Vectra AI Platform

Advanced Investigation QuickStart Guide

Version 1.5

Table of Contents

What is Vectra Investigate? 2

Before you begin 2

How to create and run a query 2

How to add or remove filters 4

How to modify the query's search period 6

How to add/remove and re-order columns in the results 7

How to run a query from Instant Investigation 9

Query Examples 10

- Investigating an Azure AD attack with Powershell 10
- Investigating a Microsoft 365 attack with Power Automate 12
- All activity around a specific AWS EC2 instance 14
- AWS activity performed with an assumed role 15
- AWS activity performed with an assumed role on a different region 16

Troubleshooting 16

- “Search could not be completed” or “Search timed out” 16
- “Search could not be completed” (with error id) 19
- “Something went wrong” 20

Related articles 20

What is Vectra Investigate?

Advanced Investigation (or *Investigate* in the SaaS UI) provides more details and context into Indicators of Compromise (IOC) associated with detections, by allowing customers to explore Azure AD, M365 or AWS Control Plane logs directly within our platform.

With this feature, users can create a query (or search) to narrow down results as part of their incident analysis.

In this QuickStart Guide we will also provide some examples to help get you started with this feature.

Before you begin

Please note that to be able to run a query for AWS, you must first create a CDR for AWS connection in the *Data Sources* section of your UI. To learn more please see: *Vectra CDR for AWS Deployment Guide*

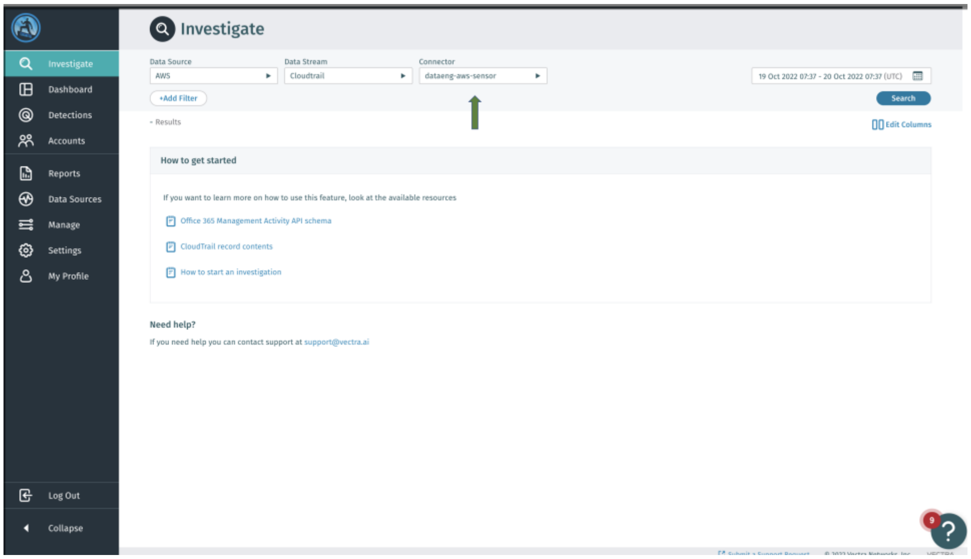
To be able to create queries for Azure AD & M365, you need to create a Azure AD & M365 connection in the *Data Sources* section of your UI. To learn more please see: *IDR for Azure AD and CDR for M365 Quick Start Guide*

To be able to create queries for Network, you need to create a Network sensor in the Data Sources section of your UI. To learn more please see: *Vectra Respond UX Deployment Guide*

How to create and run a query

1. Log in to your Vectra SaaS instance and navigate to *Investigate.* Select the Data Source, Data Stream and Connector you plan to investigate. *Please check the "Before you Begin" section in this document if you don't have a connector.*

If your query is for Network metadata, you will only need to select the Data Source and Data Stream.



Data Source: AWS

Data Stream: Cloudtrail

Connector: dataeng-aws-sensor

19 Oct 2022 07:37 - 20 Oct 2022 07:37 (UTC)

- Results

How to get started

If you want to learn more on how to use this feature, look at the available resources

Office 365 Management Activity API schema

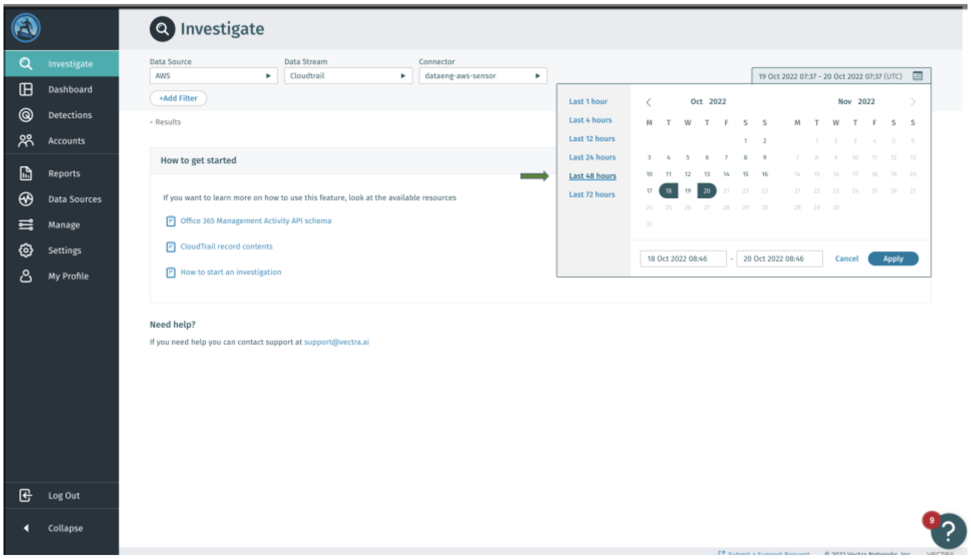
CloudTrail record contents

How to start an investigation

Need help?

If you need help you can contact support at support@vectra.ai

2. Select the search period for your query and click Apply.



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: dataeng-aws-sensor

+Add Filter

- Results

How to get started

If you want to learn more on how to use this feature, look at the available resources

- Office 365 Management Activity API schema
- CloudTrail record contents
- How to start an investigation

Need help?

If you need help you can contact support at support@vectra.ai

19 Oct 2022 07:37 - 20 Oct 2022 07:37 (UTC)

Last 1 hour
Last 4 hours
Last 12 hours
Last 24 hours
Last 48 hours
Last 72 hours

Oct 2022

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

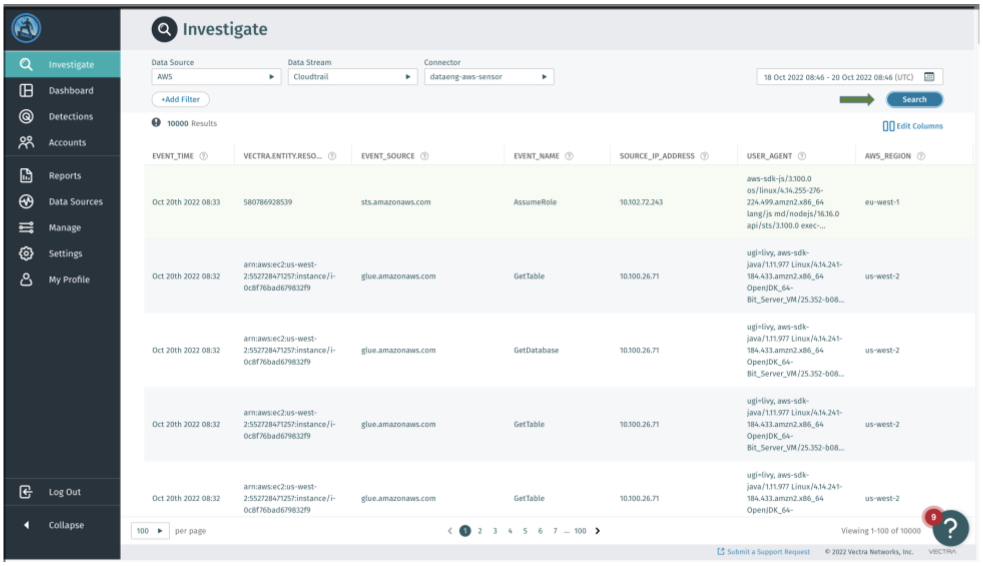
Nov 2022

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

18 Oct 2022 08:46 - 20 Oct 2022 08:46

Cancel   Apply

3. Click on the Search button.



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: dataeng-aws-sensor

18 Oct 2022 08:46 - 20 Oct 2022 08:46 (UTC)

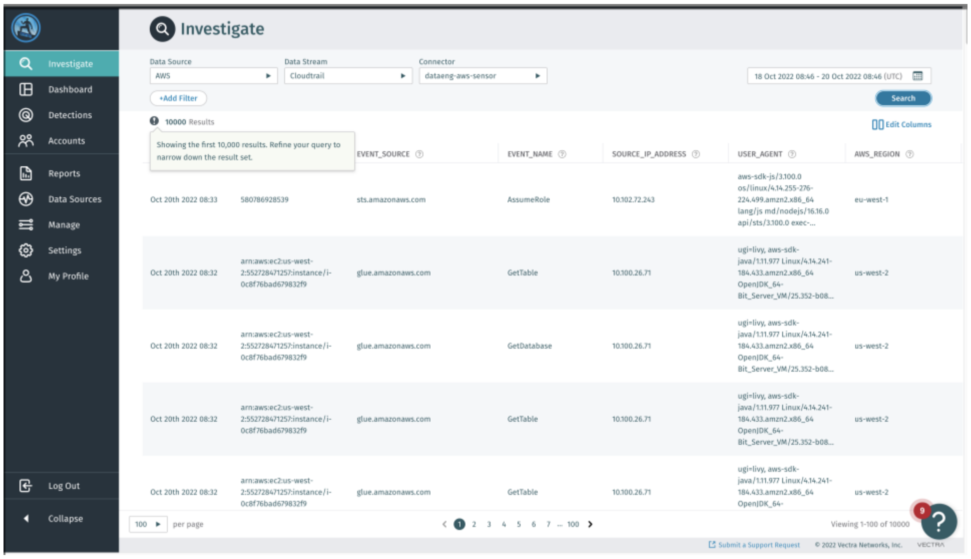
+Add Filter   Search

10000 Results   Edit Columns

EVENT_TIME	VECTRA.ENTITY.RESO...	EVENT_SOURCE	EVENT_NAME	SOURCE_IP_ADDRESS	USER_AGENT	AWS_REGION
Oct 20th 2022 08:33	580786928539	sts.amazonaws.com	AssumeRole	10.102.72.243	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-...	eu-west-1
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetDatabase	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-	us-west-2

100 per page   ‹ 1 2 3 4 5 6 7 ... 100 ›   Viewing 1-100 of 10000

4. The results' view will display 10000 results, starting by the most recent events.



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: dataeng-aws-sensor

18 Oct 2022 08:46 - 20 Oct 2022 08:46 (UTC)

+Add Filter   Search

10000 Results   Edit Columns

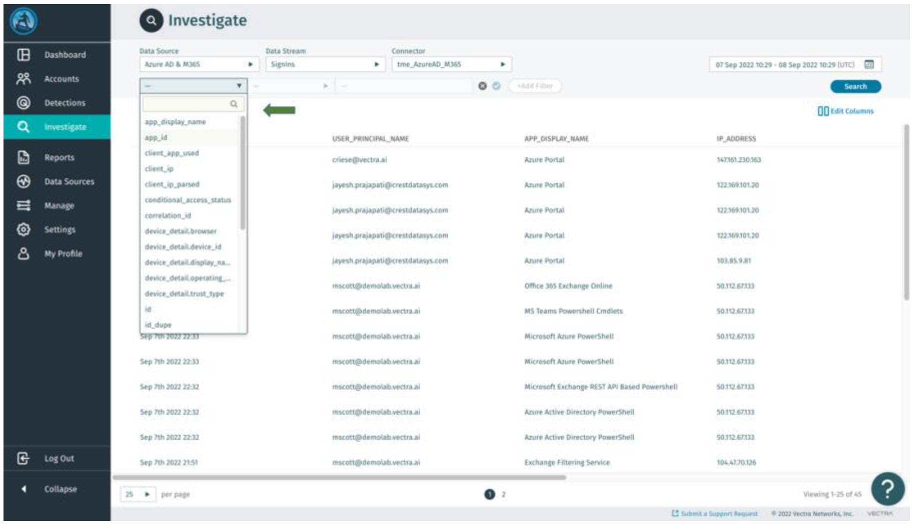
Showing the first 10,000 results. Refine your query to narrow down the result set.

