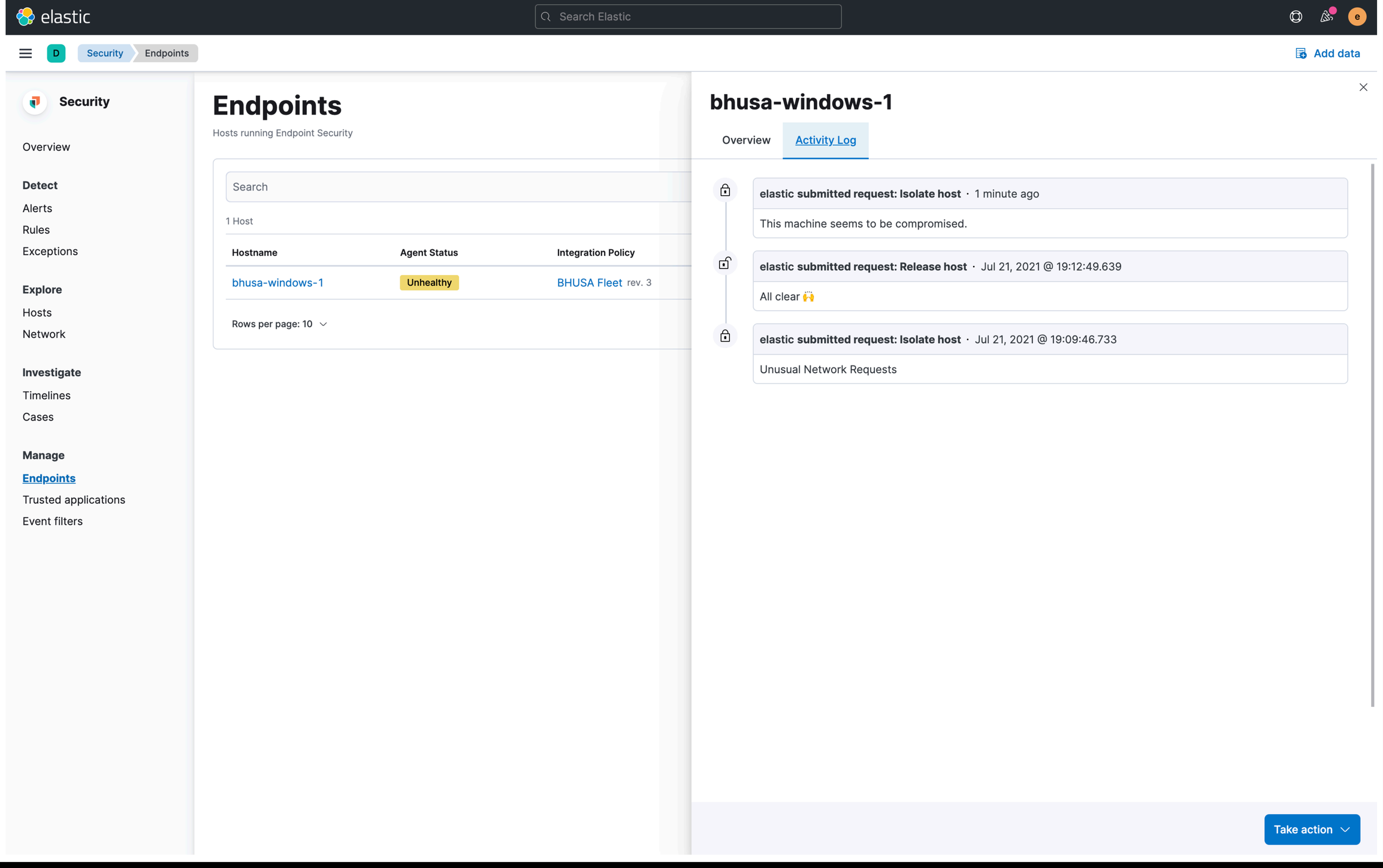
message

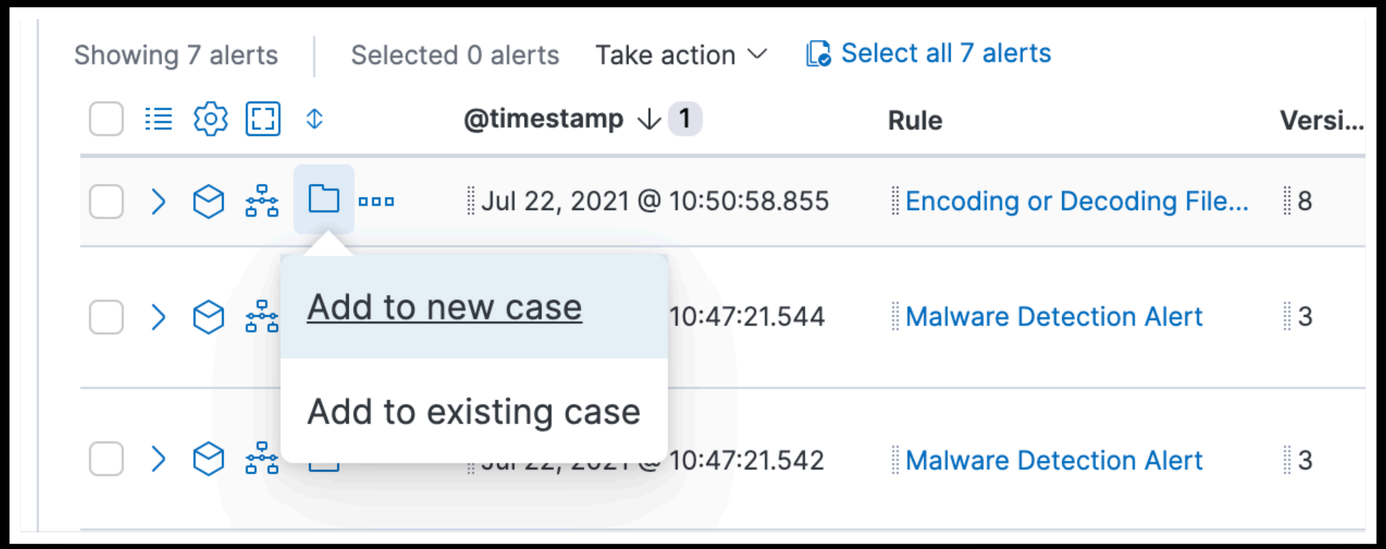
message	DNS query is completed for the name cdnverify.net, type 28, query options 2251800887582720 with status 0 Results ::ffff:35.198.74.222;

