Release Notes

FortiNDR Cloud 2023

February 27, 2025
FortiNDR Cloud 2023 Release Notes
78-242-1113279-20250227

TABLE OF CONTENTS

FortiNDR Cloud release notes

This document provides information about FortiNDR Cloud releases.

FortiNDR Cloud is a SaaS network security monitoring platform designed to facilitate rapid detection, investigations, and threat hunting within your environment. FortiNDR Cloud is designed to be scalable and to remove the responsibilities of maintaining tooling from security analysts. For more information, see the FortiNDR Cloud User Guide.

Version History (2023)

Date	Version
13 December 2023	2023.12
15 November 2023	2023.11
25 October 2023	2023.10
11 October 2023	2023.9.1
27 September 2023	2023.9
13 September 2023	2023.8.1
21 August 2023	2023.8
31 July 2023	2023.7
17 July 2023	2023.6.1
26 June 2023	2023.6
12 June 2023	2023.5.1
25 May 2023	2023.5.0
15 May 2023	2023.4.1
24 April 2023	2023.4.0
10 April 2023	2023.3.1
27 March 2023	2023.3
13 March 2023	2023.2.1
27 February 2023	2023.2
07 February 2023	2023.1.1
30 January 2023	2023.1

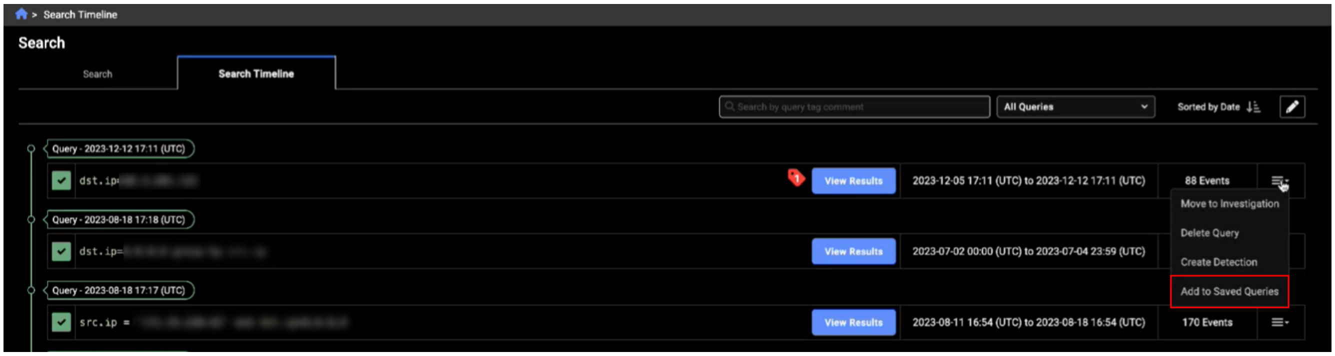
13 December 2023 Version 2023.12.0

- New Functionality
  - Search Timeline
- Improved functionality
  - Management Rules page
  - Entity panel
  - Query History
- Resolved Issues

New Functionality

Search Timeline

You can now save a query from the *Search Timeline* page. To save the query, click the *Actions* menu and select *Add to Saved Queries*.



Query - 2023-12-12 17:11 (UTC)
dst.ip[redacted] 2023-12-05 17:11 (UTC) to 2023-12-12 17:11 (UTC) 88 Events

Query - 2023-08-18 17:18 (UTC)
dst.ip=[redacted] 2023-07-02 00:00 (UTC) to 2023-07-04 23:59 (UTC)

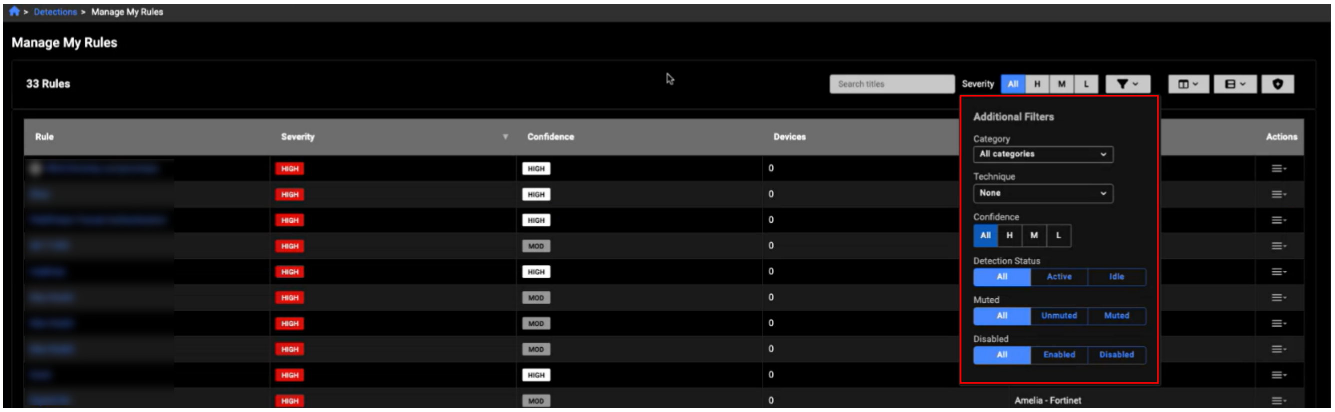
Query - 2023-08-18 17:17 (UTC)
src.ip = [redacted] 2023-08-11 16:54 (UTC) to 2023-08-18 16:54 (UTC) 170 Events

Improved functionality

Management Rules page

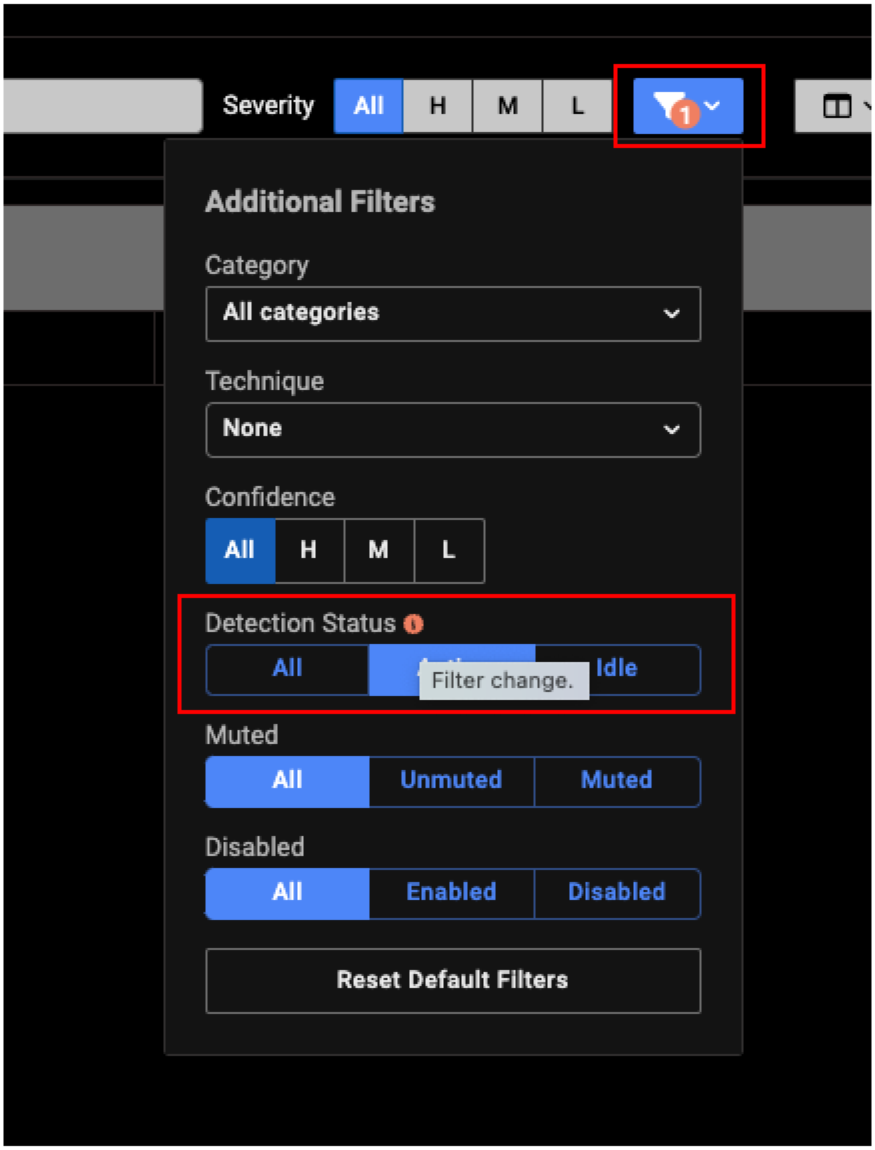
When you edit a rule you are returned to the *Manage My Rules* page after you click *Cancel* or *Save Rule*. In previous versions, you remained on the rule page after saving or canceling your edits.

The *Additional Filters* menu now defaults to *All* for *Detection Status*, *Muted* and *Disabled*. This allows you to see all the rules at a glance.



Rule	Severity	Confidence	Devices		Actions
[redacted]	HIGH	HIGH	0		
[redacted]	HIGH	HIGH	0		
[redacted]	HIGH	HIGH	0		
[redacted]	HIGH	MOD	0		
[redacted]	HIGH	HIGH	0		
[redacted]	HIGH	MOD	0		
[redacted]	HIGH	MOD	0		
[redacted]	HIGH	MOD	0		
[redacted]	HIGH	HIGH	0		
[redacted]	HIGH	MOD	0	Amelia - Fortinet	

The filters also persist until you refresh the page (except for the *Search* title). An indicator has been added to the filters when you change a filter from the default. A number indicates the number of changes that were applied. A *Reset to Default* was also added to the filter panel.



Severity: All | H | M | L

Additional Filters

Category: All categories

Technique: None

Confidence: All | H | M | L

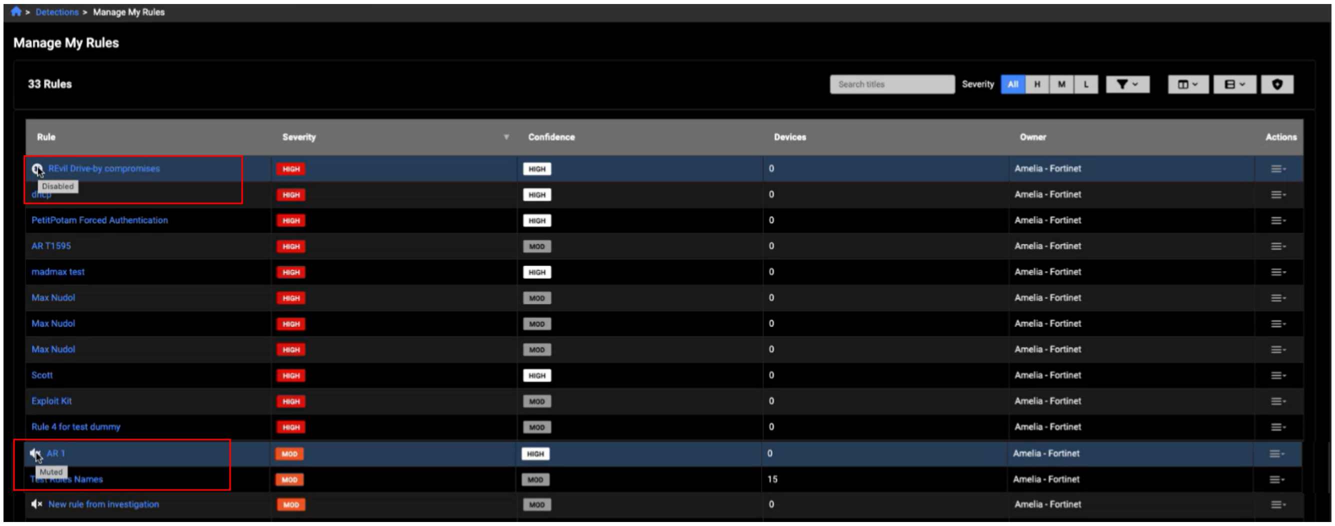
Detection Status: All | Filter change. | Idle

Muted: All | Unmuted | Muted

Disabled: All | Enabled | Disabled

Reset Default Filters

A *Muted* and *Disabled* icon has been added to the *Rules* column. This helps distinguish muted and disabled rules When the filter is set to *All*.



Detections > Manage My Rules

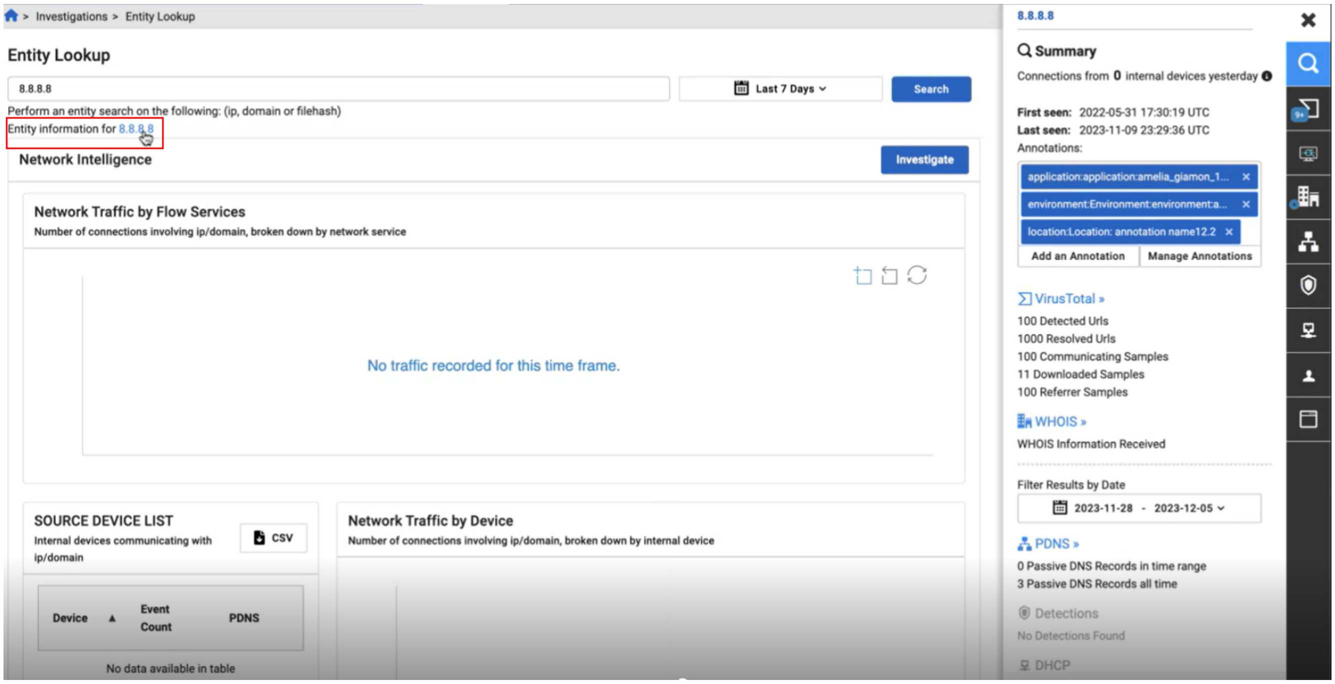
Manage My Rules

33 Rules

Rule	Severity	Confidence	Devices	Owner	Actions
REvil Drive-by compromises	HIGH	HIGH	0	Amelia - Fortinet	≡
dhcp	HIGH	HIGH	0	Amelia - Fortinet	≡
PetitPotam Forced Authentication	HIGH	HIGH	0	Amelia - Fortinet	≡
AR T1595	HIGH	MOD	0	Amelia - Fortinet	≡
madmax test	HIGH	HIGH	0	Amelia - Fortinet	≡
Max Nudol	HIGH	MOD	0	Amelia - Fortinet	≡
Max Nudol	HIGH	MOD	0	Amelia - Fortinet	≡
Max Nudol	HIGH	MOD	0	Amelia - Fortinet	≡
Scott	HIGH	HIGH	0	Amelia - Fortinet	≡
Exploit Kit	HIGH	MOD	0	Amelia - Fortinet	≡
Rule 4 for test dummy	HIGH	MOD	0	Amelia - Fortinet	≡
AR 1	MOD	HIGH	0	Amelia - Fortinet	≡
Test Rules Names	MOD	MOD	15	Amelia - Fortinet	≡
New rule from investigation	MOD	MOD	0	Amelia - Fortinet	≡

Entity panel

There is now a shortcut from the *Entity Lookup* page to the *Entity Panel*. This allows you to view information in the panel that is not in the lookup page.



Investigations > Entity Lookup

Entity Lookup

8.8.8.8

Last 7 Days

Search

Perform an entity search on the following: (ip, domain or filehash)

Entity information for 8.8.8.8

Network Intelligence

Investigate

Network Traffic by Flow Services

Number of connections involving ip/domain, broken down by network service

No traffic recorded for this time frame.

SOURCE DEVICE LIST

Internal devices communicating with ip/domain

CSV

Device	Event Count	PDNS
No data available in table		

Network Traffic by Device

Number of connections involving ip/domain, broken down by internal device

8.8.8.8

Summary

Connections from **0** internal devices yesterday

First seen: 2022-05-31 17:30:19 UTC

Last seen: 2023-11-09 23:29:36 UTC

Annotations:

- application:application:amelia_giamon_1...
- environment:Environment:environment:a...
- location:Location: annotation name12.2

Add an Annotation

Manage Annotations

VirusTotal »

100 Detected Urls
1000 Resolved Urls
100 Communicating Samples
11 Downloaded Samples
100 Referrer Samples

WHOIS »

WHOIS Information Received

Filter Results by Date

2023-11-28 - 2023-12-05

PDNS »

0 Passive DNS Records in time range
3 Passive DNS Records all time

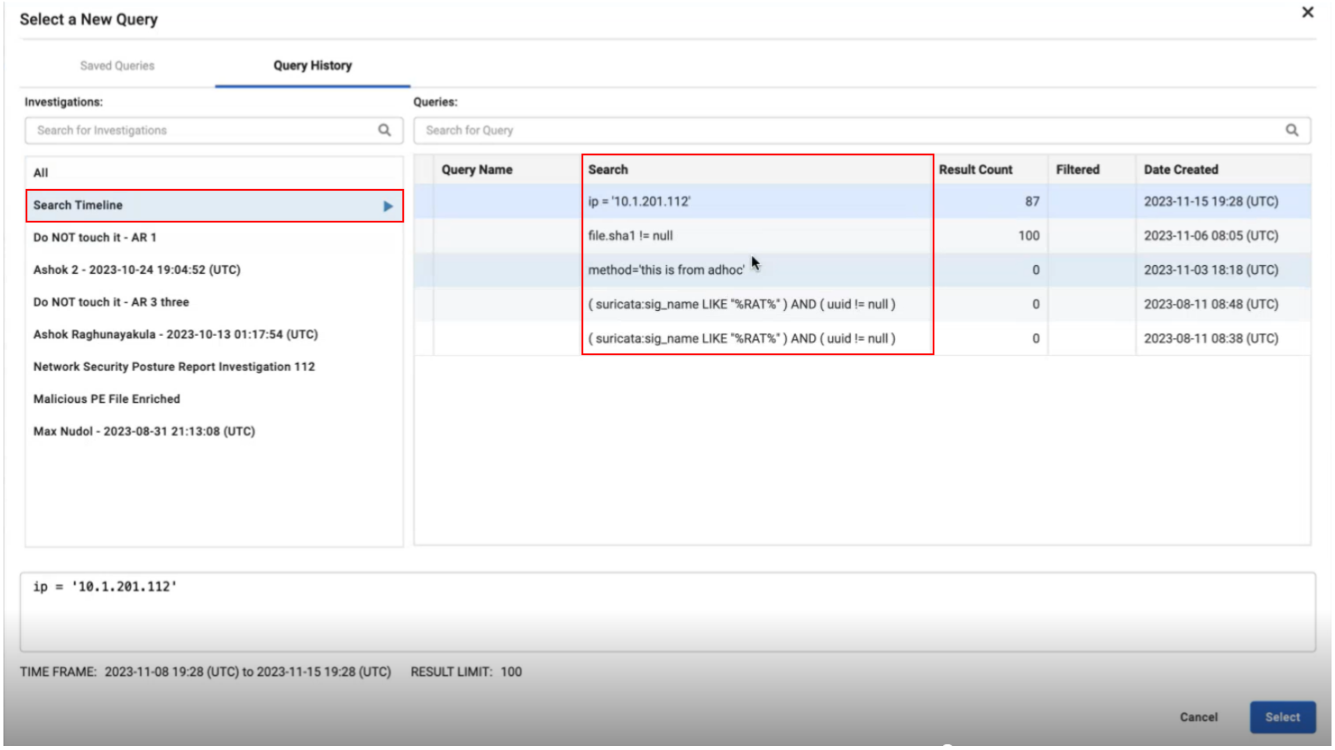
Detections

No Detections Found

DHCP

Query History

A new *Search Timeline* section was added to the *Query History* tab allowing you to view adhoc queries without a filter.



Select a New Query

Investigations:

- All
- Search Timeline
- Do NOT touch it - AR 1
- Ashok 2 - 2023-10-24 19:04:52 (UTC)
- Do NOT touch it - AR 3 three
- Ashok Raghunayakula - 2023-10-13 01:17:54 (UTC)
- Network Security Posture Report Investigation 112
- Malicious PE File Enriched
- Max Nudol - 2023-08-31 21:13:08 (UTC)

Queries:

Query Name	Search	Result Count	Filtered	Date Created
	ip = '10.1.201.112'	87		2023-11-15 19:28 (UTC)
	file.sha1 != null	100		2023-11-06 08:05 (UTC)
	method='this is from adhoc'	0		2023-11-03 18:18 (UTC)
	(suricata:sig_name LIKE "%RAT%") AND (uuid != null)	0		2023-08-11 08:48 (UTC)
	(suricata:sig_name LIKE "%RAT%") AND (uuid != null)	0		2023-08-11 08:38 (UTC)

```
ip = '10.1.201.112'
```

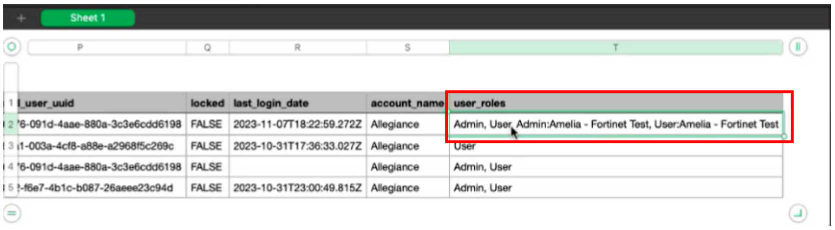
TIME FRAME: 2023-11-08 19:28 (UTC) to 2023-11-15 19:28 (UTC) RESULT LIMIT: 100

15 November 2023 Version 2023.11.0

New functionality

User management

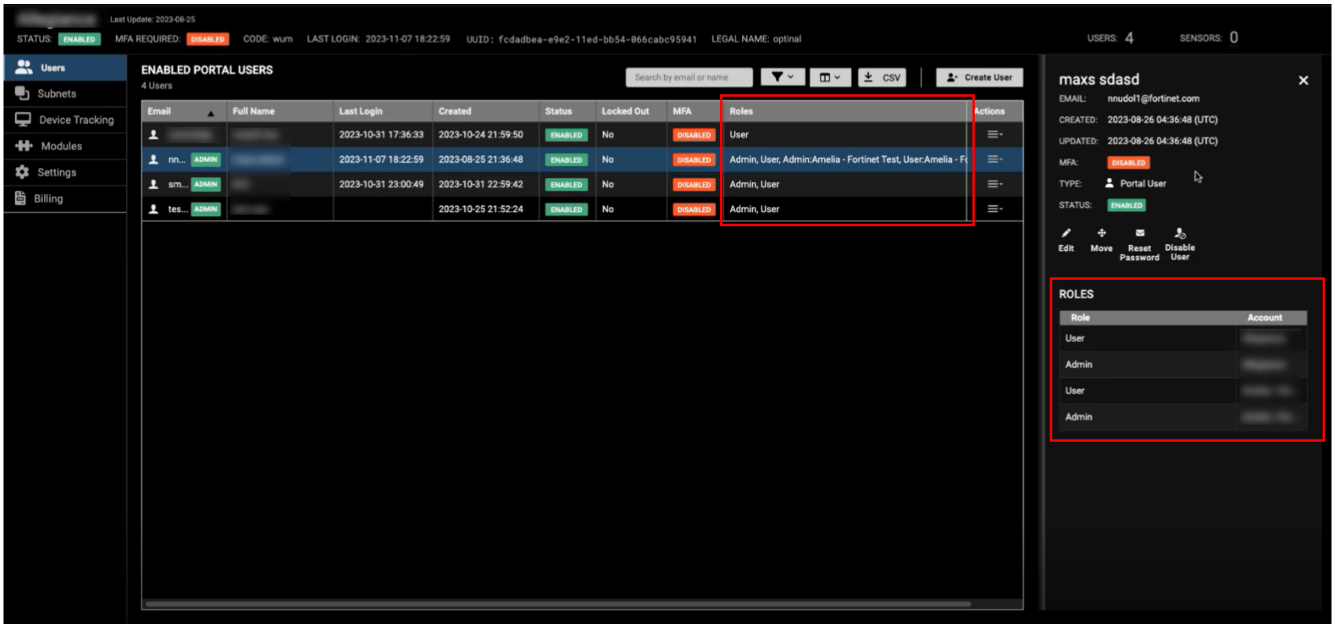
We have reduced the amount of information in the CSV export making it easier to navigate in the file and find the information are looking for. Much of this information has been consolidated into the *user_role* column. If there is no account name in front of the role, this indicates the user belongs to the current account (*Admin*, *User*, *Limited User*). If the user has the same roles in two or more accounts, the account name is displayed followed by a colon (:) followed by the user role.



Sheet 1

	P	Q	R	S	T
1	l_user_uuid	locked	last_login_date	account_name	user_roles
2	'6-091d-4aae-880a-3c3e6cdd6198	FALSE	2023-11-07T18:22:59.272Z	Allegiance	Admin, User, Admin:Amelia - Fortinet Test, User:Amelia - Fortinet Test
3	ı1-003a-4cf8-a88e-a2968f5c269c	FALSE	2023-10-31T17:36:33.027Z	Allegiance	User
4	'6-091d-4aae-880a-3c3e6cdd6198	FALSE		Allegiance	Admin, User
5	?-f6e7-4b1c-b087-26aeee23c94d	FALSE	2023-10-31T23:00:49.815Z	Allegiance	Admin, User

A new *Roles* column has been added to the *Users* page. When you can click the row the *User Details* pane displays all the roles and accounts assigned to the user.



[redacted] Last Update: 2023-08-25

STATUS: ENABLED MFA REQUIRED: DISABLED CODE: wum LAST LOGIN: 2023-11-07 18:22:59 UUID: fcdadbea-e9e2-11ed-bb54-066cabc95941 LEGAL NAME: optinal USERS: 4 SENSORS: 0

ENABLED PORTAL USERS
4 Users

Email	Full Name	Last Login	Created	Status	Locked Out	MFA	Roles	Actions
[redacted]	[redacted]	2023-10-31 17:36:33	2023-10-24 21:59:50	ENABLED	No	DISABLED	User	
nn... ADMIN	[redacted]	2023-11-07 18:22:59	2023-08-25 21:36:48	ENABLED	No	DISABLED	Admin, User, Admin:Amelia - Fortinet Test, User:Amelia - Fc	
sm... ADMIN	[redacted]	2023-10-31 23:00:49	2023-10-31 22:59:42	ENABLED	No	DISABLED	Admin, User	
tes... ADMIN	[redacted]		2023-10-25 21:52:24	ENABLED	No	DISABLED	Admin, User	

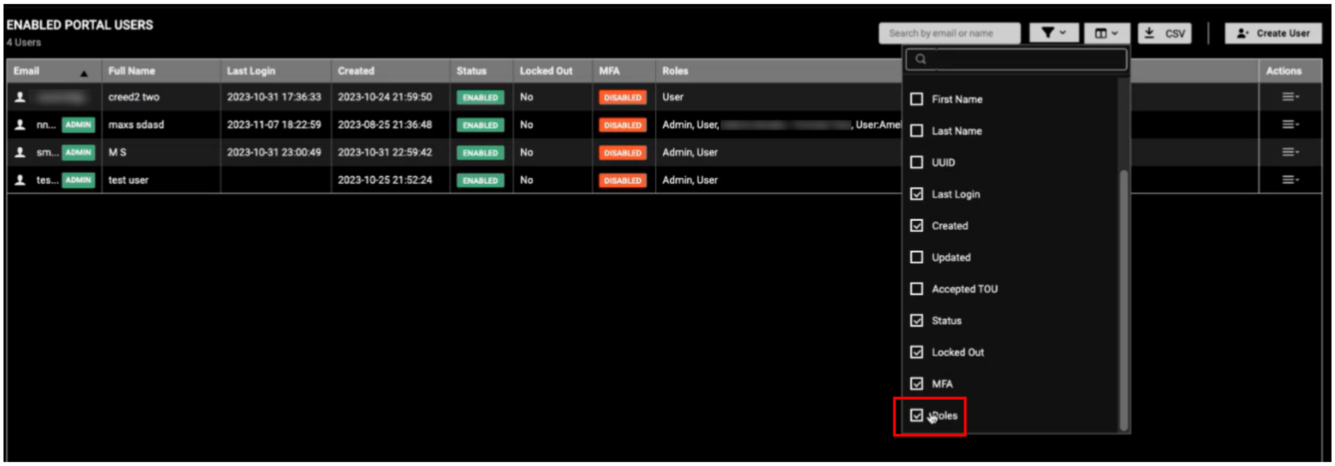
maxs sdasd

EMAIL: nnudol1@fortinet.com
CREATED: 2023-08-26 04:36:48 (UTC)
UPDATED: 2023-08-26 04:36:48 (UTC)
MFA: DISABLED
TYPE: Portal User
STATUS: ENABLED

ROLES

Role	Account
User	[redacted]
Admin	[redacted]
User	[redacted]
Admin	[redacted]

If you do not see the *Roles* column by default, you can add it manually.