		EVENT_SOURCE	EVENT_NAME	SOURCE_IP_ADDRESS	USER_AGENT	AWS_REGION
Oct 20th 2022 08:33	580786928539	sts.amazonaws.com	AssumeRole	10.102.72.243	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-...	eu-west-1
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetDatabase	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.352-b08...	us-west-2
Oct 20th 2022 08:32	arn:aws:ec2:us-west-2:552728471257:instance/i-0c8f76bad679832f9	glue.amazonaws.com	GetTable	10.100.26.71	ugi=livy, aws-sdk-java/1.11.977 Linux/4.14.241-184.433.amzn2.x86_64 OpenJDK_64-	us-west-2

100 per page   ‹ 1 2 3 4 5 6 7 ... 100 ›   Viewing 1-100 of 10000

How to add or remove filters

1. Click on the *Add Filter* button and select the field to use from the dropdown menu.



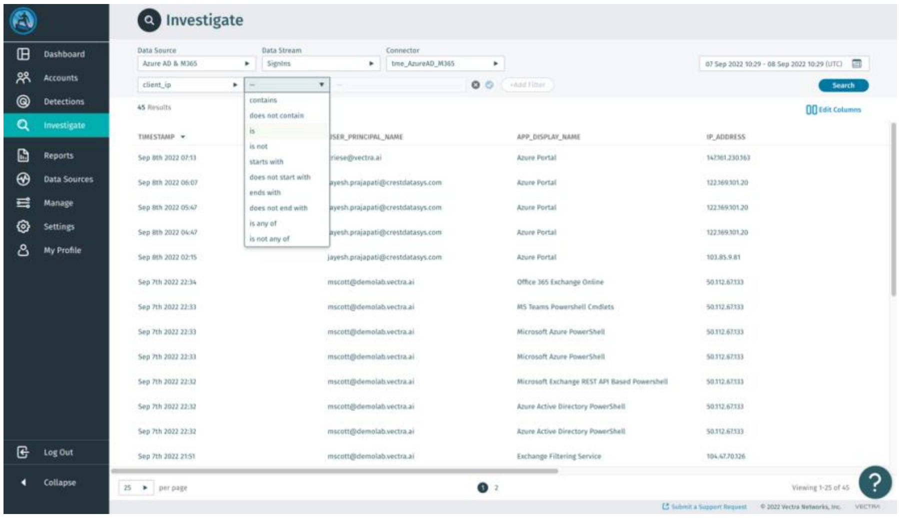
Data Source: Azure AD & M365
Data Stream: Signins
Connector: tme_AzureAD_M365
07 Sep 2022 10:29 - 08 Sep 2022 10:29 (UTC)

	USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	IP_ADDRESS
	criese@vectra.ai	Azure Portal	147.161.230.163
	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
	jayesh.prajapati@crestdatasys.com	Azure Portal	103.85.9.81
	mscott@demolab.vectra.ai	Office 365 Exchange Online	50.112.67.133
	mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 21:51	mscott@demolab.vectra.ai	Exchange Filtering Service	104.47.70.126

25 per page 1 2 Viewing 1-25 of 45

Submit a Support Request © 2022 Vectra Networks, Inc. VECTRA

2. Select the operator to use from the dropdown menu.



Data Source: Azure AD & M365
Data Stream: Signins
Connector: tme_AzureAD_M365
client_ip
07 Sep 2022 10:29 - 08 Sep 2022 10:29 (UTC)

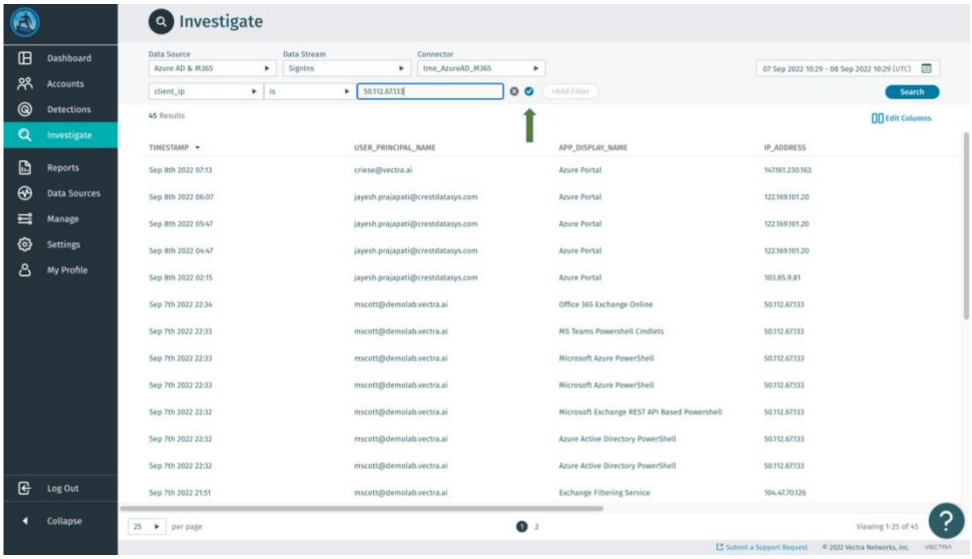
45 Results

TIMESTAMP	USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	IP_ADDRESS
Sep 8th 2022 07:13	criese@vectra.ai	Azure Portal	147.161.230.163
Sep 8th 2022 06:07	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 05:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 04:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 02:15	jayesh.prajapati@crestdatasys.com	Azure Portal	103.85.9.81
Sep 7th 2022 22:34	mscott@demolab.vectra.ai	Office 365 Exchange Online	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 21:51	mscott@demolab.vectra.ai	Exchange Filtering Service	104.47.70.126

25 per page 1 2 Viewing 1-25 of 45

Submit a Support Request © 2022 Vectra Networks, Inc. VECTRA

3. Enter the value (in this example, an IP address of interest) and click on the check button on the right of the entered value field to add the filter.



Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
07 Sep 2022 10:29 - 08 Sep 2022 10:29 (UTC)

client_ip · is · 50.112.67.133

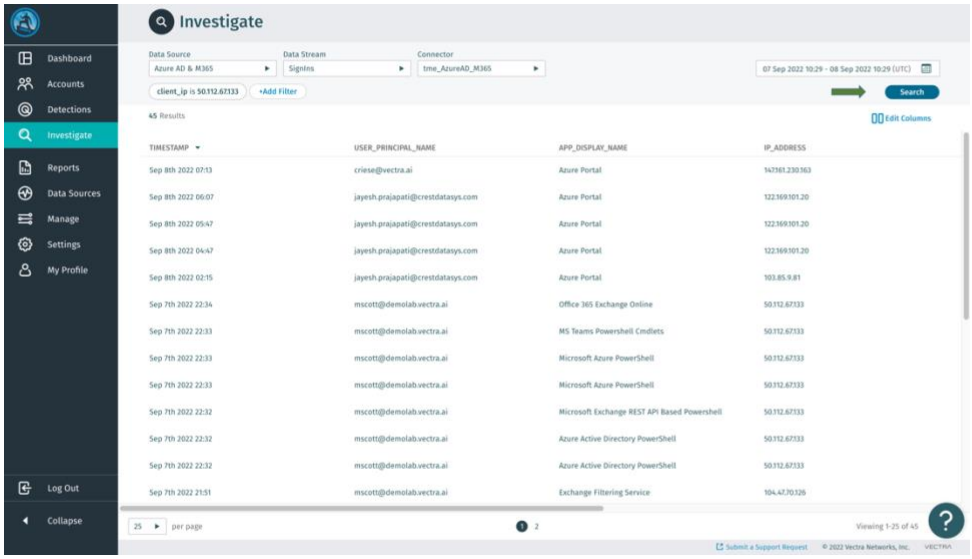
45 Results

TIMESTAMP	USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	IP_ADDRESS
Sep 8th 2022 07:13	criese@vectra.ai	Azure Portal	147.161.230.163
Sep 8th 2022 06:07	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 05:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 04:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 02:15	jayesh.prajapati@crestdatasys.com	Azure Portal	103.85.9.81
Sep 7th 2022 22:34	mscott@demolab.vectra.ai	Office 365 Exchange Online	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 21:51	mscott@demolab.vectra.ai	Exchange Filtering Service	104.47.70.126

25 per page · 1 2 · Viewing 1-25 of 45

© 2022 Vectra Networks, Inc.

4. Click on the *Search* button.



Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
07 Sep 2022 10:29 - 08 Sep 2022 10:29 (UTC)

client_ip is 50.112.67.133

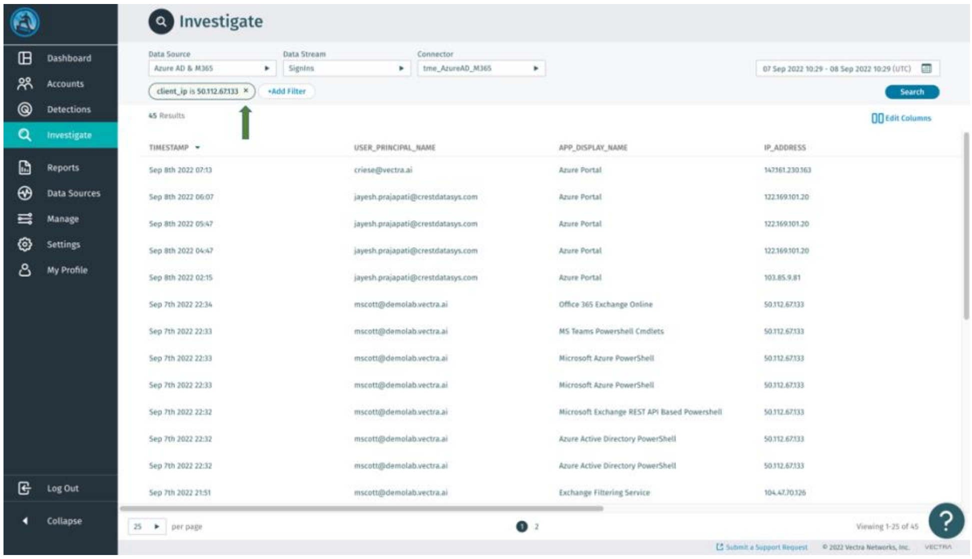
45 Results

TIMESTAMP	USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	IP_ADDRESS
Sep 8th 2022 07:13	criese@vectra.ai	Azure Portal	147.161.230.163
Sep 8th 2022 06:07	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 05:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 04:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 02:15	jayesh.prajapati@crestdatasys.com	Azure Portal	103.85.9.81
Sep 7th 2022 22:34	mscott@demolab.vectra.ai	Office 365 Exchange Online	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 21:51	mscott@demolab.vectra.ai	Exchange Filtering Service	104.47.70.126

25 per page · 1 2 · Viewing 1-25 of 45

© 2022 Vectra Networks, Inc.

5. To remove a filter hover on the statement that contains the filter to be removed and click on the *X* on the right of the filter. Click on the *Search* button again to run the search with the new parameters.



Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
07 Sep 2022 10:29 - 08 Sep 2022 10:29 (UTC)

client_ip is 50.112.67.133 ×

45 Results

TIMESTAMP	USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	IP_ADDRESS
Sep 8th 2022 07:13	criese@vectra.ai	Azure Portal	147.161.230.163
Sep 8th 2022 06:07	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 05:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 04:47	jayesh.prajapati@crestdatasys.com	Azure Portal	122.169.101.20
Sep 8th 2022 02:15	jayesh.prajapati@crestdatasys.com	Azure Portal	103.85.9.81
Sep 7th 2022 22:34	mscott@demolab.vectra.ai	Office 365 Exchange Online	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:33	mscott@demolab.vectra.ai	Microsoft Azure PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 22:32	mscott@demolab.vectra.ai	Azure Active Directory PowerShell	50.112.67.133
Sep 7th 2022 21:51	mscott@demolab.vectra.ai	Exchange Filtering Service	104.47.70.126

25 per page · 1 2 · Viewing 1-25 of 45

© 2022 Vectra Networks, Inc.

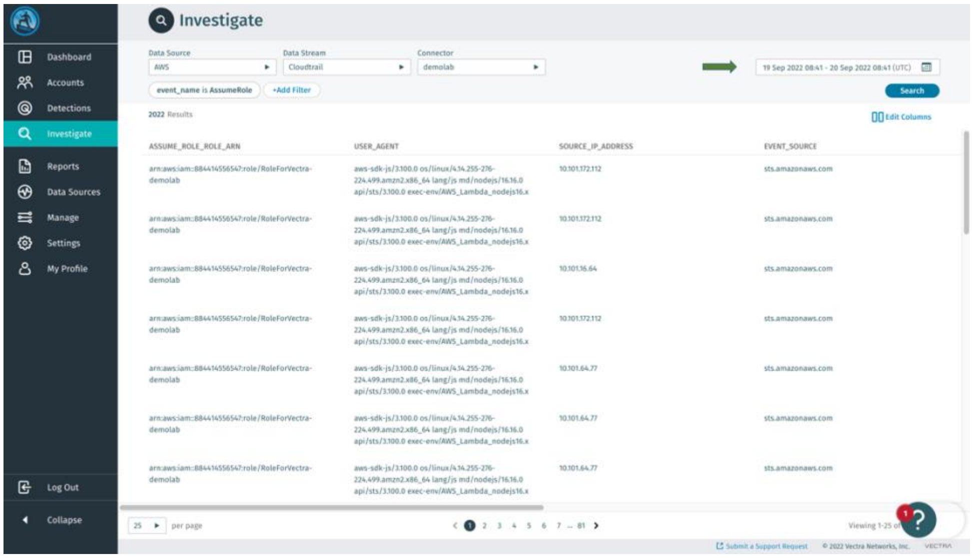
How to modify the query's search period

The default search period for running queries is set at 'Last 6 hours.' In this section, we will explain how to customize this default search period.

Another critical timeframe to consider for metadata searches is the retention period. This period represents the maximum number of days that Vectra retains customer data. By default, this retention period is set at 72 hours. However, customers have the option to extend the metadata retention period by purchasing either a 14 or 30-day license.

To modify the search period:

1. Click on the time picker located on the top right side of the screen to select the search period you would like to use for the query and click on the *Apply* button. In this case we've selected the last 4 hours.



