SCOPE CERTIFIED APPLICATION INSTALLATION AND CONFIGURATION GUIDE

Vectra Detect ServiceNow SIR Integration (1.1.0)

Contents

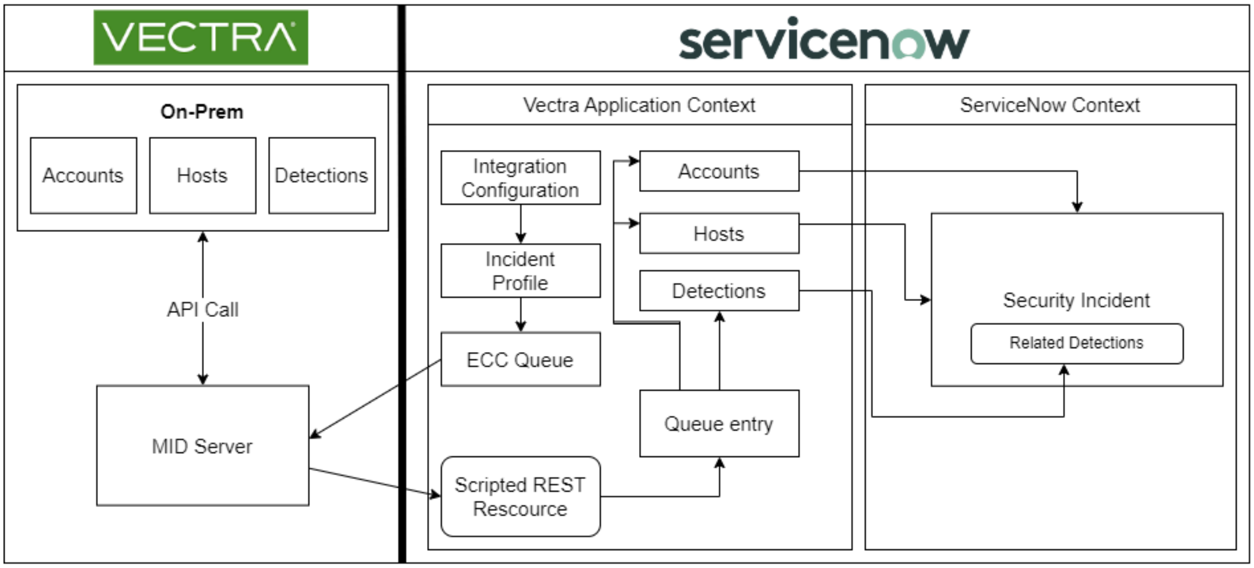
1. Overview

The Vectra threat detection & response platform captures packets and logs across your public cloud, SaaS, federated identity, and data center networks. It applies patented security-led AI to the surface, prioritizes threats, and integrates into your security stack for rapid response.

1.1. Vectra ServiceNow Application

Vectra Detect for SIR application fetches all active Accounts, Hosts, and Detections from the Vectra Detect and ingests data into the ServiceNow. It provides the capability of creating "Security Incidents" based on the defined condition/criteria. It provides support to perform manual actions on fetched accounts, hosts, and detections and also provides support for SOAR Action: Observable Enrichment.

System Architecture



1.2. Application features

The main features of the integration include:

1. Ability to fetch all the active accounts and/or hosts from the Vectra Detect.
2. Ability to fetch detections associated with accounts and/or hosts.
3. Ability to configure Security Incident creation criteria and create Security Incidents based on the same.

4. Ability to assign Security Incidents to a specific user.
5. Ability to map account/host fields with Security Incident fields.
6. Ability to add/remove a tag to a host, account, or detection in Vectra Detect.
7. Ability to add a note to a host, account, or detection in Vectra Detect.
8. Ability to download a PCAP attached to a detection.
9. Ability to mark the detection/s as fixed from ServiceNow.
10. Ability to enrich the observables based on IP(s).

1.3. Compatibility Matrix

ServiceNow Version: Utah, Vancouver and Washington DC

Vectra API Version: v2.2

2. Vectra Detect for SIR

2.1. Mid Server Installation

This section describes how to set up the Mid Server. Below is the ServiceNow official document for setup the mid-server: https://docs.servicenow.com/bundle/rome-servicenow-platform/page/product/mid-server/concept/mid-server-installation.html

2.2. Installation

This section describes how to download and install the Vectra Detect for SIR application from the store.

2.3. Pre-requisites

- Security Incident Response - 12.9.5
- Threat Intelligence - 13.1.1

2.3.1. Permissions and Roles

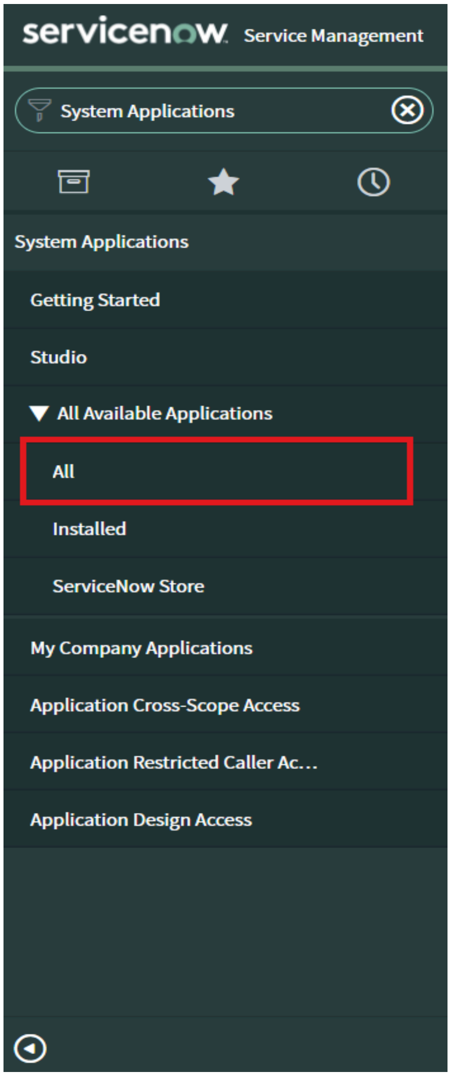
These are the ServiceNow roles and the permissions that are needed to install and use the application.

Role	Permissions
System Administrator (admin)	● Application Log

Vectra SIR Admin (x_cdsp_vectra_sir.admin, sn_si.admin,export_set_scheduler, itil, view_changer)	● Authentication Tile ● Incident Profile Configuration ● Incident Assignee ● Manual Action ● SOAR Action ● Process Monitor
Vectra SIR User (x_cdsp_vectra_sir.user,sn_si.admin,export_set_scheduler,sn_ti.admin, itil, view_changer)	● View Vectra Accounts, Hosts, Detections, and Security Incidents ● Manual Action ● SOAR Action
mid_server	● Data Collection ● File Attachment

2.3.2. Application Download and Installation

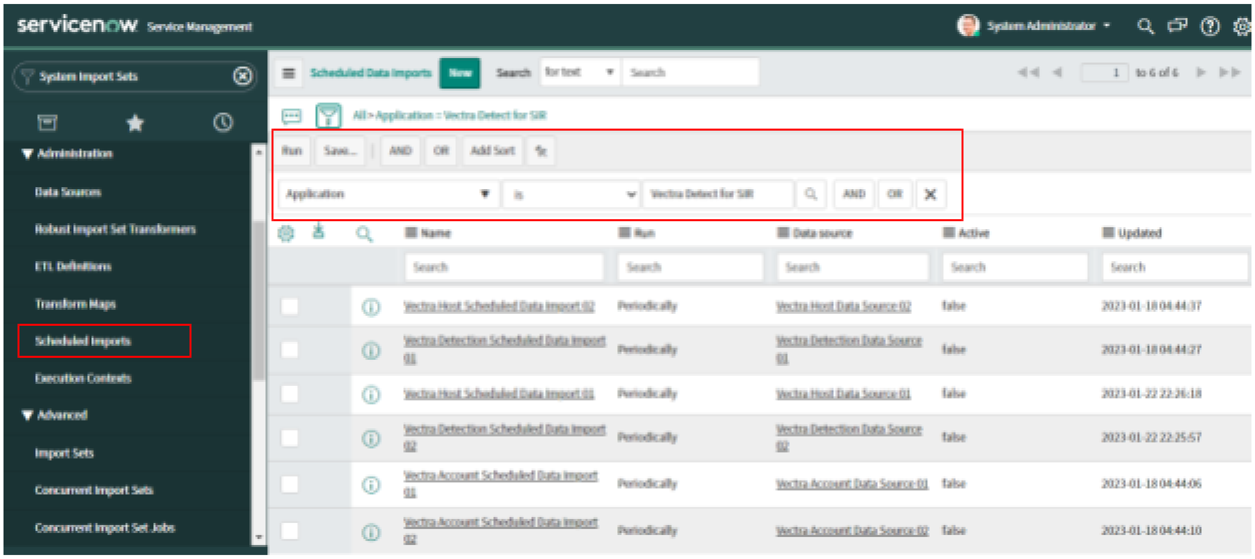
- Login to the instance on which you want to install the application.
- Navigate to “System Applications” □ “All Available applications” □ “All”.


servicenow Service Management
System Applications
System Applications
Getting Started
Studio
All Available Applications
All
Installed
ServiceNow Store
My Company Applications
Application Cross-Scope Access
Application Restricted Caller Ac...
Application Design Access

- Mark Check the “Not Installed” checkbox. A list of applications available for installation is displayed.
- Locate the Vectra Detect for SIR application, select it, and click “Install”.
- The application will be installed into your instance.