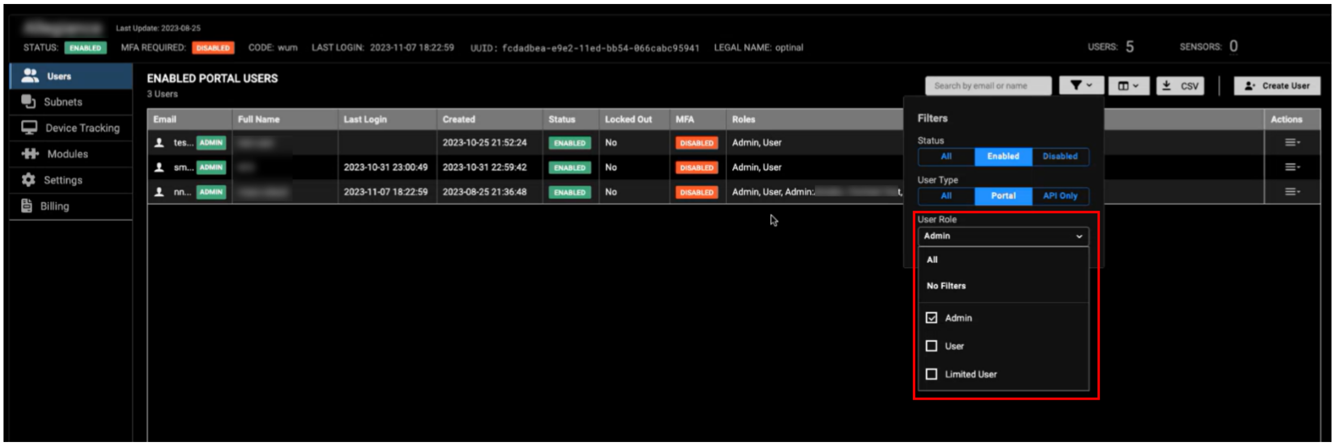


ENABLED PORTAL USERS
4 Users

Email	Full Name	Last Login	Created	Status	Locked Out	MFA	Roles	Actions
[redacted]	creed2 two	2023-10-31 17:36:33	2023-10-24 21:59:50	ENABLED	No	DISABLED	User	
nn... ADMIN	maxs sdasd	2023-11-07 18:22:59	2023-08-25 21:36:48	ENABLED	No	DISABLED	Admin, User, [redacted], User:Ame	
sm... ADMIN	M S	2023-10-31 23:00:49	2023-10-31 22:59:42	ENABLED	No	DISABLED	Admin, User	
tes... ADMIN	test user		2023-10-25 21:52:24	ENABLED	No	DISABLED	Admin, User	

- □ First Name
- □ Last Name
- □ UUID
- ☑ Last Login
- ☑ Created
- □ Updated
- □ Accepted TOU
- ☑ Status
- ☑ Locked Out
- ☑ MFA
- ☑ Roles

You can also filter the column by the user role.



[redacted] Last Update: 2023-08-25

STATUS: ENABLED MFA REQUIRED: DISABLED CODE: wum LAST LOGIN: 2023-11-07 18:22:59 UUID: fcdadbea-e9e2-11ed-bb54-066cabc95941 LEGAL NAME: optinal USERS: 5 SENSORS: 0

ENABLED PORTAL USERS

3 Users

Email	Full Name	Last Login	Created	Status	Locked Out	MFA	Roles
tes... ADMIN	[redacted]		2023-10-25 21:52:24	ENABLED	No	DISABLED	Admin, User
sm... ADMIN	[redacted]	2023-10-31 23:00:49	2023-10-31 22:59:42	ENABLED	No	DISABLED	Admin, User
nn... ADMIN	[redacted]	2023-11-07 18:22:59	2023-08-25 21:36:48	ENABLED	No	DISABLED	Admin, User, Admin: [redacted] t,

Filters

Status: All [✓ Enabled] Disabled

User Type: All [✓ Portal] API Only

User Role: Admin

- All
- No Filters
- ☑ Admin
- ☐ User
- ☐ Limited User

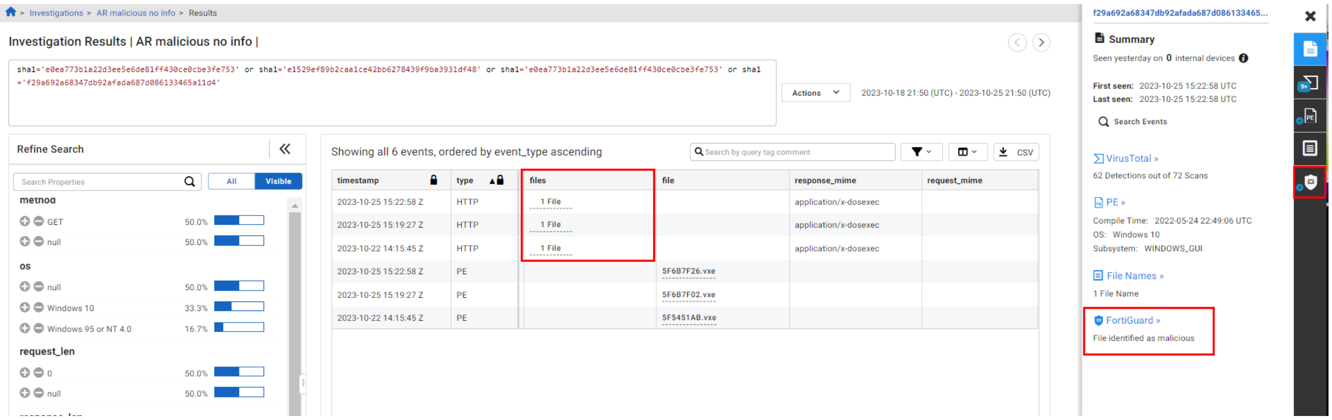
Entity Panel: FortiGuard

The *Entity Panel* now displays information about the malicious files when it is available.

To view malicious file attributes in the Entity Panel:

1. Go to *Investigations* > *Investigate*.
2. Click an investigation in the list and then click *View Results*.
3. Navigate to the *files* column and click the file link.

When a malicious file is detected, you will see the *FortiGuard* section heading in the Entity Panel with the message *File identified as malicious*.



Investigations > AR malicious no info > Results

Investigation Results | AR malicious no info |

```
sha1='e0ea773b1a22d3ee5e6de81ff430ce0cbe3fe753' or sha1='e1529ef89b2caa1ce42bb6278439f9ba3931df48' or sha1='e0ea773b1a22d3ee5e6de81ff430ce0cbe3fe753' or sha1
='f29a692a68347db92afada687d086133465a11d4'
```

2023-10-18 21:50 (UTC) - 2023-10-25 21:50 (UTC)

Refine Search

metnod

- GET 50.0%
- null 50.0%

os

- null 50.0%
- Windows 10 33.3%
- Windows 95 or NT 4.0 16.7%

request_len

- 0 50.0%
- null 50.0%

Showing all 6 events, ordered by event_type ascending

timestamp	type	files	file	response_mime	request_mime
2023-10-25 15:22:58 Z	HTTP	1 File		application/x-dosexec	
2023-10-25 15:19:27 Z	HTTP	1 File		application/x-dosexec	
2023-10-22 14:15:45 Z	HTTP	1 File		application/x-dosexec	
2023-10-25 15:22:58 Z	PE		5F6B7F26.vxe		
2023-10-25 15:19:27 Z	PE		5F6B7F02.vxe		
2023-10-22 14:15:45 Z	PE		5F5451AB.vxe		

f29a692a68347db92afada687d086133465...

Summary

Seen yesterday on 0 internal devices

First seen: 2023-10-25 15:22:58 UTC
Last seen: 2023-10-25 15:22:58 UTC

VirusTotal »

62 Detections out of 72 Scans

PE »

Compile Time: 2022-05-24 22:49:06 UTC
OS: Windows 10
Subsystem: WINDOWS_GUI

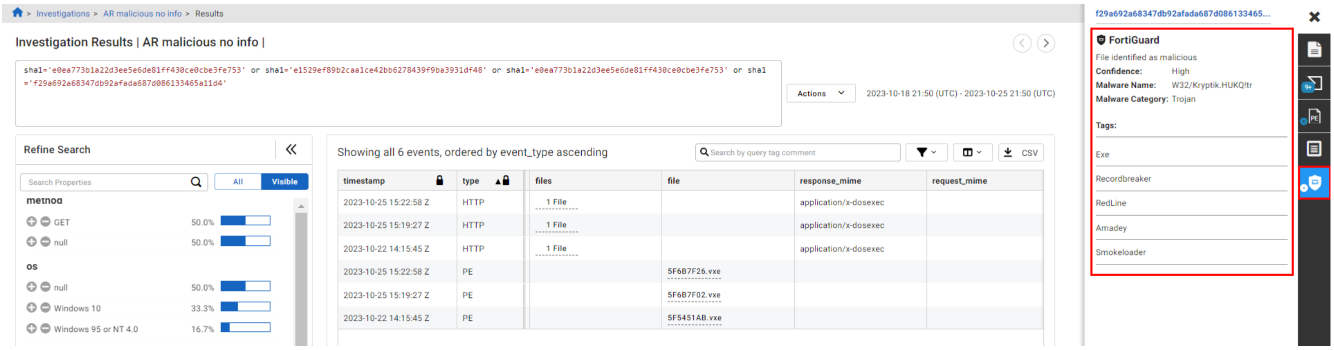
File Names »

1 File Name

FortiGuard »

File identified as malicious

Click the section header or the FortiGuard icon to view the attributes about the malicious file. If the attributes are not available, then none are displayed.


Investigations > AR malicious no info > Results
Investigation Results | AR malicious no info |
Actions
Refine Search
Search Properties
All
Visible
Search by query tag comment
CSV
f29a692a68347db92afada687d086133465...

```
sha1='e0ea773b1a22d3ee5e6de81ff430ce0cbe3fe753' or sha1='e1529ef89b2caa1ce42bb6278439f9ba3931df48' or sha1='e0ea773b1a22d3ee5e6de81ff430ce0cbe3fe753' or sha1
='f29a692a68347db92afada687d086133465a11d4'
```

2023-10-18 21:50 (UTC) - 2023-10-25 21:50 (UTC)

metnod	
GET	50.0%
null	50.0%
os	
null	50.0%
Windows 10	33.3%
Windows 95 or NT 4.0	16.7%

Showing all 6 events, ordered by event_type ascending

timestamp	type	files	file	response_mime	request_mime
2023-10-25 15:22:58 Z	HTTP	1 File		application/x-dosexec	
2023-10-25 15:19:27 Z	HTTP	1 File		application/x-dosexec	
2023-10-22 14:15:45 Z	HTTP	1 File		application/x-dosexec	
2023-10-25 15:22:58 Z	PE		5F6B7F26.vxe		
2023-10-25 15:19:27 Z	PE		5F6B7F02.vxe		
2023-10-22 14:15:45 Z	PE		5F5451AB.vxe		

FortiGuard

File identified as malicious

Confidence: High
Malware Name: W32/Kryptik.HUKQ!tr
Malware Category: Trojan

Tags:

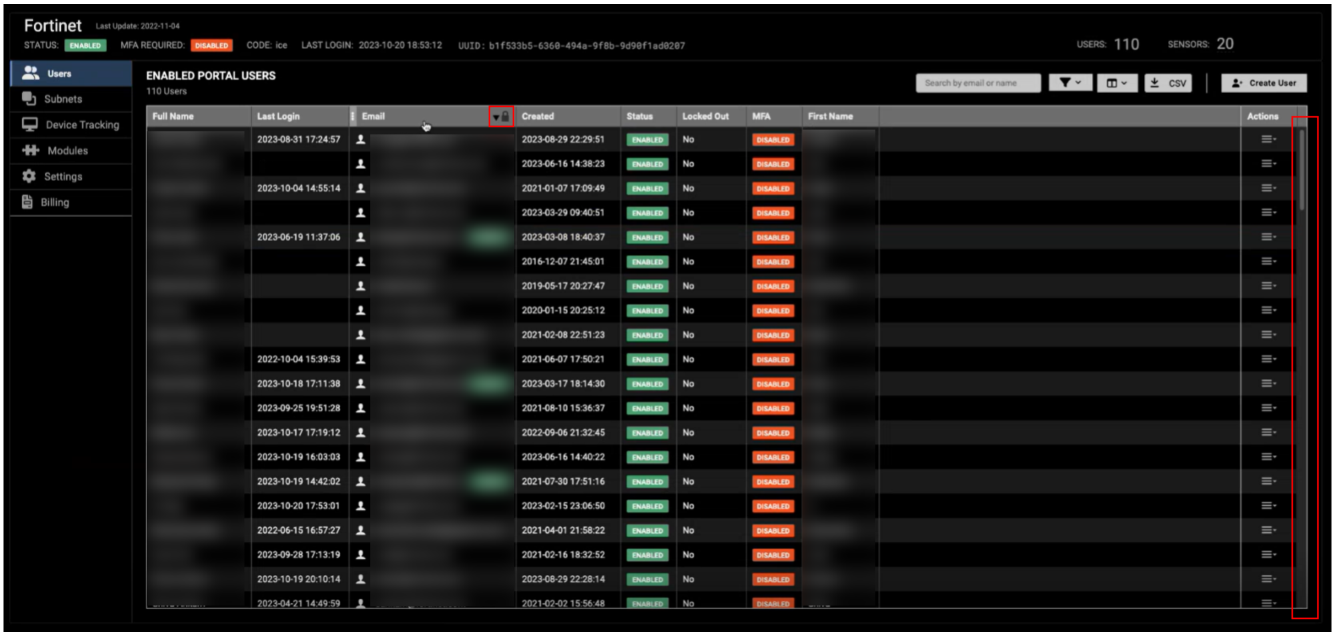
Exe
Recordbreaker
RedLine
Amadey
Smokeloader

25 October 2023 version 2023.1.0

New functionality

User management

The columns in the *User Management* table can now be locked, re-sized and rearranged. Any changes you make to the page layout are saved when you refresh the page. Pagination at the bottom of the page has been replaced with a scroll bar.

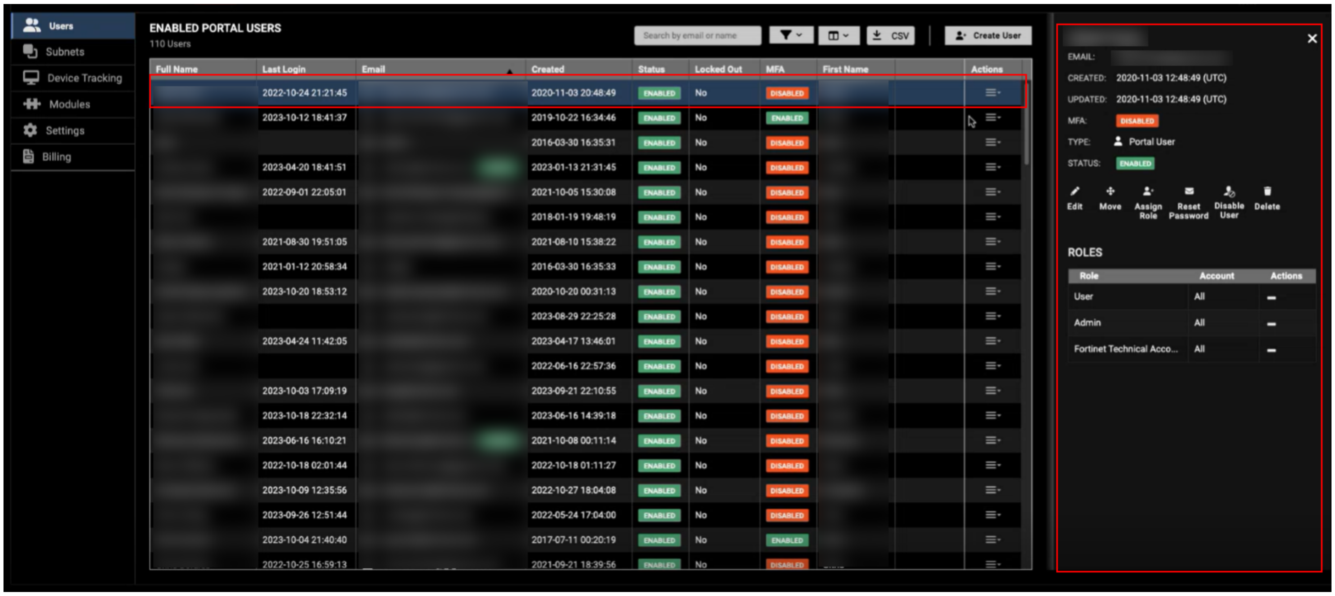


Last Update: 2022-11-04
STATUS: ENABLED MFA REQUIRED: DISABLED CODE: ice LAST LOGIN: 2023-10-20 18:53:12 UUID: b1f533b5-6360-494a-9f8b-9d90f1ad0207 USERS: 110 SENSORS: 20

ENABLED PORTAL USERS
110 Users

Full Name	Last Login	Email	Created	Status	Locked Out	MFA	First Name	Actions
[redacted]	2023-08-31 17:24:57	[redacted]	2023-08-29 22:29:51	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2023-06-16 14:38:23	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-04 14:55:14	[redacted]	2021-01-07 17:09:49	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2023-03-29 09:40:51	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-06-19 11:37:06	[redacted]	2023-03-08 18:40:37	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2016-12-07 21:45:01	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2019-05-17 20:27:47	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2020-01-15 20:25:12	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2021-02-08 22:51:23	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2022-10-04 15:39:53	[redacted]	2021-06-07 17:50:21	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-18 17:11:38	[redacted]	2023-03-17 18:14:30	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-09-25 19:51:28	[redacted]	2021-08-10 15:36:37	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-17 17:19:12	[redacted]	2022-09-06 21:32:45	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-19 16:03:03	[redacted]	2023-06-16 14:40:22	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-19 14:42:02	[redacted]	2021-07-30 17:51:16	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-20 17:53:01	[redacted]	2023-02-15 23:06:50	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2022-06-15 16:57:27	[redacted]	2021-04-01 21:58:22	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-09-28 17:13:19	[redacted]	2021-02-16 18:32:52	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-19 20:10:14	[redacted]	2023-08-29 22:28:14	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-04-21 14:49:59	[redacted]	2021-02-02 15:56:48	ENABLED	No	DISABLED	[redacted]	≡

When a user is selected, the table width adjusts to accommodate the user profile pane so there is no overlap. The user is highlighted in blue until you close the pane.



ENABLED PORTAL USERS
110 Users

Full Name	Last Login	Email	Created	Status	Locked Out	MFA	First Name	Actions
[redacted]	2022-10-24 21:21:45	[redacted]	2020-11-03 20:48:49	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-12 18:41:37	[redacted]	2019-10-22 16:34:46	ENABLED	No	ENABLED	[redacted]	≡
[redacted]		[redacted]	2016-03-30 16:35:31	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-04-20 18:41:51	[redacted]	2023-01-13 21:31:45	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2022-09-01 22:05:01	[redacted]	2021-10-05 15:30:08	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2018-01-19 19:48:19	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2021-08-30 19:51:05	[redacted]	2021-08-10 15:38:22	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2021-01-12 20:58:34	[redacted]	2016-03-30 16:35:33	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-20 18:53:12	[redacted]	2020-10-20 00:31:13	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2023-08-29 22:25:28	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-04-24 11:42:05	[redacted]	2023-04-17 13:46:01	ENABLED	No	DISABLED	[redacted]	≡
[redacted]		[redacted]	2022-06-16 22:57:36	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-03 17:09:19	[redacted]	2023-09-21 22:10:55	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-18 22:32:14	[redacted]	2023-06-16 14:39:18	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-06-16 16:10:21	[redacted]	2021-10-08 00:11:14	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2022-10-18 02:01:44	[redacted]	2022-10-18 01:11:27	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-09 12:35:56	[redacted]	2022-10-27 18:04:08	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-09-26 12:51:44	[redacted]	2022-05-24 17:04:00	ENABLED	No	DISABLED	[redacted]	≡
[redacted]	2023-10-04 21:40:40	[redacted]	2017-07-11 00:20:19	ENABLED	No	ENABLED	[redacted]	≡
[redacted]	2022-10-25 16:59:13	[redacted]	2021-09-21 18:39:56	ENABLED	No	DISABLED	[redacted]	≡

[redacted]
EMAIL: [redacted]
CREATED: 2020-11-03 12:48:49 (UTC)
UPDATED: 2020-11-03 12:48:49 (UTC)
MFA: DISABLED
TYPE: Portal User
STATUS: ENABLED

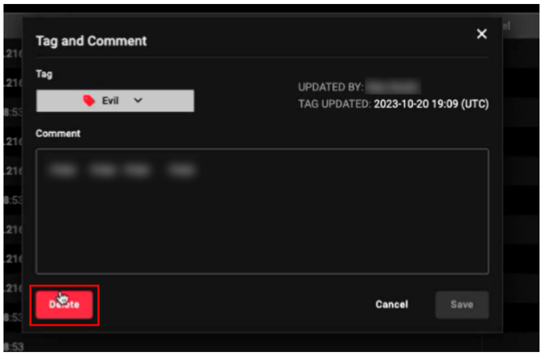
ROLES

Role	Account	Actions
User	All	—
Admin	All	—
Fortinet Technical Acco...	All	—

Improved functionality

Deleting tags

The method for deleting tags has been improved. To delete a tag, open the item and click *Delete*. The tag and any comments will be removed.



Tag and Comment

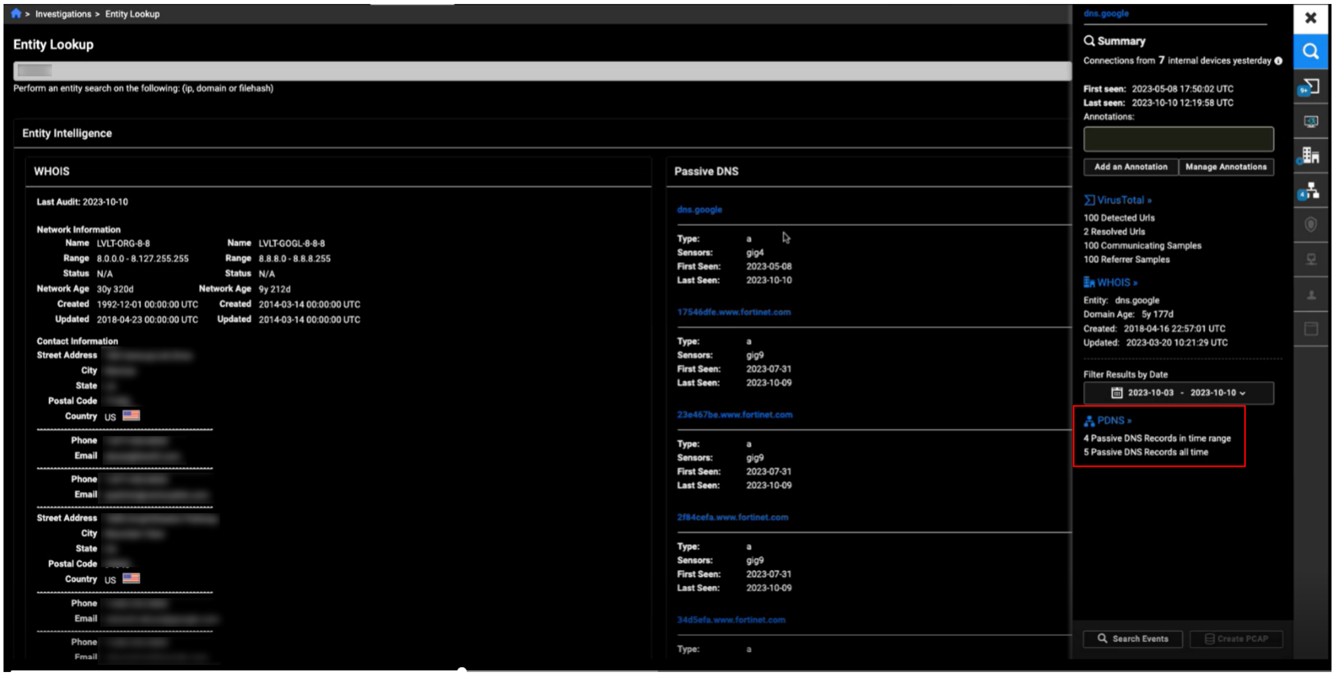
Tag: Evil

UPDATED BY: [redacted]
TAG UPDATED: 2023-10-20 19:09 (UTC)

Comment: [redacted]

Entity Panel: PDNS

The *PDNS* tab in the in the *Entity Panel* contains more information. Two sets of data are displayed: the *DNS record in the time range* and *Passive DNS record all time*.



Perform an entity search on the following: (ip, domain or filehash)

Entity Intelligence

WHOIS

Last Audit: 2023-10-10

Network Information

Name	LVLT-ORG-8-8	Name	LVLT-GOGL-8-8-8
Range	8.0.0.0 - 8.127.255.255	Range	8.8.8.0 - 8.8.8.255
Status	N/A	Status	N/A
Network Age	30y 320d	Network Age	9y 212d
Created	1992-12-01 00:00:00 UTC	Created	2014-03-14 00:00:00 UTC
Updated	2018-04-23 00:00:00 UTC	Updated	2014-03-14 00:00:00 UTC

Contact Information
Street Address [redacted]
City [redacted]
State [redacted]
Postal Code [redacted]
Country US

Phone [redacted]
Email [redacted]

Phone [redacted]
Email [redacted]

Street Address [redacted]
City [redacted]
State [redacted]
Postal Code [redacted]
Country US

Phone [redacted]
Email [redacted]

Phone [redacted]
Email [redacted]

Passive DNS

dns.google
Type: a
Sensors: gig4
First Seen: 2023-05-08
Last Seen: 2023-10-10

17546dfe.www.fortinet.com
Type: a
Sensors: gig9
First Seen: 2023-07-31
Last Seen: 2023-10-09

23e467be.www.fortinet.com
Type: a
Sensors: gig9
First Seen: 2023-07-31
Last Seen: 2023-10-09

2f84cefa.www.fortinet.com
Type: a
Sensors: gig9
First Seen: 2023-07-31
Last Seen: 2023-10-09

34d5efa.www.fortinet.com
Type: a

dns.google

Summary
Connections from 7 internal devices yesterday

First seen: 2023-05-08 17:50:02 UTC
Last seen: 2023-10-10 12:19:58 UTC
Annotations:

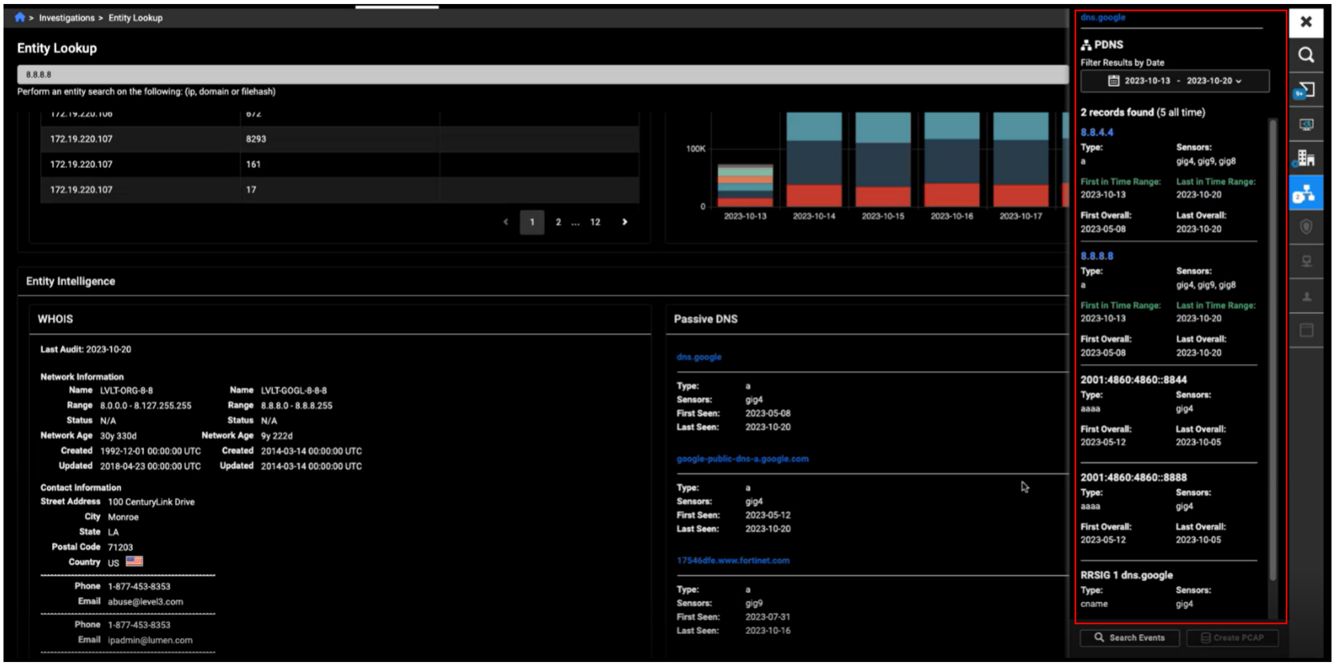
VirusTotal »
100 Detected Urls
2 Resolved Urls
100 Communicating Samples
100 Referrer Samples

WHOIS »
Entity: dns.google
Domain Age: 5y 177d
Created: 2018-04-16 22:57:01 UTC
Updated: 2023-03-20 10:21:29 UTC

Filter Results by Date
2023-10-03 - 2023-10-10

PDNS »
4 Passive DNS Records in time range
5 Passive DNS Records all time

The records are displayed in the order they were last seen. The records within the time range appear at the top of the list. Records within the time range are highlighted by *First in Time Range* and *Last in Time Range*.



Entity Lookup

8.8.8.8

Perform an entity search on the following: (ip, domain or filehash)

172.19.220.106	872
172.19.220.107	8293
172.19.220.107	161
172.19.220.107	17

‹ 1 2 ... 12 ›

Entity Intelligence

WHOIS

Last Audit: 2023-10-20

Network Information

Name	LVLT-ORG-8-8	Name	LVLT-GOGL-8-8-8
Range	8.0.0.0 - 8.127.255.255	Range	8.8.8.0 - 8.8.8.255
Status	N/A	Status	N/A
Network Age	30y 330d	Network Age	9y 222d
Created	1992-12-01 00:00:00 UTC	Created	2014-03-14 00:00:00 UTC
Updated	2018-04-23 00:00:00 UTC	Updated	2014-03-14 00:00:00 UTC

Contact Information

Street Address 100 CenturyLink Drive
City Monroe
State LA
Postal Code 71203
Country US

Phone 1-877-453-8353
Email abuse@level3.com

Phone 1-877-453-8353
Email ipadmin@lumen.com

Passive DNS

dns.google

Type: a
Sensors: gig4
First Seen: 2023-05-08
Last Seen: 2023-10-20

google-public-dns-a.google.com

Type: a
Sensors: gig4
First Seen: 2023-05-12
Last Seen: 2023-10-20

17546dfe.www.fortinet.com

Type: a
Sensors: gig9
First Seen: 2023-07-31
Last Seen: 2023-10-16

dns.google

PDNS

Filter Results by Date

2023-10-13 - 2023-10-20

2 records found (5 all time)

8.8.4.4
Type: a
Sensors: gig4, gig9, gig8
First in Time Range: 2023-10-13
Last in Time Range: 2023-10-20
First Overall: 2023-05-08
Last Overall: 2023-10-20

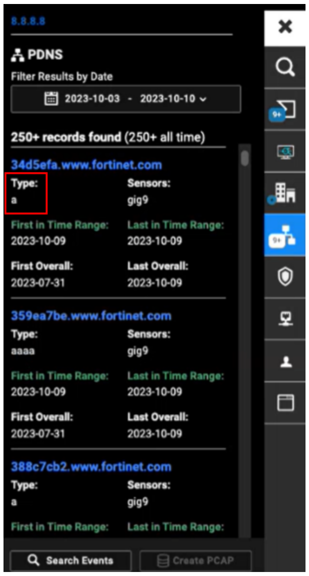
8.8.8.8
Type: a
Sensors: gig4, gig9, gig8
First in Time Range: 2023-10-13
Last in Time Range: 2023-10-20
First Overall: 2023-05-08
Last Overall: 2023-10-20

2001:4860:4860::8844
Type: aaaa
Sensors: gig4
First Overall: 2023-05-12
Last Overall: 2023-10-05

2001:4860:4860::8888
Type: aaaa
Sensors: gig4
First Overall: 2023-05-12
Last Overall: 2023-10-05

RRSIG 1 dns.google
Type: cname
Sensors: gig4

The *Type* field indicates if the DNS type such as IPv4 (*a*) or IPv6 (*aaaa*).