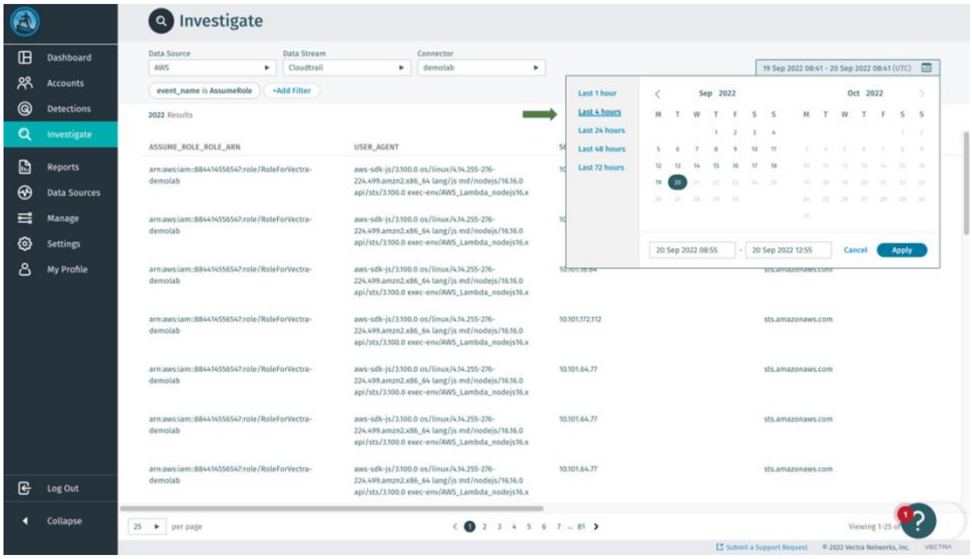
Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
19 Sep 2022 08:41 - 20 Sep 2022 08:41 (UTC)
event_name is AssumeRole

2022 Results

ASSUME_ROLE_ROLE_ARN	USER_AGENT	SOURCE_IP_ADDRESS	EVENT_SOURCE
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.172.112	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.172.112	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.16.64	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.172.112	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com

25 per page ‹ 1 2 3 4 5 6 7 ... 81 › Viewing 1-25 of

2. Click on the *Search* button, and only entries within the selected search period will be displayed.



Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
19 Sep 2022 08:41 - 20 Sep 2022 08:41 (UTC)
event_name is AssumeRole
20 Sep 2022 08:55 - 20 Sep 2022 12:55

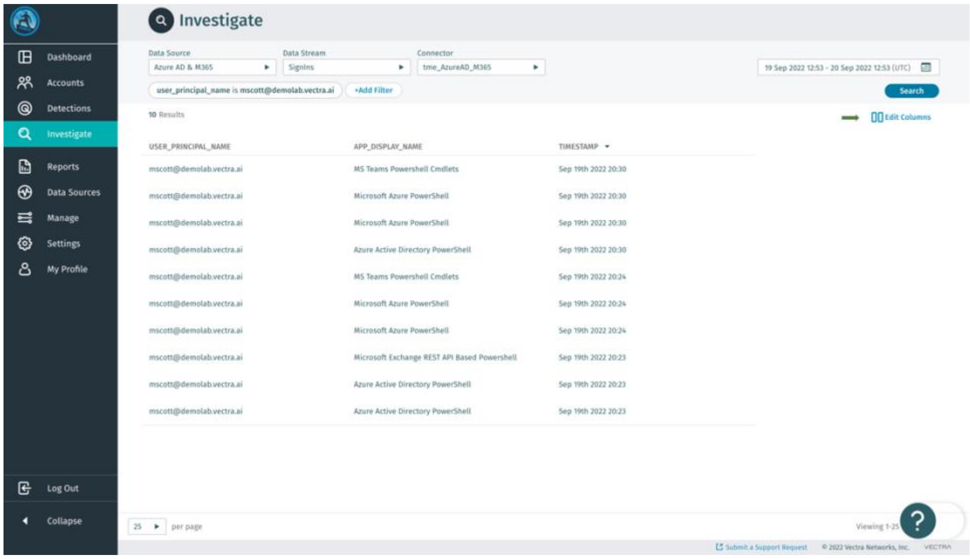
2022 Results

ASSUME_ROLE_ROLE_ARN	USER_AGENT	SOURCE_IP_ADDRESS	EVENT_SOURCE
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10	
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10	
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.16.64	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.172.112	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com
arn:aws:iam::884414556547:role/RoleForVectra-demolab	aws-sdk-js/3.100.0 os/linux/4.14.255-276-224.499.amzn2.x86_64 lang/js md/nodejs/16.16.0 api/sts/3.100.0 exec-env/AWS_Lambda_nodejs16.x	10.101.64.77	sts.amazonaws.com

25 per page ‹ 1 2 3 4 5 6 7 ... 81 › Viewing 1-25 of

How to add/remove and re-order columns in the results

1. To add columns to the results, click on the *Edit Columns* icon under the *Search* button.



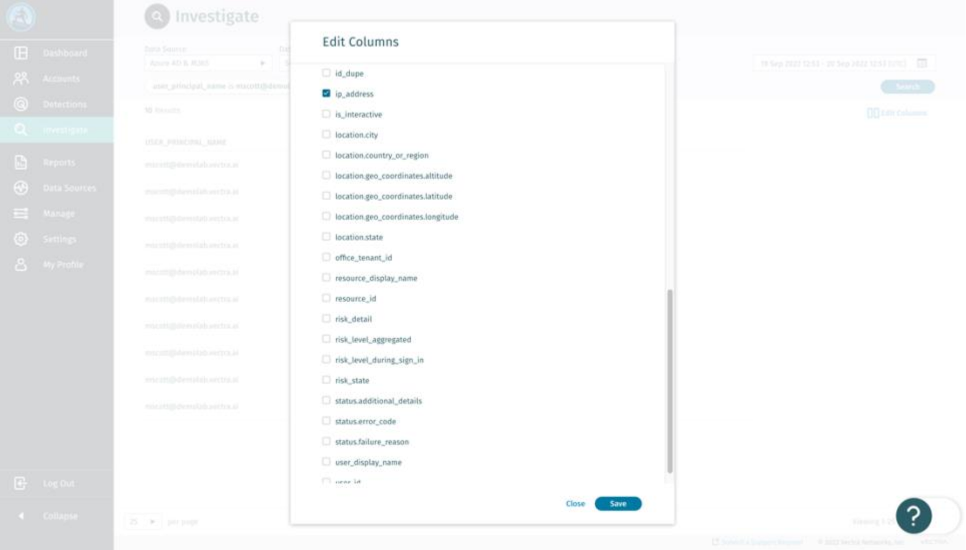
Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
19 Sep 2022 12:53 - 20 Sep 2022 12:53 (UTC)
user_principal_name is mscott@demolab.vectra.ai

10 Results

USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	TIMESTAMP
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:30
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:30
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:24
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24
mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	Sep 19th 2022 20:23
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23

25 per page
Viewing 1-25

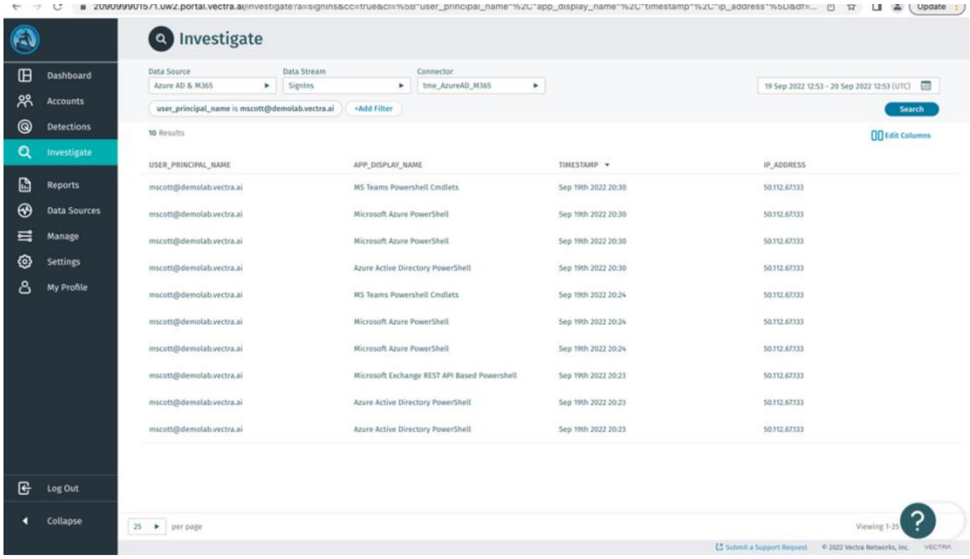
2. Select the columns to be added to the view. In this example we will add the *ip_address* column and then click save.



Edit Columns

□ id_dupe
☑ ip_address
□ is_interactive
□ location.city
□ location.country_or_region
□ location.geo_coordinates.altitude
□ location.geo_coordinates.latitude
□ location.geo_coordinates.longitude
□ location.state
□ office_tenant_id
□ resource_display_name
□ resource_id
□ risk_detail
□ risk_level_aggregated
□ risk_level_during_sign_in
□ risk_state
□ status.additional_details
□ status.error_code
□ status.failure_reason
□ user_display_name
□ user_id

3. The newly added column is added to the results.



2090999015 71.uw2.portal.vectra.ai/investigate?a=signins&cc=true&cl=%5B"user_principal_name"%2C"app_display_name"%2C"timestamp"%2C"ip_address"%5D&df=...

Investigate

Data Source: Azure AD & M365 | Data Stream: SignIns | Connector: tme_AzureAD_M365 | 19 Sep 2022 12:53 - 20 Sep 2022 12:53 (UTC)

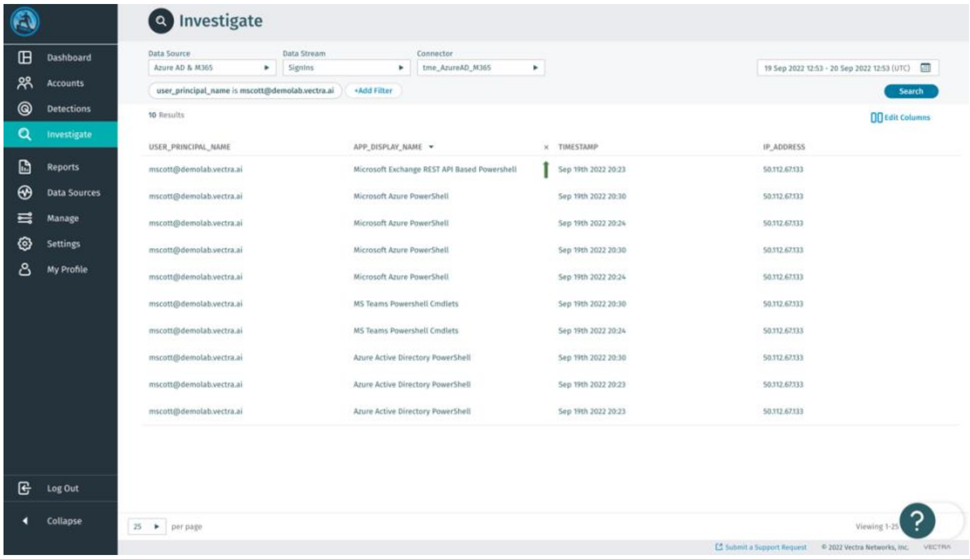
user_principal_name is mscott@demolab.vectra.ai | +Add Filter

10 Results

USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	TIMESTAMP ▾	IP_ADDRESS
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	Sep 19th 2022 20:23	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23	50.112.67.133

25 per page | Viewing 1-25

4. To remove a column from the results view, you can click on the “x” at the right side of the column’s name, or you can use the *Edit columns* option as shown before.



Investigate

Data Source: Azure AD & M365 | Data Stream: SignIns | Connector: tme_AzureAD_M365 | 19 Sep 2022 12:53 - 20 Sep 2022 12:53 (UTC)

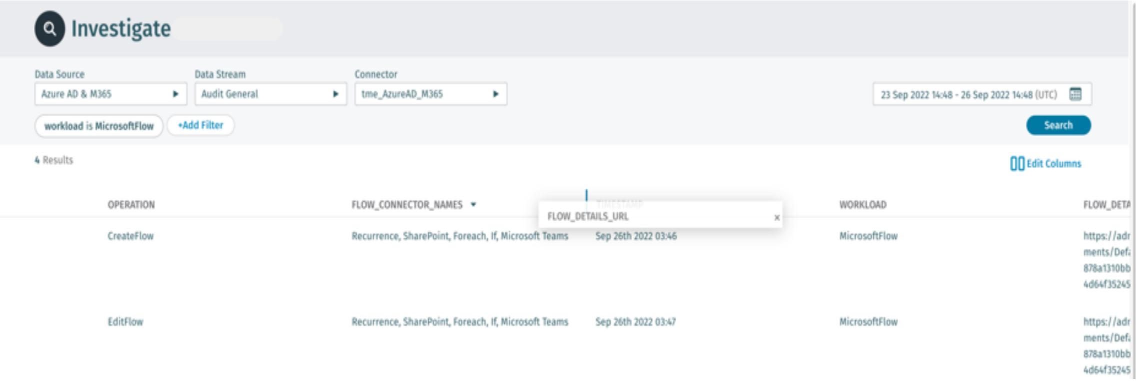
user_principal_name is mscott@demolab.vectra.ai | +Add Filter

10 Results

USER_PRINCIPAL_NAME	APP_DISPLAY_NAME ▾ ×	TIMESTAMP	IP_ADDRESS
mscott@demolab.vectra.ai	Microsoft Exchange REST API Based Powershell	Sep 19th 2022 20:23	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Microsoft Azure PowerShell	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	MS Teams Powershell Cmdlets	Sep 19th 2022 20:24	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:30	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23	50.112.67.133
mscott@demolab.vectra.ai	Azure Active Directory PowerShell	Sep 19th 2022 20:23	50.112.67.133