2.3.3. Activate Scheduled Data Import

1. Log in to the instance on which you have installed the application.
2. Navigate to “System Applications” “System Import Sets” “Administration” ” Scheduled Imports”.

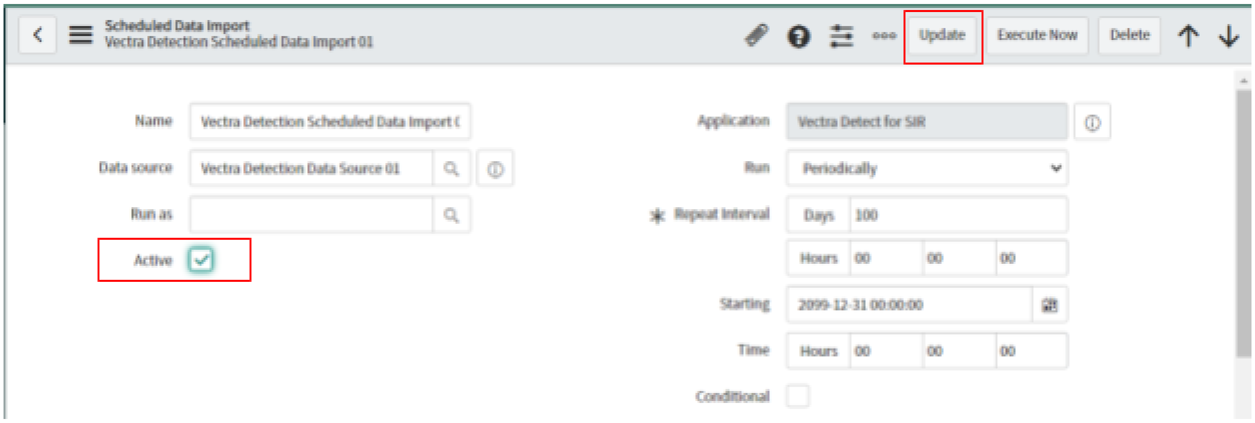


All > Application = Vectra Detect for SIR

Application ▼ is Vectra Detect for SIR

Name	Run	Data source	Active	Updated
Vectra Host Scheduled Data Import 02	Periodically	Vectra Host Data Source 02	false	2023-01-18 04:44:37
Vectra Detection Scheduled Data Import 01	Periodically	Vectra Detection Data Source 01	false	2023-01-18 04:44:27
Vectra Host Scheduled Data Import 01	Periodically	Vectra Host Data Source 01	false	2023-01-22 22:26:18
Vectra Detection Scheduled Data Import 02	Periodically	Vectra Detection Data Source 02	false	2023-01-22 22:25:57
Vectra Account Scheduled Data Import 01	Periodically	Vectra Account Data Source 01	false	2023-01-18 04:44:06
Vectra Account Scheduled Data Import 02	Periodically	Vectra Account Data Source 02	false	2023-01-18 04:44:10

3. Filter the Scheduled Data Imports by Application “Vectra Detect for SIR”.
4. Activate all Records by Marking “Active” as true and clicking on “Update”.



Scheduled Data Import
Vectra Detection Scheduled Data Import 01

Name	Vectra Detection Scheduled Data Import (	Application	Vectra Detect for SIR
Data source	Vectra Detection Data Source 01	Run	Periodically
Run as		Repeat Interval	Days 100 Hours 00 00 00
Active	☑	Starting	2099-12-31 00:00:00
		Time	Hours 00 00 00
		Conditional	□

Note: Data ingestion will not start unless Scheduled Data Imports are Inactive.

2.4. Configuration

This section describes how to configure ServiceNow and Vectra to use the application.

2.4.1. Create Users

The ServiceNow admin creates the various Vectra users.

Username (for example)	Role to be assigned
Vectra SIR admin	● x_cdsp_vectra_sir.admin ● sn_si.admin

	● export_set_schedular ● Itil ● view_changer
Vectra SIR user	● x_cdsp_vectra_sir.user ● sn_si.admin ● export_set_schedular ● Itil ● view_changer
MID Server user	● x_cdsp_vectra_sir.admin ● mid_server

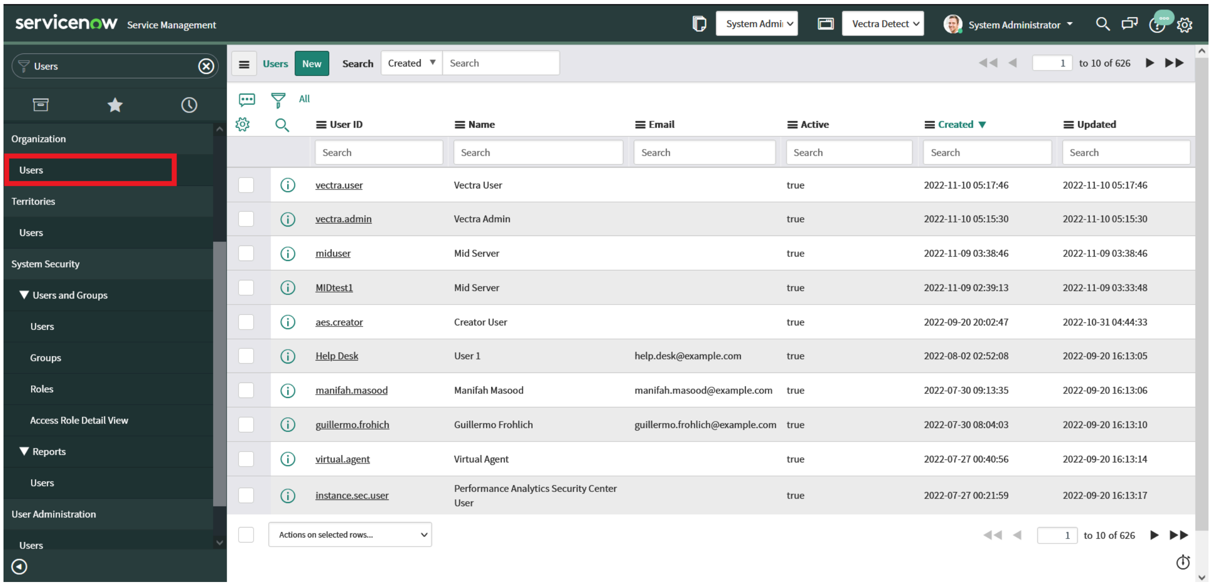
Note: MID Server user should have x_cdsp_vectra_sir.admin role for Vectra Detect for SIR data ingestion.

Below is the example showing how to create a Vectra user and assign the role to it.

Role Required: System Administrator (admin)

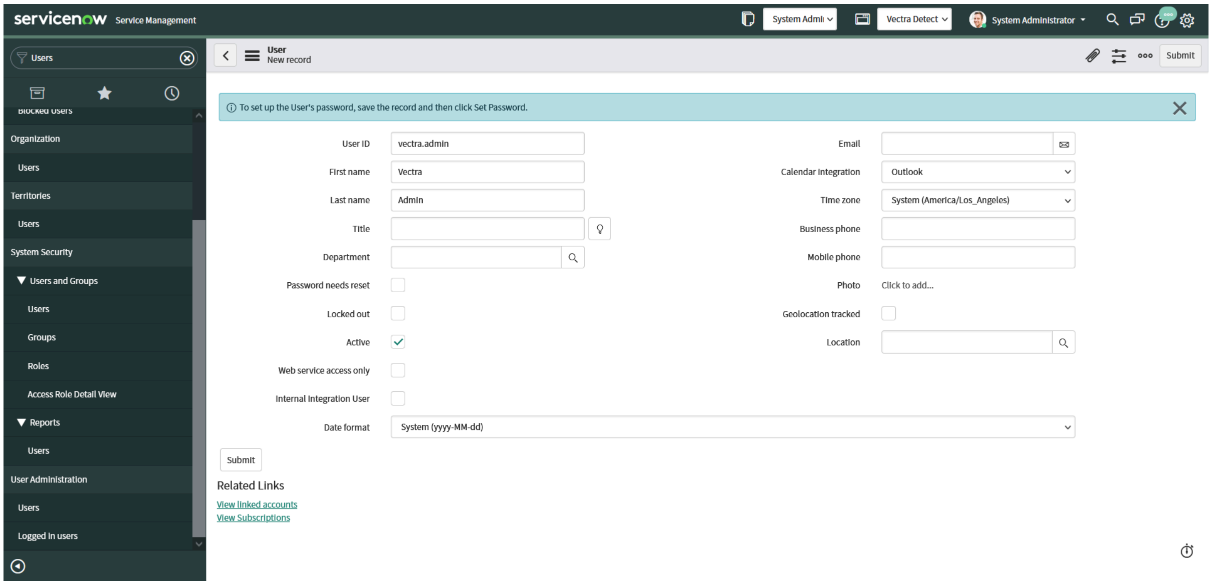
Procedure:

1. Navigate to “Organization” “Users”.
2. Click the “Users” module.



User ID	Name	Email	Active	Created	Updated
vectra.user	Vectra User		true	2022-11-10 05:17:46	2022-11-10 05:17:46
vectra.admin	Vectra Admin		true	2022-11-10 05:15:30	2022-11-10 05:15:30
miduser	Mid Server		true	2022-11-09 03:38:46	2022-11-09 03:38:46
MIDtest1	Mid Server		true	2022-11-09 02:39:13	2022-11-09 03:33:48
aes.creator	Creator User		true	2022-09-20 20:02:47	2022-10-31 04:44:33
Help Desk	User 1	help.desk@example.com	true	2022-08-02 02:52:08	2022-09-20 16:13:05
manifah.masood	Manifah Masood	manifah.masood@example.com	true	2022-07-30 09:13:35	2022-09-20 16:13:06
guillermo.frohich	Guillermo Frohlich	guillermo.frohlich@example.com	true	2022-07-30 08:04:03	2022-09-20 16:13:10
virtual.agent	Virtual Agent		true	2022-07-27 00:40:56	2022-09-20 16:13:14
instance.sec.user	Performance Analytics Security Center User		true	2022-07-27 00:21:59	2022-09-20 16:13:17

3. On the Users list, click "New". A new user form is displayed.



To set up the User's password, save the record and then click Set Password.