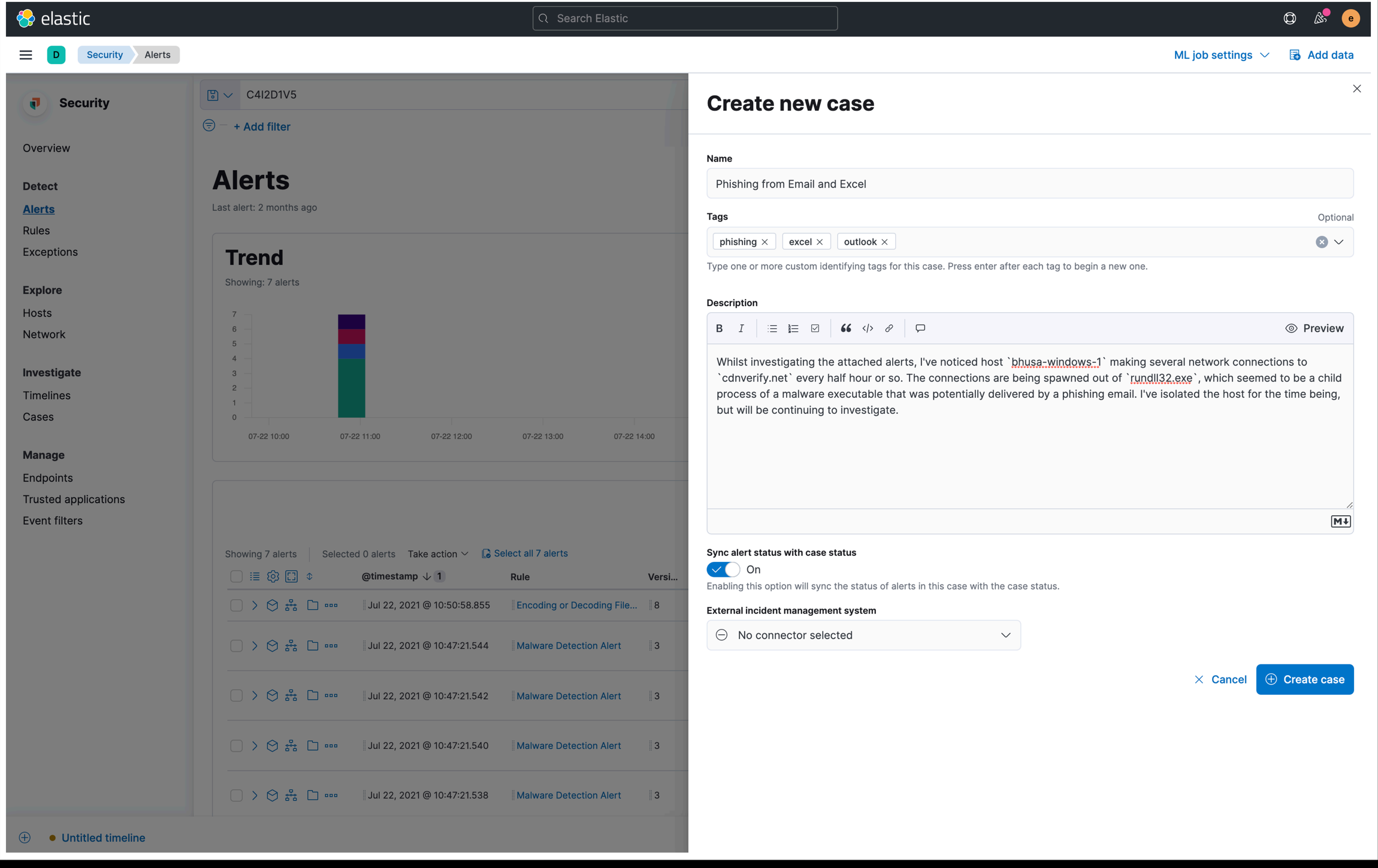
network


elastic
Search Elastic
Security
Alerts
ML job settings
Add data
C4I2D1V5
KQL
Jul 22, 2021 @ 10:00:00.00 → Jul 22, 2021 @ 20:00:00.00
Refresh
+ Add filter
Showing 7 alerts
Selected 0 alerts
Take action
Select all 7 alerts
Additional filters
@timestamp 1
Rule
Versi...
Method
Severity
Risk Score
event.module
event.action
event.category
host.name
user.name
Jul 22, 2021 @ 10:46:31.967
Suspicious MS Office Chil...
8
eql
medium
47
endpoint
start
process
bhusa-windows...
james_spiteri
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 started process >_ certutil.exe (4024) certutil -decode C:\Programdata\N1F4L3N6.txt C:\Programdata\C4I2D1V5.exe via parent process EXCEL.EXE (7444)
48922bb6498c432dd248cd337f4dcee0bfe77ee3ecbb1f8020d6db1f135e8e00
Jul 22, 2021 @ 10:46:47.909
Uncommon Registry Persi...
3
eql
medium
47
endpoint
modification
registry
bhusa-windows...
james_spiteri
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 modified registry key S-1-5-21-3516025311-1467260923-3174935514-1000\Environment with new value
HKEY_USERS\S-1-5-21-3516025311-1467260923-3174935514-1000\Environment\UserInitMprLogonScript via >_ C4I2D1V5.exe (4208)
Jul 22, 2021 @ 10:47:21.538
Malware Detection Alert
3
query
critical
99
endpoint
creation
malware
intrusion_detection
file
bhusa-windows...
james_spiteri