8.8.8.8

PDNS

Filter Results by Date

2023-10-03 - 2023-10-10

250+ records found (250+ all time)

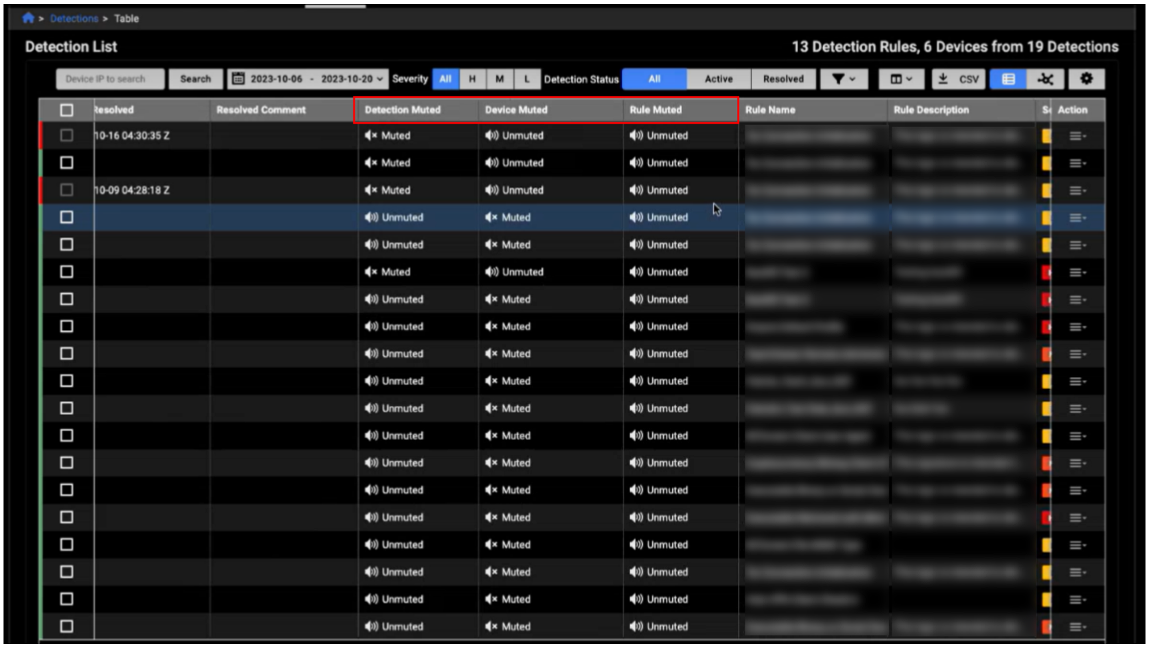
34d5efa.www.fortinet.com
Type: a
Sensors: gig9
First in Time Range: 2023-10-09
Last in Time Range: 2023-10-09
First Overall: 2023-07-31
Last Overall: 2023-10-09

359ea7be.www.fortinet.com
Type: aaaa
Sensors: gig9
First in Time Range: 2023-10-09
Last in Time Range: 2023-10-09
First Overall: 2023-07-31
Last Overall: 2023-10-09

388c7cb2.www.fortinet.com
Type: a
Sensors: gig9
First in Time Range:
Last in Time Range:

Detections table: Muting

Two new columns were added to the Detections Table. The *Detections Muted* and *Device Muted* work with the *Rule Muted* column to accommodate changes to the muting filter.



Detections > Table

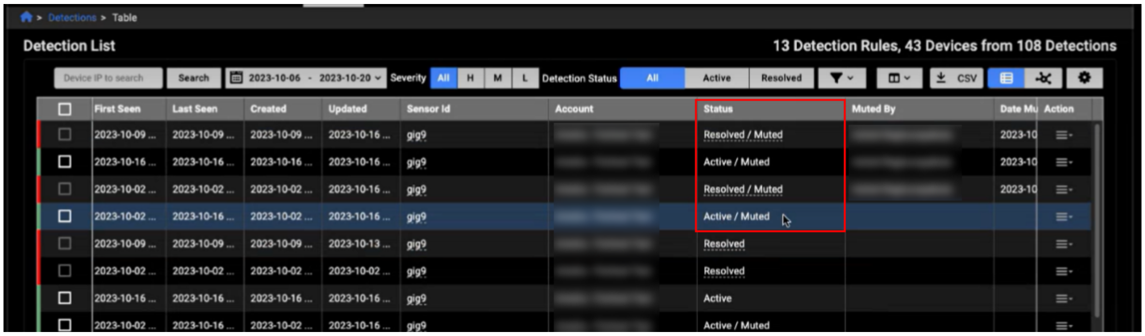
Detection List

13 Detection Rules, 6 Devices from 19 Detections

Device IP to search | Search | 2023-10-06 - 2023-10-20 | Severity: All H M L | Detection Status: All Active Resolved | CSV

□	Resolved	Resolved Comment	Detection Muted	Device Muted	Rule Muted	Rule Name	Rule Description	S	Action
□	10-16 04:30:35 Z		Muted	Unmuted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Muted	Unmuted	Unmuted	[redacted]	[redacted]	🟨	≡
□	10-09 04:28:18 Z		Muted	Unmuted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Muted	Unmuted	Unmuted	[redacted]	[redacted]	🟥	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟥	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟥	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟧	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟧	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟧	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟥	≡
□			Unmuted	Muted	Unmuted	[redacted]		🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]		🟨	≡
□			Unmuted	Muted	Unmuted	[redacted]	[redacted]	🟧	≡

Muted detections are now flagged with *Muted* in the *Status* column.



Detections > Table

Detection List

13 Detection Rules, 43 Devices from 108 Detections

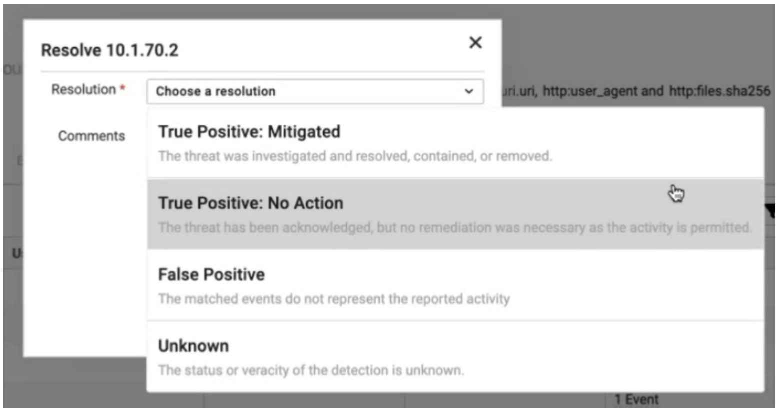
Device IP to search | Search | 2023-10-06 - 2023-10-20 | Severity: All H M L | Detection Status: All Active Resolved | CSV

□	First Seen	Last Seen	Created	Updated	Sensor Id	Account	Status	Muted By	Date Mu	Action
□	2023-10-09 ...	2023-10-09 ...	2023-10-09 ...	2023-10-16 ...	gig9	[redacted]	Resolved / Muted	[redacted]	2023-10	≡
□	2023-10-16 ...	2023-10-16 ...	2023-10-16 ...	2023-10-16 ...	gig9	[redacted]	Active / Muted	[redacted]	2023-10	≡
□	2023-10-02 ...	2023-10-02 ...	2023-10-02 ...	2023-10-16 ...	gig9	[redacted]	Resolved / Muted	[redacted]	2023-10	≡
□	2023-10-02 ...	2023-10-16 ...	2023-10-02 ...	2023-10-16 ...	gig9	[redacted]	Active / Muted			≡
□	2023-10-09 ...	2023-10-09 ...	2023-10-09 ...	2023-10-13 ...	gig9	[redacted]	Resolved			≡
□	2023-10-02 ...	2023-10-02 ...	2023-10-02 ...	2023-10-02 ...	gig9	[redacted]	Resolved			≡
□	2023-10-16 ...	2023-10-16 ...	2023-10-16 ...	2023-10-16 ...	gig9	[redacted]	Active			≡
□	2023-10-02 ...	2023-10-16 ...	2023-10-02 ...	2023-10-16 ...	gig9	[redacted]	Active / Muted			≡

Other enhancements

Resolution type

The definition of *True Positive: No Action* has been updated to *The threat has been acknowledged but no remediation was necessary as the act is permitted*.



Resolve 10.1.70.2

Resolution * Choose a resolution

Comments

True Positive: Mitigated
The threat was investigated and resolved, contained, or removed.

True Positive: No Action
The threat has been acknowledged, but no remediation was necessary as the activity is permitted.

False Positive
The matched events do not represent the reported activity

Unknown
The status or veracity of the detection is unknown.

6 October 2023 version 2023.9.1

FortiNDR Cloud 2023.9.1 includes bug fixes, but no new features. See Resolved Issues on page 50.

27 September 2023 version 2023.9

- New functionality
  - User roles
- Improved functionality
  - Search function
  - Entity Panel
  - Account management
  - Sensor versions
  - Other improvements

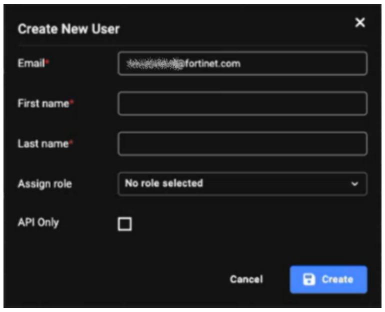
New functionality

User roles

You can now assign a user role or roles when you create new user, including *Admin*, *Training User*, and *User*.

New users are automatically assigned the Training User role on the Training Modern account, even if the administrator has not assigned any roles to the user. If the account is a parent account, and the administrator has access to child accounts, then a checkbox is available to include child accounts.

Required fields are identified with an asterisk.



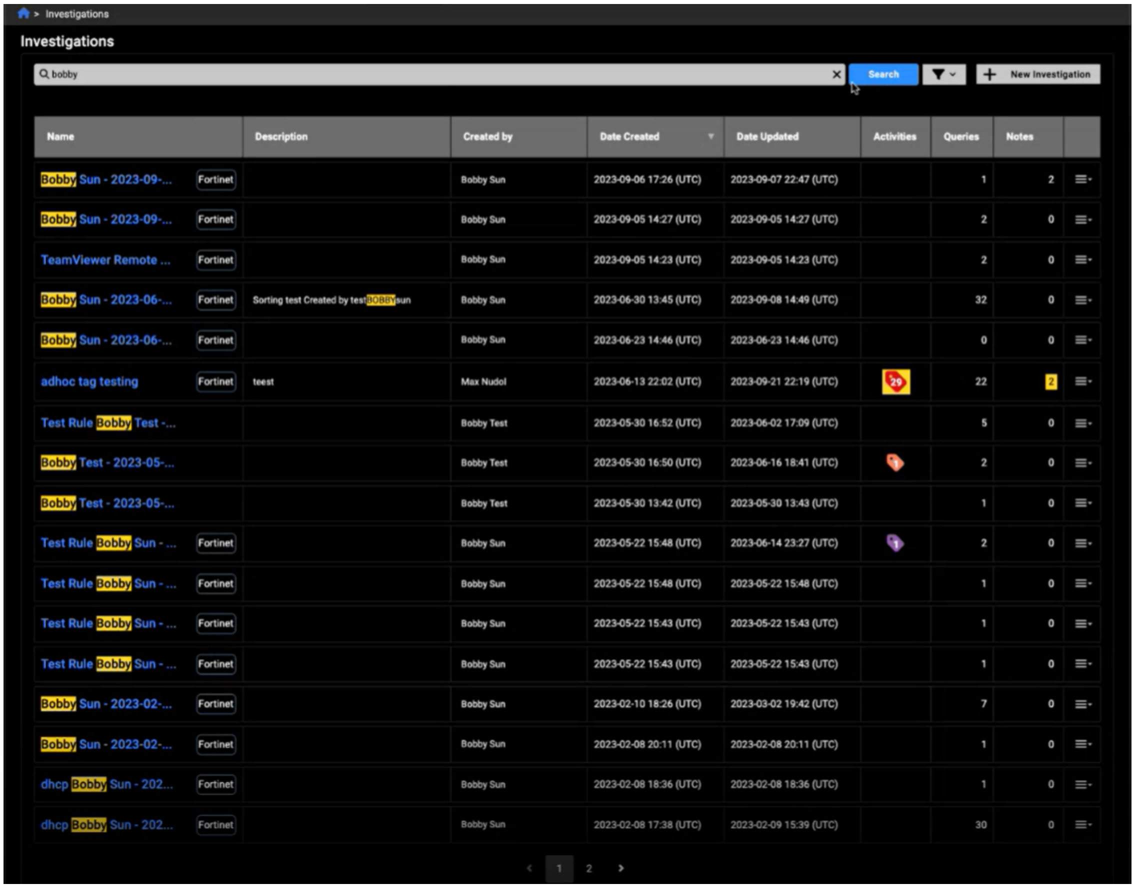
Create New User ✕

Email*	[redacted]fortinet.com
First name*	
Last name*	
Assign role	No role selected ⌄
API Only	□

Improved functionality

Search function

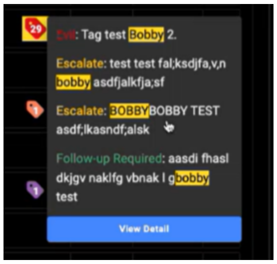
You can now use the search function in the Investigation list and details to search for text in comments and notes. Matching results are highlighted in yellow.



bobby

Name	Description	Created by	Date Created	Date Updated	Activities	Queries	Notes	
Bobby Sun - 2023-09-... Fortinet		Bobby Sun	2023-09-06 17:26 (UTC)	2023-09-07 22:47 (UTC)		1	2	≡
Bobby Sun - 2023-09-... Fortinet		Bobby Sun	2023-09-05 14:27 (UTC)	2023-09-05 14:27 (UTC)		2	0	≡
TeamViewer Remote ... Fortinet		Bobby Sun	2023-09-05 14:23 (UTC)	2023-09-05 14:23 (UTC)		2	0	≡
Bobby Sun - 2023-06-... Fortinet	Sorting test Created by testBOBBYsun	Bobby Sun	2023-06-30 13:45 (UTC)	2023-09-08 14:49 (UTC)		32	0	≡
Bobby Sun - 2023-06-... Fortinet		Bobby Sun	2023-06-23 14:46 (UTC)	2023-06-23 14:46 (UTC)		0	0	≡
adhoc tag testing Fortinet	teest	Max Nudol	2023-06-13 22:02 (UTC)	2023-09-21 22:19 (UTC)	29	22	2	≡
Test Rule Bobby Test -...		Bobby Test	2023-05-30 16:52 (UTC)	2023-06-02 17:09 (UTC)		5	0	≡
Bobby Test - 2023-05-...		Bobby Test	2023-05-30 16:50 (UTC)	2023-06-16 18:41 (UTC)	1	2	0	≡
Bobby Test - 2023-05-...		Bobby Test	2023-05-30 13:42 (UTC)	2023-05-30 13:43 (UTC)		1	0	≡
Test Rule Bobby Sun - ... Fortinet		Bobby Sun	2023-05-22 15:48 (UTC)	2023-06-14 23:27 (UTC)	1	2	0	≡
Test Rule Bobby Sun - ... Fortinet		Bobby Sun	2023-05-22 15:48 (UTC)	2023-05-22 15:48 (UTC)		1	0	≡
Test Rule Bobby Sun - ... Fortinet		Bobby Sun	2023-05-22 15:43 (UTC)	2023-05-22 15:43 (UTC)		1	0	≡
Test Rule Bobby Sun - ... Fortinet		Bobby Sun	2023-05-22 15:43 (UTC)	2023-05-22 15:43 (UTC)		1	0	≡
Bobby Sun - 2023-02-... Fortinet		Bobby Sun	2023-02-10 18:26 (UTC)	2023-03-02 19:42 (UTC)		7	0	≡
Bobby Sun - 2023-02-... Fortinet		Bobby Sun	2023-02-08 20:11 (UTC)	2023-02-08 20:11 (UTC)		1	0	≡
dhcp Bobby Sun - 202... Fortinet		Bobby Sun	2023-02-08 18:36 (UTC)	2023-02-08 18:36 (UTC)		1	0	≡
dhcp Bobby Sun - 202... Fortinet		Bobby Sun	2023-02-08 17:38 (UTC)	2023-02-09 15:39 (UTC)		30	0	≡

When you hover over the results in the Activities and notes column, you can click to open a window to view all the matches in the comments or notes. You can then click on one matched note to open the results table displaying only the matched results.



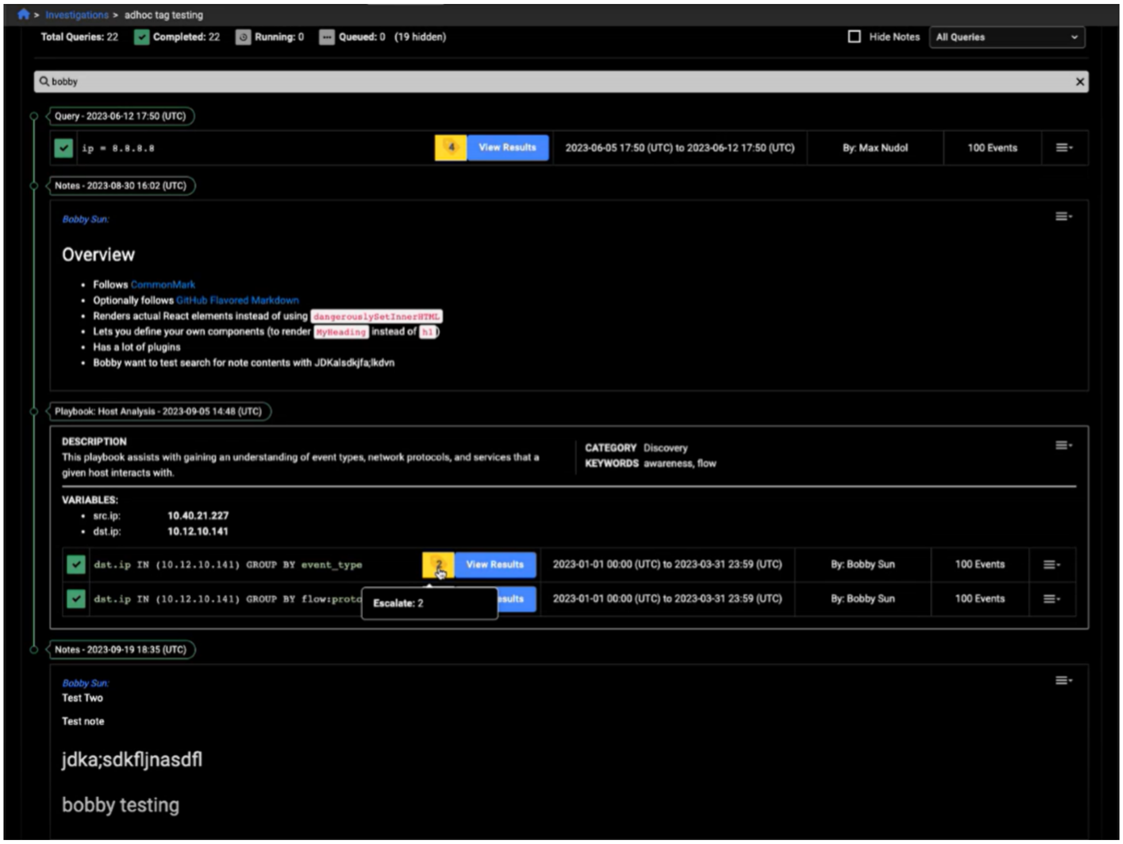
Evil: Tag test Bobby 2.

Escalate: test test fal;ksdjfa,v,n bobby asdfjalkfja;sf

Escalate: BOBBYBOBBY TEST asdf;lkasndf;alsk

Follow-up Required: aasdi fhasl dkjgv naklfg vbnak l gbobby test

Click *View Details* to open the investigation. The matched text will be highlighted.



Query - 2023-06-12 17:50 (UTC)

✓	ip = 8.8.8.8	2023-06-05 17:50 (UTC) to 2023-06-12 17:50 (UTC)	By: Max Nudol	100 Events

Notes - 2023-08-30 16:02 (UTC)

Bobby Sun:

Overview

- Follows CommonMark
- Optionally follows GitHub Flavored Markdown
- Renders actual React elements instead of using `dangerouslySetInnerHTML`
- Lets you define your own components (to render `MyHeading` instead of `h1`)
- Has a lot of plugins
- Bobby want to test search for note contents with JDKalsdkjfa;lkdvn

Playbook: Host Analysis - 2023-09-05 14:48 (UTC)

DESCRIPTION
This playbook assists with gaining an understanding of event types, network protocols, and services that a given host interacts with.

CATEGORY Discovery
KEYWORDS awareness, flow

VARIABLES:

- src.ip: 10.40.21.227
- dst.ip: 10.12.10.141

✓	dst.ip IN (10.12.10.141) GROUP BY event_type	2023-01-01 00:00 (UTC) to 2023-03-31 23:59 (UTC)	By: Bobby Sun	100 Events
✓	dst.ip IN (10.12.10.141) GROUP BY flow:proto	2023-01-01 00:00 (UTC) to 2023-03-31 23:59 (UTC)	By: Bobby Sun	100 Events

Notes - 2023-09-19 18:35 (UTC)

Bobby Sun:
Test Two

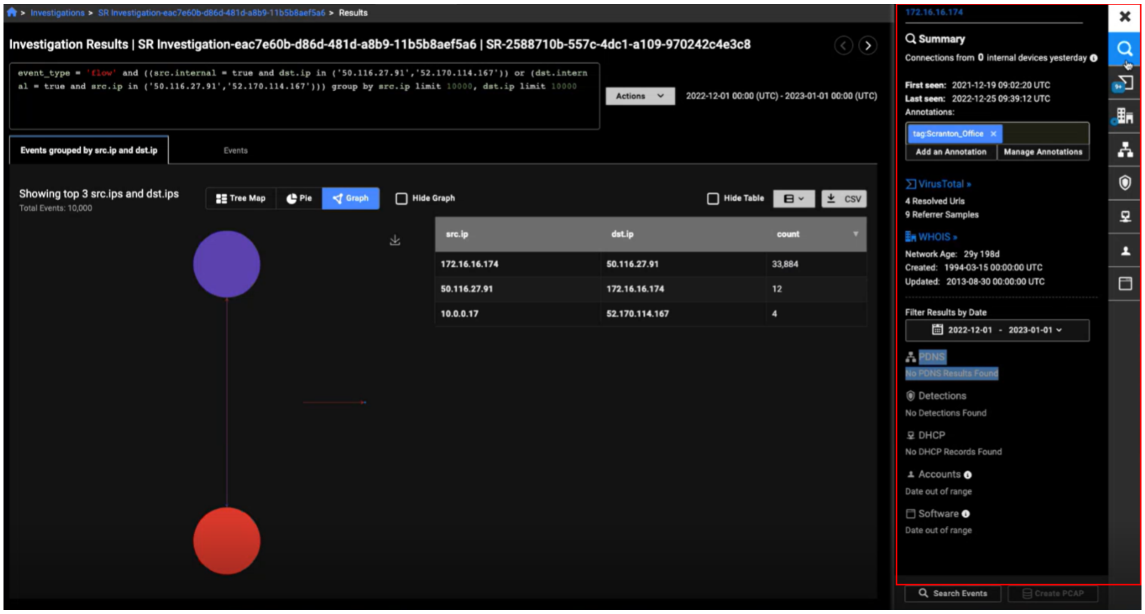
Test note

jdka;sdkfljnasdfl

bobby testing

Entity Panel

The Entity Panel has been reorganized. Virus Total and WHOIS now appear at the top of the summary and the date range filters are the bottom. The navigation tabs have been updated to match the rest of GUI.



Investigation Results | SR Investigation-eac7e60b-d86d-481d-a8b9-11b5b8aef5a6 | SR-2588710b-557c-4dc1-a109-970242c4e3c8

```
event_type = 'flow' and ((src.internal = true and dst.ip in ('50.116.27.91','52.170.114.167')) or (dst.intern
al = true and src.ip in ('50.116.27.91','52.170.114.167'))) group by src.ip limit 10000, dst.ip limit 10000
```

2022-12-01 00:00 (UTC) - 2023-01-01 00:00 (UTC)

Showing top 3 src.ips and dst.ips
Total Events: 10,000

src.ip	dst.ip	count
172.16.16.174	50.116.27.91	33,884
50.116.27.91	172.16.16.174	12
10.0.0.17	52.170.114.167	4

172.16.16.174

Summary
Connections from 0 internal devices yesterday

First seen: 2021-12-19 09:02:20 UTC
Last seen: 2022-12-25 09:39:12 UTC
Annotations:
tag:Scranton_Office

VirusTotal »
4 Resolved Urls
9 Referrer Samples

WHOIS »
Network Age: 29y 198d
Created: 1994-03-15 00:00:00 UTC
Updated: 2013-08-30 00:00:00 UTC

Filter Results by Date
2022-12-01 - 2023-01-01

PDNS
No PDNS Results Found

Detections
No Detections Found

DHCP
No DHCP Records Found

Accounts
Date out of range

Software
Date out of range

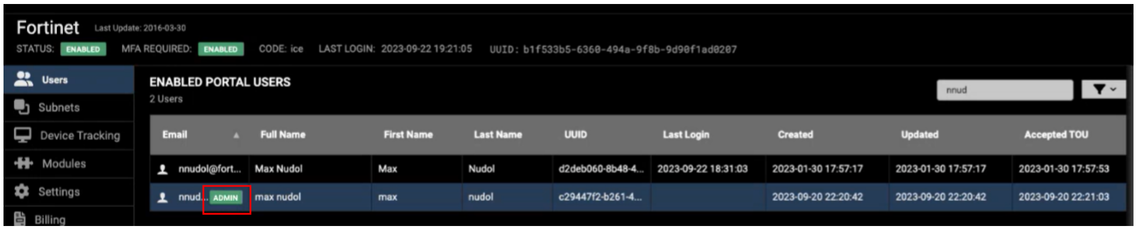
Investigations > SR Investigation-eac7e60b-d86d-481d-a8b9-11b5b8aef5a6 > Results
Actions
Events grouped by src.ip and dst.ip
Events
Tree Map
Pie
Graph
Hide Graph
Hide Table
CSV
Add an Annotation
Manage Annotations
Search Events
Create PCAP

The date range on Entity Panel now defaults to the time range based on where the panel is opened.

- The time range in the Entity Panel will match the range entered in the following pages: Entity Lookup, Visualizer, Detection Table , Sensor Visibility, Investigate Results, Adhoc Search and Observation Detail.
- The default time range is 7 days in the following pages: Detection, Detection-Indicator and Detection-Triage.

Account management

We have added a tag next to a user's email address to identify users with Admin roles. The tag is only visible the user is the Admin on the current account.



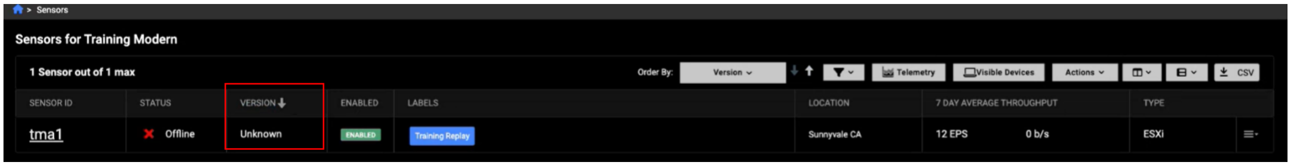
Fortinet Last Update: 2016-03-30
STATUS: ENABLED MFA REQUIRED: ENABLED CODE: ice LAST LOGIN: 2023-09-22 19:21:05 UUID: b1f533b5-6360-494a-9f8b-9d90f1ad0207

ENABLED PORTAL USERS
2 Users

Email	Full Name	First Name	Last Name	UUID	Last Login	Created	Updated	Accepted TOU
nnudol@fort...	Max Nudol	Max	Nudol	d2deb060-8b48-4...	2023-09-22 18:31:03	2023-01-30 17:57:17	2023-01-30 17:57:17	2023-01-30 17:57:53
nnud... ADMIN	max nudol	max	nudol	c29447f2-b261-4...		2023-09-20 22:20:42	2023-09-20 22:20:42	2023-09-20 22:21:03

Sensor versions

The sensor version is now displayed in the in the *Version* column of the *Sensor* page. The column can be sorted, and when there is no data for the version, *Unknown* is displayed.