25 per page | Viewing 1-25

5. To re-order the columns you can simply drag and drop them in the desired order.



Investigate

Data Source: Azure AD & M365 | Data Stream: Audit General | Connector: tme_AzureAD_M365 | 23 Sep 2022 14:48 - 26 Sep 2022 14:48 (UTC)

workload is MicrosoftFlow | +Add Filter

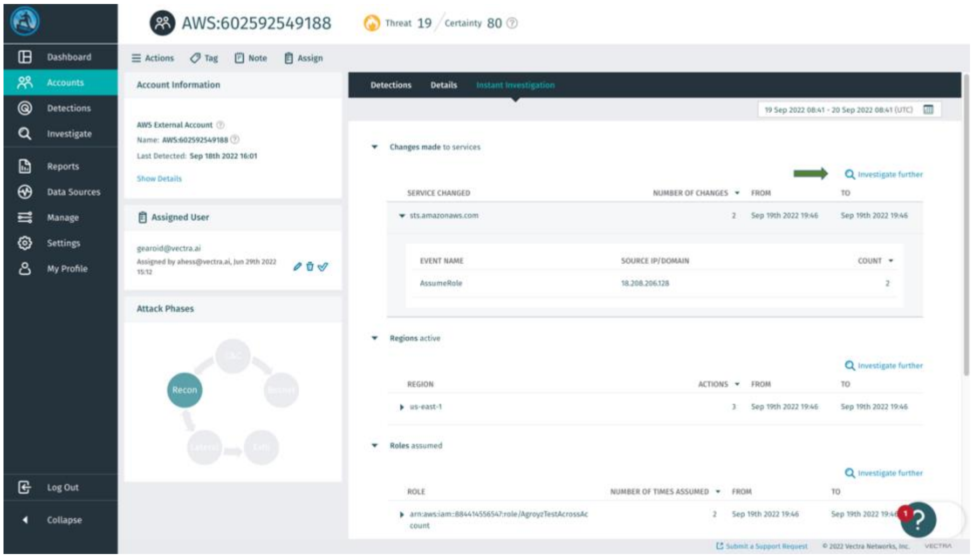
4 Results

OPERATION	FLOW_CONNECTOR_NAMES ▾	TIMESTAMP	WORKLOAD	FLOW_DETA
CreateFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	Sep 26th 2022 03:46	MicrosoftFlow	https://adr ments/Defa 878a1310bb 4d64f35245
EditFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	Sep 26th 2022 03:47	MicrosoftFlow	https://adr ments/Defa 878a1310bb 4d64f35245

How to run a query from Instant Investigation

In this example, we will assume that an AWS account has been identified to be of interest in *Instant Investigation.* Using the source IP address, we would like to investigate further.

Clicking on *Investigate Further* takes us to the Advanced Investigation (*Investigate)* landing page.



AWS:602592549188 Threat 19 / Certainty 80

Account Information

AWS External Account
Name: AWS:602592549188
Last Detected: Sep 18th 2022 16:01
Show Details

Assigned User

gearoid@vectra.ai
Assigned by ahess@vectra.ai, Jun 29th 2022 15:12

Attack Phases

19 Sep 2022 08:41 - 20 Sep 2022 08:41 (UTC)

Changes made to services

Investigate further

SERVICE CHANGED	NUMBER OF CHANGES	FROM	TO
sts.amazonaws.com	2	Sep 19th 2022 19:46	Sep 19th 2022 19:46

EVENT NAME	SOURCE IP/DOMAIN	COUNT
AssumeRole	18.208.206.128	2

Regions active

Investigate further

REGION	ACTIONS	FROM	TO
us-east-1	3	Sep 19th 2022 19:46	Sep 19th 2022 19:46

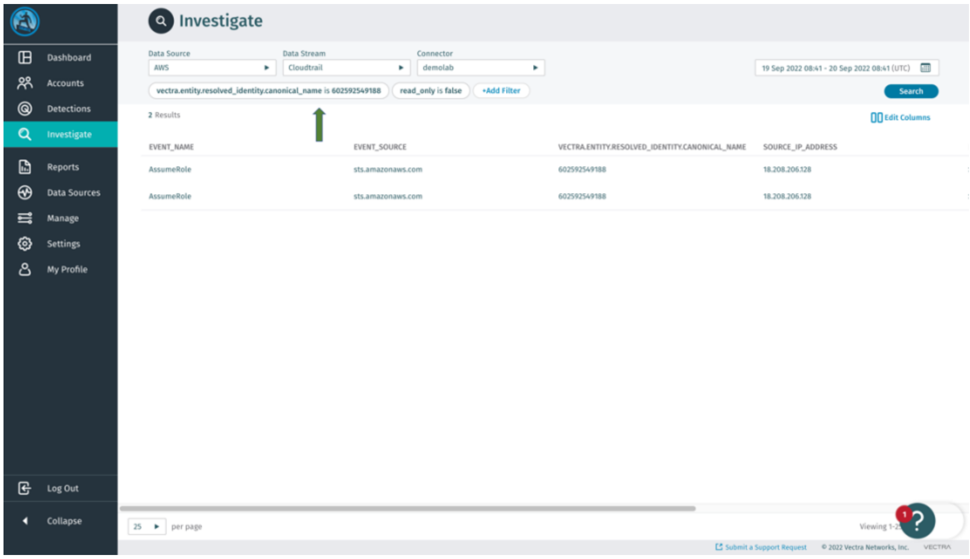
Roles assumed

Investigate further

ROLE	NUMBER OF TIMES ASSUMED	FROM	TO
arn:aws:iam::884414556547:role/AgroyzTestAcrossAccount	2	Sep 19th 2022 19:46	Sep 19th 2022 19:46

© 2022 Vectra Networks, Inc.

Once in *Investigate*, the filters from Instant Investigation are carried into *Advanced Investigation* and you can add/remove filters, change the search period, etc.



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab

19 Sep 2022 08:41 - 20 Sep 2022 08:41 (UTC)

vectra.entity.resolved_identity.canonical_name is 602592549188
read_only is false

2 Results

EVENT_NAME	EVENT_SOURCE	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_NAME	SOURCE_IP_ADDRESS
AssumeRole	sts.amazonaws.com	602592549188	18.208.206.128
AssumeRole	sts.amazonaws.com	602592549188	18.208.206.128

25 per page

Viewing 1-2

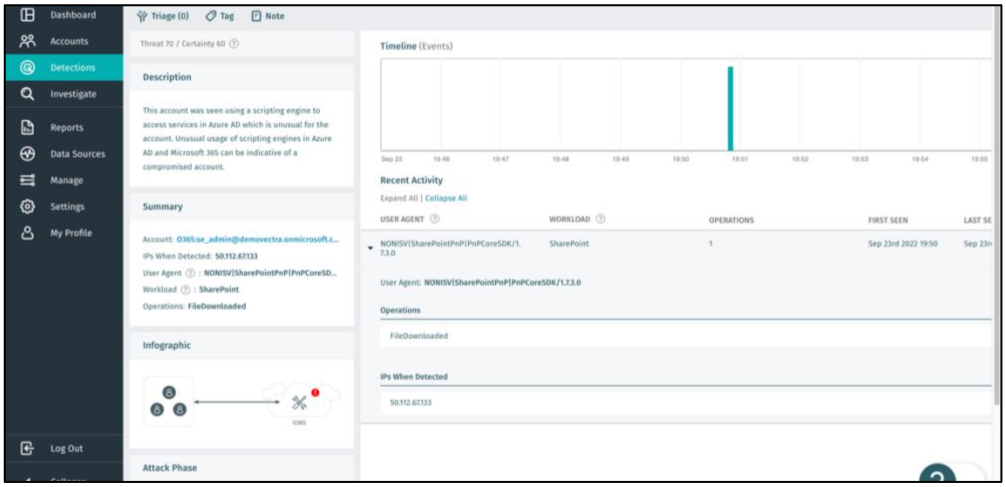
© 2022 Vectra Networks, Inc.

Query Examples

Investigating an Azure AD attack with Powershell

Attackers will use Powershell to automate parts of their attack. Vectra enables fast response to Powershell-based attacks with effective detections and functionality to rapidly investigate and understand the breadth of an attack.

A Vectra Azure AD Scripting Engine detection will identify the use of unusual scripting engines like Powershell.



Threat 70 / Certainty 60

Description

This account was seen using a scripting engine to access services in Azure AD which is unusual for the account. Unusual usage of scripting engines in Azure AD and Microsoft 365 can be indicative of a compromised account.

Summary

Account: O365:se_admin@demovectra.onmicrosoft.c...
IPs When Detected: 50.112.67.133
User Agent: NONISV|SharePointPnP|PnPCoreSD...
Workload: SharePoint
Operations: FileDownloaded

Attack Phase

Recent Activity

USER AGENT	WORKLOAD	OPERATIONS	FIRST SEEN	LAST SE
NONISV|SharePointPnP|PnPCoreSDK/1.7.3.0	SharePoint	1	Sep 23rd 2022 19:50	Sep 23r

User Agent: NONISV|SharePointPnP|PnPCoreSDK/1.7.3.0

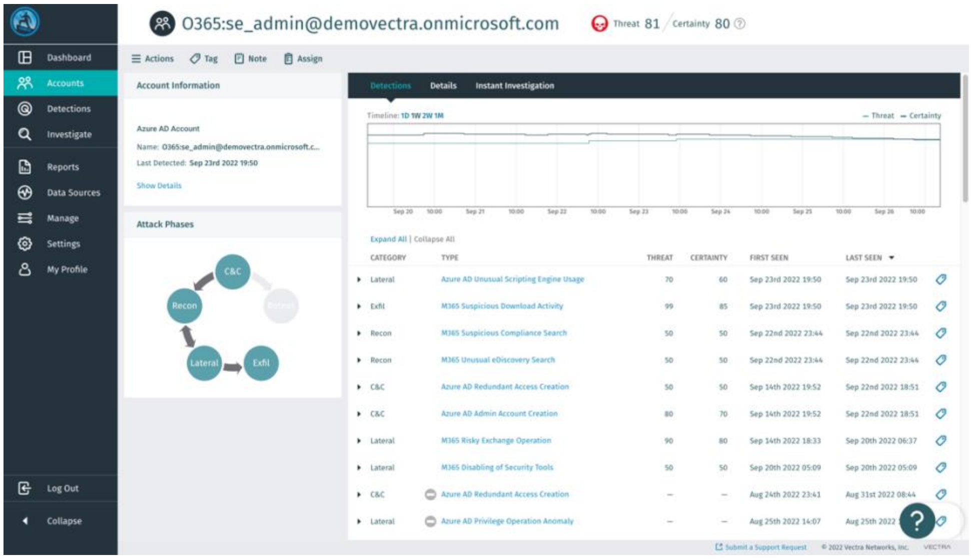
Operations

FileDownloaded

IPs When Detected

50.112.67.133

To investigate the impact of the Powershell usage during an attack, analysts can pivot to the account page and access the *Instant Investigation* tab



O365:se_admin@demovectra.onmicrosoft.com Threat 81 / Certainty 80

Account Information

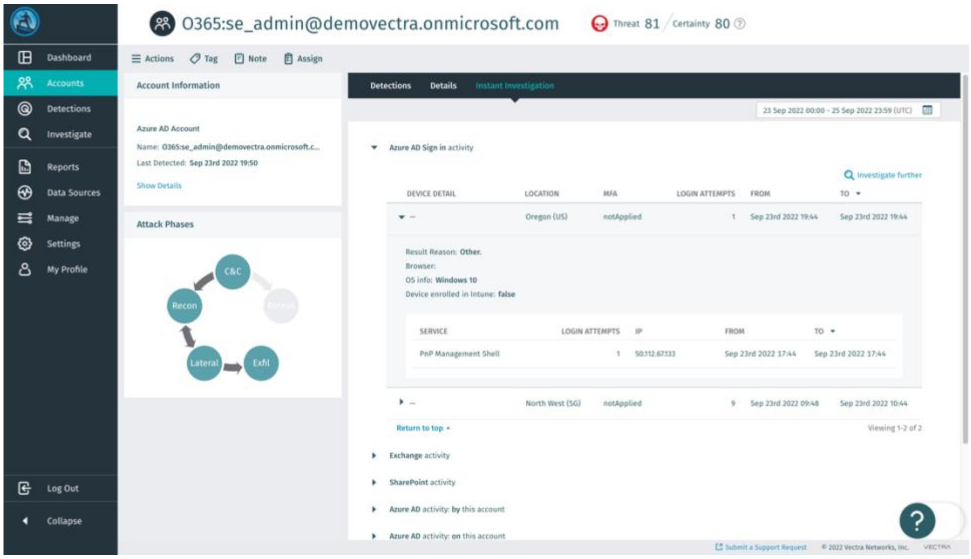
Azure AD Account
Name: O365:se_admin@demovectra.onmicrosoft.c...
Last Detected: Sep 23rd 2022 19:50
Show Details

Attack Phases

CATEGORY	TYPE	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN
Lateral	Azure AD Unusual Scripting Engine Usage	70	60	Sep 23rd 2022 19:50	Sep 23rd 2022 19:50
Exfil	M365 Suspicious Download Activity	99	85	Sep 23rd 2022 19:50	Sep 23rd 2022 19:50
Recon	M365 Suspicious Compliance Search	50	50	Sep 22nd 2022 23:44	Sep 22nd 2022 23:44
Recon	M365 Unusual eDiscovery Search	50	50	Sep 22nd 2022 23:44	Sep 22nd 2022 23:44
C&C	Azure AD Redundant Access Creation	50	50	Sep 14th 2022 19:52	Sep 22nd 2022 18:51
C&C	Azure AD Admin Account Creation	80	70	Sep 14th 2022 19:52	Sep 22nd 2022 18:51
Lateral	M365 Risky Exchange Operation	90	80	Sep 14th 2022 18:33	Sep 20th 2022 06:37
Lateral	M365 Disabling of Security Tools	50	50	Sep 20th 2022 05:09	Sep 20th 2022 05:09
C&C	Azure AD Redundant Access Creation	–	–	Aug 24th 2022 23:41	Aug 31st 2022 08:44
Lateral	Azure AD Privilege Operation Anomaly	–	–	Aug 25th 2022 14:07	Aug 25th 2022

© 2022 Vectra Networks, Inc.