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected creating a malicious file C4I2D1V5.exe in C:\Programdata\C4I2D1V5.exe via >_ certutil.exe (4024) certutil -decode
C:\Programdata\N1F4L3N6.txt C:\Programdata\C4I2D1V5.exe via parent process EXCEL.EXE (7444) with result success
ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8
Jul 22, 2021 @ 10:47:21.540
Malware Detection Alert
3
query
critical
99
endpoint
execution
malware
intrusion_detection
process
bhusa-windows...
james_spiteri
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected executing a malicious process >_ C4I2D1V5.exe (4208) C:\Programdata\C4I2D1V5.exe via parent process EXCEL.EXE (7444) with result success
ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8
Jul 22, 2021 @ 10:47:21.542
Malware Detection Alert
3
query
critical
99
endpoint
load
malware
intrusion_detection
library
bhusa-windows...
james_spiteri
Jul 22, 2021 @ 10:47:21.544
Malware Detection Alert
3
query
critical
99
endpoint
creation
malware
intrusion_detection
file
bhusa-windows...
james_spiteri
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected creating a malicious file cdnver.dll in C:\Users\james_spiteri\AppData\Local\cdnver.dll via >_ C4I2D1V5.exe (4208) C:\Programdata\C4I2D1V5.exe
via parent process EXCEL.EXE (7444) with result success
12e6642cf6413bdf5388bee663080fa299591b2ba023d069286f3be9647547c8
Jul 22, 2021 @ 10:50:58.855
Encoding or Decoding File...
8
eql
medium
47
endpoint
start
process
bhusa-windows...
james_spiteri
Untitled timeline