User ID	vectra.admin	Email	
First name	Vectra	Calendar integration	Outlook
Last name	Admin	Time zone	System (America/Los_Angeles)
Title		Business phone	
Department		Mobile phone	
Password needs reset	□	Photo	Click to add...
Locked out	□	Geolocation tracked	□
Active	☑	Location	
Web service access only	□		
Internal Integration User	□		
Date format	System (yyyy-MM-dd)		

Related Links

View linked accounts

View Subscriptions

4. Fill in the form.

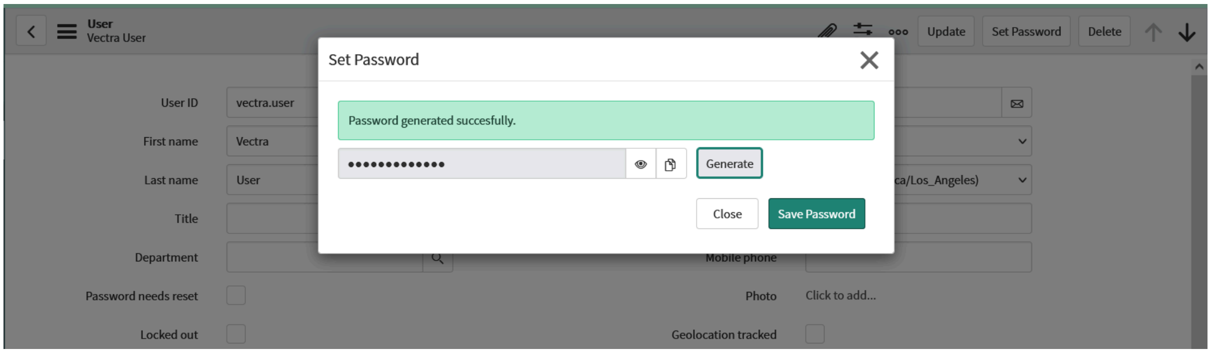
Note: The values for the User ID, title, and email address shown in the following table and figure are example values.

Field	Description
User ID	Unique User ID for the role in your ServiceNow Platform

	instance. An example is Vectra_sir_admin.
First Name	First Name of the user you are assigning
Last Name	Last Name of the user you are assigning
Title	Job Title, for example, Vectra Admin
Password	Unique password created for this role
Email	Unique email address

Note: From San Diego and later versions of ServiceNow password creation is changed.

5. Click “Submit”. Once submitted, you can assign the role.
6. On the Users list, click on the name of the new user you created, Vectra_sir_admin, for example.
7. Once the record is open, the Set Password UI is visible in the form view of the record.
8. Click on the Set Password UI action.



User
Vectra User

Set Password

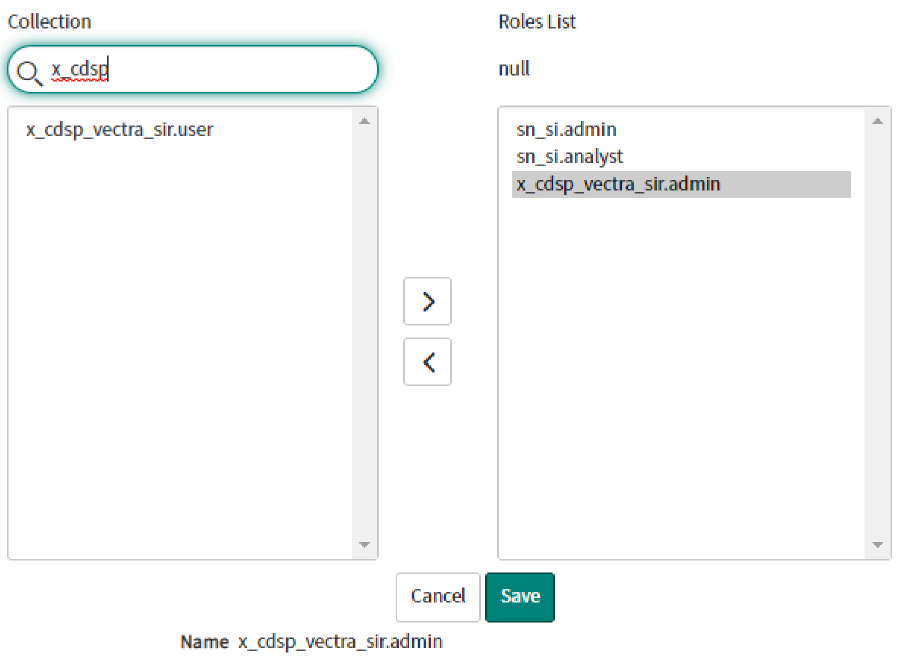
Password generated succesfully.

•••••••••••••

User ID	vectra.user
First name	Vectra
Last name	User
Title	
Department	
Password needs reset	□
Locked out	□
Mobile phone	
Photo	Click to add...
Geolocation tracked	□

ca/Los_Angeles)

9. One pop-up will be displayed by clicking on “Generate” this will generate a unique password for the created user that needs to be changed on the first log-in.
10. Copy the generated password and close the popup.
11. Once the record is open, go to the Roles section, and click “Edit”.
12. On the Edit Members form, enter the required role in the Collection field.
13. In the Collection column, select and move the required roles to the Roles List.



14. Click “Save”.

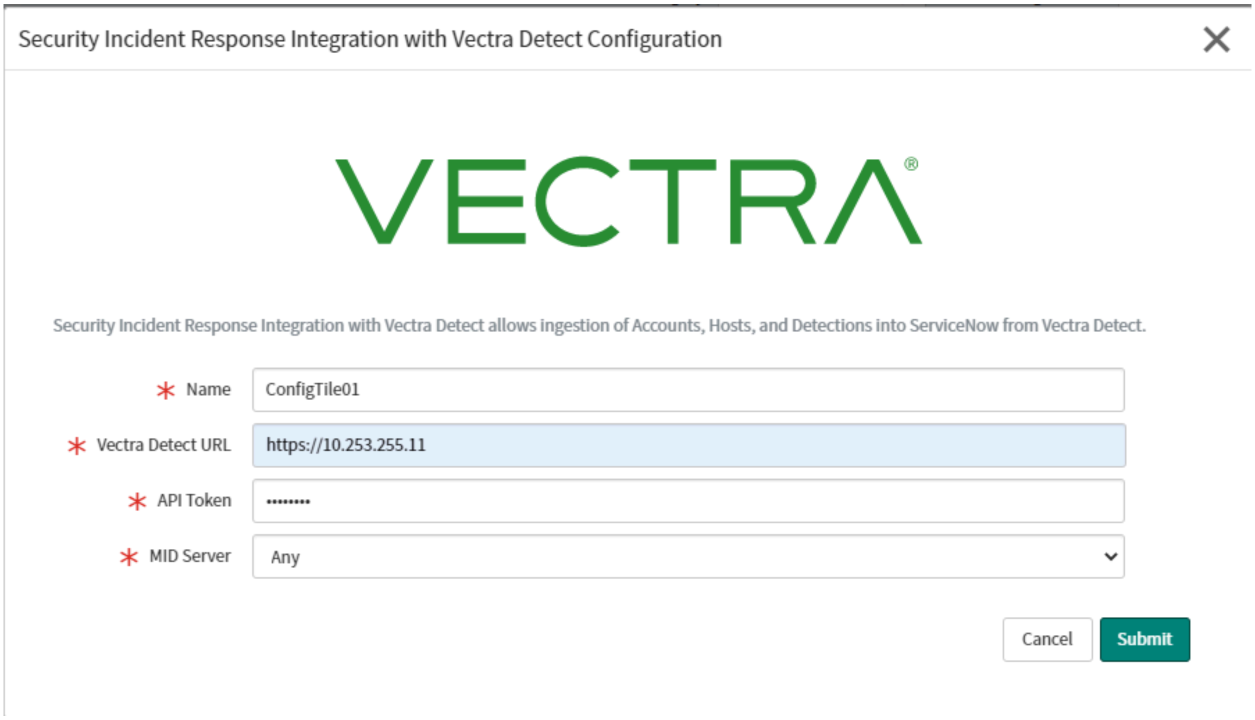
2.4.2. Integration Configuration

This section describes how to configure the integration tile, which is used in Incident Profile as authentication to populate ServiceNow with Security Incidents from Vectra, perform manual actions, and observable enrichment.

Role Required: x_cdsp_vectra_sir.admin,sn_si.admin

Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Security Operations > Integrations > Integration Configurations”.
3. Click on the “Configure” button of the “Security Incident Response Integration with Vectra Detect” Integration tile.



Security Incident Response Integration with Vectra Detect Configuration

Security Incident Response Integration with Vectra Detect allows ingestion of Accounts, Hosts, and Detections into ServiceNow from Vectra Detect.

* Name	ConfigTile01
* Vectra Detect URL	https://10.253.255.11
* API Token	••••••••
* MID Server	Any

4. Insert valid Name, Vectra Detect URL, and API Token, and also Select MID Server.
5. Click on “Submit” to authenticate.
6. On success “Authentication is Successful” message is shown.