From the *Instant Investigation* tab teams can quickly review the sign in activity



O365:se_admin@demovectra.onmicrosoft.com Threat 81 / Certainty 80

Account Information

Azure AD Account
Name: O365:se_admin@demovectra.onmicrosoft.c...
Last Detected: Sep 23rd 2022 19:50
Show Details

Attack Phases

Detections | Details | Instant Investigation

23 Sep 2022 00:00 - 25 Sep 2022 23:59 (UTC)

Azure AD Sign in activity

Investigate further

DEVICE DETAIL	LOCATION	MFA	LOGIN ATTEMPTS	FROM	TO
–	Oregon (US)	notApplied	1	Sep 23rd 2022 19:44	Sep 23rd 2022 19:44

Result Reason: Other.
Browser:
OS info: Windows 10
Device enrolled in Intune: false

SERVICE	LOGIN ATTEMPTS	IP	FROM	TO
PnP Management Shell	1	50.112.67.133	Sep 23rd 2022 17:44	Sep 23rd 2022 17:44

DEVICE DETAIL	LOCATION	MFA	LOGIN ATTEMPTS	FROM	TO
–	North West (SG)	notApplied	9	Sep 23rd 2022 09:48	Sep 23rd 2022 10:44

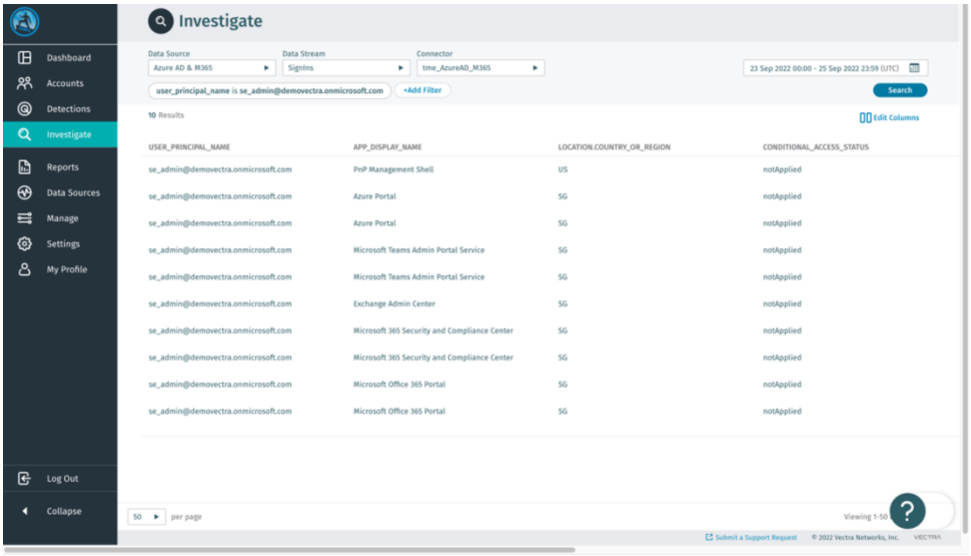
Return to top
Viewing 1-2 of 2

Exchange activity
SharePoint activity
Azure AD activity: by this account
Azure AD activity: on this account

Submit a Support Request © 2022 Vectra Networks, Inc. VECTRA

Teams wanting to dive in deeper, can use the *Investigate further* action to review more details.

The full timeline of Powershell usage and instances of other federated SaaS applications being accessed without Powershell are shown.



Investigate

Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
23 Sep 2022 00:00 - 25 Sep 2022 23:59 (UTC)
user_principal_name is se_admin@demovectra.onmicrosoft.com +Add Filter

10 Results

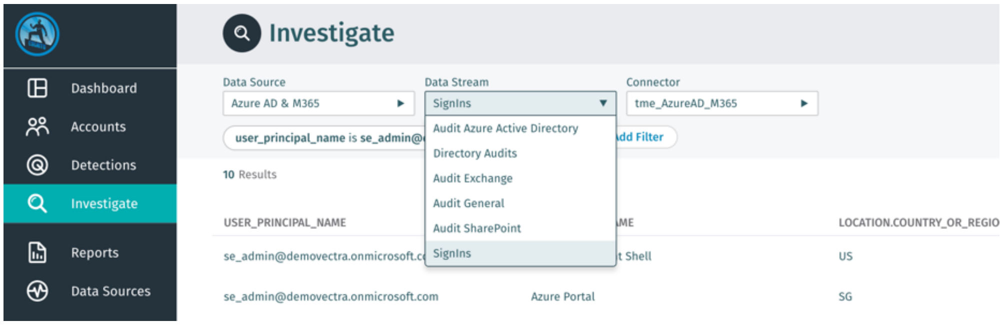
USER_PRINCIPAL_NAME	APP_DISPLAY_NAME	LOCATION.COUNTRY_OR_REGION	CONDITIONAL_ACCESS_STATUS
se_admin@demovectra.onmicrosoft.com	PnP Management Shell	US	notApplied
se_admin@demovectra.onmicrosoft.com	Azure Portal	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Azure Portal	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft Teams Admin Portal Service	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft Teams Admin Portal Service	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Exchange Admin Center	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft 365 Security and Compliance Center	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft 365 Security and Compliance Center	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft Office 365 Portal	SG	notApplied
se_admin@demovectra.onmicrosoft.com	Microsoft Office 365 Portal	SG	notApplied

50 per page
Viewing 1-50

Submit a Support Request © 2022 Vectra Networks, Inc. VECTRA

To understand further how an attacker might have used Powershell to propagate, review other logs.

For instance, the Audit Exchange data stream can be reviewed to see mailbox related activity, Audit SharePoint for file and data related activity, and Directory Audits for high impact Azure AD backend activities.



Investigate

Data Source: Azure AD & M365
Data Stream: SignIns
Connector: tme_AzureAD_M365
user_principal_name is se_admin@ ... dd Filter

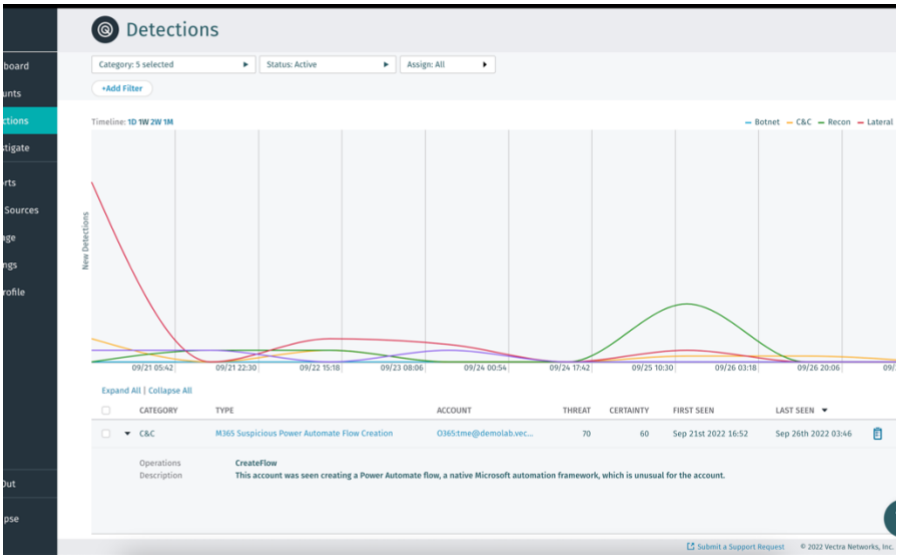
10 Results

USER_PRINCIPAL_NAME	...ME	LOCATION.COUNTRY_OR_REGIO
se_admin@demovectra.onmicrosoft.c...	...t Shell	US
se_admin@demovectra.onmicrosoft.com	Azure Portal	SG

Investigating a Microsoft 365 attack with Power Automate

Attackers will abuse the Power Automate suite to automate their attacks. Connectors set up reoccurring data movements that allow data theft to occur continuously without manual action. Detection events related to the abuse of Power Automate can be remediated quickly with the knowledge Vectra's Advanced Investigation feature provides.

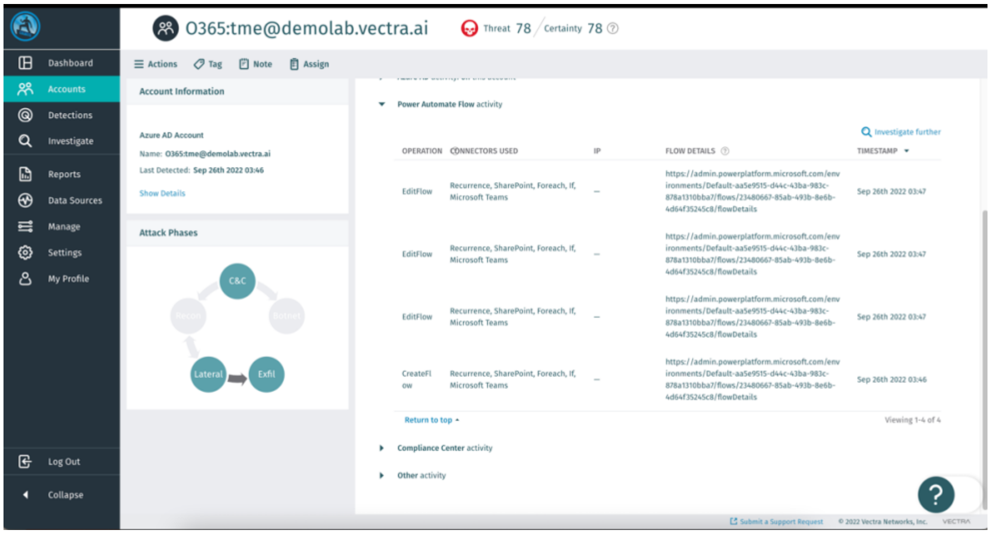
A Vectra M365 Suspect Power Automate Flow Creation alert will identify anomalous use of Power Automate.



CATEGORY	TYPE	ACCOUNT	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN
C&C	M365 Suspicious Power Automate Flow Creation	O365:tme@demolab.vec...	70	60	Sep 21st 2022 16:52	Sep 26th 2022 03:46

Operations: CreateFlow
Description: This account was seen creating a Power Automate flow, a native Microsoft automation framework, which is unusual for the account.

To investigate the details of the Power Automate usage during the attack, analysts can pivot to the account page and access the *Instant Investigation* tab to review the Power Automate activity.



Account Information

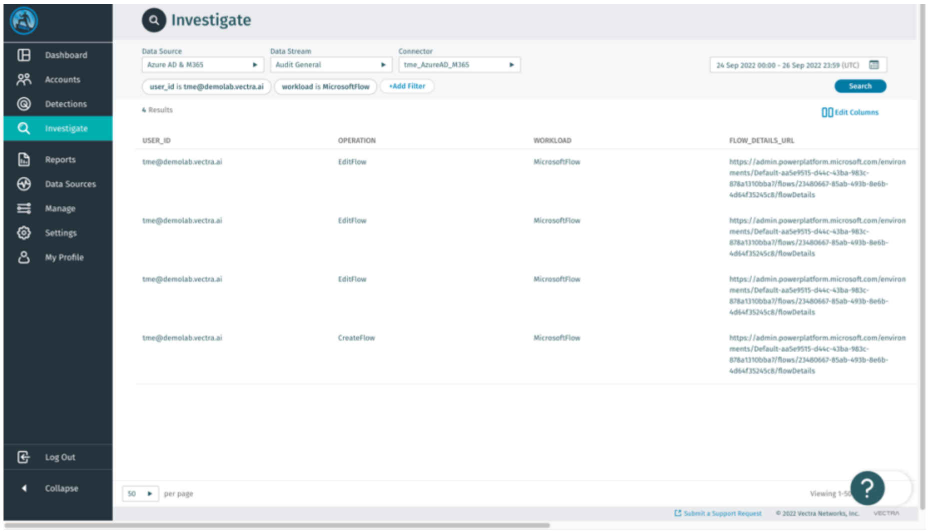
Azure AD Account
Name: O365:tme@demolab.vectra.ai
Last Detected: Sep 26th 2022 03:46

Power Automate Flow activity

OPERATION	CONNECTORS USED	IP	FLOW DETAILS	TIMESTAMP
EditFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	–	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Sep 26th 2022 03:47
EditFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	–	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Sep 26th 2022 03:47
EditFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	–	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Sep 26th 2022 03:47
CreateFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	–	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Sep 26th 2022 03:46

Viewing 1-4 of 4

Teams wanting to dive in deeper, can use the *Investigate further* action to review more details.