elastic
Search Elastic
Security
Alerts
ML job settings
Add data
C4I2D1V5
+ Add filter
Showing 7 alerts
Selected 0 alerts
Take action
Select all 7 alerts
@timestamp
Rule
Versi...
Method
Severity
Jul 22, 2021 @ 10:46:31.967
Suspicious MS Office Chil...
8
eql
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 started process certutil.exe (4024)
48922bb6498c432dd248cd337
Jul 22, 2021 @ 10:46:47.909
Uncommon Registry Persi...
3
eql
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 modified re
HKEY_USERS\S-1-5-21-3516025311-1467260923-3174935514-10
Jul 22, 2021 @ 10:47:21.538
Malware Detection Alert
3
query
critical
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected creating a malicious file
C:\Programdata\N1F4L3N6.txt
C:\Programdata\C4I2D1V5.
ff808d0a12676bfac88fd26f955
Jul 22, 2021 @ 10:47:21.540
Malware Detection Alert
3
query
critical
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected executing a malicious process
ff808d0a12676bfac88fd26f955
Jul 22, 2021 @ 10:47:21.542
Malware Detection Alert
3
query
critical
Jul 22, 2021 @ 10:47:21.544
Malware Detection Alert
3
query
critical
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 was detected creating a malicious file
via parent process
EXCEL.E
12e6642cf6413bdf5388bee663
Jul 22, 2021 @ 10:50:58.855
Encoding or Decoding File...
8
eql
Untitled timeline
Alert details
Isolate host
Isolate host bhusa-windows-1 from network.
Isolating a host will disconnect it from the network. The host will only be able to communicate with the Kibana platform. This action will be added to 0 cases associated with this host.
Comment
This machine seems to be compromised.
Cancel
Confirm


elastic
Search Elastic
D
Security
Endpoints
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Endpoints
Hosts running Endpoint Security
Search
1 Host
Hostname
Agent Status
Integration Policy
bhusa-windows-1
Unhealthy
BHUSA Fleet rev. 3
Rows per page: 10
bhusa-windows-1
Overview
Activity Log
elastic submitted request: Isolate host · 1 minute ago
This machine seems to be compromised.
elastic submitted request: Release host · Jul 21, 2021 @ 19:12:49.639
All clear 🙌
elastic submitted request: Isolate host · Jul 21, 2021 @ 19:09:46.733
Unusual Network Requests
Take action


Showing 7 alerts
Selected 0 alerts
Take action
Select all 7 alerts
@timestamp
1
Rule
Versi...
Jul 22, 2021 @ 10:50:58.855
Encoding or Decoding File...
8
Add to new case
Add to existing case
10:47:21.544
Malware Detection Alert
3
10:47:21.542
Malware Detection Alert
3