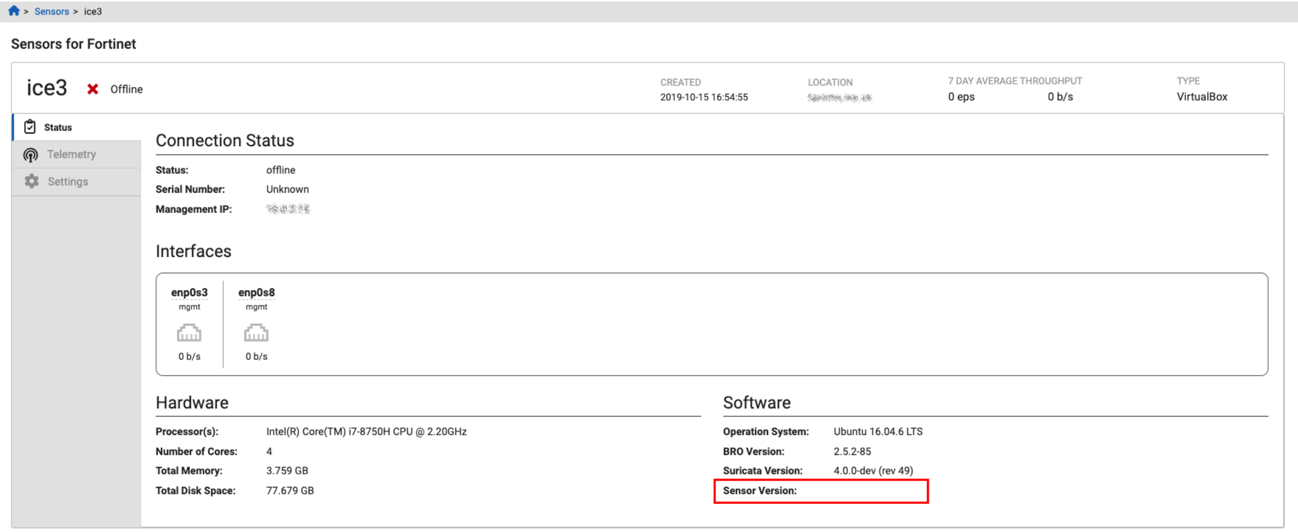
Sensors for Training Modern

1 Sensor out of 1 max

Order By: Version

SENSOR ID	STATUS	VERSION	ENABLED	LABELS	LOCATION	7 DAY AVERAGE THROUGHPUT		TYPE
tma1	Offline	Unknown	ENABLED	Training Replay	Sunnyvale CA	12 EPS	0 b/s	ESXi

The sensor version is also shown on the *Sensor Detail* page in the *Software* section on the *Status* tab. When there is no data for the version, the field is blank.



Sensors > ice3

Sensors for Fortinet

ice3 ✖ Offline

CREATED	LOCATION	7 DAY AVERAGE THROUGHPUT		TYPE
2019-10-15 16:54:55	[redacted]	0 eps	0 b/s	VirtualBox

Connection Status

Status:	offline
Serial Number:	Unknown
Management IP:	[redacted]

Interfaces

enp0s3	enp0s8
mgmt	mgmt
0 b/s	0 b/s

Hardware

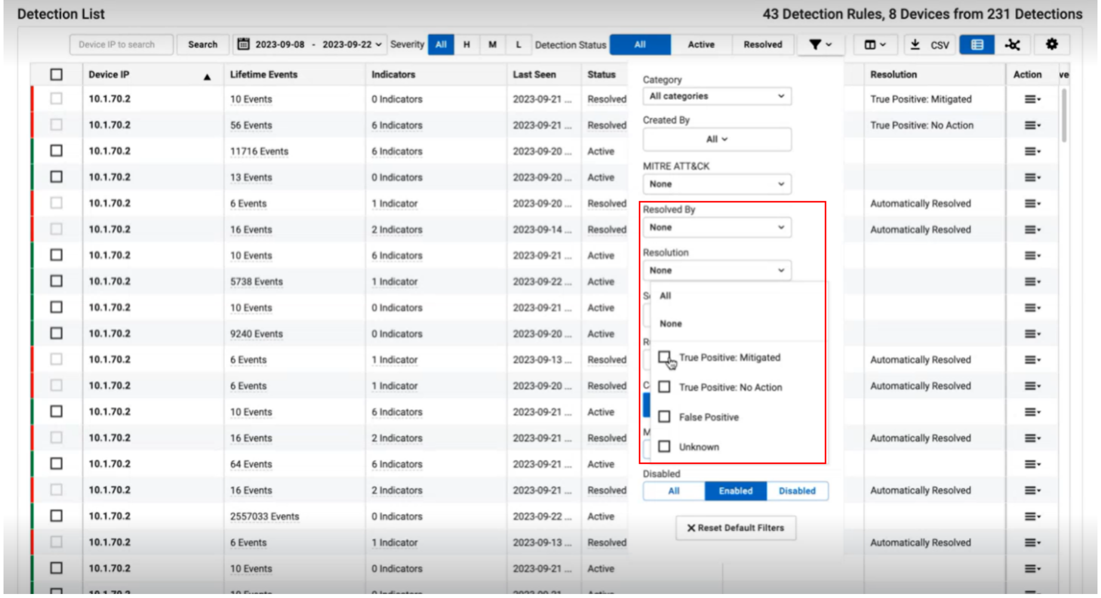
Processor(s):	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz
Number of Cores:	4
Total Memory:	3.759 GB
Total Disk Space:	77.679 GB

Software

Operation System:	Ubuntu 16.04.6 LTS
BRO Version:	2.5.2-85
Suricata Version:	4.0.0-dev (rev 49)
Sensor Version:	

Detection list filters

Two new filters were added to the detections table: Resolved by and Resolution.



Detection List

43 Detection Rules, 8 Devices from 231 Detections

☐	Device IP ▲	Lifetime Events	Indicators	Last Seen	Status	Resolution	Action
☐	10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Resolved	True Positive: Mitigated	≡
☐	10.1.70.2	56 Events	6 Indicators	2023-09-21 ...	Resolved	True Positive: No Action	≡
☐	10.1.70.2	11716 Events	6 Indicators	2023-09-20 ...	Active		≡
☐	10.1.70.2	13 Events	0 Indicators	2023-09-20 ...	Active		≡
☐	10.1.70.2	6 Events	1 Indicator	2023-09-20 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	16 Events	2 Indicators	2023-09-14 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	10 Events	6 Indicators	2023-09-21 ...	Active		≡
☐	10.1.70.2	5738 Events	1 Indicator	2023-09-22 ...	Active		≡
☐	10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Active		≡
☐	10.1.70.2	9240 Events	0 Indicators	2023-09-20 ...	Active		≡
☐	10.1.70.2	6 Events	1 Indicator	2023-09-13 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	6 Events	1 Indicator	2023-09-20 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	10 Events	6 Indicators	2023-09-21 ...	Active		≡
☐	10.1.70.2	16 Events	2 Indicators	2023-09-21 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	64 Events	6 Indicators	2023-09-21 ...	Active		≡
☐	10.1.70.2	16 Events	2 Indicators	2023-09-21 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	2557033 Events	0 Indicators	2023-09-22 ...	Active		≡
☐	10.1.70.2	6 Events	1 Indicator	2023-09-13 ...	Resolved	Automatically Resolved	≡
☐	10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Active		≡

Category: All categories

Created By: All

MITRE ATT&CK: None

Resolved By: None

Resolution: None

- All
- None
- ☐ True Positive: Mitigated
- ☐ True Positive: No Action
- ☐ False Positive
- ☐ Unknown

Disabled: All | **Enabled** | Disabled

Other improvements

- All columns in tables are sortable.

13 September 2023 version 2023.8.1

FortiNDR Cloud 2023.8.1 includes bug fixes, but no new features. See Resolved Issues on page 50.

21 August 2023 version 2023.8

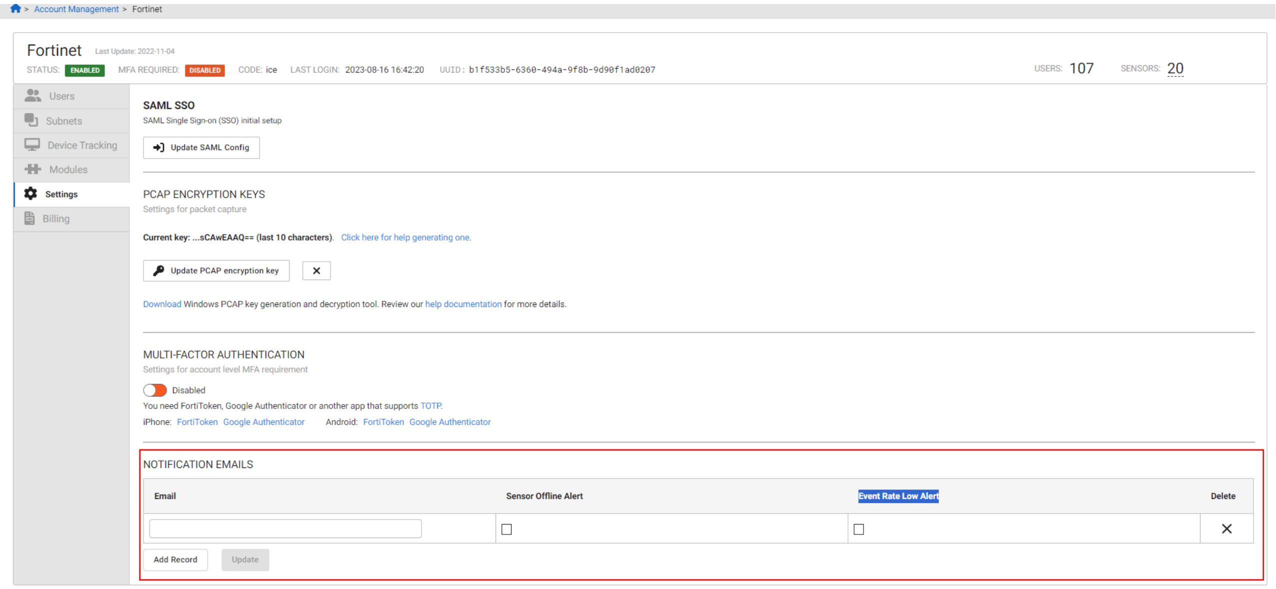
New functionality

Sensor email alerts

Administrators can now create email notifications alerts when a sensor is offline or the event rate is low.

To create a sensor email alert:

1. Go to *Account Management* > *Settings*.
2. Under *Notification Emails*, click *Add Record*.



Fortinet Last Update: 2022-11-04

STATUS: ENABLED MFA REQUIRED: DISABLED CODE: ice LAST LOGIN: 2023-08-16 16:42:20 UUID: b1f533b5-6360-494a-9f8b-9d90f1ad0207 USERS: 107 SENSORS: 20

SAML SSO

SAML Single Sign-on (SSO) initial setup

Update SAML Config

PCAP ENCRYPTION KEYS

Settings for packet capture

Current key: ...sCAwEAAQ== (last 10 characters). Click here for help generating one.

Update PCAP encryption key ✕

Download Windows PCAP key generation and decryption tool. Review our help documentation for more details.

MULTI-FACTOR AUTHENTICATION

Settings for account level MFA requirement

Disabled

You need FortiToken, Google Authenticator or another app that supports TOTP.

iPhone: FortiToken Google Authenticator Android: FortiToken Google Authenticator

NOTIFICATION EMAILS

Email	Sensor Offline Alert	Event Rate Low Alert	Delete
	□	□	✕

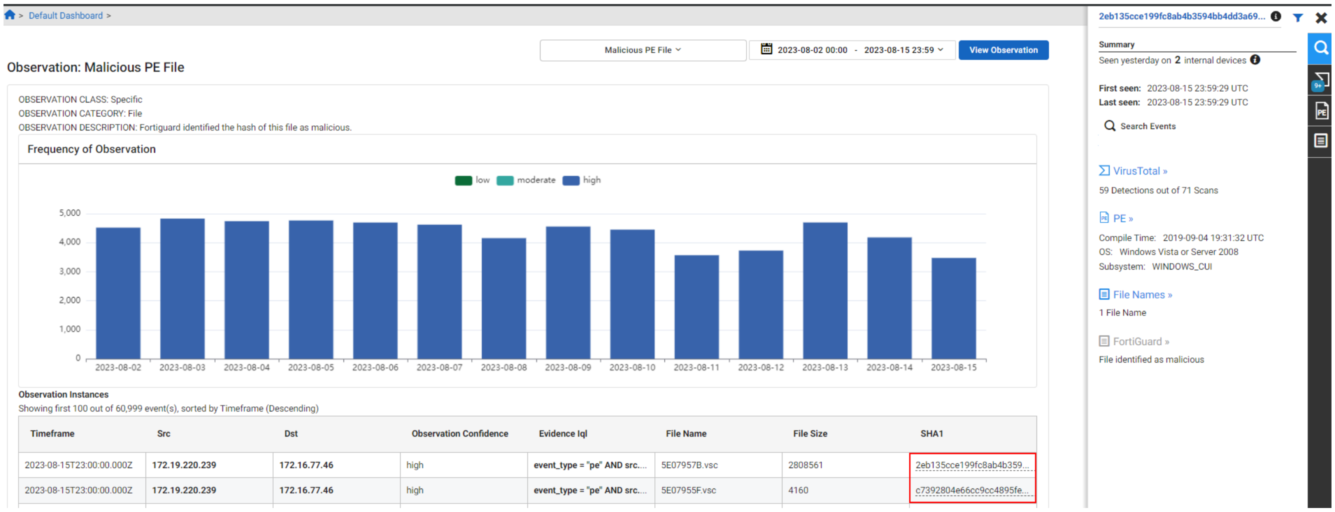
Add Record Update

3. In the *Email* field, enter a recipient's email address.
4. Select *Sensor Offline Alert* and/or *Event Rate Low Alert*.
5. Click *Update*.

Enhanced functionality

Malicious PE file observation

The *Sha1* field is now linked to the Entity Panel.



Observation: Malicious PE File

OBSERVATION CLASS: Specific
OBSERVATION CATEGORY: File
OBSERVATION DESCRIPTION: Fortiguard identified the hash of this file as malicious.

Frequency of Observation

Observation Instances
Showing first 100 out of 60,999 event(s), sorted by Timeframe (Descending)

Timeframe	Src	Dst	Observation Confidence	Evidence Iql	File Name	File Size	SHA1
2023-08-15T23:00:00.000Z	172.19.220.239	172.16.77.46	high	event_type = "pe" AND src....	5E07957B.vsc	2808561	2eb135cce199fc8ab4b359...
2023-08-15T23:00:00.000Z	172.19.220.239	172.16.77.46	high	event_type = "pe" AND src....	5E07955F.vsc	4160	c7392804e66cc9cc4895fe...

2eb135cce199fc8ab4b3594bb4dd3a69...

Summary
Seen yesterday on 2 internal devices

First seen: 2023-08-15 23:59:29 UTC
Last seen: 2023-08-15 23:59:29 UTC

59 Detections out of 71 Scans

Compile Time: 2019-09-04 19:31:32 UTC
OS: Windows Vista or Server 2008
Subsystem: WINDOWS_CUI

1 File Name

File identified as malicious

Other Enhancements

- You can now sort the *Detections Table* by *Resolution*.
- In *Search Timeline*, you can use the *Date Picker* to search any time period within the last 365 days as long as it is limited to seven days.

31 July 2023 version 2023.7

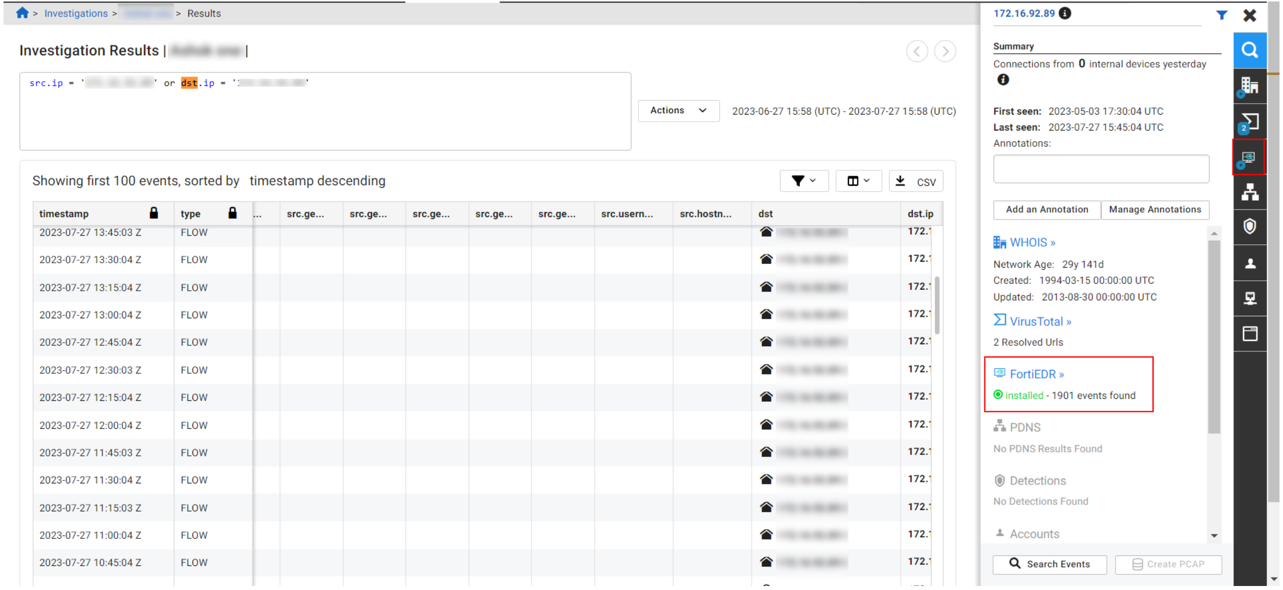
New Functionality

Investigate FortiEDR Host

The *Entity Panel* now links directly to a specific host in FortiEDR.

To view the FortiEDR host:

1. Click the *FortiEDR* link in the Entity Panel.



Investigation Results | [redacted] |

```
src.ip = '[redacted]' or dst.ip = '[redacted]'
```

2023-06-27 15:58 (UTC) - 2023-07-27 15:58 (UTC)

Showing first 100 events, sorted by timestamp descending

timestamp	type	...	src.ge...	src.ge...	src.ge...	src.ge...	src.ge...	src.usern...	src.hostn...	dst	dst.ip
2023-07-27 13:45:03 Z	FLOW									[redacted]	172.'
2023-07-27 13:30:04 Z	FLOW									[redacted]	172.'
2023-07-27 13:15:04 Z	FLOW									[redacted]	172.'
2023-07-27 13:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:45:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:30:03 Z	FLOW									[redacted]	172.'
2023-07-27 12:15:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 11:45:03 Z	FLOW									[redacted]	172.'
2023-07-27 11:30:04 Z	FLOW									[redacted]	172.'
2023-07-27 11:15:03 Z	FLOW									[redacted]	172.'
2023-07-27 11:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 10:45:04 Z	FLOW									[redacted]	172.'

172.16.92.89

Summary

Connections from **0** internal devices yesterday

First seen: 2023-05-03 17:30:04 UTC
Last seen: 2023-07-27 15:45:04 UTC
Annotations:

WHOIS »

Network Age: 29y 141d
Created: 1994-03-15 00:00:00 UTC
Updated: 2013-08-30 00:00:00 UTC

VirusTotal »

2 Resolved Urls

FortiEDR »

installed - 1901 events found

PDNS

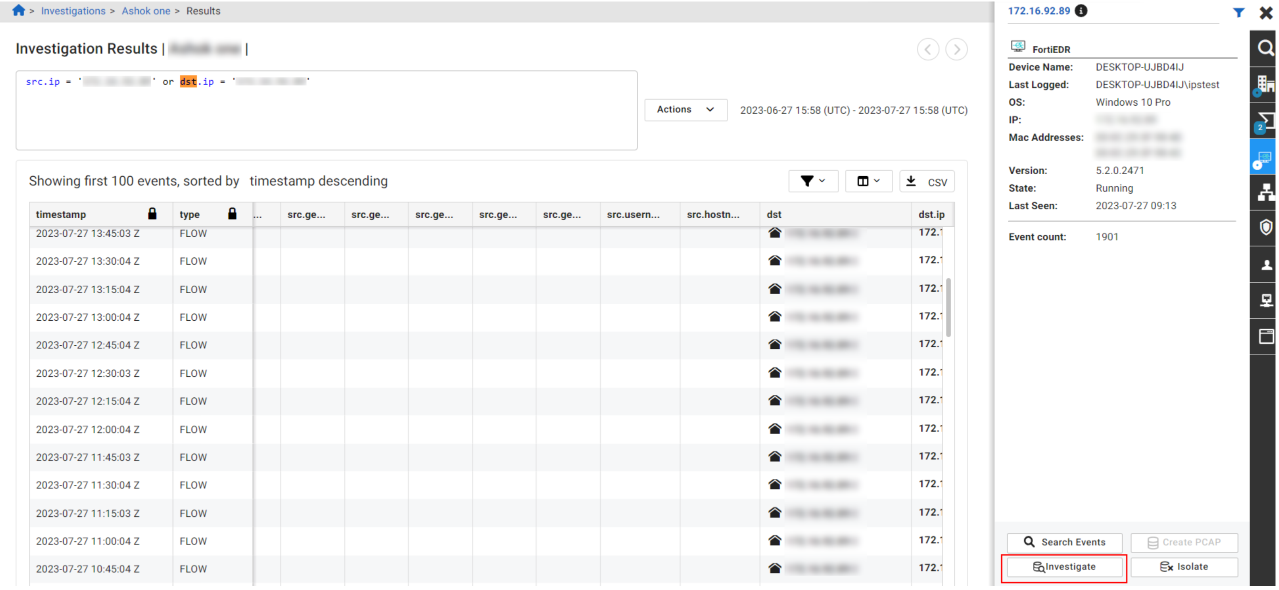
No PDNS Results Found

Detections

No Detections Found

Accounts

2. Click *Investigate* to open FortiEDR. If you are not logged into FortiEDR you will be redirected to login page.



Investigation Results | [redacted] |

```
src.ip = '[redacted]' or dst.ip = '[redacted]'
```

2023-06-27 15:58 (UTC) - 2023-07-27 15:58 (UTC)

Showing first 100 events, sorted by timestamp descending

timestamp	type	...	src.ge...	src.ge...	src.ge...	src.ge...	src.ge...	src.usern...	src.hostn...	dst	dst.ip
2023-07-27 13:45:03 Z	FLOW									[redacted]	172.'
2023-07-27 13:30:04 Z	FLOW									[redacted]	172.'
2023-07-27 13:15:04 Z	FLOW									[redacted]	172.'
2023-07-27 13:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:45:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:30:03 Z	FLOW									[redacted]	172.'
2023-07-27 12:15:04 Z	FLOW									[redacted]	172.'
2023-07-27 12:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 11:45:03 Z	FLOW									[redacted]	172.'
2023-07-27 11:30:04 Z	FLOW									[redacted]	172.'
2023-07-27 11:15:03 Z	FLOW									[redacted]	172.'
2023-07-27 11:00:04 Z	FLOW									[redacted]	172.'
2023-07-27 10:45:04 Z	FLOW									[redacted]	172.'

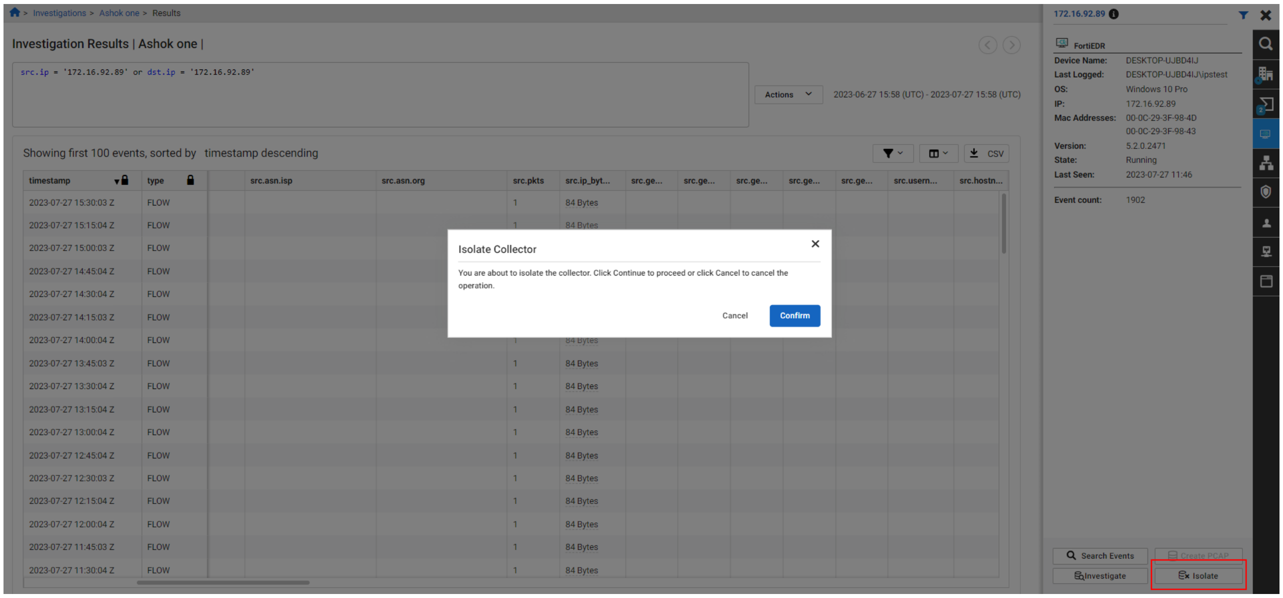
172.16.92.89

FortiEDR

Device Name: DESKTOP-UJBD4IJ
Last Logged: DESKTOP-UJBD4IJ\ipstest
OS: Windows 10 Pro
IP: [redacted]
Mac Addresses: [redacted]
Version: 5.2.0.2471
State: Running
Last Seen: 2023-07-27 09:13

Event count: 1901

3. Click *Isolate* to isolate the collector.



Investigation Results | Ashok one |

```
src.ip = '172.16.92.89' or dst.ip = '172.16.92.89'
```

2023-06-27 15:58 (UTC) - 2023-07-27 15:58 (UTC)

Showing first 100 events, sorted by timestamp descending

timestamp	type	src.asn.isp	src.asn.org	src.pkts	src.ip_byt...	src.ge...	src.ge...	src.ge...	src.ge...	src.ge...	src.usern...	src.hostn...
2023-07-27 15:30:03 Z	FLOW			1	84 Bytes							
2023-07-27 15:15:04 Z	FLOW			1	84 Bytes							
2023-07-27 15:00:03 Z	FLOW											
2023-07-27 14:45:04 Z	FLOW											
2023-07-27 14:30:04 Z	FLOW											
2023-07-27 14:15:03 Z	FLOW											
2023-07-27 14:00:04 Z	FLOW			1	84 Bytes							
2023-07-27 13:45:03 Z	FLOW			1	84 Bytes							
2023-07-27 13:30:04 Z	FLOW			1	84 Bytes							
2023-07-27 13:15:04 Z	FLOW			1	84 Bytes							
2023-07-27 13:00:04 Z	FLOW			1	84 Bytes							
2023-07-27 12:45:04 Z	FLOW			1	84 Bytes							
2023-07-27 12:30:03 Z	FLOW			1	84 Bytes							
2023-07-27 12:15:04 Z	FLOW			1	84 Bytes							
2023-07-27 12:00:04 Z	FLOW			1	84 Bytes							
2023-07-27 11:45:03 Z	FLOW			1	84 Bytes							
2023-07-27 11:30:04 Z	FLOW			1	84 Bytes							

Isolate Collector

You are about to isolate the collector. Click Continue to proceed or click Cancel to cancel the operation.

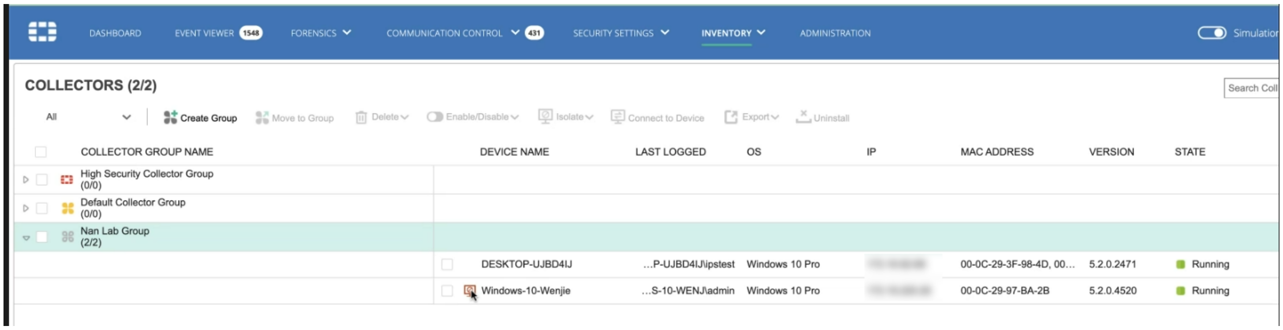
172.16.92.89

FortiEDR

Device Name: DESKTOP-UJBD4IJ
Last Logged: DESKTOP-UJBD4IJ\ipstest
OS: Windows 10 Pro
IP: 172.16.92.89
Mac Addresses: 00-0C-29-3F-98-4D
00-0C-29-3F-98-43
Version: 5.2.0.2471
State: Running
Last Seen: 2023-07-27 11:46

Event count: 1902

4. FortiEDR displays the isolated collector.



COLLECTORS (2/2)

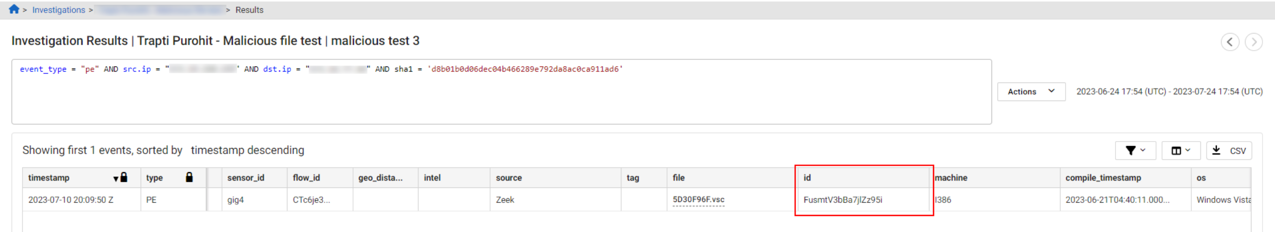
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE
High Security Collector Group (0/0)							
Default Collector Group (0/0)							
Nan Lab Group (2/2)							
	DESKTOP-UJBD4IJ	...P-UJBD4IJ\ipstest	Windows 10 Pro	[redacted]	00-0C-29-3F-98-4D, 00...	5.2.0.2471	🟩 Running
	Windows-10-Wenjie	...S-10-WENJ\admin	Windows 10 Pro	[redacted]	00-0C-29-97-BA-2B	5.2.0.4520	🟩 Running

Malicious files flag

The *Entity Panel* now flags malicious files with FortiGuard.