Investigate

Data Source: Azure AD & M365
Data Stream: Audit General
Connector: tme_AzureAD_M365
24 Sep 2022 00:00 - 26 Sep 2022 23:59 (UTC)

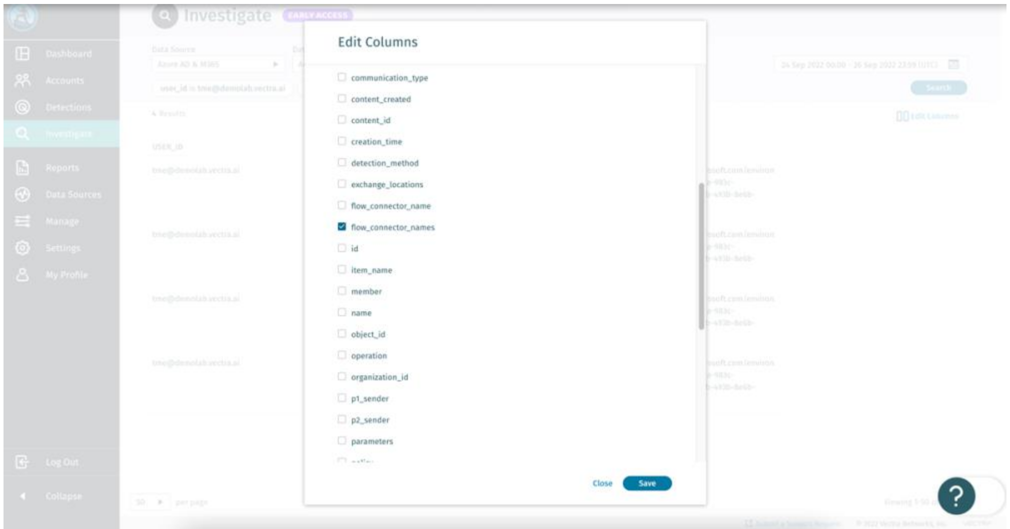
user_id is tme@demolab.vectra.ai | workload is MicrosoftFlow

4 Results

USER_ID	OPERATION	WORKLOAD	FLOW_DETAILS_URL
tme@demolab.vectra.ai	EditFlow	MicrosoftFlow	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails
tme@demolab.vectra.ai	EditFlow	MicrosoftFlow	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails
tme@demolab.vectra.ai	EditFlow	MicrosoftFlow	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails
tme@demolab.vectra.ai	CreateFlow	MicrosoftFlow	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails

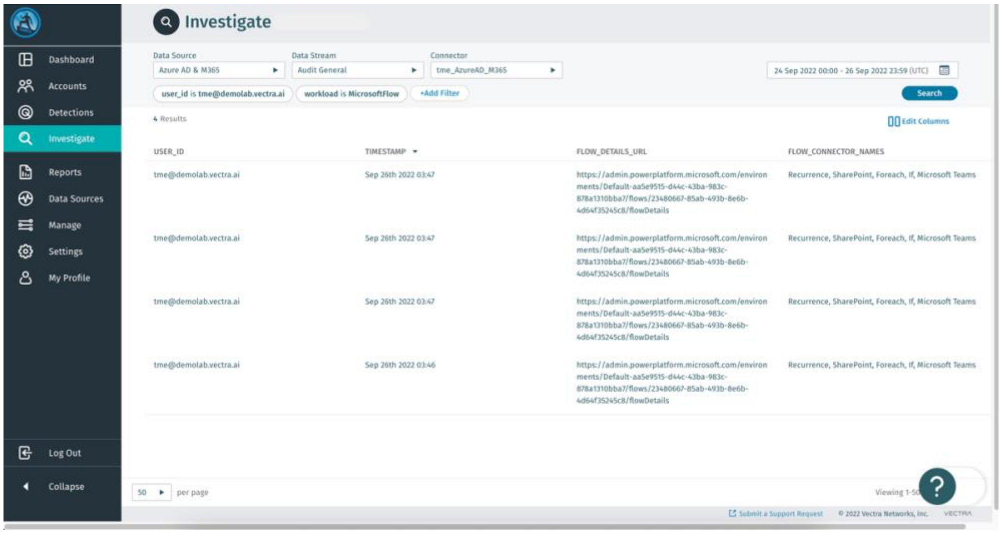
50 per page | Viewing 1-50

To view the flow connectors that were used during the attack select *Edit Columns* and add the "flow_connector_names" column.



Edit Columns

- ☐ communication_type
- ☐ content_created
- ☐ content_id
- ☐ creation_time
- ☐ detection_method
- ☐ exchange_locations
- ☐ flow_connector_name
- ☑ flow_connector_names
- ☐ id
- ☐ item_name
- ☐ member
- ☐ name
- ☐ object_id
- ☐ operation
- ☐ organization_id
- ☐ p1_sender
- ☐ p2_sender
- ☐ parameters



Investigate

Data Source: Azure AD & M365
Data Stream: Audit General
Connector: tme_AzureAD_M365
24 Sep 2022 00:00 - 26 Sep 2022 23:59 (UTC)

user_id is tme@demolab.vectra.ai | workload is MicrosoftFlow

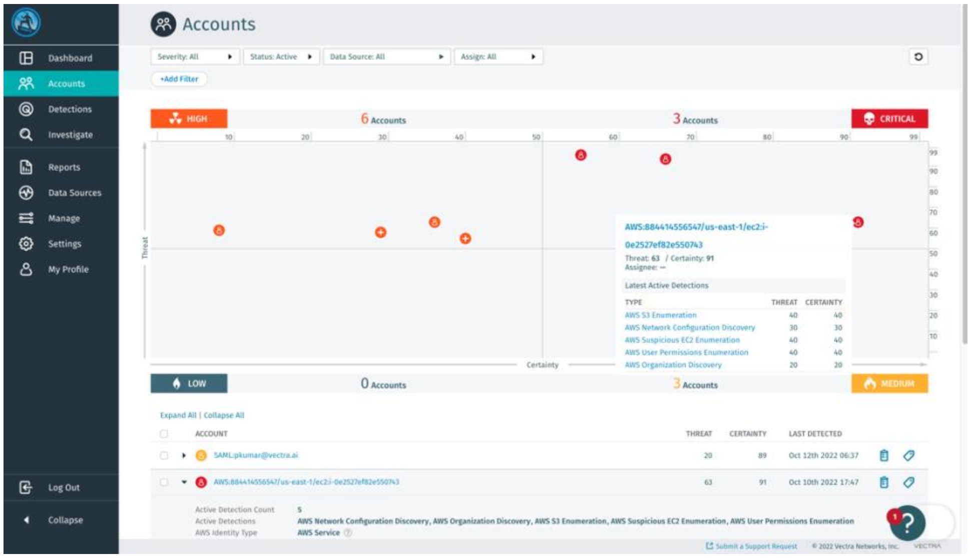
4 Results

USER_ID	TIMESTAMP ▾	FLOW_DETAILS_URL	FLOW_CONNECTOR_NAMES
tme@demolab.vectra.ai	Sep 26th 2022 03:47	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Recurrence, SharePoint, Foreach, If, Microsoft Teams
tme@demolab.vectra.ai	Sep 26th 2022 03:47	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Recurrence, SharePoint, Foreach, If, Microsoft Teams
tme@demolab.vectra.ai	Sep 26th 2022 03:47	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Recurrence, SharePoint, Foreach, If, Microsoft Teams
tme@demolab.vectra.ai	Sep 26th 2022 03:46	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Recurrence, SharePoint, Foreach, If, Microsoft Teams

50 per page | Viewing 1-50

All activity around a specific AWS EC2 instance

In this example, while in the *Accounts* page we decide to investigate an AWS account that's currently in the Critical quadrant.



Accounts

Severity: All | Status: Active | Data Source: All | Assign: All

+Add Filter

6 Accounts | 3 Accounts | 0 Accounts | 3 Accounts

AWS:884414556547/us-east-1/ec2:i-0e2527ef82e550743
Threat: 63 / Certainty: 91
Assignee: —

Latest Active Detections

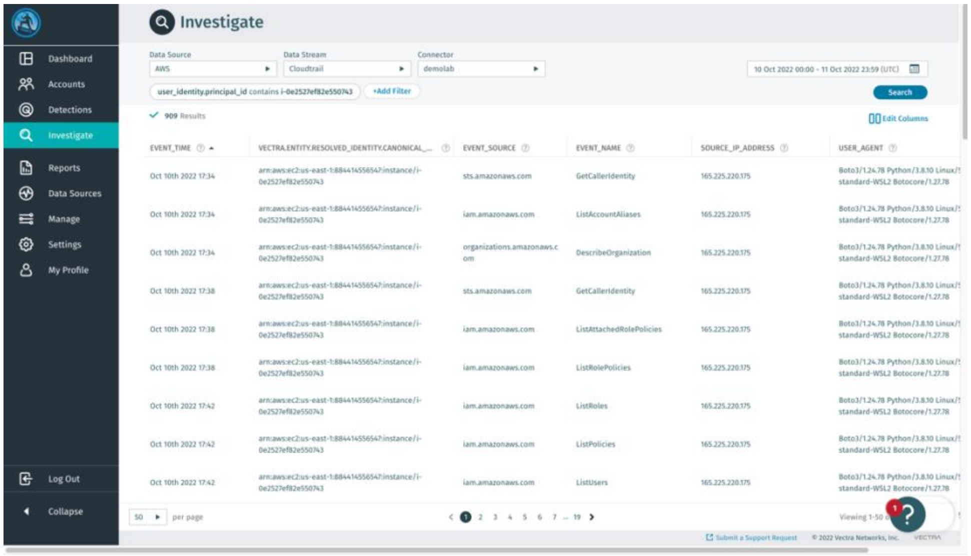
TYPE	THREAT	CERTAINTY
AWS S3 Enumeration	40	40
AWS Network Configuration Discovery	30	30
AWS Suspicious EC2 Enumeration	40	40
AWS User Permissions Enumeration	40	40
AWS Organization Discovery	20	20

ACCOUNT	THREAT	CERTAINTY	LAST DETECTED
SAML:pkumar@vectra.ai	20	89	Oct 12th 2022 06:37
AWS:884414556547/us-east-1/ec2:i-0e2527ef82e550743	63	91	Oct 10th 2022 17:47

Active Detection Count 5
Active Detections AWS Network Configuration Discovery, AWS Organization Discovery, AWS S3 Enumeration, AWS Suspicious EC2 Enumeration, AWS User Permissions Enumeration
AWS Identity Type AWS Service

© 2022 Vectra Networks, Inc.

To investigate the activities related to an EC2 instance, we could create a filter in *Advanced Investigation* using part of the AWS account name of interest in the filter.



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
10 Oct 2022 00:00 - 11 Oct 2022 23:59 (UTC)

user_identity.principal_id contains i-0e2527ef82e550743 +Add Filter

✓ 909 Results

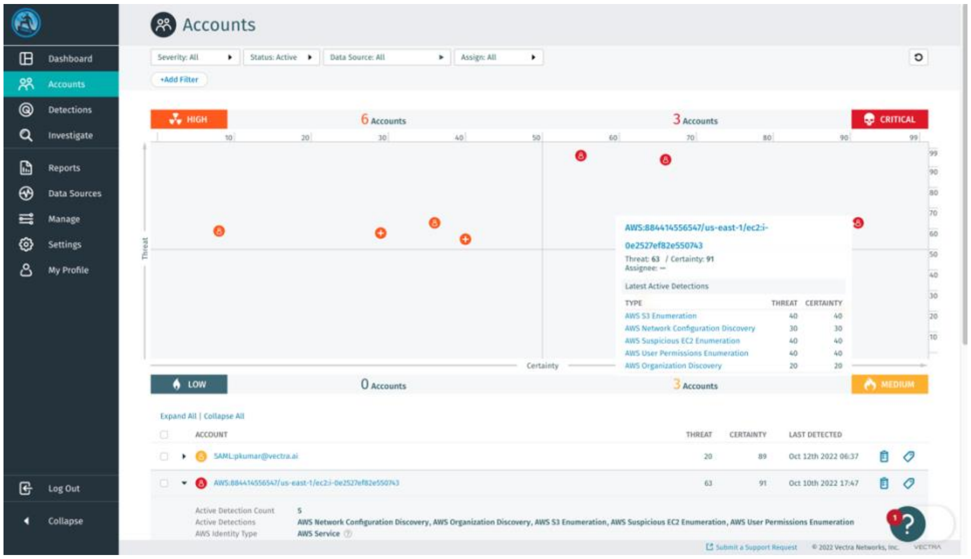
EVENT_TIME	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_...	EVENT_SOURCE	EVENT_NAME	SOURCE_IP_ADDRESS	USER_AGENT
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAccountAliases	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	organizations.amazonaws.com	DescribeOrganization	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAttachedRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRoles	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListPolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListUsers	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78

50 per page < 1 2 3 4 5 6 7 … 19 > Viewing 1-50

© 2022 Vectra Networks, Inc.

AWS activity performed with an assumed role

In this example, we'd like to know all activity this EC2 instance performed. One way to gather this information is to query for all activity by an AWS role attached to the EC2 instance.