elastic
Search Elastic
Security
Alerts
ML job settings
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
C4I2D1V5
+ Add filter
Alerts
Last alert: 2 months ago
Trend
Showing: 7 alerts
07-22 10:00
07-22 11:00
07-22 12:00
07-22 13:00
07-22 14:00
Showing 7 alerts
Selected 0 alerts
Take action
Select all 7 alerts
@timestamp
Rule
Versi...
Jul 22, 2021 @ 10:50:58.855
Encoding or Decoding File...
Jul 22, 2021 @ 10:47:21.544
Malware Detection Alert
Jul 22, 2021 @ 10:47:21.542
Malware Detection Alert
Jul 22, 2021 @ 10:47:21.540
Malware Detection Alert
Jul 22, 2021 @ 10:47:21.538
Malware Detection Alert
Untitled timeline
Create new case
Name
Phishing from Email and Excel
Tags
Optional
phishing
excel
outlook
Type one or more custom identifying tags for this case. Press enter after each tag to begin a new one.
Description
Preview
Whilst investigating the attached alerts, I've noticed host `bhusa-windows-1` making several network connections to `cdnverify.net` every half hour or so. The connections are being spawned out of `rundll32.exe`, which seemed to be a child process of a malware executable that was potentially delivered by a phishing email. I've isolated the host for the time being, but will be continuing to investigate.
Sync alert status with case status
On
Enabling this option will sync the status of alerts in this case with the case status.
External incident management system
No connector selected
Cancel
Create case

Security

Overview

Detect
Alerts
Rules
Exceptions

Explore
Hosts
Network

Investigate
Timelines
Cases

Manage
Endpoints
Trusted applications
Event filters

Back to cases

Phishing from Email and Excel

Status Open
Case opened 1 minute ago
Sync alerts
Refresh case

elastic added description 1 minute ago

Whilst investigating the attached alerts, I've noticed host `bhusa-windows-1` making several network connections to `cdnverify.net` every half hour or so. The connections are being spawned out of `rundll32.exe`, which seemed to be a child process of a malware executable that was potentially delivered by a phishing email. I've isolated the host for the time being, but will be continuing to investigate.

elastic added an alert from Encoding or Decoding Files via CertUtil 1 minute ago

Preview

Mark in progress
Add comment

Reporter
elastic

Participants
elastic

Tags
phishing excel outlook

External incident management system

Select an external connector

To create and update a case in an external system, select a connector.

Add connector

elastic

Search Elastic

Security / Alerts

ML job settings | Add data

Untitled timeline

Untitled timeline

Unsaved

Add a description

Processes	Users	Hosts	Source IPs	Destination IPs
4	2	1	0	0

Remove from favorites | Attach to case

Query 62 | Correlation 24 | Analyzer | Notes | Pinned

Jul 21, 2021 @ 12:58:54.025 → Jul 22, 2021 @ 22:10:07.316

Refresh | All data sources

dns.question.name: "cdnverify.net"

OR + Add field

AND Filter | Search | KQL

+ Add filter

@timestamp ↓ 1	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Jul 22, 2021 @ 17:06:00.007	DNS query is completed for ...	network	lookup_result	bhusa-windows-1	—	—	james_spiteri
	dns.question.name matched cdnverify.net indicator_match_rule						
Jul 22, 2021 @ 17:06:00.006	DNS query is completed for ...	network	lookup_requested	bhusa-windows-1	—	—	james_spiteri
	dns.question.name matched cdnverify.net indicator_match_rule						
Jul 22, 2021 @ 17:05:48.861	DNS query is completed for ...	network	lookup_result	bhusa-windows-1	—	—	james_spiteri
	james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 asked for cdnverify.net with question type AAAA via >_ rundll32.exe (2208) dns						
Jul 22, 2021 @ 17:05:48.860	DNS query is completed for ...	network	lookup_requested	bhusa-windows-1	—	—	james_spiteri
	james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 asked for cdnverify.net with question type A via >_ rundll32.exe (2208) dns						
Jul 22, 2021 @ 16:18:42.430	DNS query is completed for ...	network	lookup_result	bhusa-windows-1	—	—	james_spiteri
	dns.question.name matched cdnverify.net indicator_match_rule						
Jul 22, 2021 @ 16:18:42.429	DNS query is completed for ...	network	lookup_requested	bhusa-windows-1	—	—	james_spiteri

25 of 62

1 2 3

Updated 1 minute ago

@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip
Jul 22, 2021 @ 10:46:22.935	Endpoint network event	network	connection_attempted	bhusa-windows-1	10.132.0.52	35.198.74.222
Jul 22, 2021 @ 10:46:23.011	—	network	firewall-rule	james-fleet-714	10.132.0.52	35.198.74.222