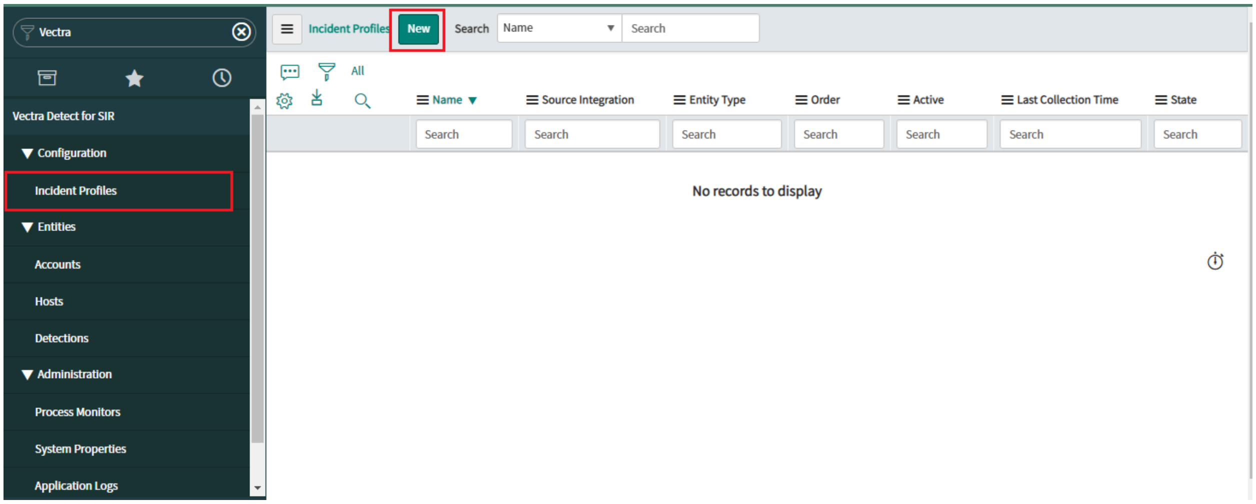
2.4.3. Incident Profile

This section describes how to configure a profile for receiving the Accounts, Hosts, and Detections for the “Vectra Detect for SIR” application, which is used to populate ServiceNow’s with Security Incidents.

Role Required: x_cdsp_vectra_sir.admin

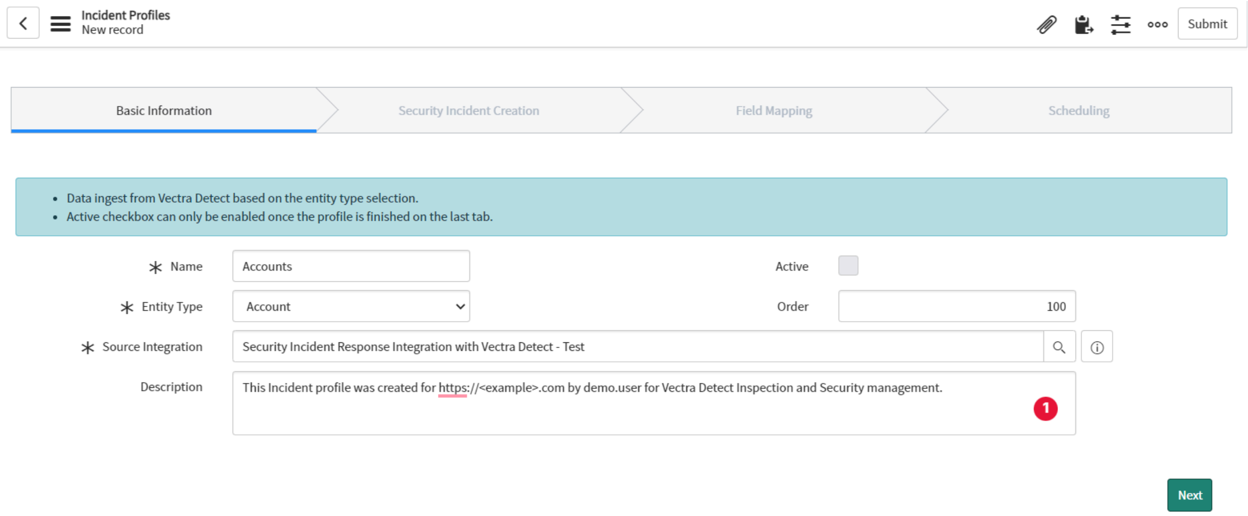
Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR” ⍰ “Configuration”.
3. Click on “Incident Profile”.



4. Click on New. It will open a new Incident profile view.
5. In the “Basic Information” section select Source Integration and Entity Type record for which data needs to be collected and enter Name, Order, and Description. Then click on “Next”.

Note: The below shown active field will be read-only unless all the tabs for the incident profile are configured and data ingestion will not start unless the profile is active.

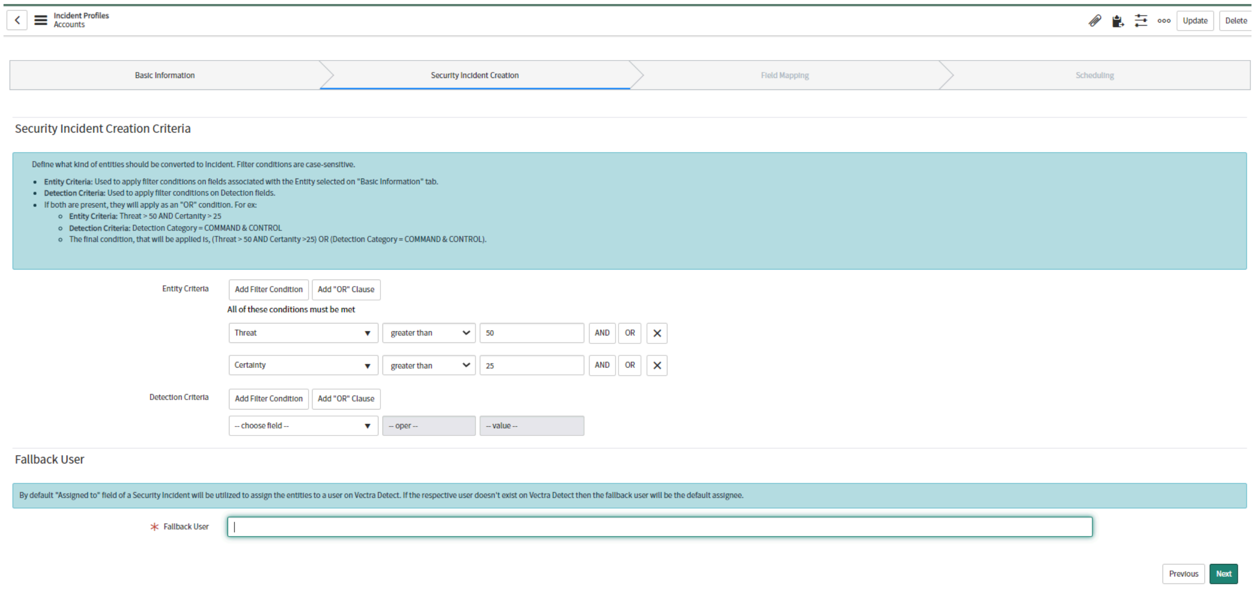


- Data ingest from Vectra Detect based on the entity type selection.
- Active checkbox can only be enabled once the profile is finished on the last tab.

* Name	Accounts	Active	□
* Entity Type	Account	Order	100
* Source Integration	Security Incident Response Integration with Vectra Detect - Test		
Description	This Incident profile was created for https://<example>.com by demo.user for Vectra Detect Inspection and Security management.		

6. In the “Security Incident Creation” section users can provide Security Incident Creation Criteria and Fallback User.
   6.1. Security Incidents will be created as per the conditions specified in the Creation Criteria.
   6.2. If no condition is provided then a Security Incident will be created for all entities (Account/Host) fetched.
   6.3. If the Security Incident Assignee does not exist on the Vectra Detect then the

associated Account/Host will be assigned to configured Fallback User on the Vectra Detect.



Security Incident Creation Criteria

Define what kind of entities should be converted to Incident. Filter conditions are case-sensitive.

- **Entity Criteria:** Used to apply filter conditions on fields associated with the Entity selected on "Basic Information" tab.
- **Detection Criteria:** Used to apply filter conditions on Detection fields.
- If both are present, they will apply as an "OR" condition. For ex:
  - **Entity Criteria:** Threat > 50 AND Certanity > 25
  - **Detection Criteria:** Detection Category = COMMAND & CONTROL
  - The final condition, that will be applied is, (Threat > 50 AND Certanity >25) OR (Detection Category = COMMAND & CONTROL).

Entity Criteria

All of these conditions must be met

Threat greater than 50

Certainty greater than 25

Detection Criteria

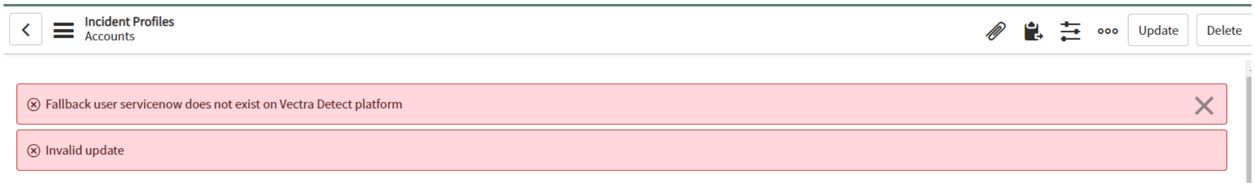
-- choose field -- -- oper -- -- value --

Fallback User

By default "Assigned to" field of a Security Incident will be utilized to assign the entities to a user on Vectra Detect. If the respective user doesn't exist on Vectra Detect then the fallback user will be the default assignee.