To view the Malicious flag:

1. In the investigation results, click the link in the *File* column.



Investigation Results | Trapti Purohit - Malicious file test | malicious test 3

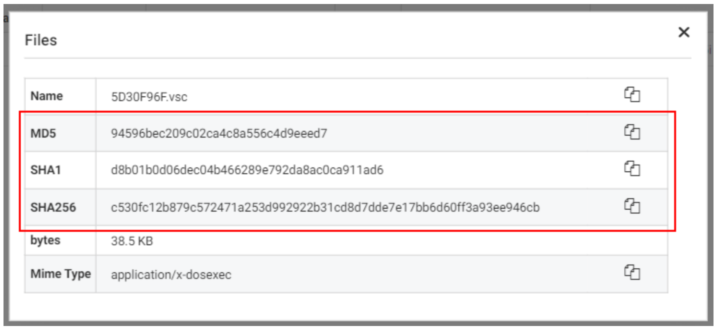
```
event_type = "pe" AND src.ip = "[redacted]" AND dst.ip = "[redacted]" AND sha1 = 'd8b01b0d06dec04b466289e792da8ac0ca911ad6'
```

2023-06-24 17:54 (UTC) - 2023-07-24 17:54 (UTC)

Showing first 1 events, sorted by timestamp descending

timestamp	type	sensor_id	flow_id	geo_dista...	intel	source	tag	file	id	machine	compile_timestamp	os
2023-07-10 20:09:50 Z	PE	gig4	CTc6je3...			Zeek		5D30F96F.vsc	FusmtV3bBa7jlZz95i	I386	2023-06-21T04:40:11.000...	Windows Vista

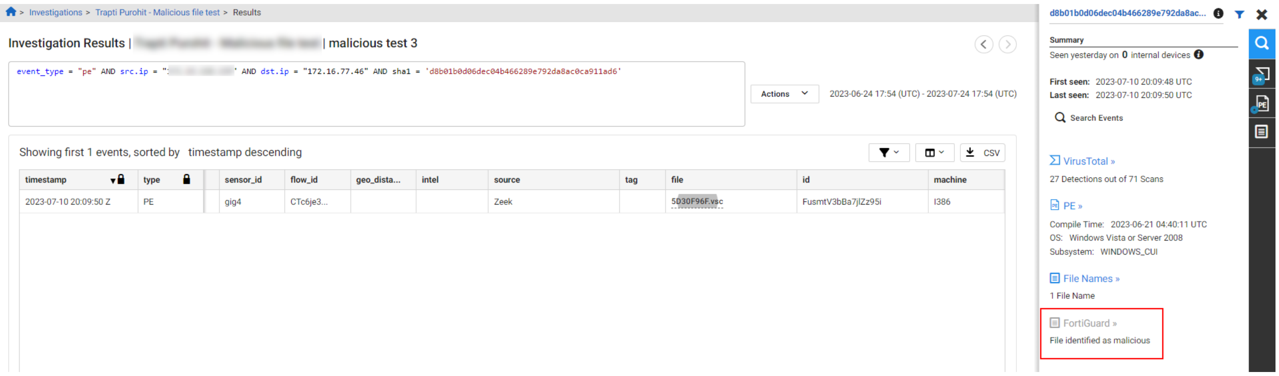
2. Click a link in the *Files* dialog.



Files

Name	5D30F96F.vsc
MD5	94596bec209c02ca4c8a556c4d9eeed7
SHA1	d8b01b0d06dec04b466289e792da8ac0ca911ad6
SHA256	c530fc12b879c572471a253d992922b31cd8d7dde7e17bb6d60ff3a93ee946cb
bytes	38.5 KB
Mime Type	application/x-dosexec

3. The flag appears in the *FortiGuard* section.



Investigations > Trapti Purohit - Malicious file test > Results

Investigation Results | [redacted] | malicious test 3

```
event_type = "pe" AND src.ip = "[redacted]" AND dst.ip = "172.16.77.46" AND sha1 = 'd8b01b0d06dec04b466289e792da8ac0ca911ad6'
```

2023-06-24 17:54 (UTC) - 2023-07-24 17:54 (UTC)

Showing first 1 events, sorted by timestamp descending

timestamp	type	sensor_id	flow_id	geo_dista...	intel	source	tag	file	id	machine
2023-07-10 20:09:50 Z	PE	gig4	CTc6je3...			Zeek		5D30F96F.vsc	FusmtV3bBa7jlZz95i	I386

d8b01b0d06dec04b466289e792da8ac...

Summary

Seen yesterday on 0 internal devices

First seen: 2023-07-10 20:09:48 UTC
Last seen: 2023-07-10 20:09:50 UTC

VirusTotal »

27 Detections out of 71 Scans

PE »

Compile Time: 2023-06-21 04:40:11 UTC
OS: Windows Vista or Server 2008
Subsystem: WINDOWS_CUI

File Names »

1 File Name

FortiGuard »

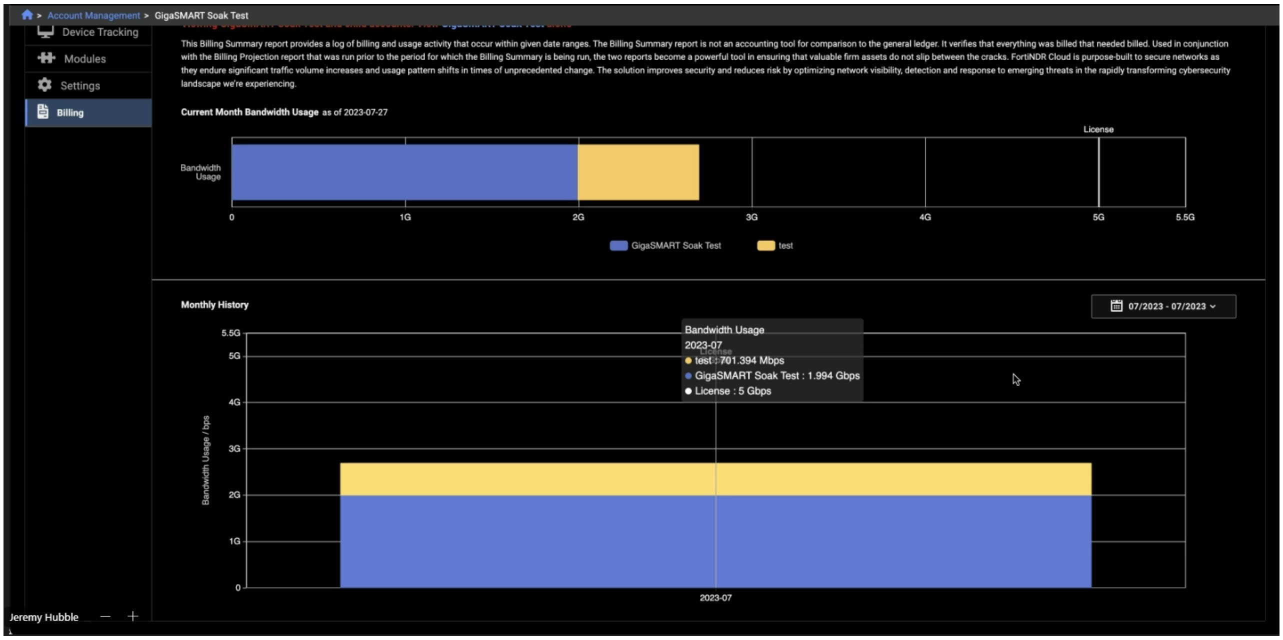
File identified as malicious

Parent/Child Account Bandwidth View

The *Account Management* page now displays the total bandwidth used by both parent and child accounts.

To view the Parent/Child Account Bandwidth:

1. Go to *Account Management* > *Billing*. The Parent/Child bandwidth is displayed.

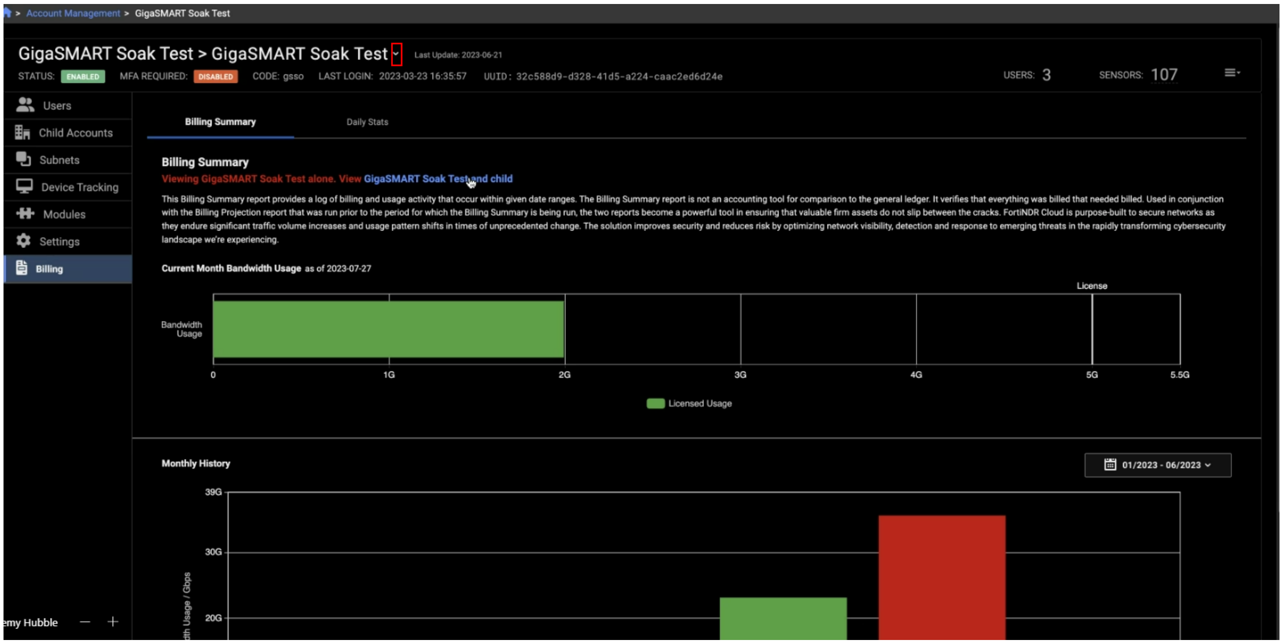


This Billing Summary report provides a log of billing and usage activity that occur within given date ranges. The Billing Summary report is not an accounting tool for comparison to the general ledger. It verifies that everything was billed that needed billed. Used in conjunction with the Billing Projection report that was run prior to the period for which the Billing Summary is being run, the two reports become a powerful tool in ensuring that valuable firm assets do not slip between the cracks. FortiNDR Cloud is purpose-built to secure networks as they endure significant traffic volume increases and usage pattern shifts in times of unprecedented change. The solution improves security and reduces risk by optimizing network visibility, detection and response to emerging threats in the rapidly transforming cybersecurity landscape we're experiencing.

Current Month Bandwidth Usage as of 2023-07-27

Monthly History

2. Click the toggle to view only the parent account.



GigaSMART Soak Test > GigaSMART Soak Test

STATUS: ENABLED MFA REQUIRED: DISABLED CODE: gsso LAST LOGIN: 2023-03-23 16:35:57 UUID: 32c588d9-d328-41d5-a224-caac2ed6d24e USERS: 3 SENSORS: 107

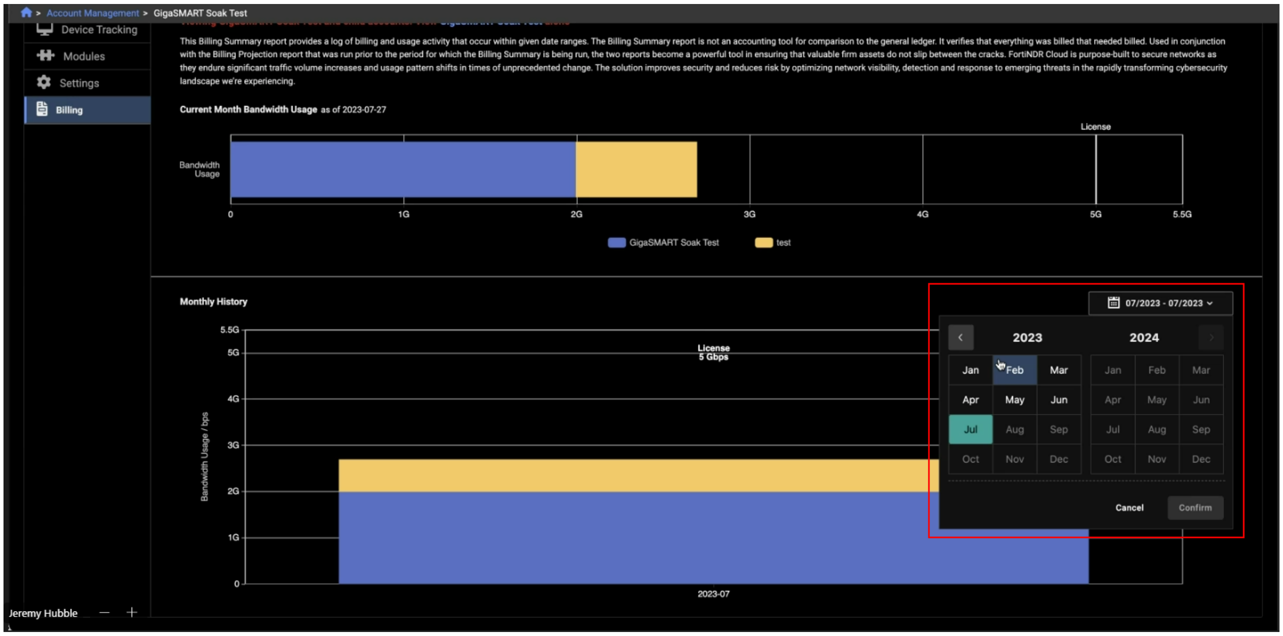
Billing Summary

Viewing GigaSMART Soak Test alone. View GigaSMART Soak Test and child

This Billing Summary report provides a log of billing and usage activity that occur within given date ranges. The Billing Summary report is not an accounting tool for comparison to the general ledger. It verifies that everything was billed that needed billed. Used in conjunction with the Billing Projection report that was run prior to the period for which the Billing Summary is being run, the two reports become a powerful tool in ensuring that valuable firm assets do not slip between the cracks. FortiNDR Cloud is purpose-built to secure networks as they endure significant traffic volume increases and usage pattern shifts in times of unprecedented change. The solution improves security and reduces risk by optimizing network visibility, detection and response to emerging threats in the rapidly transforming cybersecurity landscape we're experiencing.

Current Month Bandwidth Usage as of 2023-07-27

3. You can also view the usage for a previous month in the billing cycle.



This Billing Summary report provides a log of billing and usage activity that occur within given date ranges. The Billing Summary report is not an accounting tool for comparison to the general ledger. It verifies that everything was billed that needed billed. Used in conjunction with the Billing Projection report that was run prior to the period for which the Billing Summary is being run, the two reports become a powerful tool in ensuring that valuable firm assets do not slip between the cracks. FortiNDR Cloud is purpose-built to secure networks as they endure significant traffic volume increases and usage pattern shifts in times of unprecedented change. The solution improves security and reduces risk by optimizing network visibility, detection and response to emerging threats in the rapidly transforming cybersecurity landscape we're experiencing.

Current Month Bandwidth Usage as of 2023-07-27

17 July 2023 version 2023.6.1

FortiNDR Cloud 2023.6.1 includes bug fixes, but no new features. See Resolved Issues on page 50.

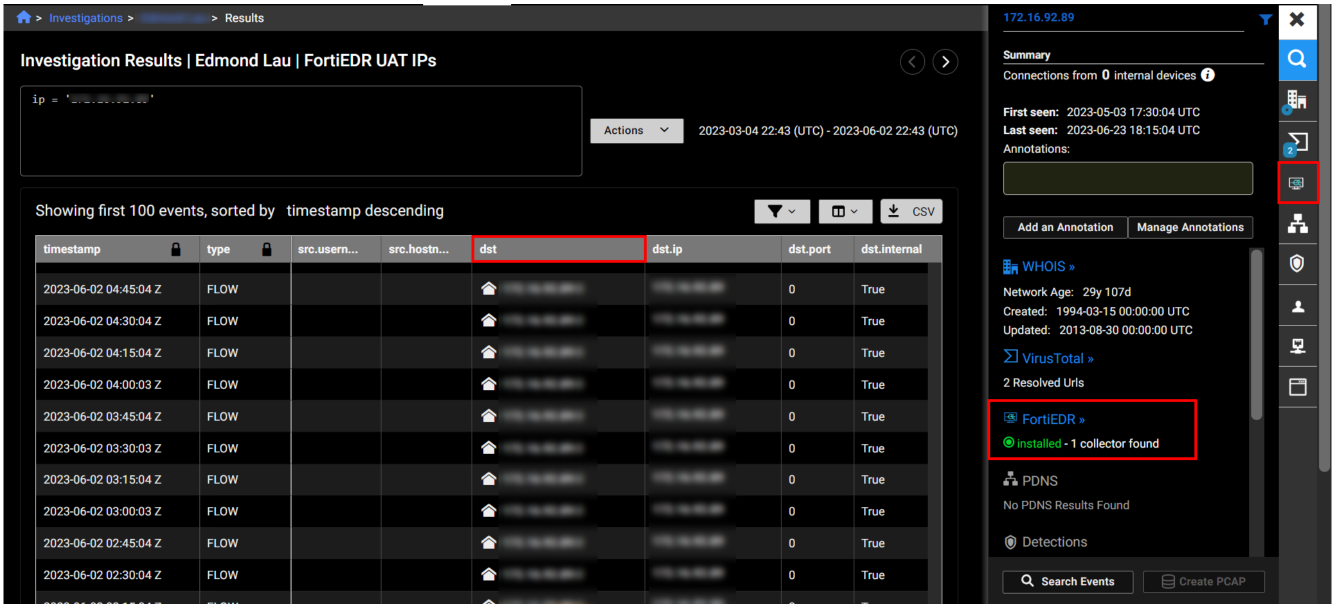
26 June 2023 version 2023.6

- New Functionality
  - FortiEDR integration
- Enhanced functionality
  - Pivot to Detections Table from the default dashboard
  - Enhanced date filtering
  - Enhanced tagging
  - GUI improvements: Detections Table
- New detection rules and observations

New Functionality

FortiEDR integration

Integration with FortiEDR is available and can be enabled from the *Account Management* page in the *Modules* tab. Once the integration is enabled, you can view the FortiEDR information in the *Entity Panel* from any events table in the portal.



Investigations > [redacted] > Results

Investigation Results | Edmond Lau | FortiEDR UAT IPs

```
ip = '[redacted]'
```

Actions

2023-03-04 22:43 (UTC) - 2023-06-02 22:43 (UTC)

Showing first 100 events, sorted by timestamp descending

timestamp	type	src.usern...	src.hostn...	dst	dst.ip	dst.port	dst.internal
2023-06-02 04:45:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 04:30:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 04:15:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 04:00:03 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 03:45:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 03:30:03 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 03:15:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 03:00:03 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 02:45:04 Z	FLOW			[redacted]	[redacted]	0	True
2023-06-02 02:30:04 Z	FLOW			[redacted]	[redacted]	0	True

172.16.92.89

Summary

Connections from 0 internal devices

First seen: 2023-05-03 17:30:04 UTC

Last seen: 2023-06-23 18:15:04 UTC

Annotations:

Add an Annotation | Manage Annotations

WHOIS »

Network Age: 29y 107d

Created: 1994-03-15 00:00:00 UTC

Updated: 2013-08-30 00:00:00 UTC

VirusTotal »

2 Resolved Urls

FortiEDR »

installed - 1 collector found

PDNS

No PDNS Results Found

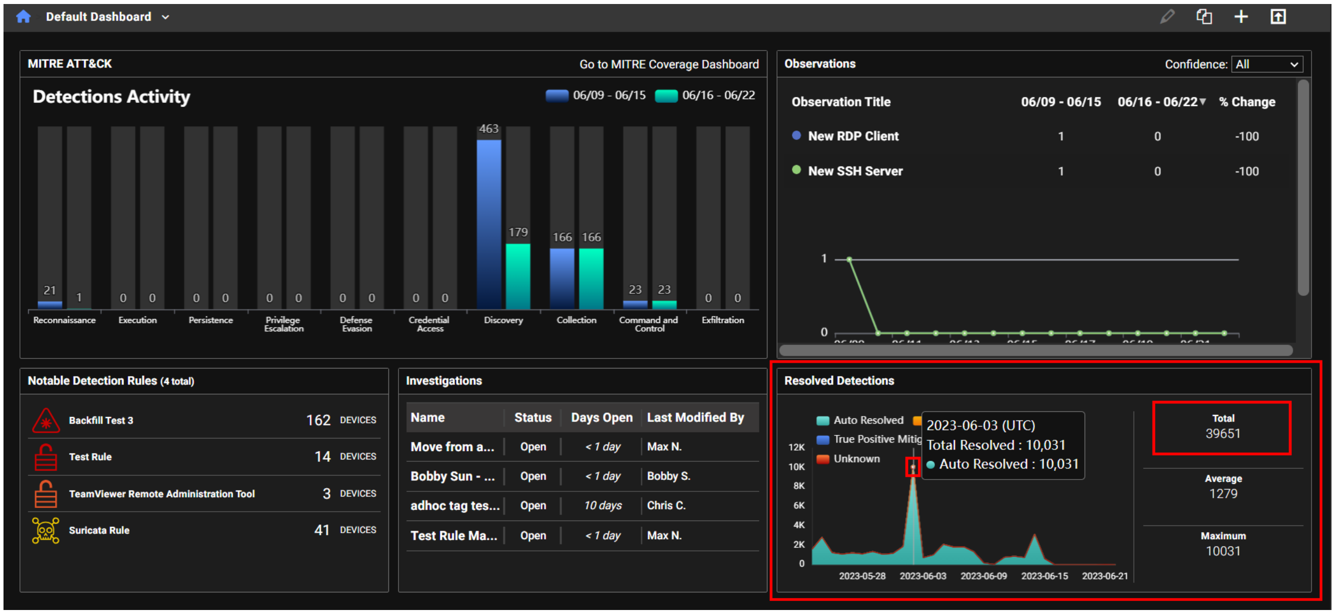
Detections

Search Events | Create PCAP

Enhanced functionality

Pivot to Detections Table from the default dashboard

In the *Resolved Detections* widget, you can click a data point in the chart or the *Total* detections to view all the resolved detections in the *Detections Table*.



Observation Title	06/09 - 06/15	06/16 - 06/22	% Change
New RDP Client	1	0	-100
New SSH Server	1	0	-100

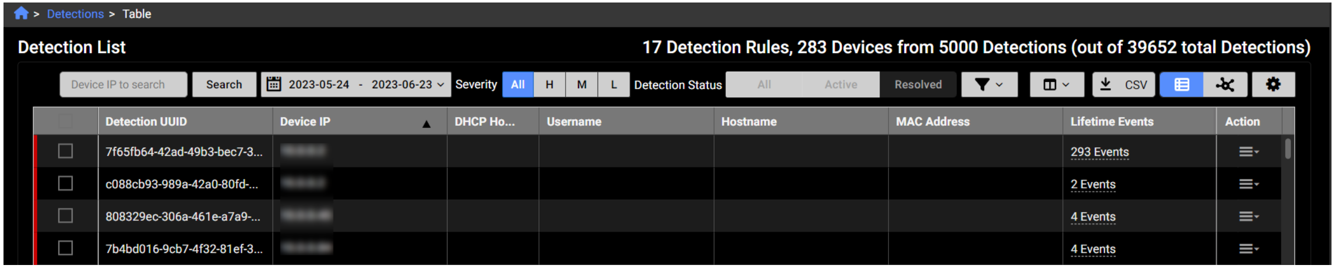
Notable Detection Rules (4 total)

Backfill Test 3	162	DEVICES
Test Rule	14	DEVICES
TeamViewer Remote Administration Tool	3	DEVICES
Suricata Rule	41	DEVICES

Investigations

Name	Status	Days Open	Last Modified By
Move from a...	Open	< 1 day	Max N.
Bobby Sun - ...	Open	< 1 day	Bobby S.
adhoc tag tes...	Open	10 days	Chris C.
Test Rule Ma...	Open	< 1 day	Max N.

The *Detections Table* displays the resolved detections reported in the widget.



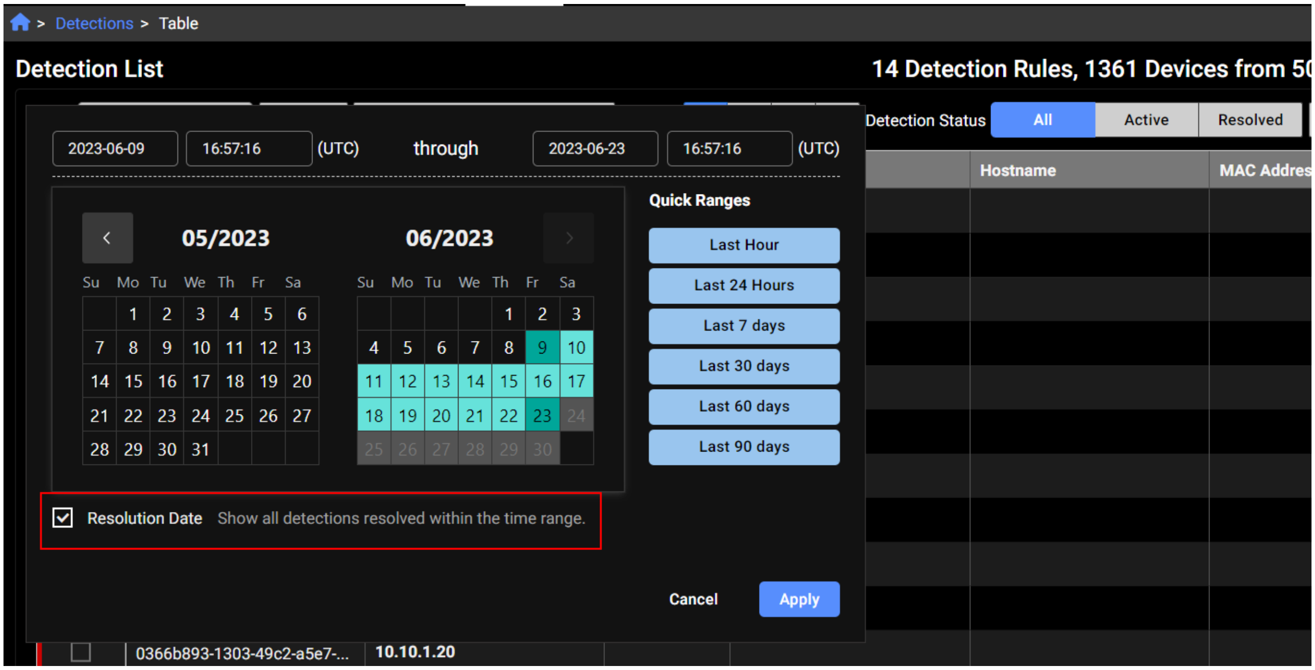
Detection List

17 Detection Rules, 283 Devices from 5000 Detections (out of 39652 total Detections)

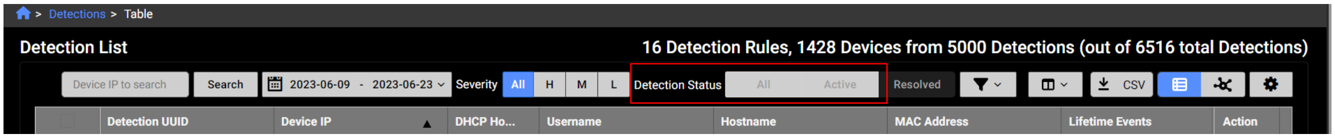
	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Action
□	7f65fb64-42ad-49b3-bec7-3...	[redacted]					293 Events	≡
□	c088cb93-989a-42a0-80fd-...	[redacted]					2 Events	≡
□	808329ec-306a-461e-a7a9-...	[redacted]					4 Events	≡
□	7b4bd016-9cb7-4f32-81ef-3...	[redacted]					4 Events	≡

Enhanced date filtering

The date filter now includes an option to only show resolved detections within the selected time range.

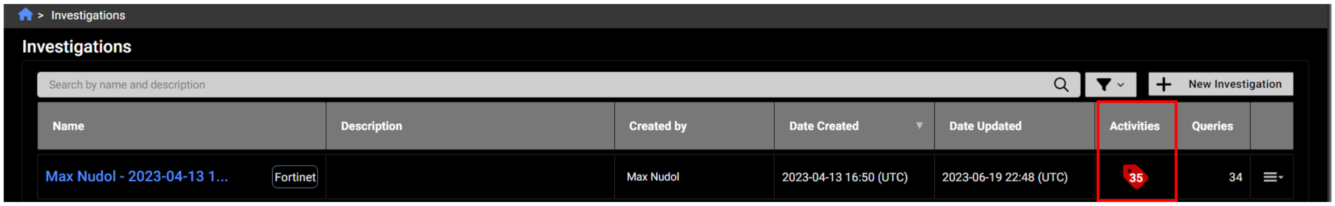

Detections > Table
Detection List
14 Detection Rules, 1361 Devices from 50
2023-06-09 16:57:16 (UTC) through 2023-06-23 16:57:16 (UTC)
05/2023
06/2023
Quick Ranges
Last Hour
Last 24 Hours
Last 7 days
Last 30 days
Last 60 days
Last 90 days
☑ Resolution Date Show all detections resolved within the time range.
Cancel
Apply
Detection Status All Active Resolved
Hostname
MAC Addres
0366b893-1303-49c2-a5e7-...
10.10.1.20

Enabling this option will disable the buttons in the *Severity* filter until you disable it again.



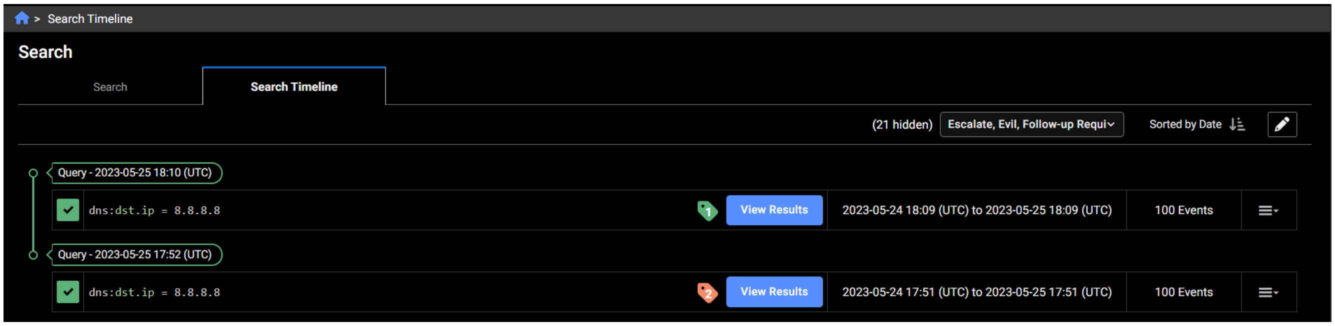
Enhanced tagging

A new *Activities* column has been added to the *Investigate* tab. This column indicates the investigation was tagged, as well the number of tags, and the tag label.