Security

Overview

Detect
Alerts
Rules
Exceptions

Explore
Hosts
Network

Investigate
Timelines
Cases

Manage
Endpoints
Trusted applications
Event filters

Back to cases

Phishing from Email and Excel

Status Open

Case opened 28 minutes ago

Sync alerts

Refresh case

elastic added description 28 minutes ago

Whilst investigating the attached alerts, I've noticed host `bhusa-windows-1` making several network connections to `cdnverify.net` every half hour or so. The connections are being spawned out of `rundll32.exe`, which seemed to be a child process of a malware executable that was potentially delivered by a phishing email. I've isolated the host for the time being, but will be continuing to investigate.

elastic added an alert from Encoding or Decoding Files via CertUtil 28 minutes ago

elastic 4 minutes ago

We saw that an email created an EXE which ran on our machine. We can confirm that data was sent outside our network.

Hunting for firewall activity

B I Preview

Mark in progress

Add comment

Reporter

elastic

Participants

elastic

Tags

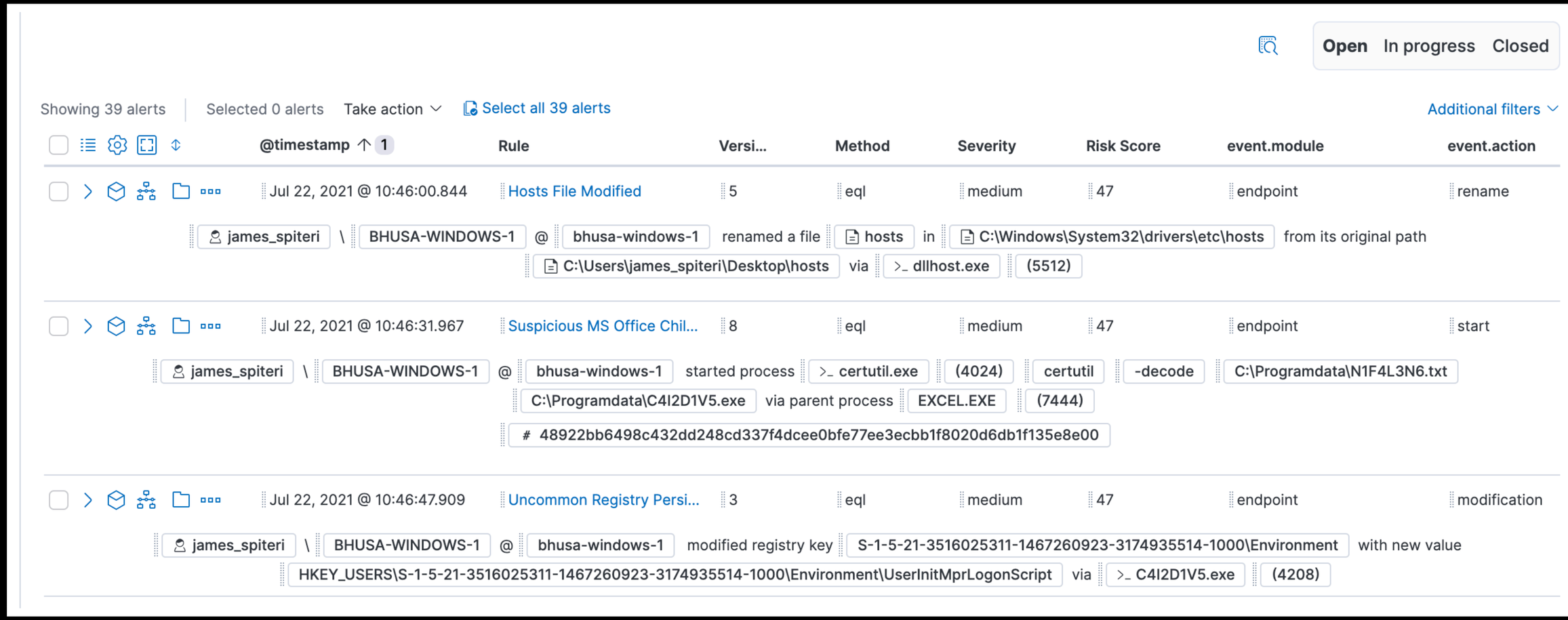
phishing excel outlook

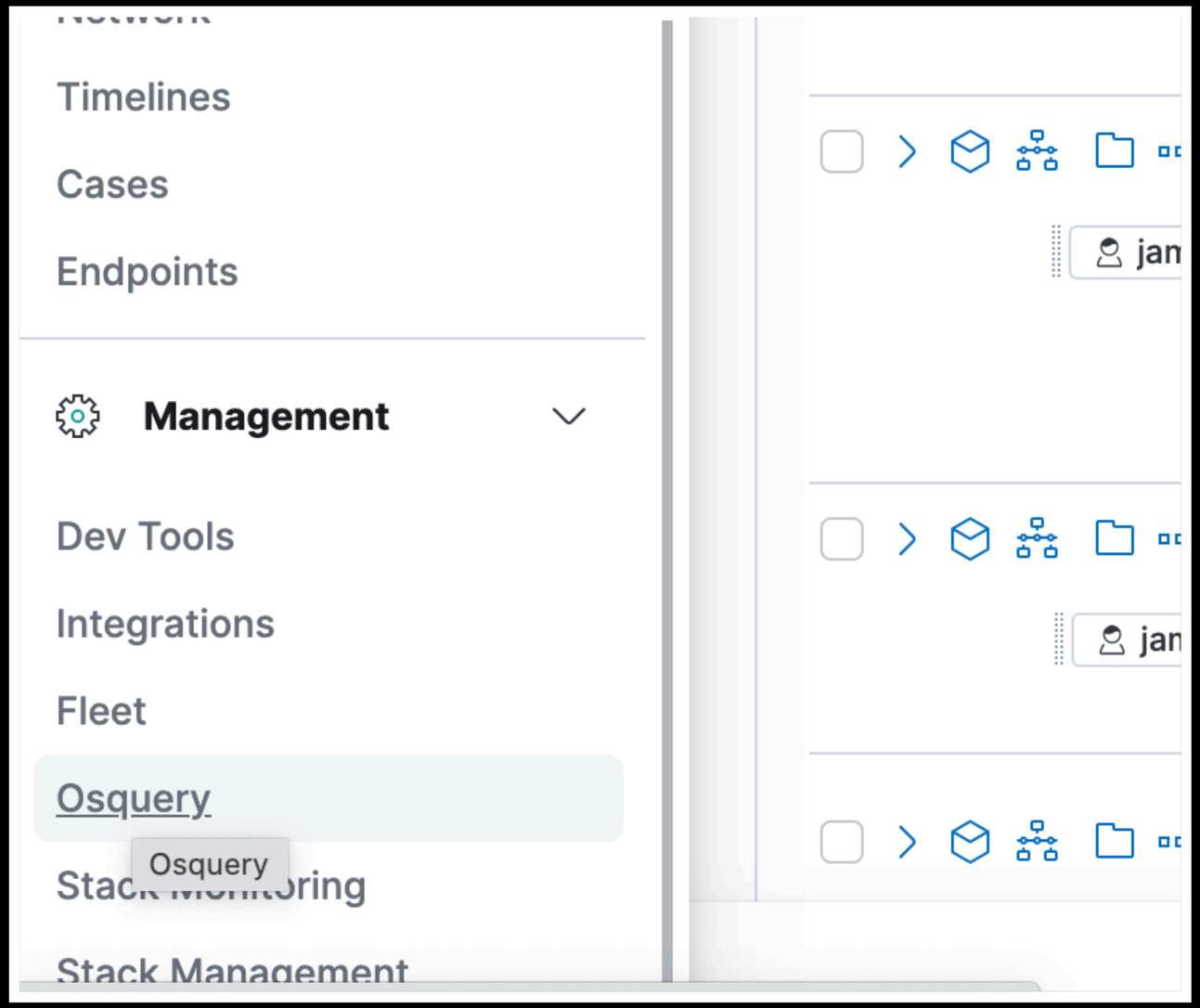
External incident management system

Select an external connector

To create and update a case in an external system, select a connector.