* Fallback User

Note: If a user enters a username that does not exist on the Vectra Detect, an error message will be shown at the top of the incident profile.



Fallback user servicenow does not exist on Vectra Detect platform

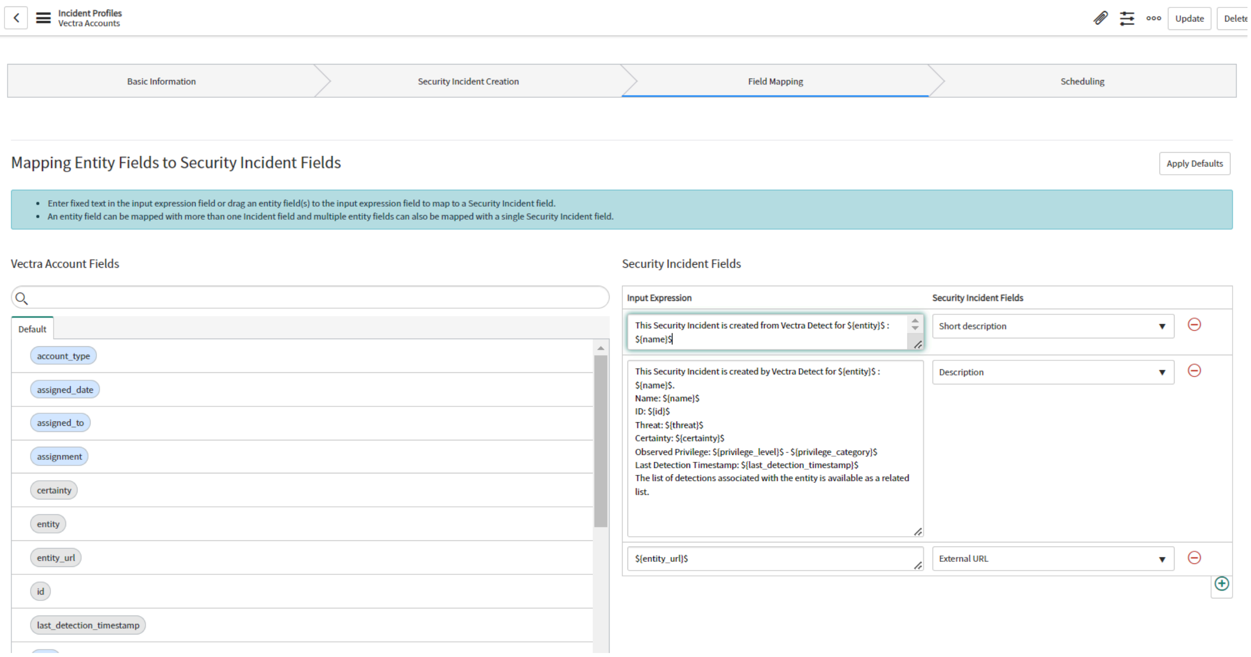
Invalid update

7. After Configuring the Security Incident Criterion Tab user can navigate to Field Mapping by clicking on the ‘Next” button.

   7.1. In the “Field Mapping” section, users can map the Vectra entity (Account/Host) fields to the Security Incidents fields and click on the next button.

   7.2. Users can reapply for the default mapping by clicking on the “Apply Defaults” button.

   7.3. If no field is mapped then the ID will be mapped to a short description.



Mapping Entity Fields to Security Incident Fields

- Enter fixed text in the input expression field or drag an entity field(s) to the input expression field to map to a Security Incident field.
- An entity field can be mapped with more than one Incident field and multiple entity fields can also be mapped with a single Security Incident field.

Vectra Account Fields

Security Incident Fields

Input Expression	Security Incident Fields
This Security Incident is created from Vectra Detect for ${entity}$: ${name}$	Short description
This Security Incident is created by Vectra Detect for ${entity}$: ${name}$. Name: ${name}$ ID: ${id}$ Threat: ${threat}$ Certainty: ${certainty}$ Observed Privilege: ${privilege_level}$ - ${privilege_category}$ Last Detection Timestamp: ${last_detection_timestamp}$ The list of detections associated with the entity is available as a related list.	Description
${entity_url}$	External URL

8. The user can ingest the data using the scheduling tab.

   8.1. One-Time Data Collection: The user can fetch the historical data for the selected entity using One-Time Data Collection.

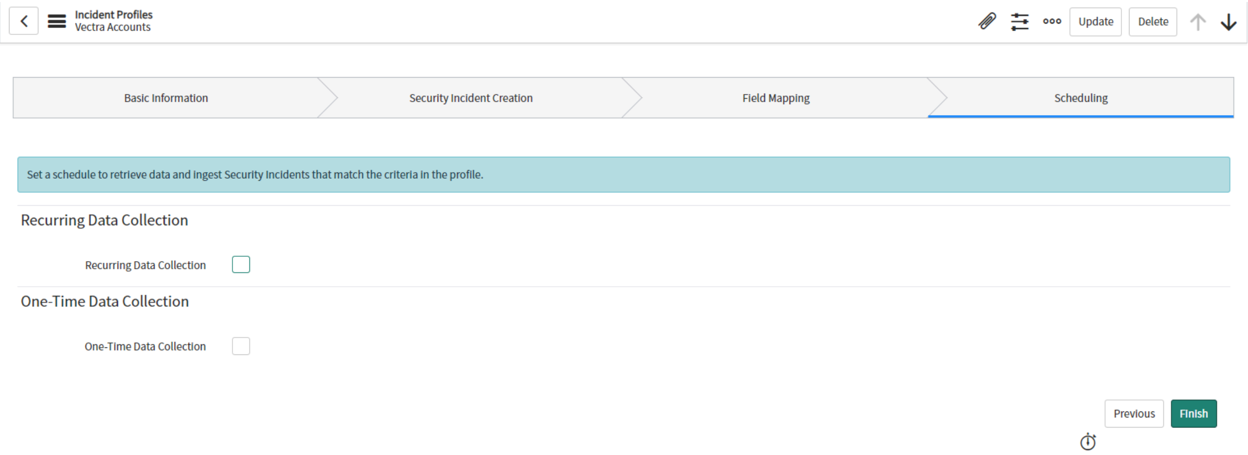
   8.2. Recurring Data Collection: The user can start recurring data collection by enabling the Recurring Data Collection. The user can specify the interval time(more than 18 sec) to run the recurring data collection.

   Note: The time interval should be greater than 18 seconds. Recurring start time will control when to begin this ingestion, if left empty, data ingestion will begin as soon as you click on update and your profile is in the active state.

   8.3. First Collection Time: Date/Time of first data collection.

   8.4. Last Collection Time: Date/Time of the last collection was completed.

   8.5. Next Collection Time: Date/Time of the next collection will start.



Set a schedule to retrieve data and ingest Security Incidents that match the criteria in the profile.

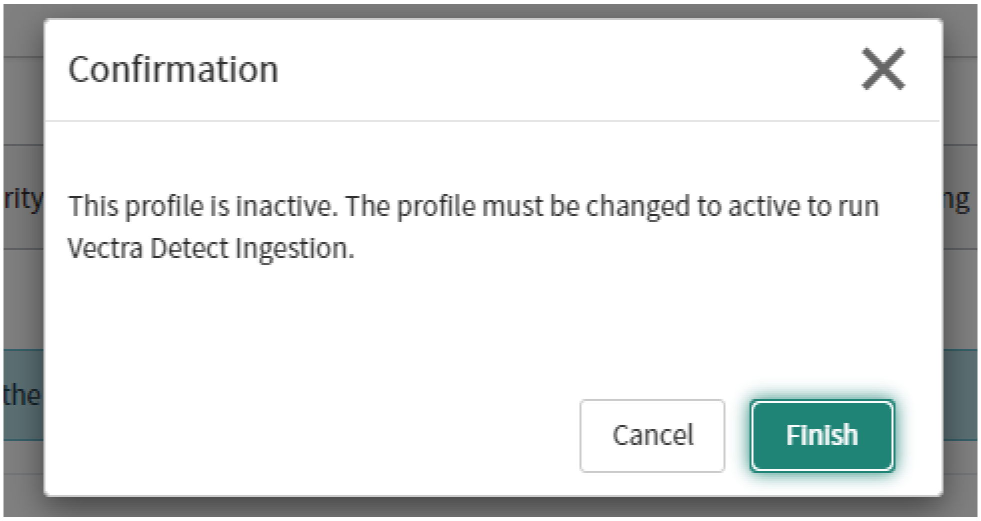
Recurring Data Collection

Recurring Data Collection □

One-Time Data Collection

One-Time Data Collection □

9. On clicking on the finish button the user will be prompted with the message that notifies the user that the profile is inactive and that for data collection the user needs to activate the incident profile.



This profile is inactive. The profile must be changed to active to run Vectra Detect Ingestion.

10. The user needs to revisit the same incident profile and mark the active checkbox as true under the basic information tab to start the data ingestion.

Note:

- It is recommended not to change any Incident profile configuration when the state of the profile is “Running”.
- Marking the field as inactive and then marking it again active for recurring data will lead to data loss.
- Changing the time field with improper date time will lead to data loss.

2.5. Entities

This section populates the records of different entities (Account/Host/Detections) with Security Incidents (Account/Host) and also provides a detailed view of the selected entity record that is fetched through data collection.

Prerequisite: Authentication configuration. (See Integration Configuration).