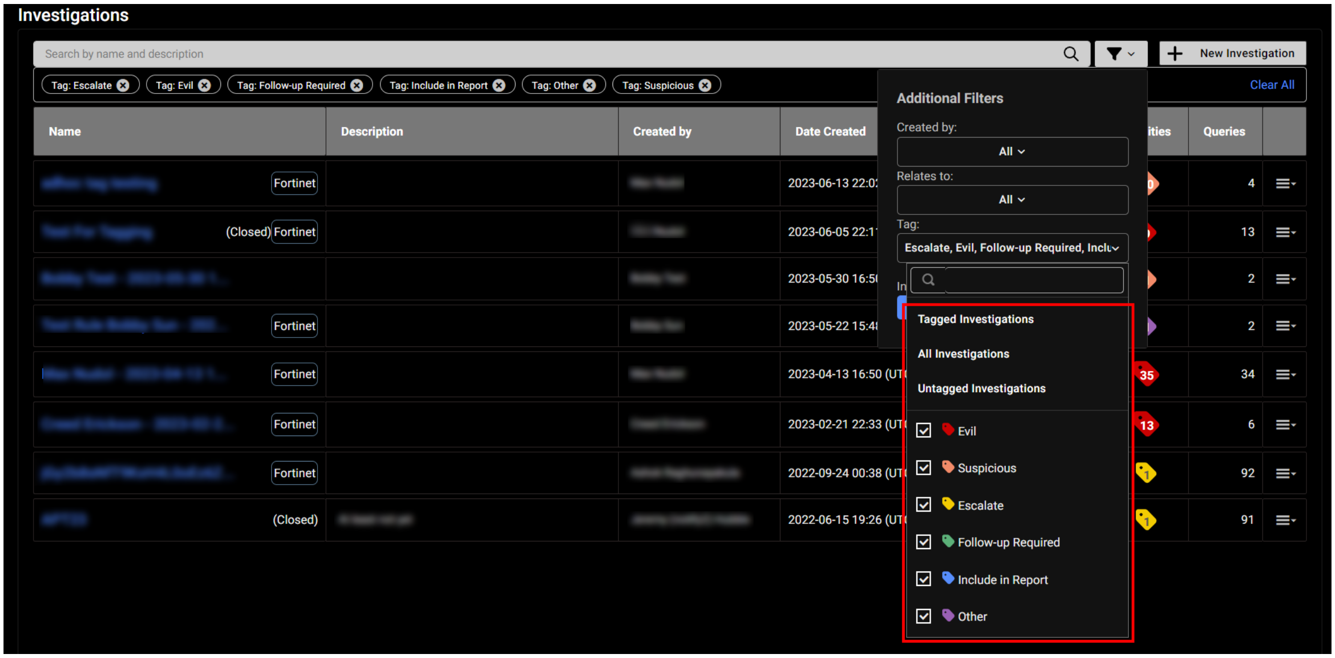
Name	Description	Created by	Date Created	Date Updated	Activities	Queries
Max Nudol - 2023-04-13 1... Fortinet		Max Nudol	2023-04-13 16:50 (UTC)	2023-06-19 22:48 (UTC)	35	34

Tags are also visible in the *Search Timeline* tab.


Search Timeline
Search
Search
Search Timeline
(21 hidden)
Escalate, Evil, Follow-up Requi
Sorted by Date
Query - 2023-05-25 18:10 (UTC)
Query - 2023-05-25 17:52 (UTC)
View Results

```
dns:dst.ip = 8.8.8.8    1    2023-05-24 18:09 (UTC) to 2023-05-25 18:09 (UTC)    100 Events
dns:dst.ip = 8.8.8.8    2    2023-05-24 17:51 (UTC) to 2023-05-25 17:51 (UTC)    100 Events
```

You can filter the page to show only tagged Investigations, or tagged investigations by tag label.



Investigations

Search by name and description

New Investigation

Tag: Escalate ⊗ Tag: Evil ⊗ Tag: Follow-up Required ⊗ Tag: Include in Report ⊗ Tag: Other ⊗ Tag: Suspicious ⊗

Clear All

Name	Description	Created by	Date Created	ities	Queries
[redacted] Fortinet		[redacted]	2023-06-13 22:0		4
[redacted] (Closed) Fortinet		[redacted]	2023-06-05 22:1		13
[redacted]		[redacted]	2023-05-30 16:5		2
[redacted] Fortinet		[redacted]	2023-05-22 15:4		2
[redacted] Fortinet		[redacted]	2023-04-13 16:50 (UT	35	34
[redacted] Fortinet		[redacted]	2023-02-21 22:33 (UT	13	6
[redacted] Fortinet		[redacted]	2022-09-24 00:38 (UT	1	92
[redacted] (Closed)	[redacted]	[redacted]	2022-06-15 19:26 (UT	1	91

Additional Filters

Created by: All

Relates to: All

Tag: Escalate, Evil, Follow-up Required, Inclu

Tagged Investigations

All Investigations

Untagged Investigations

☑ Evil

☑ Suspicious

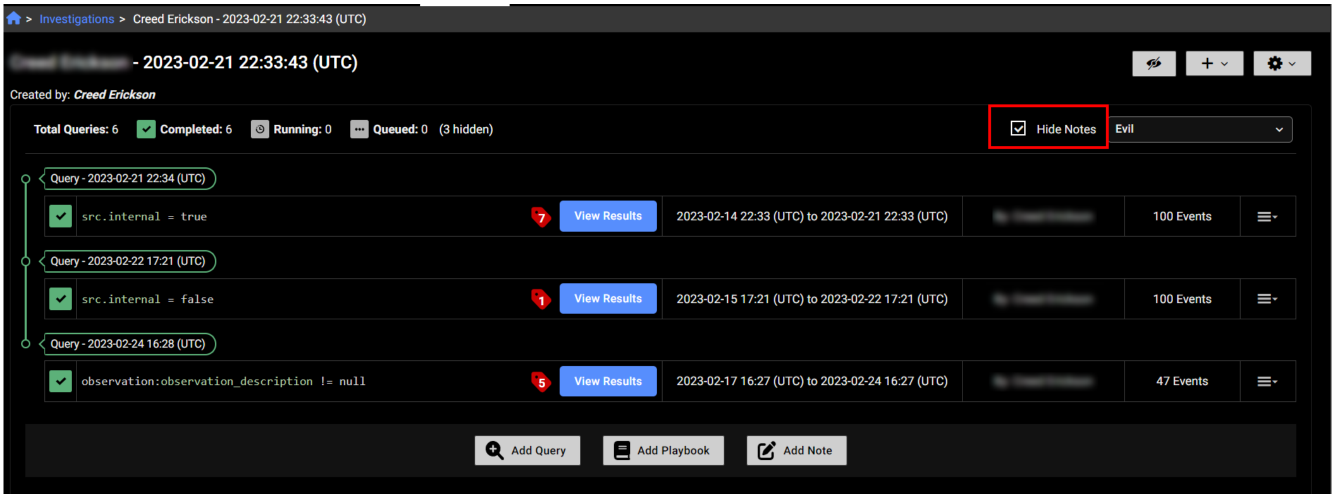
☑ Escalate

☑ Follow-up Required

☑ Include in Report

☑ Other

As you drill down in the investigation, you are able to hide notes.



Investigations > Creed Erickson - 2023-02-21 22:33:43 (UTC)

[redacted] - 2023-02-21 22:33:43 (UTC)

Created by: *Creed Erickson*

Total Queries: 6 ✓ Completed: 6 Running: 0 Queued: 0 (3 hidden)

☑ Hide Notes Evil

Query - 2023-02-21 22:34 (UTC)

```
src.internal = true
```

7 View Results 2023-02-14 22:33 (UTC) to 2023-02-21 22:33 (UTC) [redacted] 100 Events

Query - 2023-02-22 17:21 (UTC)

```
src.internal = false
```

1 View Results 2023-02-15 17:21 (UTC) to 2023-02-22 17:21 (UTC) [redacted] 100 Events

Query - 2023-02-24 16:28 (UTC)

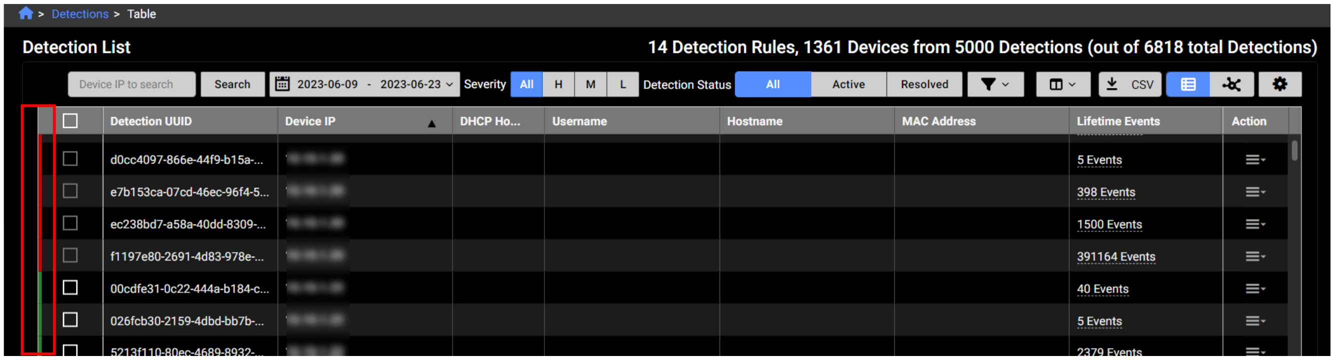
```
observation:observation_description != null
```

5 View Results 2023-02-17 16:27 (UTC) to 2023-02-24 16:27 (UTC) [redacted] 47 Events

Add Query Add Playbook Add Note

GUI improvements: Detections Table

A color-coded bar has been added to the left side of the *Detections Table*. A red bar indicates Resolved events and a green bar indicates Active events.



Detection List

14 Detection Rules, 1361 Devices from 5000 Detections (out of 6818 total Detections)

□	Detection UUID	Device IP ▲	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Action
□	d0cc4097-866e-44f9-b15a-...	[redacted]					5 Events	≡
□	e7b153ca-07cd-46ec-96f4-5...	[redacted]					398 Events	≡
□	ec238bd7-a58a-40dd-8309-...	[redacted]					1500 Events	≡
□	f1197e80-2691-4d83-978e-...	[redacted]					391164 Events	≡
□	00cdfe31-0c22-444a-b184-c...	[redacted]					40 Events	≡
□	026fcb30-2159-4dbd-bb7b-...	[redacted]					5 Events	≡
□	5213f110-80ec-4689-8932-...	[redacted]					2379 Events	≡

New detection rules and observations

The following table lists the new detections rules and observations in FortiNDR Cloud:

Name	Analytic Type	Description
Unusually High Bandwidth RDP Activity	Observation	This observation identifies a higher-than-normal volume of data exiting the device the user RDP'd into. This could indicate a user is trying to extract information from the system in an abusive use case.

12 June 2023 version 2023.5.1

FortiNDR Cloud 2023.5.1 includes bug fixes, but no new features. SeeResolved Issues on page 50.

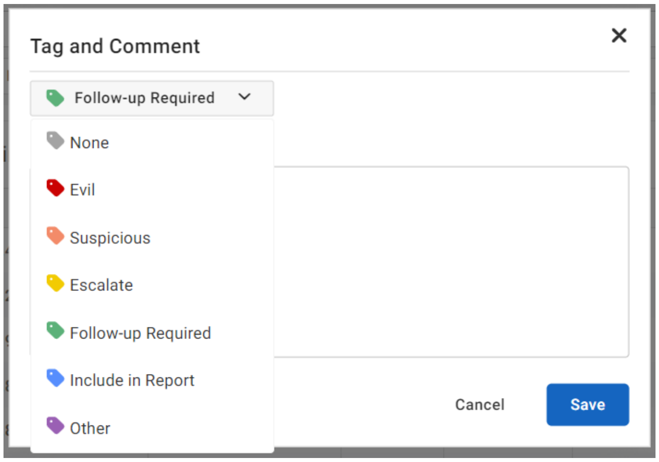
25 May 2023 version 2023.5.0

- New Functionality
  - Tag and comment events
- Improved Functionality
  - FortiNDR Cloud Sensor v1.9.0
- Resolved Issues

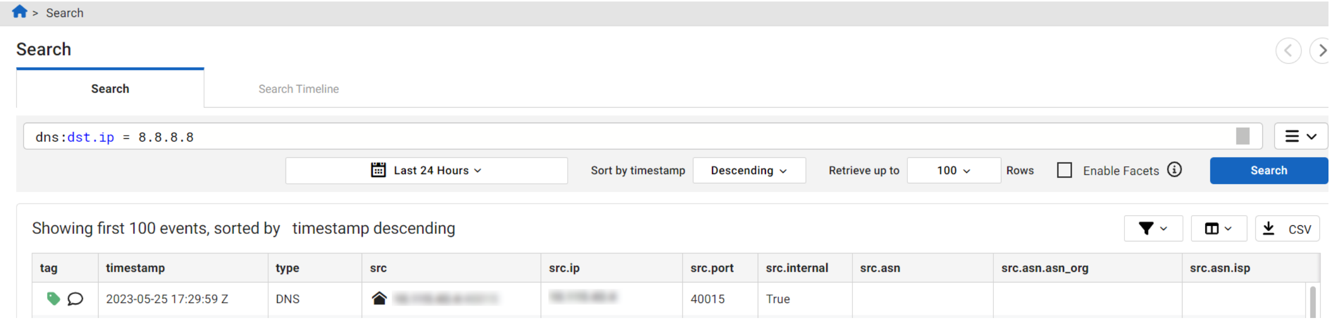
New Functionality

Tag and comment events

You can communicate with other members of the security team by adding a tag to an event in an investigation. The new Tags column is available from the investigation results and *Search Timeline* modules. To tag an event, click the *Tag* column next to the event to open the *Tag and Comment* dialog.



After the tag and comment are saved, an icon appears in the *Tag* column informing other members of team further action is required.

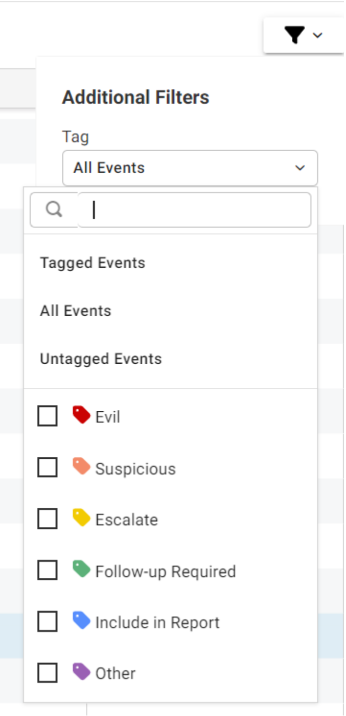


```
dns:dst.ip = 8.8.8.8
```

Showing first 100 events, sorted by timestamp descending

tag	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org	src.asn.isp
🟩 💬	2023-05-25 17:29:59 Z	DNS	[redacted]	[redacted]	40015	True			

You can also search for a tag using the *Additional Filters* dropdown.



Improved Functionality

FortiNDR Cloud Sensor v1.9.0

- The FortiNDR Cloud sensor image has been updated to version 1.9.0. For more information, see *FortiNDR Cloud sensor release notes*.

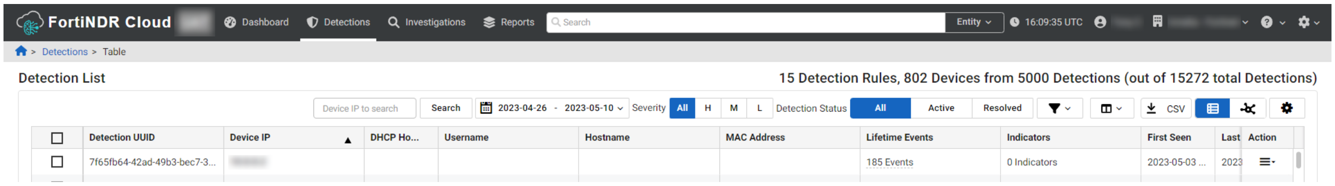
15 May 2023 version 2023.4.1

- Improved functionality
    - Detections table
- Resolved Issues

Improved functionality

Detections table

- The *Visualizer* view was added to the toolbar in the *Detections Table*.
- The total number of detections is displayed in the banner above the *Detections Table* in both *Visualizer* and *Table* views. This is useful when there are more detections that are visible in the view.



Detection List

15 Detection Rules, 802 Devices from 5000 Detections (out of 15272 total Detections)

□	Detection UUID	Device IP ▲	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last	Action
□	7f65fb64-42ad-49b3-bec7-3...	[redacted]					185 Events	0 Indicators	2023-05-03 ...	2023	≡

24 April 2023 version 2023.4

- New Functionality
    - Detections table
    - Bulk Entity Export
    - Muted Devices page
- Improved Functionality
    - Enable/Disable Subscriptions
- Resolved issues

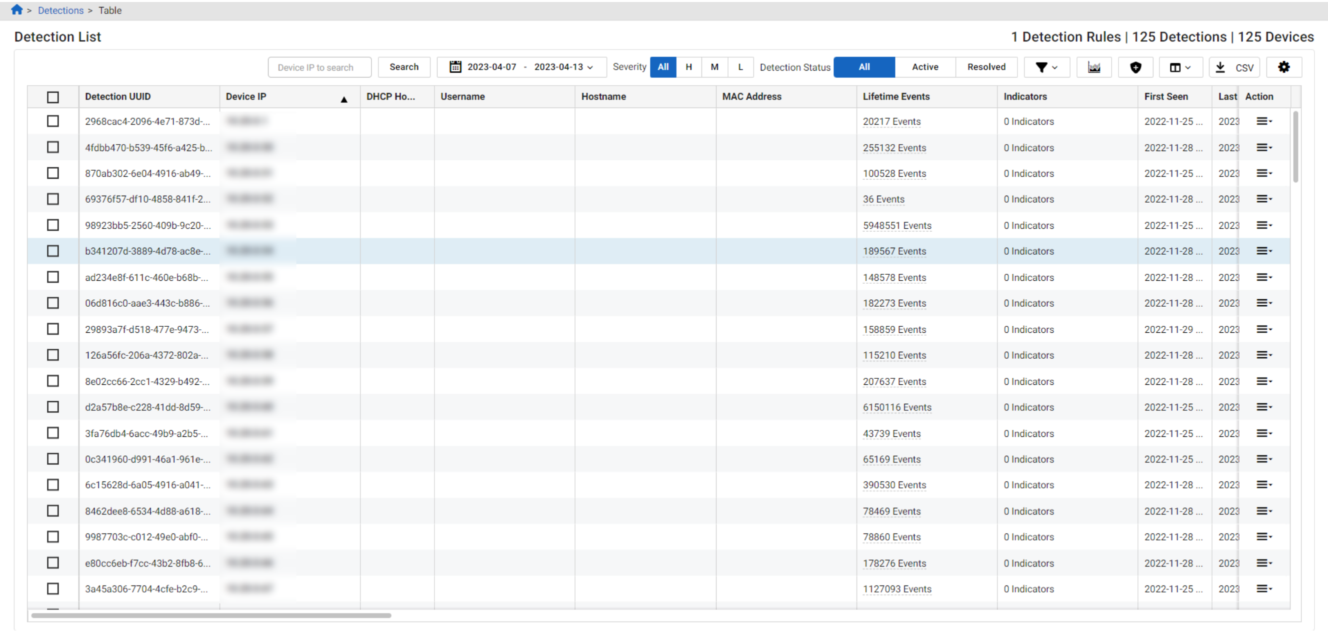
New Functionality

Detections table

The new *Detections Table* view displays the detections visible on the *MITRE ATT&CK* dashboard widget as a filterable table. By default, the table displays detections for the last two weeks and displays information about the detection and the rule. Click the link in the *Lifetime Events* column to view related pages.

To access the *Detections Table*:

- Click a detection in the *MITRE ATT&CK* dashboard widget
- Go to *Detections* > *Detections Table*.



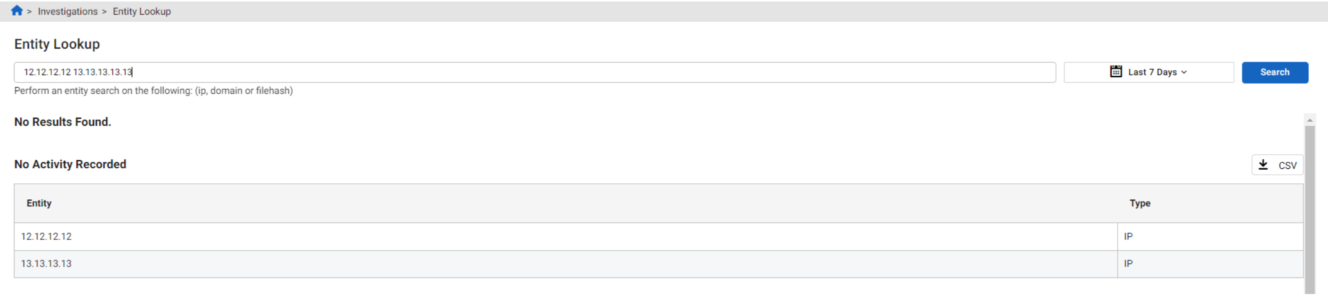
Detection List

1 Detection Rules | 125 Detections | 125 Devices

□	Detection UUID	Device IP ▲	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last	Action
□	2968cac4-2096-4e71-873d-...	[redacted]					20217 Events	0 Indicators	2022-11-25 ...	2023	≡
□	4fdbb470-b539-45f6-a425-b...	[redacted]					255132 Events	0 Indicators	2022-11-28 ...	2023	≡
□	870ab302-6e04-4916-ab49-...	[redacted]					100528 Events	0 Indicators	2022-11-25 ...	2023	≡
□	69376f57-df10-4858-841f-2...	[redacted]					36 Events	0 Indicators	2022-11-28 ...	2023	≡
□	98923bb5-2560-409b-9c20-...	[redacted]					5948551 Events	0 Indicators	2022-11-25 ...	2023	≡
□	b341207d-3889-4d78-ac8e-...	[redacted]					189567 Events	0 Indicators	2022-11-28 ...	2023	≡
□	ad234e8f-611c-460e-b68b-...	[redacted]					148578 Events	0 Indicators	2022-11-28 ...	2023	≡
□	06d816c0-aae3-443c-b886-...	[redacted]					182273 Events	0 Indicators	2022-11-28 ...	2023	≡
□	29893a7f-d518-477e-9473-...	[redacted]					158859 Events	0 Indicators	2022-11-29 ...	2023	≡
□	126a56fc-206a-4372-802a-...	[redacted]					115210 Events	0 Indicators	2022-11-28 ...	2023	≡
□	8e02cc66-2cc1-4329-b492-...	[redacted]					207637 Events	0 Indicators	2022-11-28 ...	2023	≡
□	d2a57b8e-c228-41dd-8d59-...	[redacted]					6150116 Events	0 Indicators	2022-11-25 ...	2023	≡
□	3fa76db4-6acc-49b9-a2b5-...	[redacted]					43739 Events	0 Indicators	2022-11-25 ...	2023	≡
□	0c341960-d991-46a1-961e-...	[redacted]					65169 Events	0 Indicators	2022-11-25 ...	2023	≡
□	6c15628d-6a05-4916-a041-...	[redacted]					390530 Events	0 Indicators	2022-11-28 ...	2023	≡
□	8462dee8-6534-4d88-a618-...	[redacted]					78469 Events	0 Indicators	2022-11-28 ...	2023	≡
□	9987703c-c012-49e0-abf0-...	[redacted]					78860 Events	0 Indicators	2022-11-28 ...	2023	≡
□	e80cc6eb-f7cc-43b2-8fb8-6...	[redacted]					178276 Events	0 Indicators	2022-11-28 ...	2023	≡
□	3a45a306-7704-4cfe-b2c9-...	[redacted]					1127093 Events	0 Indicators	2022-11-25 ...	2023	≡

Bulk Entity Export

The *Entity Lookup* page now supports bulk searches and exports. To use this feature, enter multiple IPs or domains in the search field separating each entity with a space. After the results are returned, you can click the *Export* button to download the data in CSV format.



Entity Lookup

12.12.12.12 13.13.13.13

Perform an entity search on the following: (ip, domain or filehash)

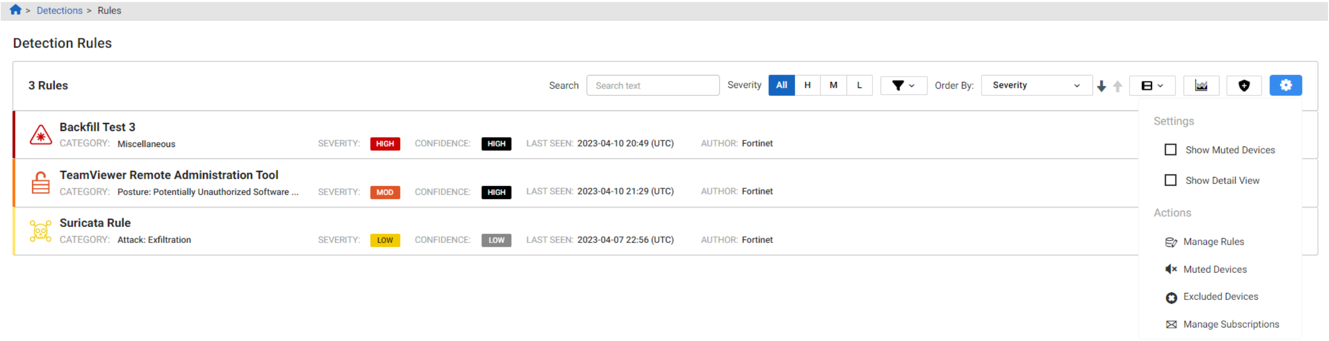
No Results Found.

No Activity Recorded

Entity	Type
12.12.12.12	IP
13.13.13.13	IP

Muted Devices page

Muted devices are now displayed in their own page. To view the *Muted Devices* page, open a rule and click the *Settings* menu and then select *Muted Devices*.



Detection Rules

3 Rules

Backfill Test 3
CATEGORY: Miscellaneous SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2023-04-10 20:49 (UTC) AUTHOR: Fortinet

TeamViewer Remote Administration Tool
CATEGORY: Posture: Potentially Unauthorized Software ... SEVERITY: MOD CONFIDENCE: HIGH LAST SEEN: 2023-04-10 21:29 (UTC) AUTHOR: Fortinet

Suricata Rule
CATEGORY: Attack: Exfiltration SEVERITY: LOW CONFIDENCE: LOW LAST SEEN: 2023-04-07 22:56 (UTC) AUTHOR: Fortinet

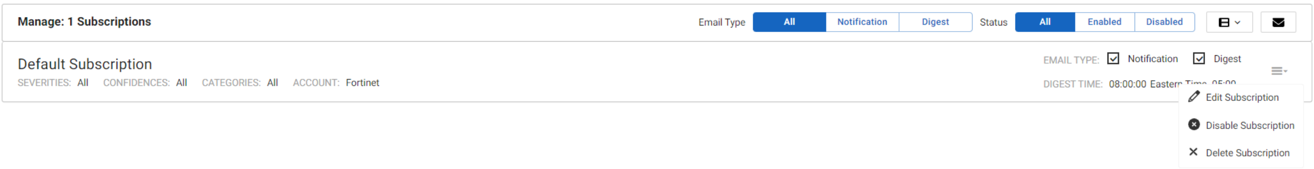
Settings
- ☐ Show Muted Devices
- ☐ Show Detail View

Actions
- Manage Rules
- Muted Devices
- Excluded Devices
- Manage Subscriptions

Improved Functionality

Enable/Disable Subscriptions

The *My Subscriptions* page has been simplified. The Disable was removed from the left side of the page. To enbable/disable click use the Actions menu at the right side of the page.



Manage: 1 Subscriptions

Default Subscription
SEVERITIES: All CONFIDENCES: All CATEGORIES: All ACCOUNT: Fortinet
EMAIL TYPE: ☑ Notification ☑ Digest
DIGEST TIME: 08:00:00 Eastern Time -05:00

- Edit Subscription
- Disable Subscription
- Delete Subscription

10 April 2023 version 2023.3.1

FortiNDR Cloud 2023.3.1 includes bug fixes but no new features were released.

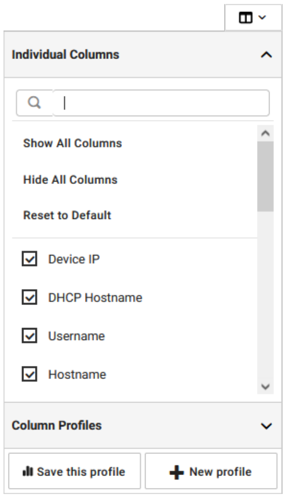
27 Mar 2023 version 2023.3

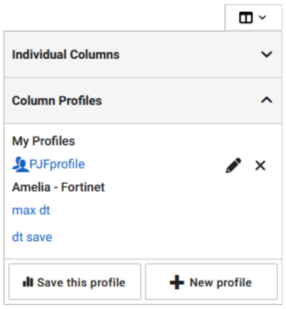
- New Functionality
  - Column profiles
  - Manage annotations
- Improved Functionality
  - Observations
  - MITRE ATT&CK drop-downs
  - Sensor release notes
- Resolved issues

New Functionality

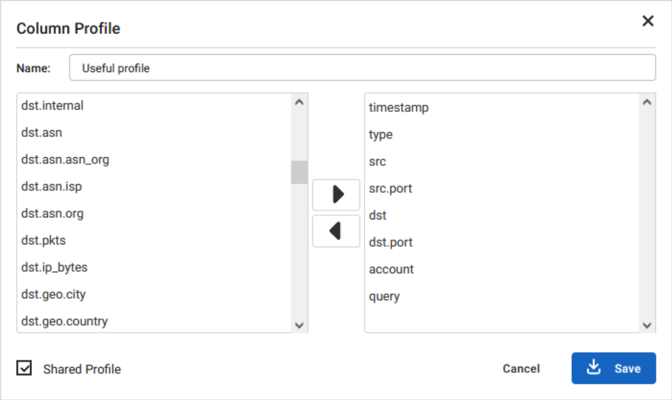
Column profiles

Custom column profiles can be created for any table that allows columns to be selected. When selecting the individual columns or column profile for a table, they are organized into groups.





Custom profiles can be shared with other users in your company by selecting *Shared Profile* when creating or editing a profile.