AWS:884414556547/us-east-1/ec2:i-0e2527ef82e550743
Threat: 63 / Certainty: 91
Assignee: --

Latest Active Detections

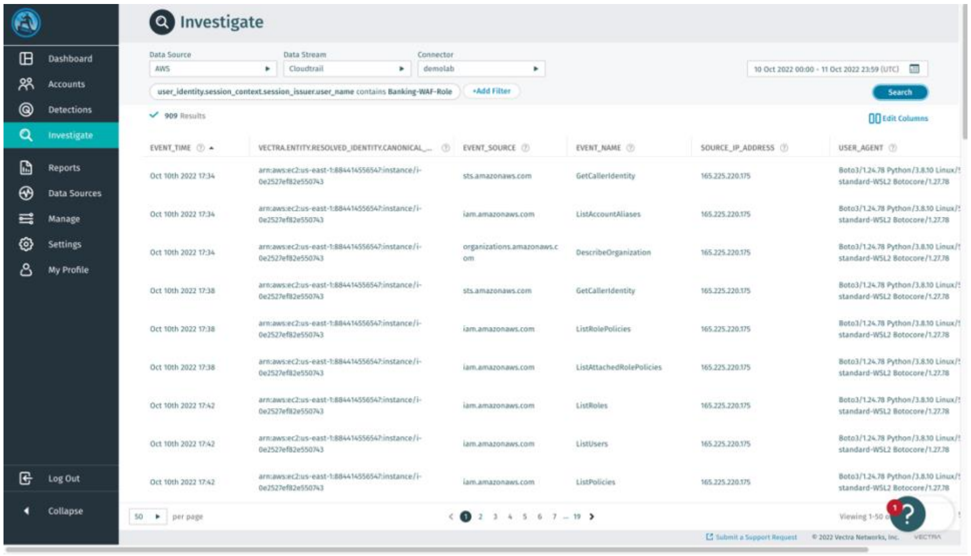
TYPE	THREAT	CERTAINTY
AWS S3 Enumeration	40	40
AWS Network Configuration Discovery	30	30
AWS Suspicious EC2 Enumeration	40	40
AWS User Permissions Enumeration	40	40
AWS Organization Discovery	20	20

Expand All | Collapse All

ACCOUNT	THREAT	CERTAINTY	LAST DETECTED
SAML:pkumar@vectra.ai	20	89	Oct 12th 2022 06:37
AWS:884414556547/us-east-1/ec2:i-0e2527ef82e550743	63	91	Oct 10th 2022 17:47

Active Detection Count 5
Active Detections AWS Network Configuration Discovery, AWS Organization Discovery, AWS S3 Enumeration, AWS Suspicious EC2 Enumeration, AWS User Permissions Enumeration
AWS Identity Type AWS Service

To investigate the activities related to an EC2 instance, we could create a filter in *Advanced Investigation* like the one shown in the image.



Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
10 Oct 2022 00:00 - 11 Oct 2022 23:59 (UTC)

user_identity.session_context.session_issuer.user_name contains Banking-WAF-Role

909 Results

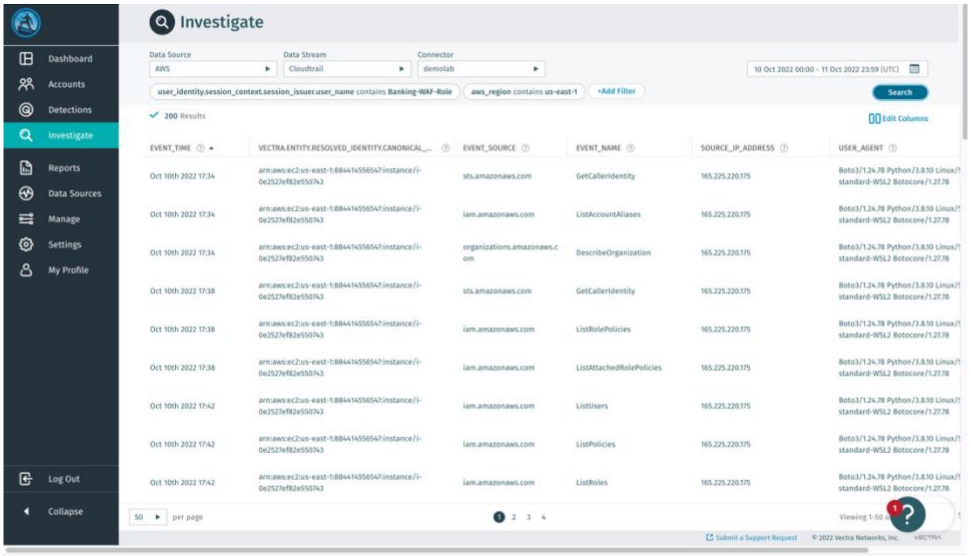
EVENT_TIME	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_...	EVENT_SOURCE	EVENT_NAME	SOURCE_IP_ADDRESS	USER_AGENT
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAccountAliases	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	organizations.amazonaws.com	DescribeOrganization	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAttachedRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRoles	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListUsers	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListPolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/ standard-WSL2 Botocore/1.27.78

50 per page

AWS activity performed with an assumed role on a different region

Continuing the previous example, we could add a filter to check the activities the EC2 has performed with the assumed IAM role.

This EC2 is in the us-east-1 region, but we can see that the IAM role attached to the EC2 instance has made API calls for different regions.



Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
10 Oct 2022 00:00 - 11 Oct 2022 23:59 (UTC)

user_identity.session_context.session_issuer.user_name contains Banking-WAF-Role
aws_region contains us-east-1

✓ 200 Results

EVENT_TIME	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_...	EVENT_SOURCE	EVENT_NAME	SOURCE_IP_ADDRESS	USER_AGENT
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAccountAliases	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:34	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	organizations.amazonaws.com	DescribeOrganization	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	sts.amazonaws.com	GetCallerIdentity	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:38	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListAttachedRolePolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListUsers	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListPolicies	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78
Oct 10th 2022 17:42	arn:aws:ec2:us-east-1:884414556547:instance/i-0e2527ef82e550743	iam.amazonaws.com	ListRoles	165.225.220.175	Boto3/1.24.78 Python/3.8.10 Linux/5 standard-WSL2 Botocore/1.27.78

50 per page · 1 2 3 4 · Viewing 1-50 o

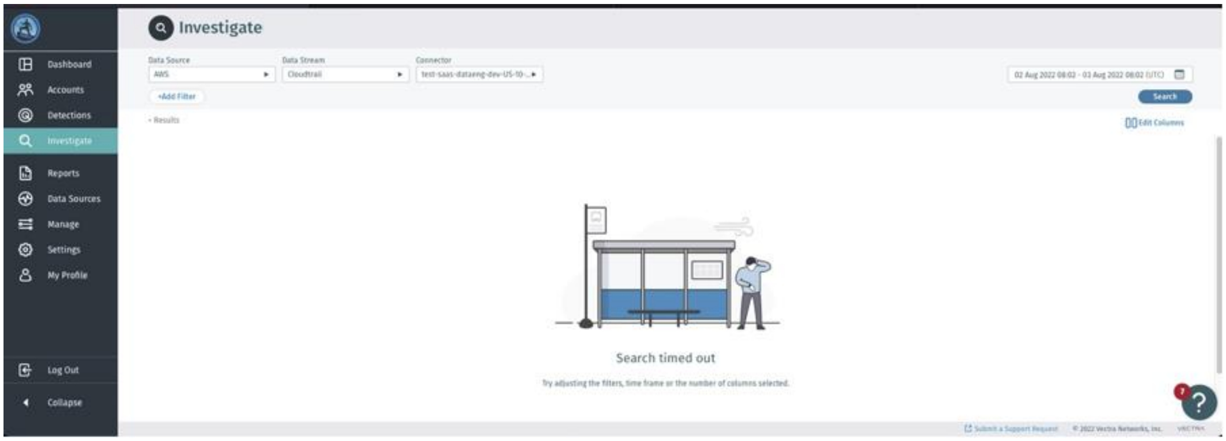
Submit a Support Request · © 2022 Vectra Networks, Inc.

Troubleshooting

There are cases in which a query cannot be completed due to a variety of reasons; in this section, we propose different actions to take that help avoid those situations.

“Search could not be completed” or “Search timed out”

In cases where the data sets to be retrieved are very large, the query may time out and you will see a message like the one shown below:



Data Source: AWS
Data Stream: Cloudtrail
Connector: test-saas-dataeng-dev-US-10-...
02 Aug 2022 08:02 - 03 Aug 2022 08:02 (UTC)

- Results

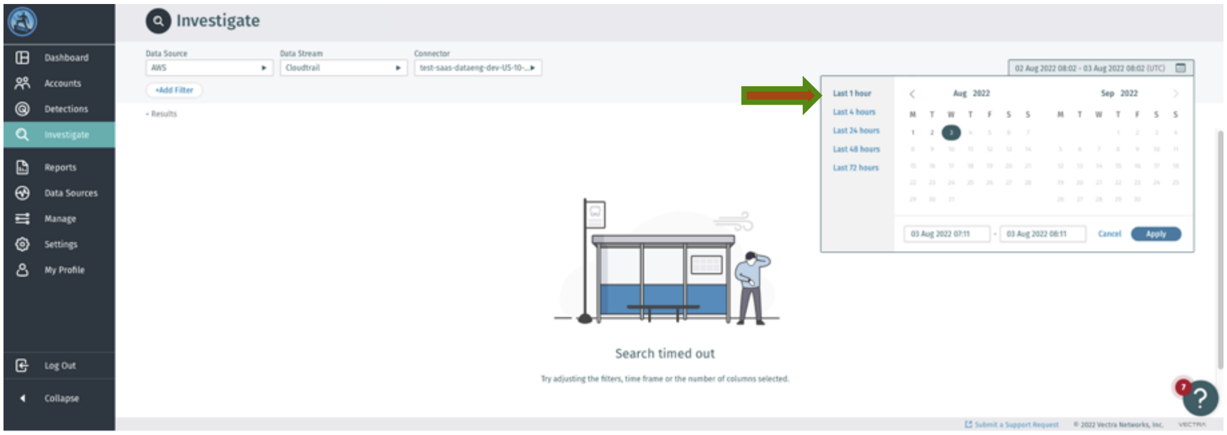
Search timed out

Try adjusting the filters, time frame or the number of columns selected.

Submit a Support Request · © 2022 Vectra Networks, Inc.

If that's the case, you can try the following steps:

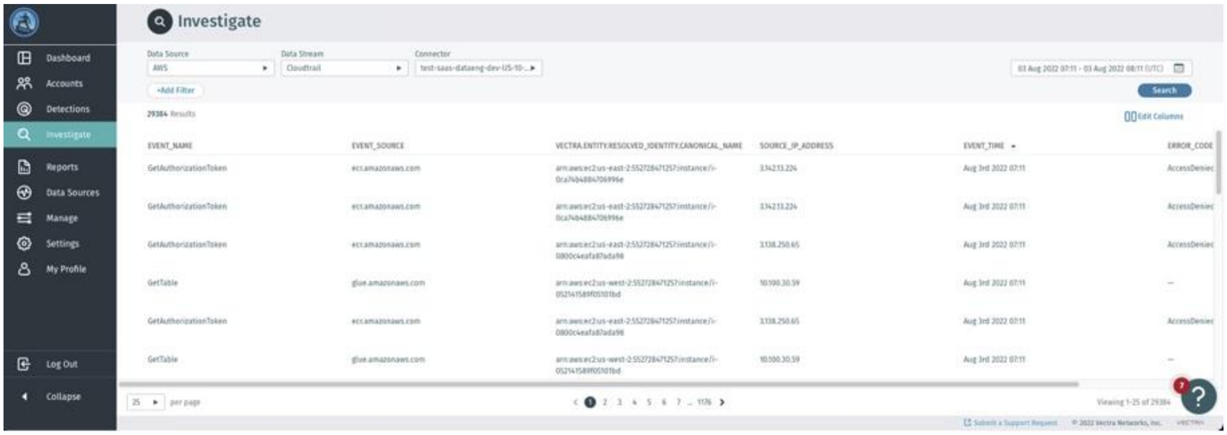
1. Reduce the search period for the query to one of the lower possible values. In this example, we've reduced it to *Last 1 hour*, click *Apply* and click *Search.*



Data Source: AWS
Data Stream: Cloudtrail
Connector: test-saas-dataeng-dev-US-10-...
02 Aug 2022 08:02 - 03 Aug 2022 08:02 (UTC)
- Results
03 Aug 2022 07:11 - 03 Aug 2022 08:11

Search timed out

Try adjusting the filters, time frame or the number of columns selected.



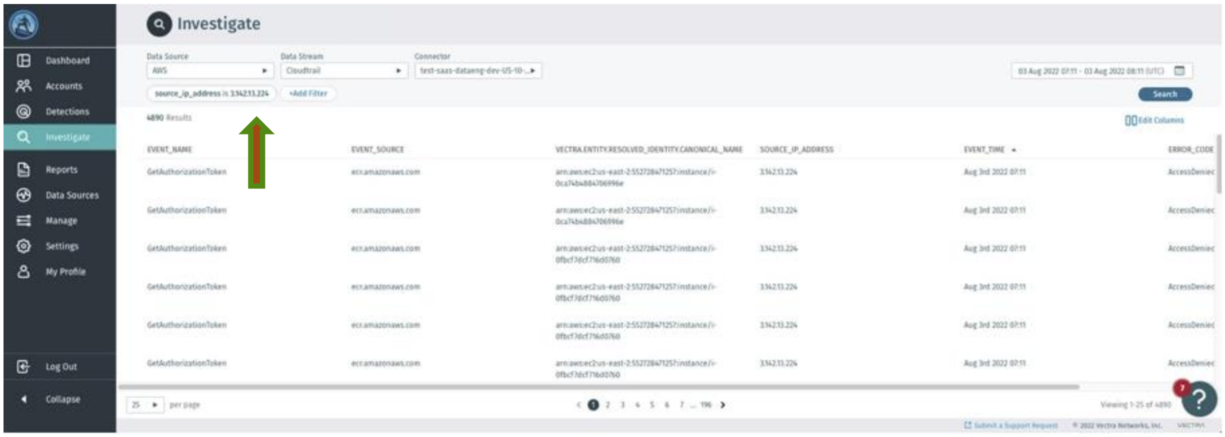
Data Source: AWS
Data Stream: Cloudtrail
Connector: test-saas-dataeng-dev-US-10-...
03 Aug 2022 07:11 - 03 Aug 2022 08:11 (UTC)

29384 Results

EVENT_NAME	EVENT_SOURCE	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_NAME	SOURCE_IP_ADDRESS	EVENT_TIME	ERROR_CODE
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0ca74b4884706996e	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0ca74b4884706996e	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0800c4eafa87ada98	3.138.250.65	Aug 3rd 2022 07:11	AccessDeniec
GetTable	glue.amazonaws.com	arn:aws:ec2:us-west-2:552728471257:instance/i-052141589f05101bd	10.100.30.59	Aug 3rd 2022 07:11	--
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0800c4eafa87ada98	3.138.250.65	Aug 3rd 2022 07:11	AccessDeniec
GetTable	glue.amazonaws.com	arn:aws:ec2:us-west-2:552728471257:instance/i-052141589f05101bd	10.100.30.59	Aug 3rd 2022 07:11	--

25 per page
1 2 3 4 5 6 7 ... 1176
Viewing 1-25 of 29384

2. If the results yield a field you may want to use as a filter, add a filter for it. In this case, we're filtering by an IP address of interest. Please see *How to add/remove filters* in this document for more details.