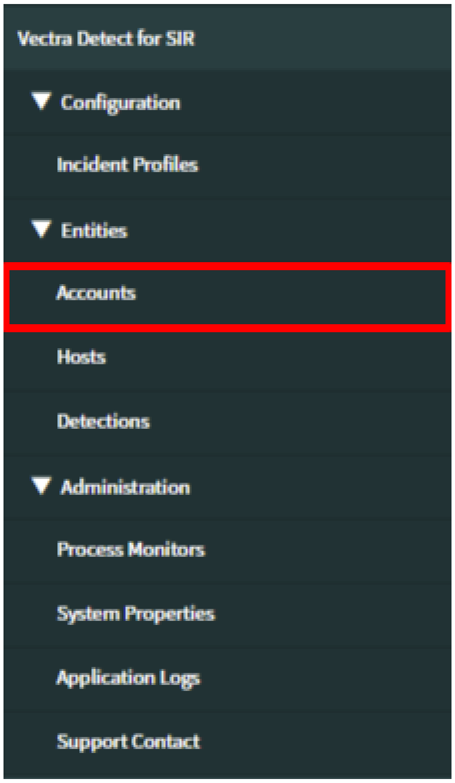
2.5.1. Accounts

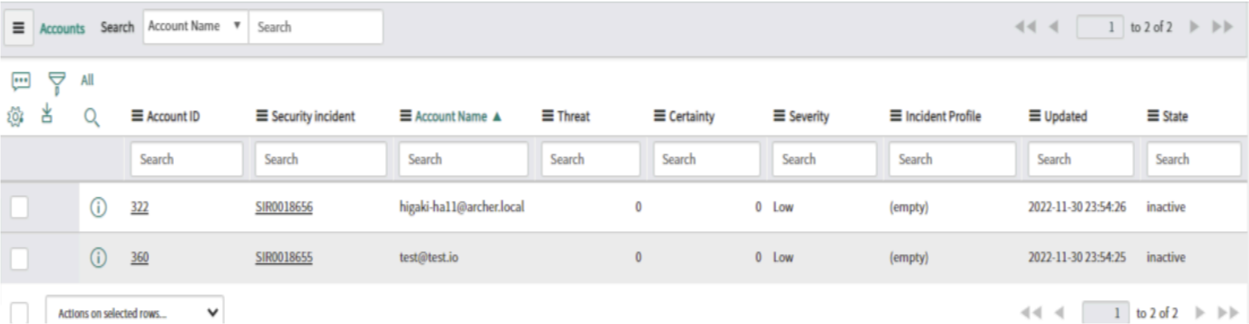
Users can view accounts that have been fetched from the Vectra Detect in the "Account" section. A list of accounts and their details is available to users. Users can also create a Security Incident from a specific account.

Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

1. Log in to ServiceNow Instance
2. Navigate to “Vectra Detect for SIR > Entities > Accounts”.

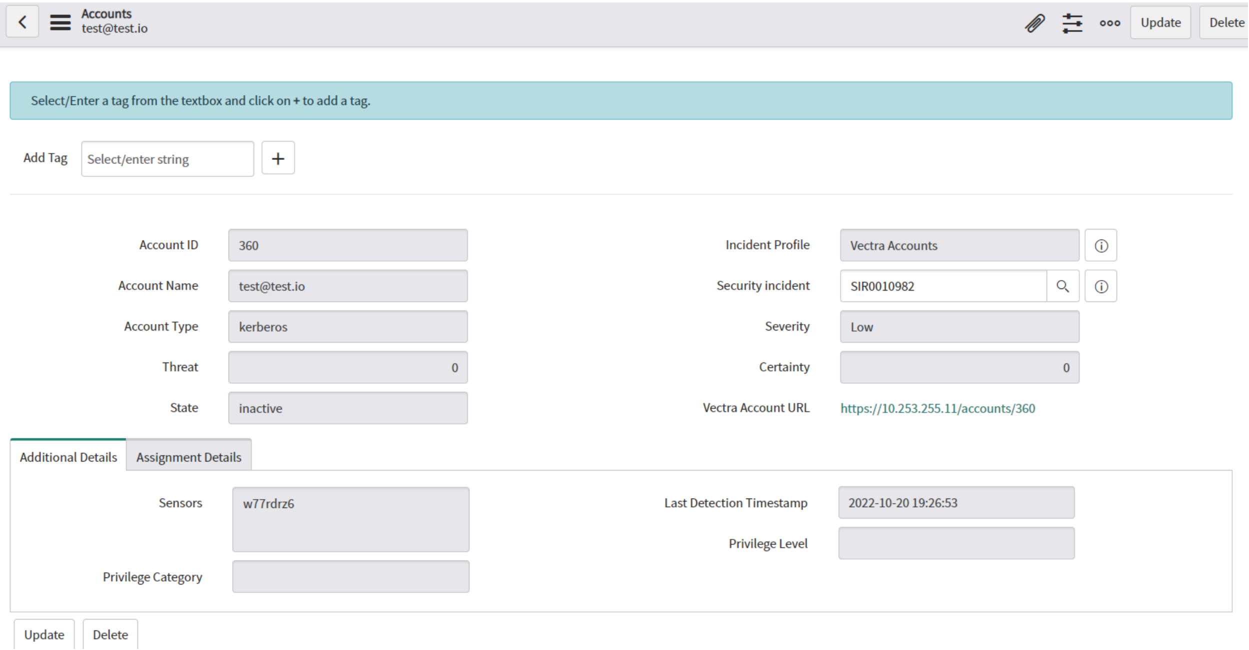




Account ID	Security incident	Account Name ▲	Threat	Certainty	Severity	Incident Profile	Updated	State
322	SIR0018656	higaki-ha11@archer.local	0	0	Low	(empty)	2022-11-30 23:54:26	inactive
360	SIR0018655	test@test.io	0	0	Low	(empty)	2022-11-30 23:54:25	inactive

3. Click on any Account record that you want to open.

4. Users can view account details. The user can see all the tags at the top of the form, and all fields—aside from the "Security Incident Field"—will be read-only.



Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag: Select/enter string

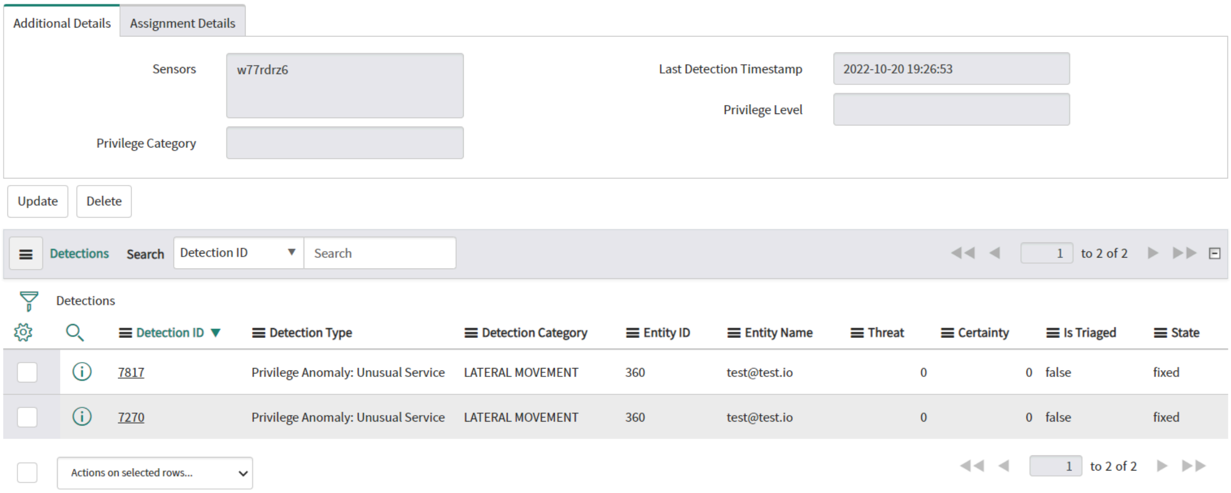
Account ID	360	Incident Profile	Vectra Accounts
Account Name	test@test.io	Security incident	SIR0010982
Account Type	kerberos	Severity	Low
Threat	0	Certainty	0
State	inactive	Vectra Account URL	https://10.253.255.11/accounts/360

Sensors	w77rdrz6	Last Detection Timestamp	2022-10-20 19:26:53
		Privilege Level	
Privilege Category			

5. Reference link for the associated Security Incident is available if the selected record satisfies the condition of automatic Security Incident creation criteria.

6. The user will be able to add/remove the tags and these tags will be synced back to Vectra Detect.

7. Detections related to the account will be listed at the bottom of the form.



Additional Details | Assignment Details

Sensors	w77rdrz6	Last Detection Timestamp	2022-10-20 19:26:53
		Privilege Level	
Privilege Category			

Update | Delete

Detections Search Detection ID Search 1 to 2 of 2

Detections

		Detection ID ▼	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State
□	ⓘ	7817	Privilege Anomaly: Unusual Service	LATERAL MOVEMENT	360	test@test.io	0	0	false	fixed
□	ⓘ	7270	Privilege Anomaly: Unusual Service	LATERAL MOVEMENT	360	test@test.io	0	0	false	fixed

□ Actions on selected rows... 1 to 2 of 2

8. A user may create a security incident for a given account if the security incident associated with it is either closed or blank by clicking on “Create Security Incident”.

9. When a Security Incident is created, a message with the phrase "Security Incident INCIDENT-NUMBER> created successfully" is displayed to the user.