Column Profile

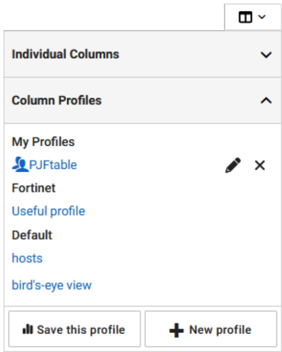
Name: Useful profile

dst.internal
dst.asn
dst.asn.asn_org
dst.asn.isp
dst.asn.org
dst.pkts
dst.ip_bytes
dst.geo.city
dst.geo.country

timestamp
type
src
src.port
dst
dst.port
account
query

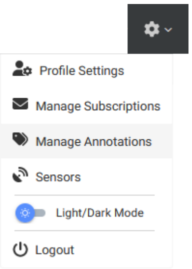
☑ Shared Profile

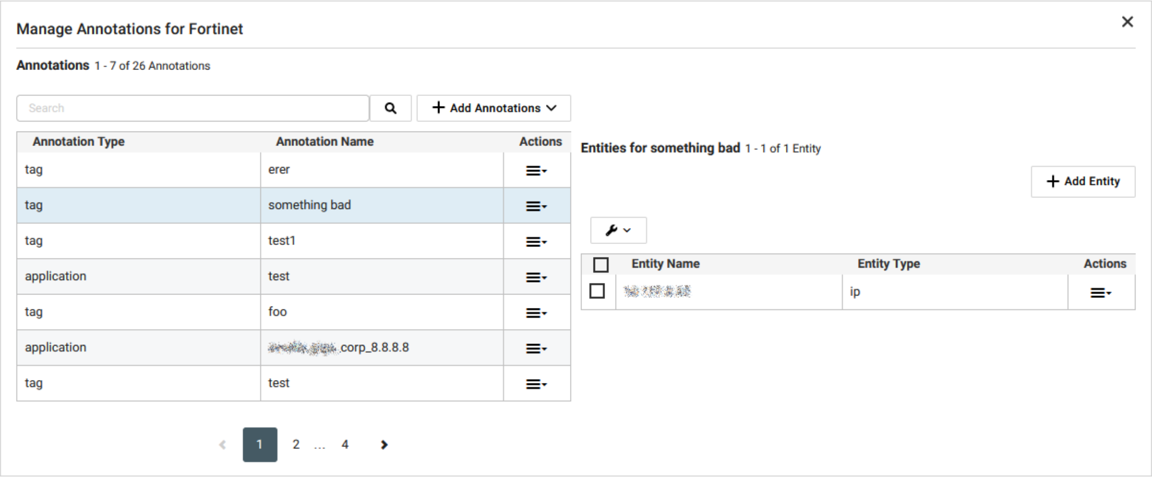
The profile will then be available to other users when they are selecting a column profile for a table.



Manage annotations

Annotations can now be accessed directly from the settings menu.





Annotations 1 - 7 of 26 Annotations

Annotation Type	Annotation Name	Actions
tag	erer	≡
tag	something bad	≡
tag	test1	≡
application	test	≡
tag	foo	≡
application	[redacted]corp_8.8.8.8	≡
tag	test	≡

‹ 1 2 … 4 ›

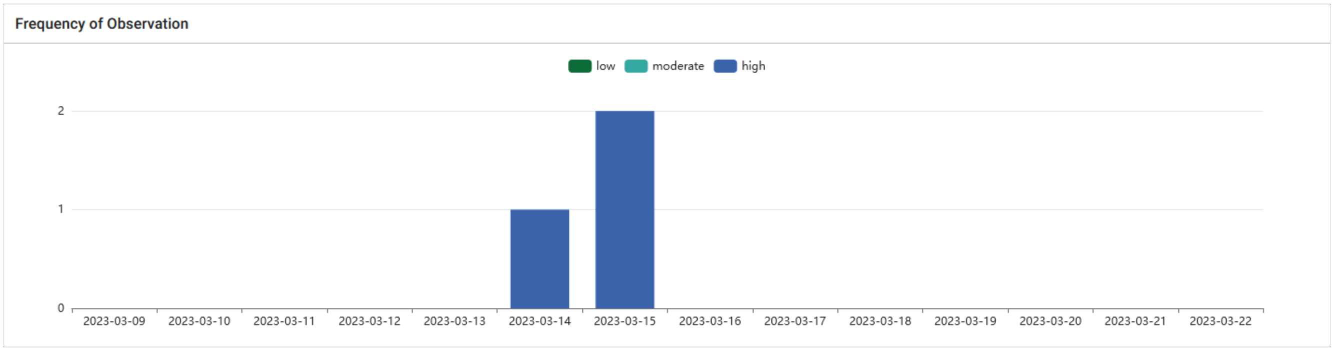
Entities for something bad 1 - 1 of 1 Entity

□	Entity Name	Entity Type	Actions
□	[redacted]	ip	≡

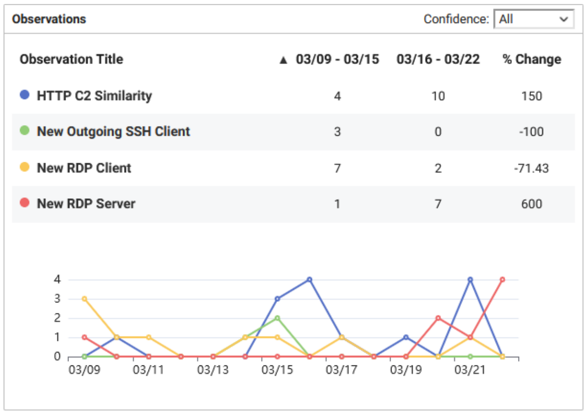
Improved Functionality

Observations

The y-axis of the Observation widget and observation details page tables no longer show decimal numbers, as all of the results are whole numbers.



The legend is removed from the bottom of the table, and instead the colored dots are next the observation titles in the observation list.



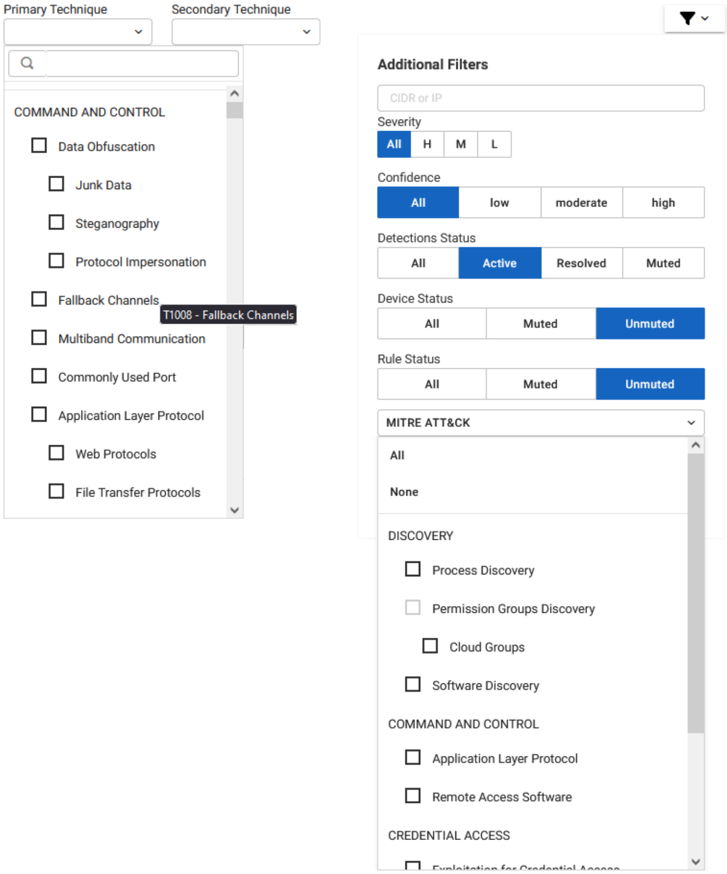
Observations — Confidence: All

Observation Title	▲ 03/09 - 03/15	03/16 - 03/22	% Change
● HTTP C2 Similarity	4	10	150
● New Outgoing SSH Client	3	0	-100
● New RDP Client	7	2	-71.43
● New RDP Server	1	7	600

MITRE ATT&CK drop-downs

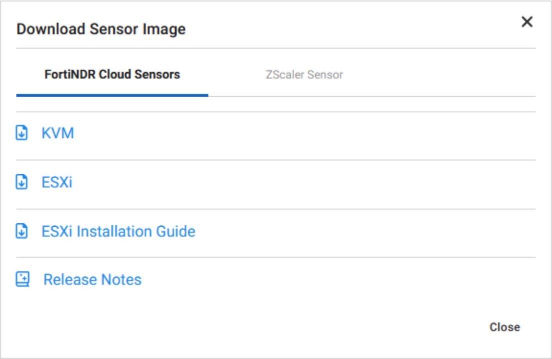
MITRE ATT&CK drop-down menus all use a tree menu to simplify selecting the requires technique or techniques. All of the techniques names are shown, and hovering over a name will show a tooltip that includes the ID and name. The MITRE ATT&CK list on the Visualizer page only shows the techniques that are present in the visualization.

The drop-downs can be searched using the ID or the name of the technique.



Sensor release notes

Sensor release notes can be accessed directly from the sensor image download page.



Download Sensor Image ✕

FortiNDR Cloud Sensors | ZScaler Sensor

- KVM
- ESXi
- ESXi Installation Guide
- Release Notes

Close

13 Mar 2023 version 2023.2.1

FortiNDR Cloud 2023.2.1 includes bug fixes, but no new features. See Resolved Issues on page 50.

27 Feb 2023 version 2023.2

- New Functionality
  - Investigations API
  - Observation descriptions
- Improved Functionality
  - Playbook access
  - Playbook time frames
  - Impacted devices table
  - Persistent investigations table
  - Flow state pop-up
  - Default investigation names
- Discontinued Functionality
  - VPC option for new detection rules
  - Legacy account version

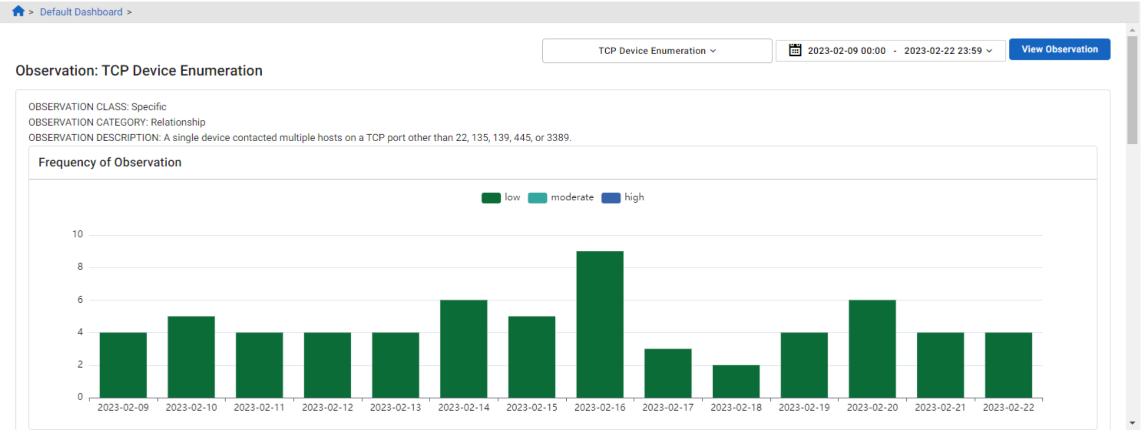
New Functionality

Investigations API

The Investigations API is a public API used to manage investigations and queries. With it, you can programmatically run queries in FortiNDR Cloud, run playbooks, and use other investigation functionality. Documentation is available upon request.

Observation descriptions

Observations include a description of the observation on the observation's detail page. The description is also available in the metastream and IQL.



Observation: TCP Device Enumeration

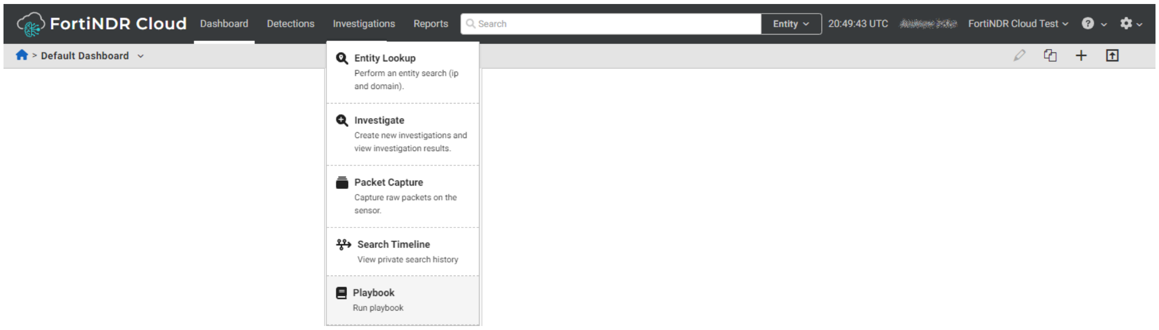
OBSERVATION CLASS: Specific
OBSERVATION CATEGORY: Relationship
OBSERVATION DESCRIPTION: A single device contacted multiple hosts on a TCP port other than 22, 135, 139, 445, or 3389.

Frequency of Observation

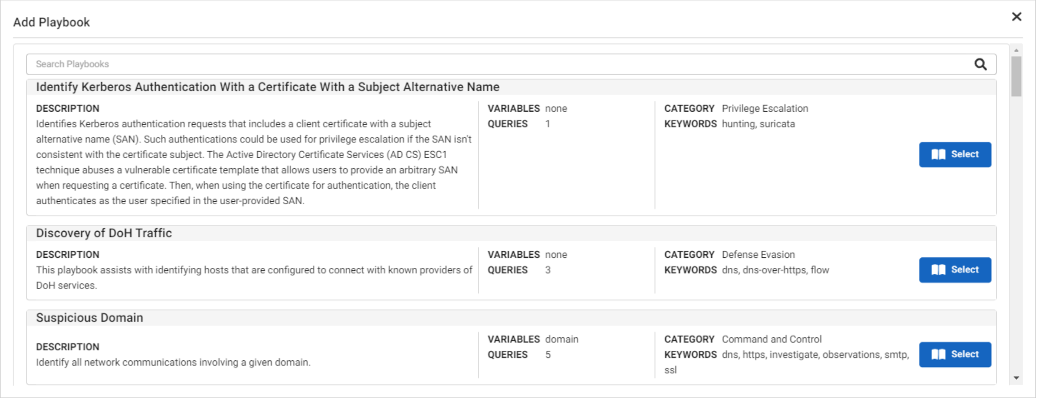
Improved Functionality

Playbook access

Playbooks can be added directly from the Investigations menu in the banner.



Clicking *Investigations* > *Playbook* opens the *Add Playbook* pop-up window.



Identify Kerberos Authentication With a Certificate With a Subject Alternative Name

DESCRIPTION
Identifies Kerberos authentication requests that includes a client certificate with a subject alternative name (SAN). Such authentications could be used for privilege escalation if the SAN isn't consistent with the certificate subject. The Active Directory Certificate Services (AD CS) ESC1 technique abuses a vulnerable certificate template that allows users to provide an arbitrary SAN when requesting a certificate. Then, when using the certificate for authentication, the client authenticates as the user specified in the user-provided SAN.

VARIABLES none
QUERIES 1

CATEGORY Privilege Escalation
KEYWORDS hunting, suricata

Select

Discovery of DoH Traffic

DESCRIPTION
This playbook assists with identifying hosts that are configured to connect with known providers of DoH services.

VARIABLES none
QUERIES 3

CATEGORY Defense Evasion
KEYWORDS dns, dns-over-https, flow

Select

Suspicious Domain

DESCRIPTION
Identify all network communications involving a given domain.

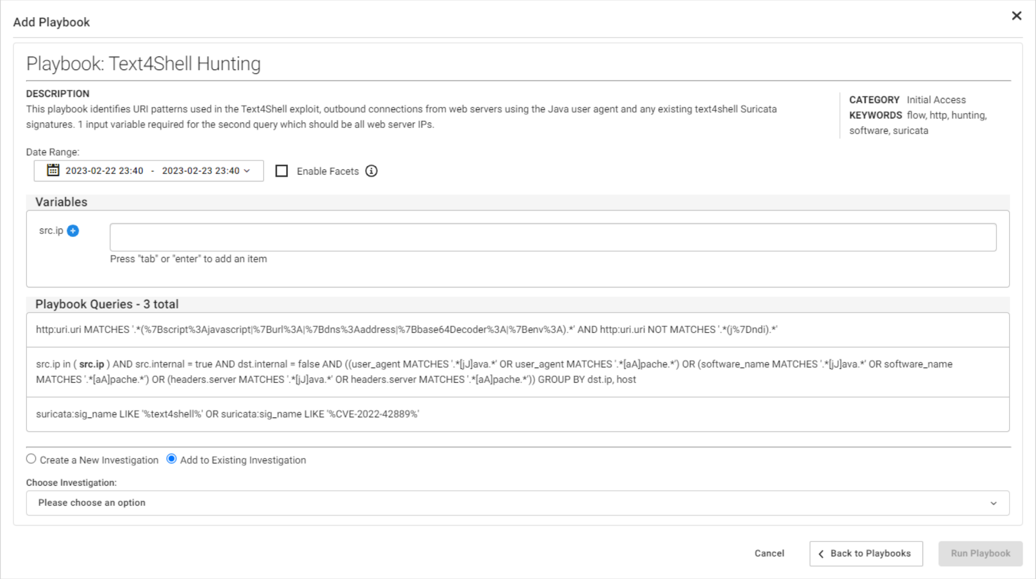
VARIABLES domain
QUERIES 5

CATEGORY Command and Control
KEYWORDS dns, https, investigate, observations, smtp, ssl

Select

Playbook time frames

The default playbook time frames are now based on the recommended time frame listed for each playbook, as opposed to defaulting to seven days for every playbook.



Add Playbook

Playbook: Text4Shell Hunting

DESCRIPTION
This playbook identifies URI patterns used in the Text4Shell exploit, outbound connections from web servers using the Java user agent and any existing text4shell Suricata signatures. 1 input variable required for the second query which should be all web server IPs.

CATEGORY Initial Access
KEYWORDS flow, http, hunting, software, suricata

Date Range: 2023-02-22 23:40 - 2023-02-23 23:40 □ Enable Facets

Variables

src.ip
Press "tab" or "enter" to add an item

Playbook Queries - 3 total

```
http:uri.uri MATCHES '.*(%7Bscript%3Ajavascript|%7Burl%3A|%7Bdns%3Aaddress|%7Bbase64Decoder%3A|%7Benv%3A).*' AND http:uri.uri NOT MATCHES '.*(j%7Dndi).*'
```

```
src.ip in ( src.ip ) AND src.internal = true AND dst.internal = false AND ((user_agent MATCHES '.*[jJ]ava.*' OR user_agent MATCHES '.*[aA]pache.*') OR (software_name MATCHES '.*[jJ]ava.*' OR software_name MATCHES '.*[aA]pache.*') OR (headers.server MATCHES '.*[jJ]ava.*' OR headers.server MATCHES '.*[aA]pache.*')) GROUP BY dst.ip, host
```

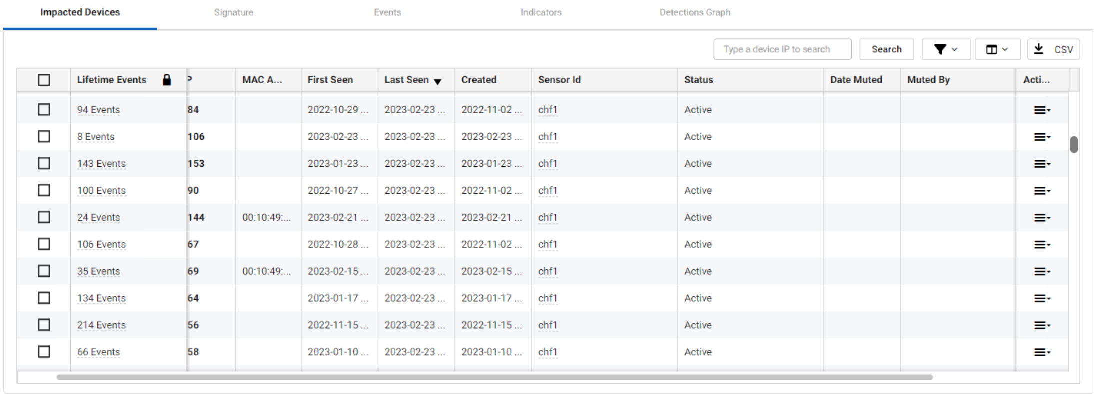
```
suricata:sig_name LIKE '%text4shell%' OR suricata:sig_name LIKE '%CVE-2022-42889%'
```

○ Create a New Investigation ● Add to Existing Investigation

Choose Investigation: Please choose an option

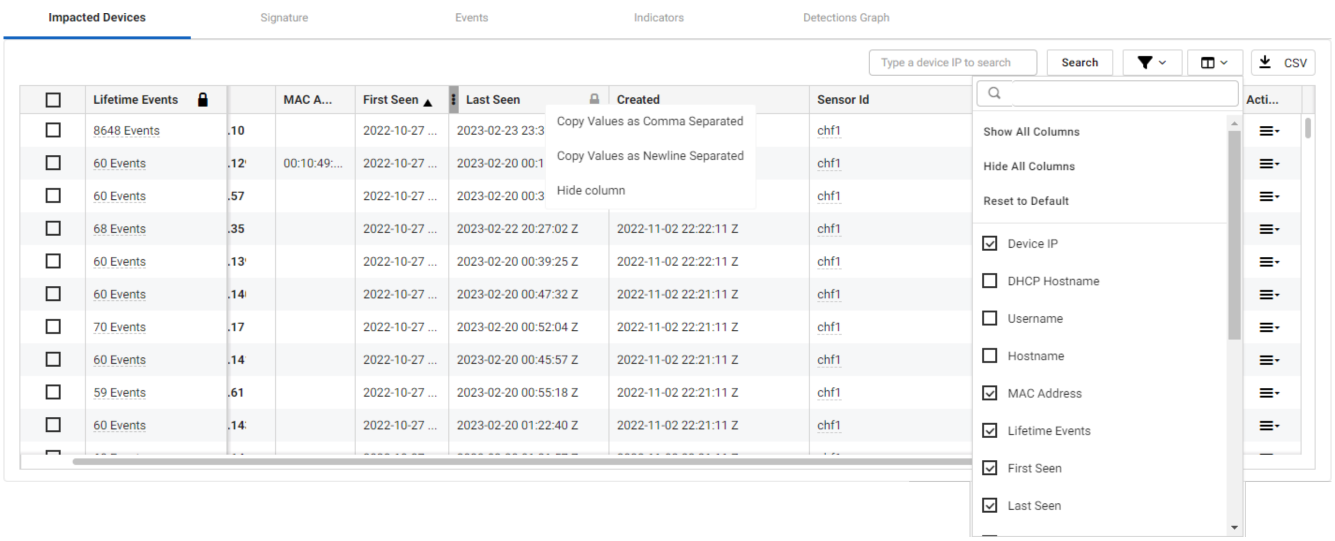
Impacted devices table

The impacted devices table is improved.



□	Lifetime Events	P	MAC A...	First Seen	Last Seen	Created	Sensor Id	Status	Date Muted	Muted By	Acti...
□	94 Events	84		2022-10-29 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active			≡
□	8 Events	106		2023-02-23 ...	2023-02-23 ...	2023-02-23 ...	chf1	Active			≡
□	143 Events	153		2023-01-23 ...	2023-02-23 ...	2023-01-23 ...	chf1	Active			≡
□	100 Events	90		2022-10-27 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active			≡
□	24 Events	144	00:10:49:...	2023-02-21 ...	2023-02-23 ...	2023-02-21 ...	chf1	Active			≡
□	106 Events	67		2022-10-28 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active			≡
□	35 Events	69	00:10:49:...	2023-02-15 ...	2023-02-23 ...	2023-02-15 ...	chf1	Active			≡
□	134 Events	64		2023-01-17 ...	2023-02-23 ...	2023-01-17 ...	chf1	Active			≡
□	214 Events	56		2022-11-15 ...	2023-02-23 ...	2022-11-15 ...	chf1	Active			≡
□	66 Events	58		2023-01-10 ...	2023-02-23 ...	2023-01-10 ...	chf1	Active			≡

- Columns can be added to and removed from the table.
- The column order and width can be adjusted by clicking and dragging the column headers.
- Columns can be locked to the left side of the table by clicking the lock icon in the column header when hovering over the header. These column will continue to be visible when you horizontally scroll through the columns in the table. The Action column is always locked to right side of the table.
- The table is not paginated; all of the rows can be seen by scrolling down.
- The table can be sorted by left clicking on a column header. Right clicking on a column gives the options to copy the column values as a comma or newline separated list, or to hide the column.
- The table layout is saved after leaving the page, and can be reset from the column selection menu.



☐	Lifetime Events		MAC A...	First Seen ▲	Last Seen	Created	Sensor Id	Acti...
☐	8648 Events	.10		2022-10-27 ...	2023-02-23 23:3		chf1	≡
☐	60 Events	.12	00:10:49:...	2022-10-27 ...	2023-02-20 00:1		chf1	≡
☐	60 Events	.57		2022-10-27 ...	2023-02-20 00:3		chf1	≡
☐	68 Events	.35		2022-10-27 ...	2023-02-22 20:27:02 Z	2022-11-02 22:22:11 Z	chf1	≡
☐	60 Events	.13		2022-10-27 ...	2023-02-20 00:39:25 Z	2022-11-02 22:22:11 Z	chf1	≡
☐	60 Events	.14		2022-10-27 ...	2023-02-20 00:47:32 Z	2022-11-02 22:21:11 Z	chf1	≡
☐	70 Events	.17		2022-10-27 ...	2023-02-20 00:52:04 Z	2022-11-02 22:21:11 Z	chf1	≡
☐	60 Events	.14		2022-10-27 ...	2023-02-20 00:45:57 Z	2022-11-02 22:21:11 Z	chf1	≡
☐	59 Events	.61		2022-10-27 ...	2023-02-20 00:55:18 Z	2022-11-02 22:21:11 Z	chf1	≡
☐	60 Events	.14		2022-10-27 ...	2023-02-20 01:22:40 Z	2022-11-02 22:21:11 Z	chf1	≡

Copy Values as Comma Separated
Copy Values as Newline Separated
Hide column

Show All Columns
Hide All Columns
Reset to Default

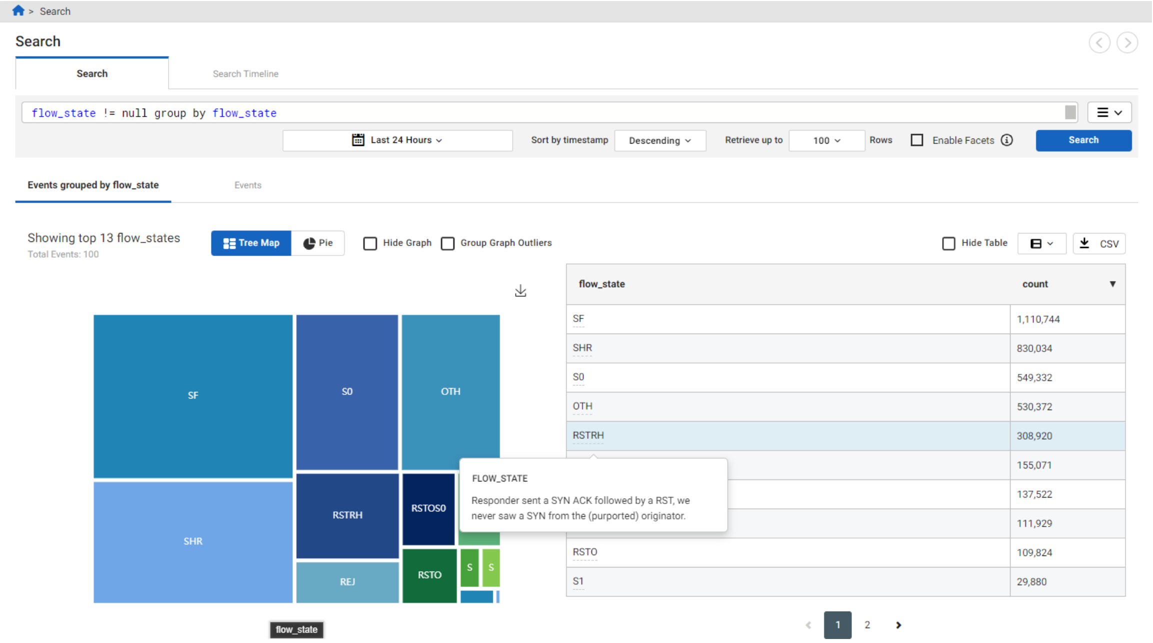
☑ Device IP
☐ DHCP Hostname
☐ Username
☐ Hostname
☑ MAC Address
☑ Lifetime Events
☑ First Seen
☑ Last Seen

Persistent investigations table

The selected sorting of the investigations table is persistent. For example, if you sort the table by date updated and then browse to a different page in the GUI, the investigations table will still be sorted by date updated when you return to the investigations page.

Flow state pop-up

After doing a timeline search, mousing over a flow state value shows a pop-up with the flow state details.



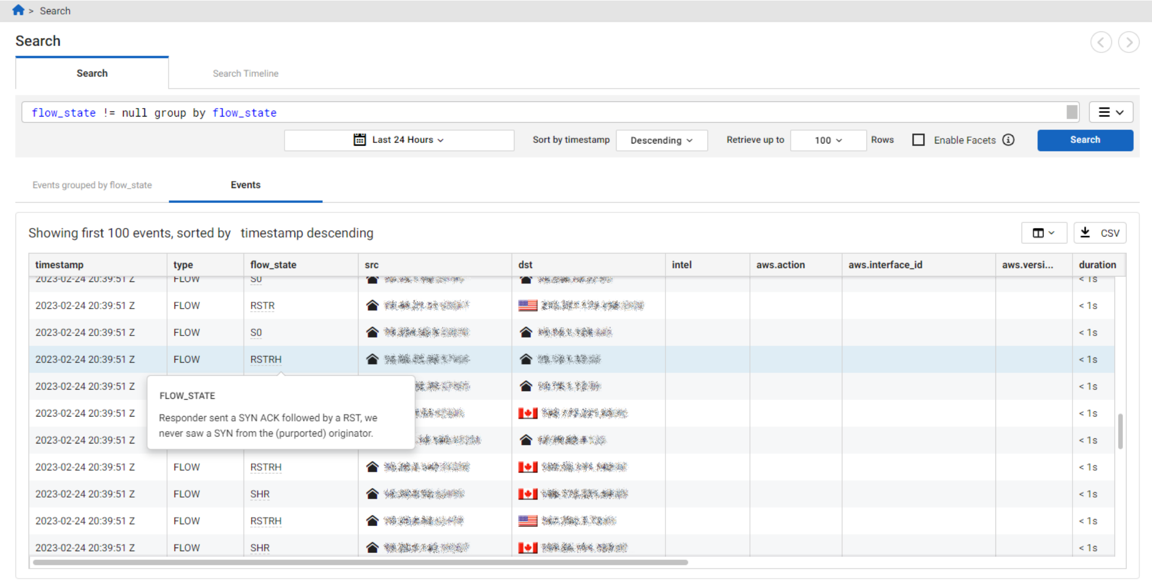
```
flow_state != null group by flow_state
```

Showing top 13 flow_states
Total Events: 100

flow_state	count ▼
SF	1,110,744
SHR	830,034
S0	549,332
OTH	530,372
RSTRH	308,920
	155,071
	137,522
	111,929
RSTO	109,824
S1	29,880

FLOW_STATE

Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.