Add connector


Open
In progress
Closed
Showing 39 alerts
Selected 0 alerts
Take action
Select all 39 alerts
Additional filters
@timestamp 1
Rule
Versi...
Method
Severity
Risk Score
event.module
event.action
Jul 22, 2021 @ 10:46:00.844
Hosts File Modified
5
eql
medium
47
endpoint
rename
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 renamed a file hosts in C:\Windows\System32\drivers\etc\hosts from its original path
C:\Users\james_spiteri\Desktop\hosts via >_ dllhost.exe (5512)
Jul 22, 2021 @ 10:46:31.967
Suspicious MS Office Chil...
8
eql
medium
47
endpoint
start
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 started process >_ certutil.exe (4024) certutil -decode C:\Programdata\N1F4L3N6.txt
C:\Programdata\C4I2D1V5.exe via parent process EXCEL.EXE (7444)
48922bb6498c432dd248cd337f4dcee0bfe77ee3ecbb1f8020d6db1f135e8e00
Jul 22, 2021 @ 10:46:47.909
Uncommon Registry Persi...
3
eql
medium
47
endpoint
modification
james_spiteri \ BHUSA-WINDOWS-1 @ bhusa-windows-1 modified registry key S-1-5-21-3516025311-1467260923-3174935514-1000\Environment with new value
HKEY_USERS\S-1-5-21-3516025311-1467260923-3174935514-1000\Environment\UserInitMprLogonScript via >_ C4I2D1V5.exe (4208)


Timelines
Cases
Endpoints
Management
Dev Tools
Integrations
Fleet
Osquery
Osquery
Stack Management

Live queries history

BETA

New live query

Query	Agents	Created at	Run by	View details
`select * from etc_hosts`	1	28 Jul 2021 08:43	elastic	
`select * from etc_hosts`	1	28 Jul 2021 08:43	elastic	
`select * from etc_hosts`	1	22 Jul 2021 16:57	elastic	
`select * from etc_hosts`	1	22 Jul 2021 15:40	elastic	
`select * from etc_hosts`	1	22 Jul 2021 11:29	elastic	
`select * from scheduled_tasks where name == "AppPool"`	1	21 Jul 2021 19:55	elastic	
`select * from logon_sessions`	1	21 Jul 2021 19:32	elastic	
`select * from logged_in_users`	1	21 Jul 2021 19:30	elastic	

View live queries history

Live query details

BETA

```
select * from etc_hosts
```

Queried 1 agent

Successful 0 Expired 1 Failed 0

Results Status

View results in Discover | View results in Lens | Columns | Density | Sort fields | Full screen

agent	address	hostnames
bhusa-windows-1	169.254.169.254	metadata.google.internal metadata
bhusa-windows-1	35.198.74.222	cdnverify.net

Security

Overview

Detect
Alerts
Rules
Exceptions

Explore
Hosts
Network

Investigate
Timelines
Cases

Manage
Endpoints
Trusted applications
Event filters

Endpoints

Hosts running Endpoint Security

Search KQL Refresh 10 seconds

1 Host

Hostname	Agent Status	Integration Policy	Policy Status	Operating System	IP Address	Version	Last Active	Actions
bhusa-windows-1	Unhealthy	BHUSA Fleet rev. 3	Success	Windows	10.132.0.52, fe80::b...	7.14.0	Jul 28, 2021 @...	▫▫▫

Rows per page: 10

1

Security

Overview

Detect
Alerts
Rules
Exceptions

Explore
Hosts
Network

Investigate
Timelines
Cases

Manage
Endpoints
Trusted applications
Event filters

Back to endpoint hosts

BHUSA Fleet

Agents	Healthy	Unhealthy	Offline
0	0	0	0

Protections

Type
Malware

Operating System
Windows, Mac, Linux

Malware protections enabled

Protection Level
- (•) Detect
- ( ) Prevent

User Notification
Agent version 7.11+

[x] Notify User

Customize notification message

Elastic Security {action} {filename}

View related detection rules. Prebuilt rules are tagged "Elastic" on the Detection Rules page.

Type
Ransomware

Operating System
Windows

Ransomware protections enabled

Protection Level
- ( ) Detect
- (•) Prevent

User Notification
Agent version 7.12+

[x] Notify User

Cancel
Save

Merci

Devoxx France

#DevoxxFR