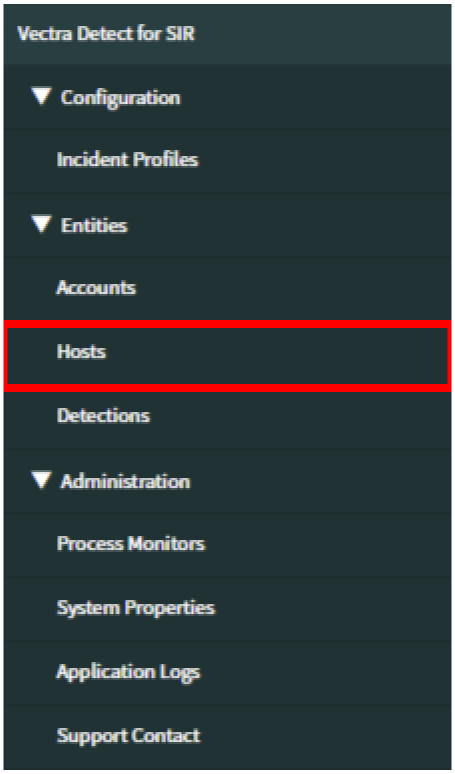
2.5.2. Hosts

The "Host" section of the user interface lets users view hosts that have been fetched from the Vectra Detect. Users can view a list of hosts. Users can also create a Security Incident for a specific host.

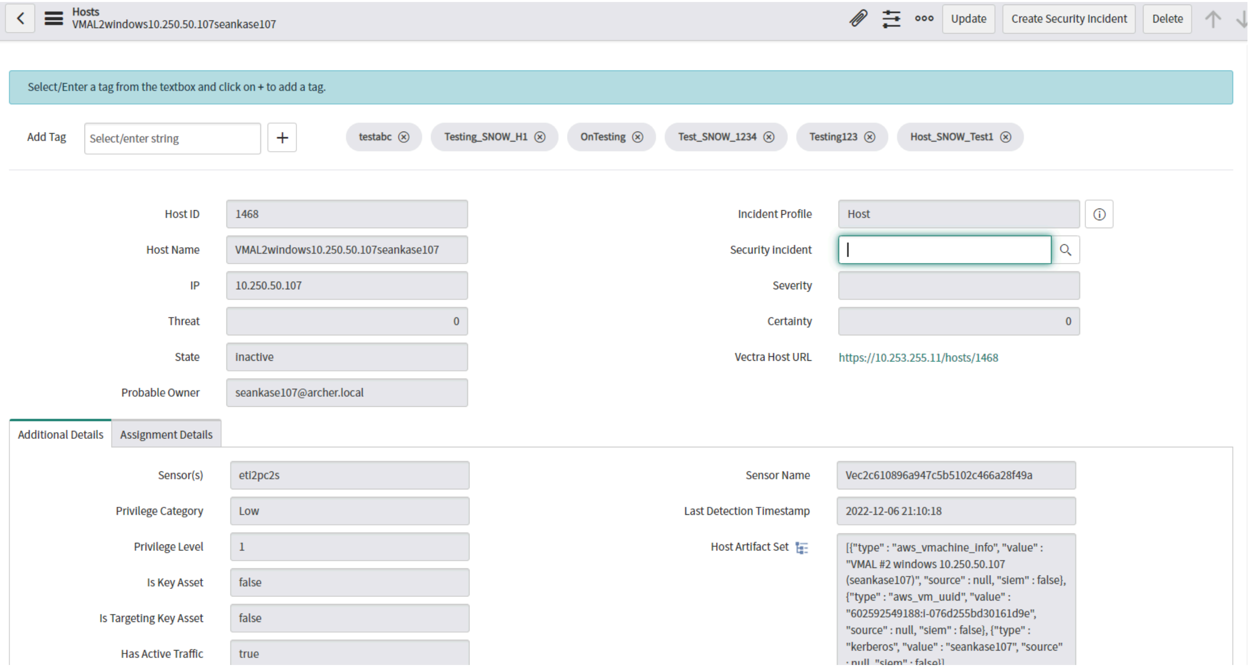
Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

1. Log in to ServiceNow Instance
2. Navigate to “Vectra Detect for SIR > Entities > Hosts”.



3. Click on any Host record that you want to open.
4. Users can view host details. The user can see all the tags at the top of the form, and all fields—aside from the "Security Incident Field"—will be read-only.
5. Reference link for the associated Security Incident is available if the selected record satisfies the condition of automatic Security Incident creation criteria.

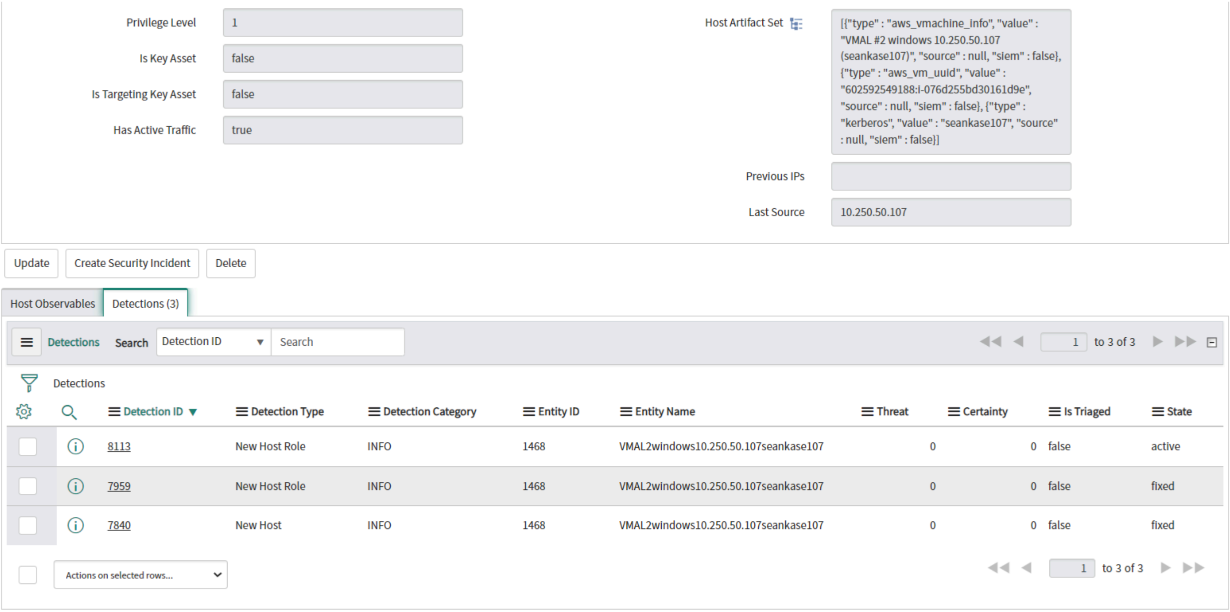


Select/Enter a tag from the textbox and click on + to add a tag.

Host ID	1468	Incident Profile	Host
Host Name	VMAL2windows10.250.50.107seankase107	Security Incident	
IP	10.250.50.107	Severity	
Threat	0	Certainty	0
State	inactive	Vectra Host URL	https://10.253.255.11/hosts/1468
Probable Owner	seankase107@archer.local		

Sensor(s)	etl2pc2s	Sensor Name	Vec2c610896a947c5b5102c466a28f49a
Privilege Category	Low	Last Detection Timestamp	2022-12-06 21:10:18
Privilege Level	1	Host Artifact Set	[{"type" : "aws_vmachine_info", "value" : "VMAL #2 windows 10.250.50.107 (seankase107)", "source" : null, "siem" : false}, {"type" : "aws_vm_uuid", "value" : "602592549188:i-076d255bd30161d9e", "source" : null, "siem" : false}, {"type" : "kerberos", "value" : "seankase107", "source" : null, "siem" : false}]
Is Key Asset	false		
Is Targeting Key Asset	false		
Has Active Traffic	true		

6. The user will be able to add/remove the tags and these tags will be synced back to Vectra Detect.
7. Related list of associated detections and host observables will be populated at the bottom of the form view.



Privilege Level	1	Host Artifact Set	[{"type" : "aws_vmachine_info", "value" : "VMAL #2 windows 10.250.50.107 (seankase107)", "source" : null, "siem" : false}, {"type" : "aws_vm_uuid", "value" : "602592549188:i-076d255bd30161d9e", "source" : null, "siem" : false}, {"type" : "kerberos", "value" : "seankase107", "source" : null, "siem" : false}]
Is Key Asset	false		
Is Targeting Key Asset	false		
Has Active Traffic	true		
		Previous IPs	
		Last Source	10.250.50.107

Detection ID ▼	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State
8113	New Host Role	INFO	1468	VMAL2windows10.250.50.107seankase107	0	0	false	active
7959	New Host Role	INFO	1468	VMAL2windows10.250.50.107seankase107	0	0	false	fixed
7840	New Host	INFO	1468	VMAL2windows10.250.50.107seankase107	0	0	false	fixed

8. A user may create a Security Incident for a given host if the incident associated with it is either closed or blank by clicking on "Create Security Incident".

9. When a Security Incident is created, a message with the phrase "Security Incident INCIDENT-NUMBER> created successfully" is displayed to the user.