Search

flow_state != null group by flow_state

Last 24 Hours · Sort by timestamp: Descending · Retrieve up to 100 Rows · □ Enable Facets

Events grouped by flow_state · Events

Showing first 100 events, sorted by timestamp descending

timestamp	type	flow_state	src	dst	intel	aws.action	aws.interface_id	aws.versi...	duration
2023-02-24 20:39:51 Z	FLOW	S0	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTR	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	S0	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z			[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z			[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z			[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	SHR	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	[redacted]	[redacted]					< 1s
2023-02-24 20:39:51 Z	FLOW	SHR	[redacted]	[redacted]					< 1s

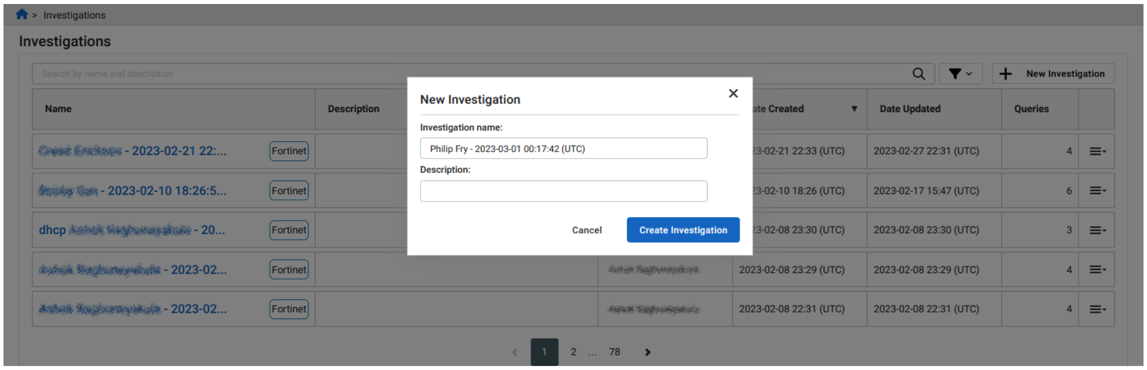
FLOW_STATE

Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.

Default investigation names

When creating a new investigation from the Investigations list view, to prevent name collisions, instead of a default name of *New Investigation*, the default name for new investigations is now the first and last name of the user that is creating the investigation with a time and date stamp of when the investigation was created.

For example: *Philip Fry - 2023-03-01 00:17:42 (UTC)*.



Investigations

New Investigation

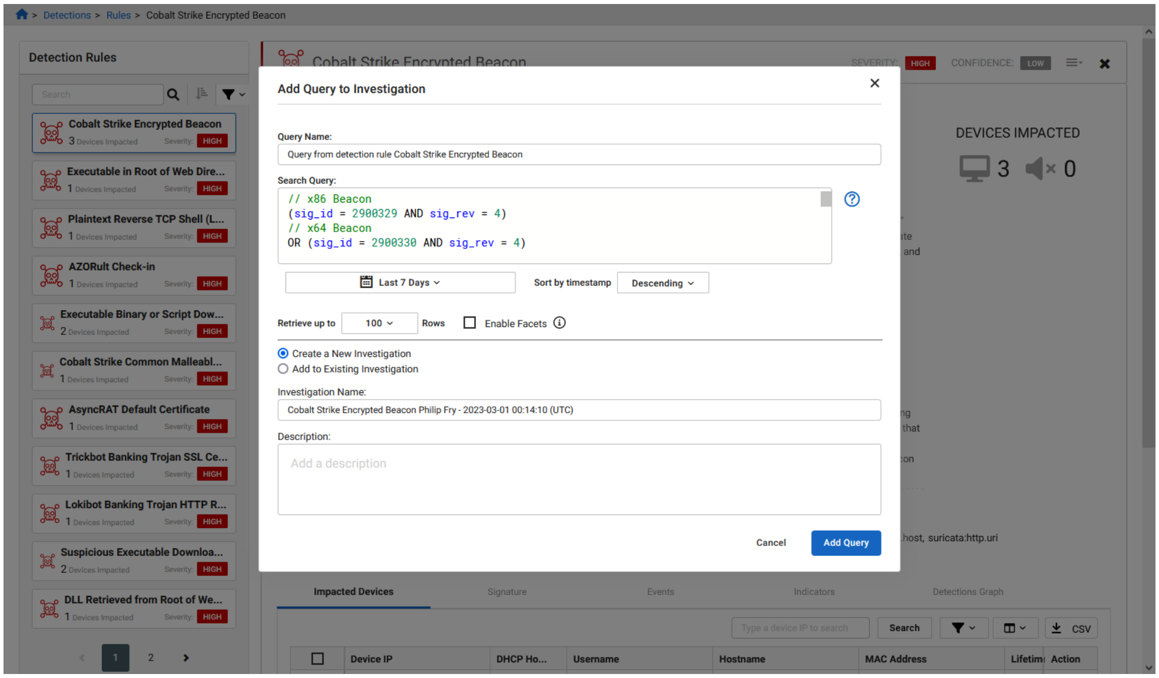
Investigation name: Philip Fry - 2023-03-01 00:17:42 (UTC)

Description:

Name	Description		ate Created ▼	Date Updated	Queries
[redacted] - 2023-02-21 22:... Fortinet			3-02-21 22:33 (UTC)	2023-02-27 22:31 (UTC)	4
[redacted] - 2023-02-10 18:26:5... Fortinet			3-02-10 18:26 (UTC)	2023-02-17 15:47 (UTC)	6
dhcp [redacted] - 20... Fortinet			3-02-08 23:30 (UTC)	2023-02-08 23:30 (UTC)	3
[redacted] - 2023-02... Fortinet		[redacted]	2023-02-08 23:29 (UTC)	2023-02-08 23:29 (UTC)	4
[redacted] - 2023-02... Fortinet		[redacted]	2023-02-08 22:31 (UTC)	2023-02-08 22:31 (UTC)	4

When creating a new investigation from a detection, to prevent the subject of the investigation from being truncated due to column width limitations, instead of a default name of *Investigation from detection rule <detection rule name>*, the default name for new investigations is now the name of the detection rule and the first and last name of the user that is creating the investigation with a time and date stamp of when the investigation was created.

For example: *Cobalt Strike Encrypted Philip Fry - 2023-03-01 00:14:10 (UTC)*.



Detections > Rules > Cobalt Strike Encrypted Beacon

Detection Rules

Rule	Devices Impacted	Severity
Cobalt Strike Encrypted Beacon	3	HIGH
Executable in Root of Web Dire...	1	HIGH
Plaintext Reverse TCP Shell (L...	1	HIGH
AZORult Check-in	1	HIGH
Executable Binary or Script Dow...	2	HIGH
Cobalt Strike Common Malleabl...	1	HIGH
AsyncRAT Default Certificate	1	HIGH
Trickbot Banking Trojan SSL Ce...	1	HIGH
Lokibot Banking Trojan HTTP R...	1	HIGH
Suspicious Executable Downloa...	2	HIGH
DLL Retrieved from Root of We...	1	HIGH

Cobalt Strike Encrypted Beacon SEVERITY: HIGH CONFIDENCE: LOW

DEVICES IMPACTED 3 0

Add Query to Investigation

Query Name: Query from detection rule Cobalt Strike Encrypted Beacon

Search Query:

```
// x86 Beacon
(sig_id = 2900329 AND sig_rev = 4)
// x64 Beacon
OR (sig_id = 2900330 AND sig_rev = 4)
```

Last 7 Days · Sort by timestamp: Descending

Retrieve up to 100 Rows · □ Enable Facets

● Create a New Investigation
○ Add to Existing Investigation

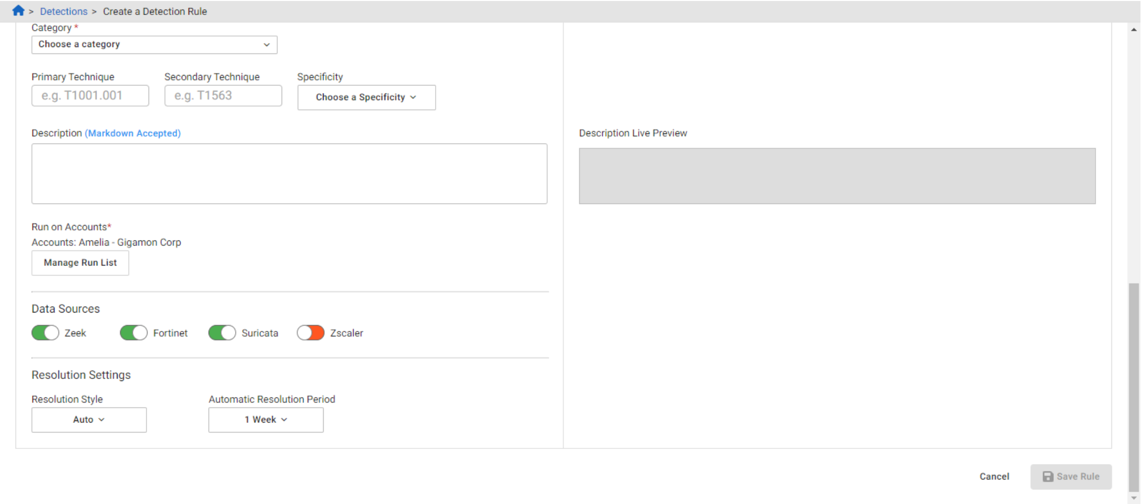
Investigation Name: Cobalt Strike Encrypted Beacon Philip Fry - 2023-03-01 00:14:10 (UTC)

Description: Add a description

Discontinued Functionality

VPC option for new detection rules

When creating a new detection rule, VPC cannot be selected as a data source.



Detections > Create a Detection Rule

Category *: Choose a category

Primary Technique: e.g. T1001.001 · Secondary Technique: e.g. T1563 · Specificity: Choose a Specificity

Description (Markdown Accepted)

Description Live Preview

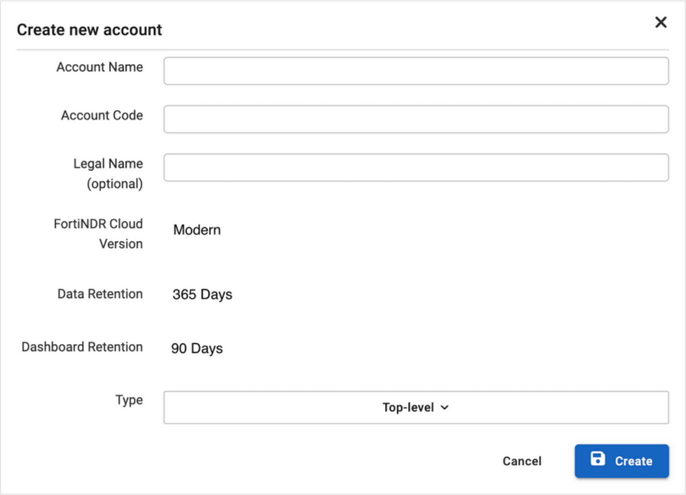
Run on Accounts*
Accounts: Amelia - Gigamon Corp

Data Sources: Zeek, Fortinet, Suricata, Zscaler

Resolution Settings
Resolution Style: Auto · Automatic Resolution Period: 1 Week

Legacy account version

When creating a new account, the FortiNDR Cloud version is set to *Modern*; *Legacy* can no longer be selected.



Create new account

Account Name	
Account Code	
Legal Name (optional)	
FortiNDR Cloud Version	Modern
Data Retention	365 Days
Dashboard Retention	90 Days
Type	Top-level

07 Feb 2023 version 2023.1.1

FortiNDR Cloud 2023.1.1 released with updated Fortinet branding. No new features were released.

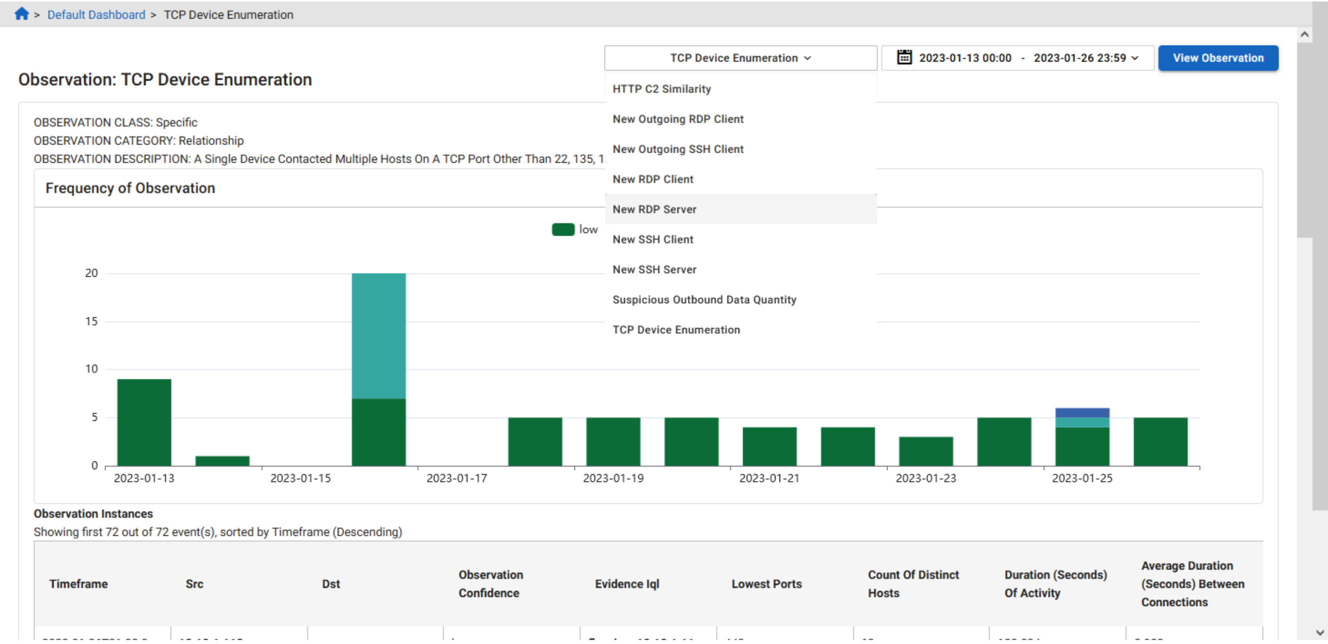
30 Jan 2023 version 2023.1

- New Functionality
  - Observation Detail Switcher
  - Forward and Back Keyboard Shortcuts
  - Bulk Entity Lookup
- Improved Functionality
  - Updated Detection API in Visualizer
  - PDNS Links on the Entity Panel

New Functionality

Observation Detail Switcher

On the Observation detail page, the observation drop down allows you to switch to other observation that are available for your account. The date range of the shown data can also be configured.

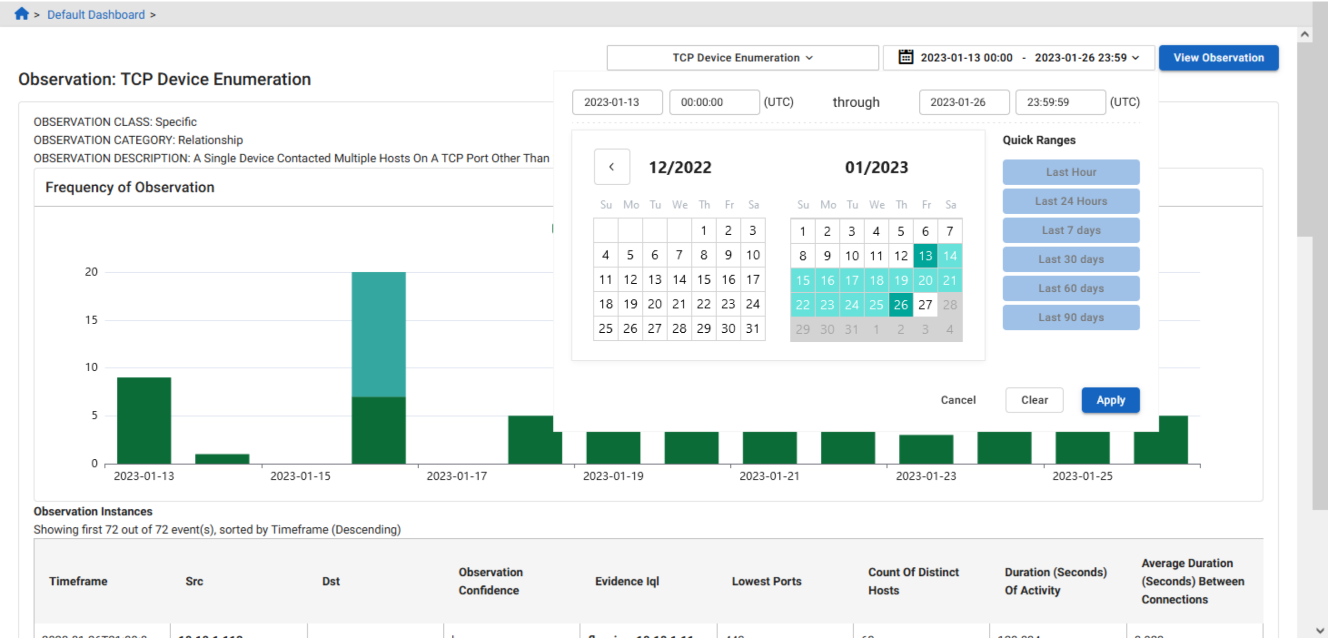


Observation: TCP Device Enumeration

OBSERVATION CLASS: Specific
OBSERVATION CATEGORY: Relationship
OBSERVATION DESCRIPTION: A Single Device Contacted Multiple Hosts On A TCP Port Other Than 22, 135, 1

Observation Instances
Showing first 72 out of 72 event(s), sorted by Timeframe (Descending)

Timeframe	Src	Dst	Observation Confidence	Evidence Iql	Lowest Ports	Count Of Distinct Hosts	Duration (Seconds) Of Activity	Average Duration (Seconds) Between Connections



Observation: TCP Device Enumeration

OBSERVATION CLASS: Specific
OBSERVATION CATEGORY: Relationship
OBSERVATION DESCRIPTION: A Single Device Contacted Multiple Hosts On A TCP Port Other Than

Observation Instances
Showing first 72 out of 72 event(s), sorted by Timeframe (Descending)

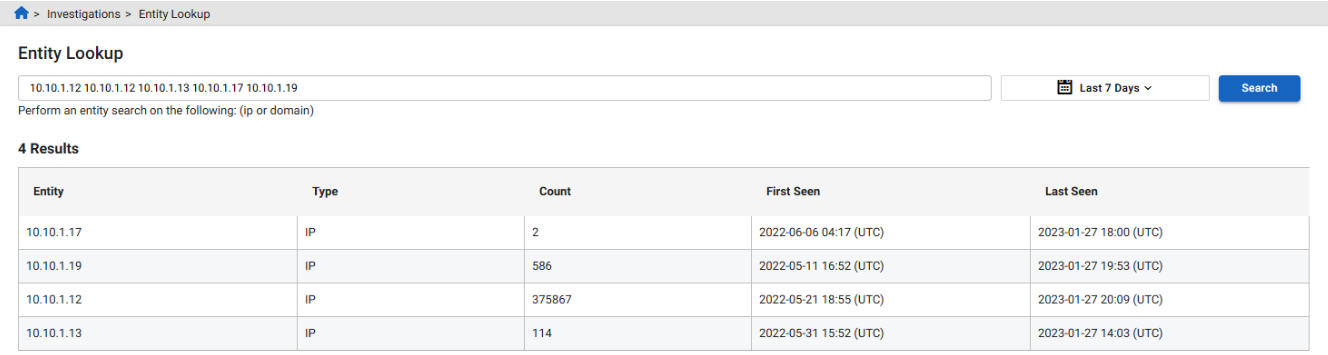
Timeframe	Src	Dst	Observation Confidence	Evidence Iql	Lowest Ports	Count Of Distinct Hosts	Duration (Seconds) Of Activity	Average Duration (Seconds) Between Connections

Forward and Back Keyboard Shortcuts

The keyboard arrow keys can be used to navigate to the previous and next query results in an investigation or ad hoc timeline when they are not active in another page element. The left arrow key navigates to the previous result, and the right arrow key navigates to the next result.

Bulk Entity Lookup

Multiple IP addresses and domain names can be looked up on the Investigation Entity Lookup page. Entries are separated by spaces.



Entity Lookup

10.10.1.12 10.10.1.12 10.10.1.13 10.10.1.17 10.10.1.19

Perform an entity search on the following: (ip or domain)

4 Results

Entity	Type	Count	First Seen	Last Seen
10.10.1.17	IP	2	2022-06-06 04:17 (UTC)	2023-01-27 18:00 (UTC)
10.10.1.19	IP	586	2022-05-11 16:52 (UTC)	2023-01-27 19:53 (UTC)
10.10.1.12	IP	375867	2022-05-21 18:55 (UTC)	2023-01-27 20:09 (UTC)
10.10.1.13	IP	114	2022-05-31 15:52 (UTC)	2023-01-27 14:03 (UTC)

Right-click on a result and select Entity Lookup to view the intelligence panes.

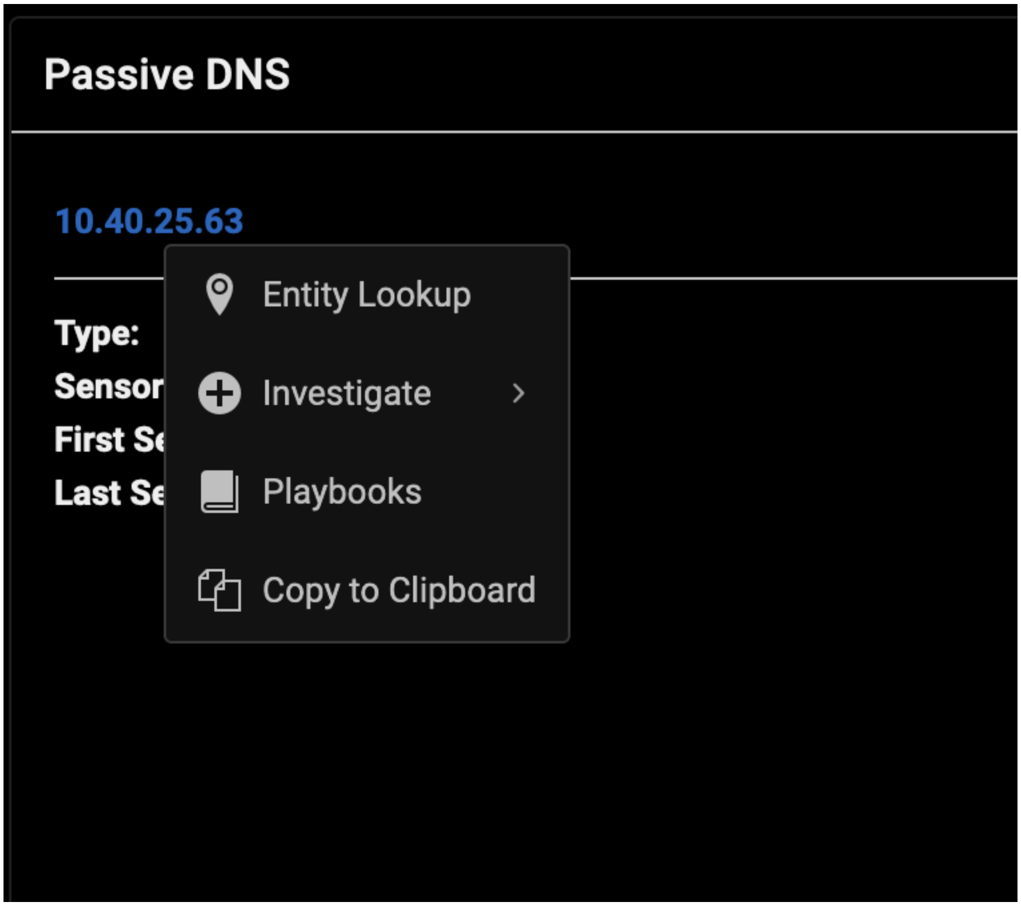
Improved Functionality

Updated Detection API in Visualizer

The time filters in the detection API are used to retrieve the detections for the selected time range, instead of retrieving all of the detections and then filtering them. This makes retrieving and filtering detections much faster. The detection limit is also increased from 1000 to 10000.

PDNS Links on the Entity Panel

PDNS links on the entity panel function like normal links. Clicking on the link replaces the entity panel with the panel for the clicked on element. Right-clicking opens a context menu.



Option	Description
Entity Lookup	Open the entity lookup page for the item.
Copy to Clipboard	Copy the item to the clipboard.
Playbooks	Launch playbooks. This options is not available for ad-hoc search result items
Investigate	Show appropriate pivots for the item type. This options is not available for ad-hoc search result items.
Search Events	Show the event searches appropriate for the type. The text in the search box is replaced, but the search will not run automatically. This options is only available for ad-hoc search result items.Types include: IP: - ip='IP' - dst.ip='IP' - src.ip='IP'domain: - domain='domain'

Resolved Issues

The following issues have been fixed in version 2023. To inquire about a particular bug, please contact Customer Service & Support.

2023.12

Description
The GUI no longer displays all users from any account in a single account view.
Billing Dashboard: On the first and second days of the month, the GUI now displays Current Month Usage is not yet available instead of No Data.
Fixed the breadcrumb thread in the My Rules page.
Admins with access to single account can no longer view messages from all accounts.
Resolved an issue where a refresh was required to view results of a specific IQL query in an investigation.
Resolved an issue where the filters in the Detections Table did not close.
The pagination in the Sensor table no longer breaks when there are too many tags.
Resolved a minor issue with the Sensor label styles.
The Edit Features settings in the Sensor details page are working as designed.
Resolved a minor issue where changes to the Sensor location setting were not being saved.
Pivoting from the Manage Rules page to the Detection Rule detail view no longer displays a rule page with empty data.
Fixed an issue where clicking Account Management in the breadcrumb displayed all users.

2023.11

An issue where the URL format was blocking SAML logins has been resolved.
The UI no longer throws an error when viewing a parent account with no children accounts.
The User Management table no longer displays all the users from all the accounts the current user has access to.

2023.10

Fixed an issue in the Detections Table where resolved detections were not being refreshed.
Updating the logic for the first time will no longer return an error in the Detections Table .
The complete domain name is no longer hidden in Entity Panel.
The Mitre Attack widget no longer returns an error when there is no in the on Rules field.

2023.9.1

Resolved an issue in the monthly billing dashboard where September disappeared and was replaced with October.
Users with access to the parent account are now able to see overall bandwidth usage without an error message.
DHCP and Mac are no longer missing for some devices
Investigation list search now shows data when a user searches from a page other than page 1.

2023.9

Description
The time range when pivoting from adhoc timeline page to search page has been fixed.
The error in Create New User has been removed.
Selecting uri search on aggregation table now shows correct query.
The Sensor api no longer throws an error in the account management page
Do not allow "include child account" unless Admin has "include child accounts" Include child account is now disabled until the Admin has enabled Include child accounts.
The alignment of the columns when the Sensor table is condensed has been fixed.

2023.8.1

Resolved an issue where logout and re-login directs user to an error page.
OSS vulnerabilities: CWE-843, CWE-915

2023.8

Observation Detail: The data displayed in the graph did not match the data displayed in the table.
Account Management: Fixed the width of Account Selection dropdown.
Billing Summary: Graph displayed incorrect bandwidth when switching accounts.
Date Picker: Error message was not appearing correctly.

2023.7

Fixed the color styling for empty table cells in dark mode.
In the child account selector, an issue with finding items in a long list has been resolved.
Portal sensor telemetry is able to display data when viewed as a group.
The Bulk Add indicator feature has been fixed.
An issue with resizing in the Investigation page has been fixed.
Resolved an issue where the sensor serial number becomes Unknown after an update.
In Detections, the custom filter test results table has been fixed.
The spacing in the date range picker has been fixed.

2023.6.1

Fixed display issues in Portal sensor telemetry view.
Improved color styling for empty columns in dark mode.
Fixed issues with the bulk indicator.
Improved user experience in the child account selector.

2023.6

Issue preventing users from accessing Account Management page has been fixed.
The Create Account button in Child Accounts tab is fixed.
Some rules will no longer display RangeError: Invalid time value when viewed from the All account

Resolved issues with Sensor Telemetry chart not showing data when Last 90 days is selected.
Unexpected behavior in custom detection has been resolved.
Fixed irregularities in Investigation List.

2023.5.1

Invalid tooltip in the Visualizer has been fixed.
Invalid dates in the date picker has been resolved.
An issue with overlapping icons in the Visualizer has been fixed.
The height selector in the Detections page has been fixed.

2023.5.0

The date picker no longer selects an invalid date when you add a query to an investigation.
The Add Notes feature in the Investigations module will no longer send blank notes.
The Enter key now works when searching annotations.
The scroll box in the Indicators in Impacted Devices pane have been improved.
Telemetry is not shown when All accounts are selected.
The rule information pane no longer takes up the entire screen in rules with long descriptions.

2023.4.1

The Detections table and Mitre-Detections widget can fetch inactive rules.
The Date Range filter in the Entity Panel shows the current range.
The row selection has been fixed in the Manage Subscription page and in Change Edit/Create Subscription Into Modal.
The digest time has been fixed in the Manage Subscription page.
The TimeZone values are now dynamic.

2023.4

Fixed styling issues for Exclude New Device dialog.
Data is copied to clipboard for the Intel field under Investigations > Events.
The Account column is no longer missing from the CSV export.
Date Picker in Adhoc search no longer shows an invalid date error for a valid date.
The Edit a excluded device/range dialog is now working as expected.
The Action column in Select New Query, no longer moves around the page.

2023.3.1

When configuring a time range, the date picker allows selecting a date outside the current month.
When managing annotations, the default resolution no longer prevents access to buttons at the bottom of the page.
Resizing a column now works as expected.
The notification widget is no longer the entire width of the browser.

2023.3

In the Resolved Detections widget, the chart no longer overlaps the legend and the chart tooltip is now constrained within the chart.
Could not add spaces to search fields in drop-down lists with checkboxes.
When adding a new query to an investigation, the date range picker now displays the correct date range.
On the Reports page, the date range picker now uses UTC instead of local time.
Packet capture breadcrumb links now work as expected.

2023.2.1

On detection details pages, the Devices Impacted number was not updated after a Bulk Resolve Detections.
Updated links to ISO images and documentation from the sensor ISO image download pane.
Extraneous This dashboard does not exist notification no longer displayed after deleting a dashboard.

Ad hoc queries can be saved from the action drop-down menu.
OSS vulnerabilities: CWE-843, CWE-915.

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.