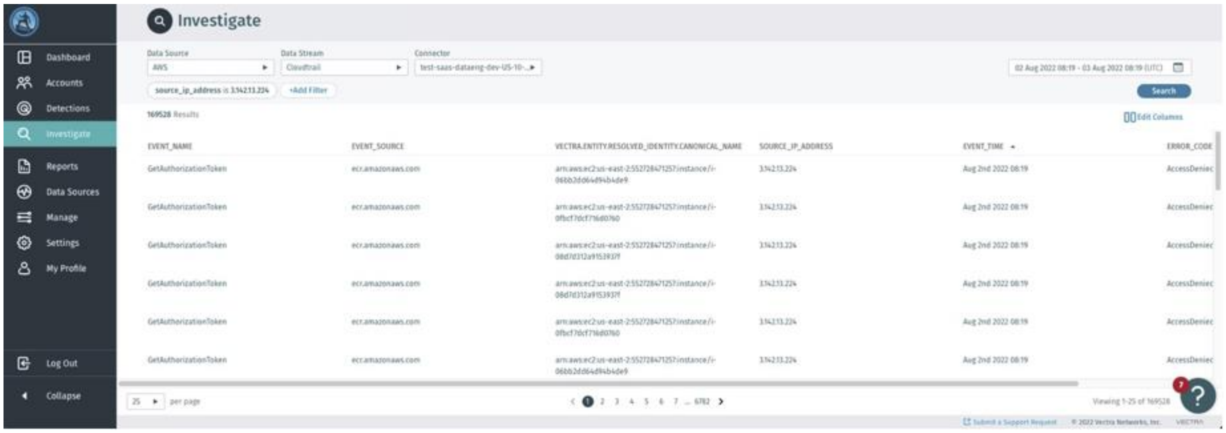
Data Source: AWS
Data Stream: Cloudtrail
Connector: test-saas-dataeng-dev-US-10-...
source_ip_address is 3.142.13.224
03 Aug 2022 07:11 - 03 Aug 2022 08:11 (UTC)

4890 Results

EVENT_NAME	EVENT_SOURCE	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_NAME	SOURCE_IP_ADDRESS	EVENT_TIME	ERROR_CODE
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0ca74b4884706996e	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0ca74b4884706996e	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 3rd 2022 07:11	AccessDeniec

25 per page   ‹ 1 2 3 4 5 6 7 … 196 ›   Viewing 1-25 of 4890

3. You could now try to change the search period back to a larger period. In this example, we've reverted to Last 24 hours. For more details on how to modify the time frame, please see *How to modify the query's search period* in this document.



Data Source: AWS
Data Stream: Cloudtrail
Connector: test-saas-dataeng-dev-US-10-...
source_ip_address is 3.142.13.224
02 Aug 2022 08:19 - 03 Aug 2022 08:19 (UTC)

169528 Results

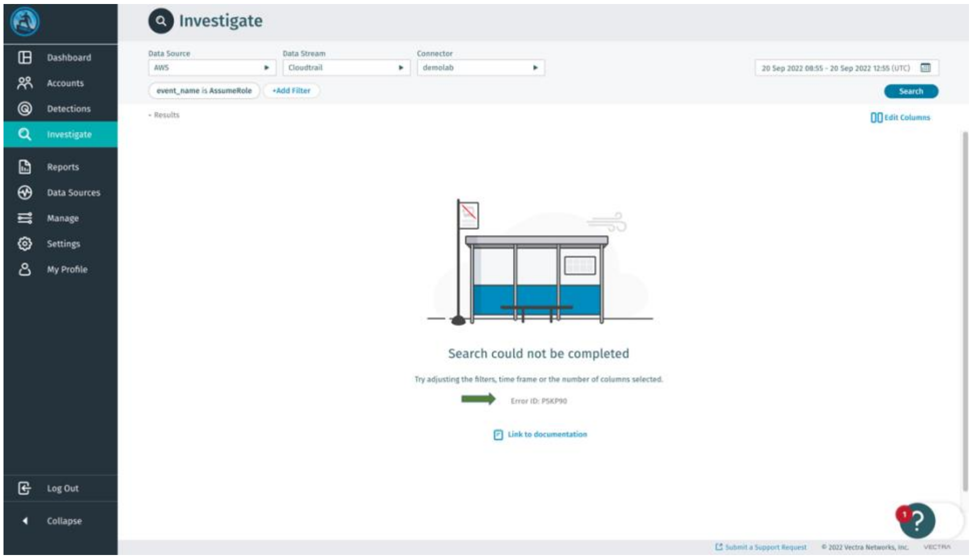
EVENT_NAME	EVENT_SOURCE	VECTRA.ENTITY.RESOLVED_IDENTITY.CANONICAL_NAME	SOURCE_IP_ADDRESS	EVENT_TIME	ERROR_CODE
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-06bb2dd64d94b4de9	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-08d7d312a9153937f	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-08d7d312a9153937f	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-0fbcf7dcf716d0760	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec
GetAuthorizationToken	ecr.amazonaws.com	arn:aws:ec2:us-east-2:552728471257:instance/i-06bb2dd64d94b4de9	3.142.13.224	Aug 2nd 2022 08:19	AccessDeniec

25 per page   ‹ 1 2 3 4 5 6 7 … 6782 ›   Viewing 1-25 of 169528

4. Depending on the size of your data set you may need to repeat this sequence of steps (reduce the time frame and add filters) until you narrow the search down to the data you're looking for.

“Search could not be completed” (with error id)

In rare occasions, an error message will be displayed, indicating the search could not be completed, and an error id is printed below the error message.



Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
20 Sep 2022 08:55 - 20 Sep 2022 12:55 (UTC)
event_name is AssumeRole

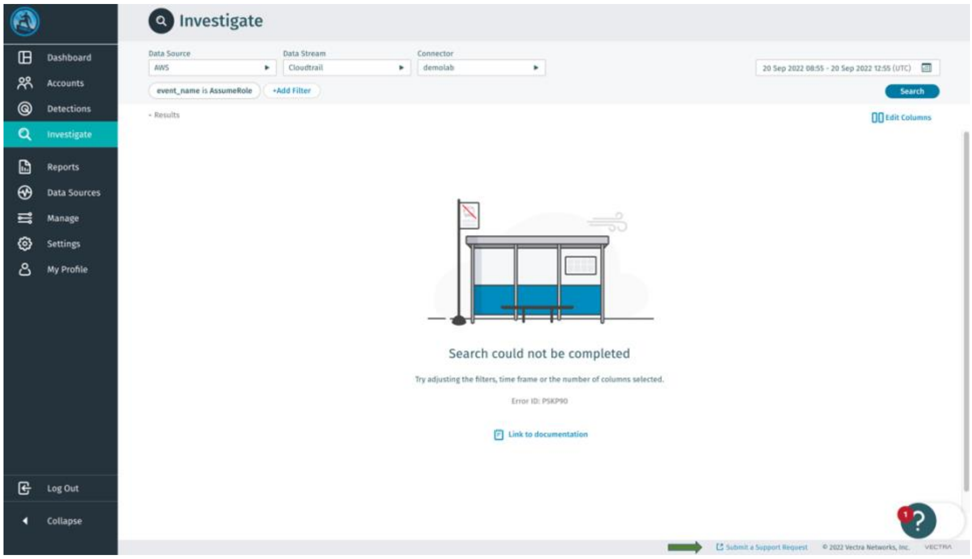
Search could not be completed

Try adjusting the filters, time frame or the number of columns selected.

Error ID: PSKP90

For the query to be executed, please follow the same steps used for the error scenario in which the error id is not being displayed (Search could not be completed section)

To help us improve, please also consider submitting a Support request, indicating the error id that was displayed for your query. Please include a snapshot of the query as well.



Data Source: AWS
Data Stream: Cloudtrail
Connector: demolab
20 Sep 2022 08:55 - 20 Sep 2022 12:55 (UTC)
event_name is AssumeRole

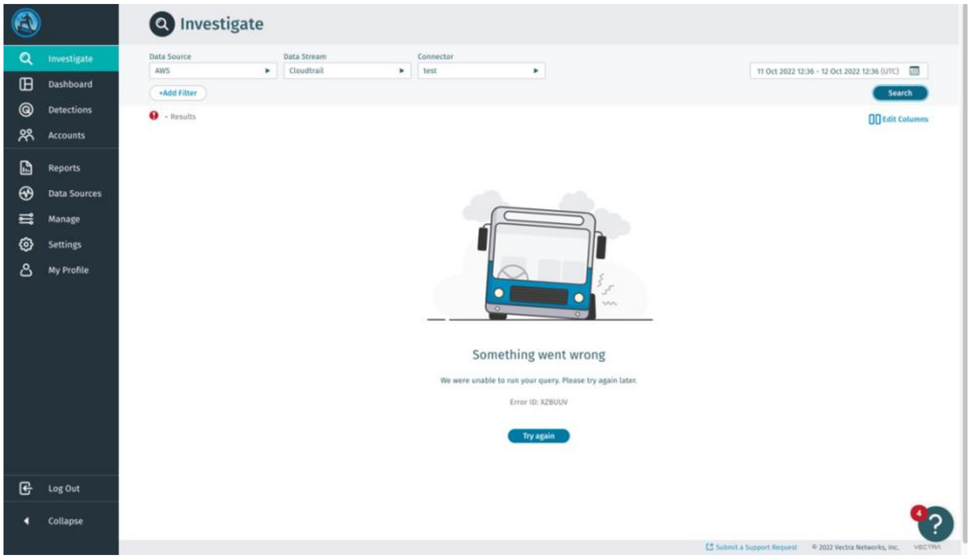
Search could not be completed

Try adjusting the filters, time frame or the number of columns selected.

Error ID: PSKP90

“Something went wrong”

In rare occasions, an error message will be displayed, indicating something has gone wrong (and most likely, the query can’t be triggered).



Investigate

Data Source: AWS
Data Stream: Cloudtrail
Connector: test
11 Oct 2022 12:36 - 12 Oct 2022 12:36 (UTC)

- Results

Something went wrong

We were unable to run your query. Please try again later.

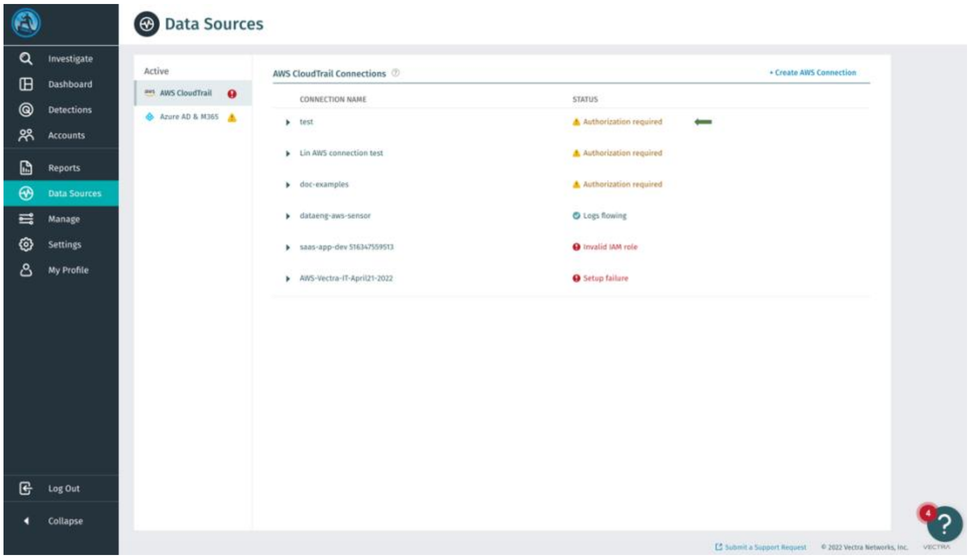
Error ID: XZBUUV

© 2022 Vectra Networks, Inc.

For the query to be executed, please check that logs are flowing successfully for the connector you’re using.

To so that, click on *Data Sources* option in the left side panel.

Once logs are flowing, try to execute the query again.



Data Sources

AWS CloudTrail Connections

CONNECTION NAME	STATUS
test	Authorization required
Lin AWS connection test	Authorization required
doc-examples	Authorization required
dataeng-aws-sensor	Logs flowing
saas-app-dev 516347559513	Invalid IAM role
AWS-Vectra-IT-April21-2022	Setup failure

© 2022 Vectra Networks, Inc.

Related articles

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html

https://docs.microsoft.com/en-us/graph/api/resources/signin?view=graph-rest-1.0

https://docs.microsoft.com/en-us/graph/api/resources/directoryaudit?view=graph-rest-1.0

https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema?view=o365-worldwide