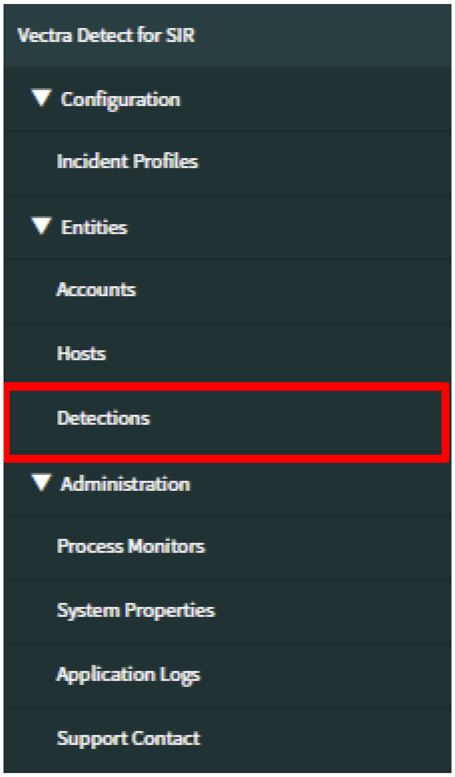
2.5.3. Detections

The "Detections" section of the user interface lets users view active detections that have been fetched from the Vectra Detect. Users can view a list of detections. The user can download a PCAP file by clicking on the “Download PCAP” button.Users can mark a detection as fixed by clicking “Mark as Fixed”. Add and remove tags. Users can also add notes that will be reflected back to the Vectra Detect.

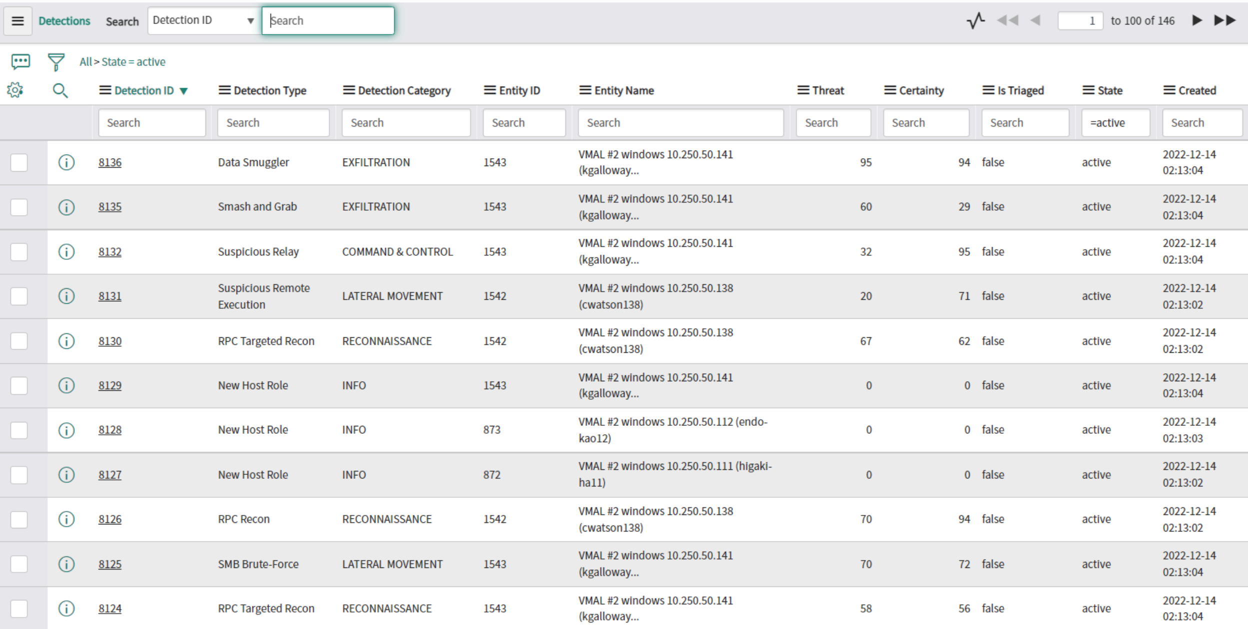
Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

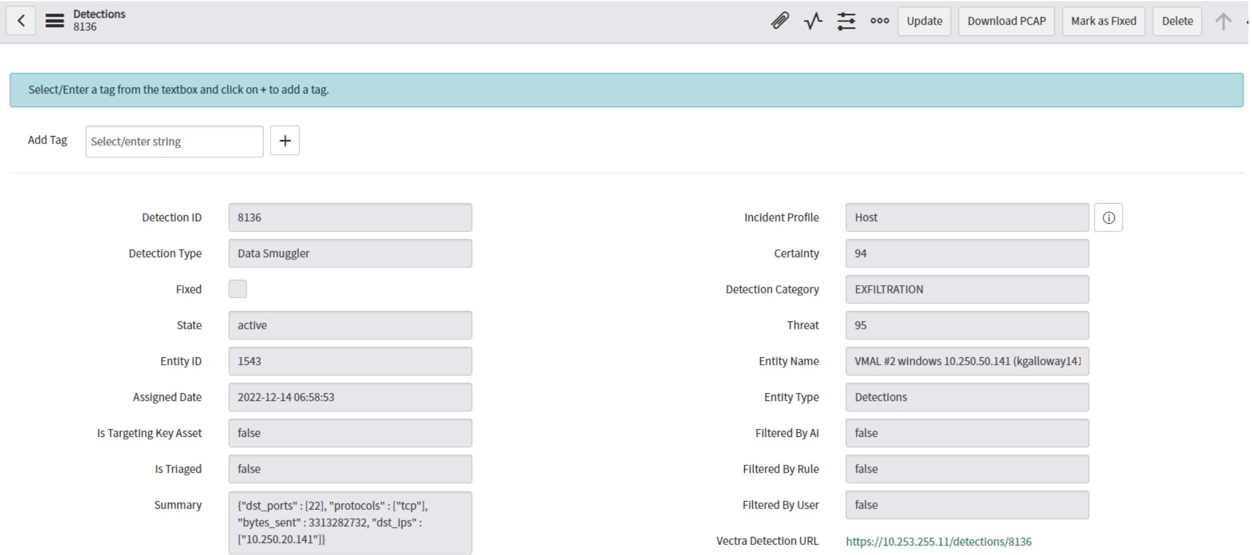
1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR > Entities > Detections”.
3. Click on any Detection record that you want to open.



4. Users can view detection details. The user can see all the tags at the top of the form, and all fields—aside from the "Notes"—will be read-only.



Detection ID	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State	Created
Search	Search	Search	Search	Search	Search	Search	Search	=active	Search
8136	Data Smuggler	EXFILTRATION	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	95	94	false	active	2022-12-14 02:13:04
8135	Smash and Grab	EXFILTRATION	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	60	29	false	active	2022-12-14 02:13:04
8132	Suspicious Relay	COMMAND & CONTROL	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	32	95	false	active	2022-12-14 02:13:04
8131	Suspicious Remote Execution	LATERAL MOVEMENT	1542	VMAL #2 windows 10.250.50.138 (cwatson138)	20	71	false	active	2022-12-14 02:13:02
8130	RPC Targeted Recon	RECONNAISSANCE	1542	VMAL #2 windows 10.250.50.138 (cwatson138)	67	62	false	active	2022-12-14 02:13:02
8129	New Host Role	INFO	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	0	0	false	active	2022-12-14 02:13:04
8128	New Host Role	INFO	873	VMAL #2 windows 10.250.50.112 (endo-kao12)	0	0	false	active	2022-12-14 02:13:03
8127	New Host Role	INFO	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	0	0	false	active	2022-12-14 02:13:02
8126	RPC Recon	RECONNAISSANCE	1542	VMAL #2 windows 10.250.50.138 (cwatson138)	70	94	false	active	2022-12-14 02:13:02
8125	SMB Brute-Force	LATERAL MOVEMENT	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	70	72	false	active	2022-12-14 02:13:04
8124	RPC Targeted Recon	RECONNAISSANCE	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	58	56	false	active	2022-12-14 02:13:04

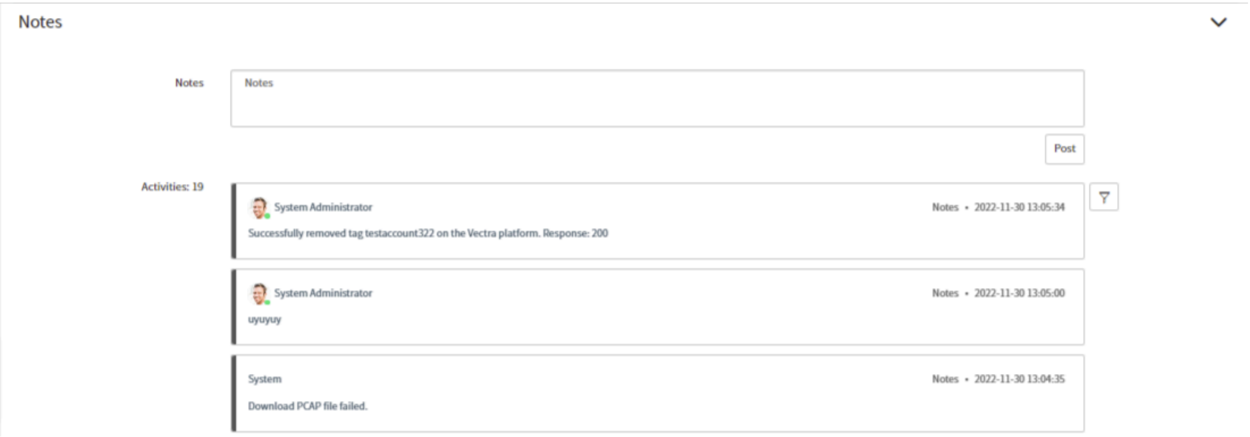


Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag: Select/enter string +

Detection ID	8136	Incident Profile	Host
Detection Type	Data Smuggler	Certainty	94
Fixed	□	Detection Category	EXFILTRATION
State	active	Threat	95
Entity ID	1543	Entity Name	VMAL #2 windows 10.250.50.141 (kgalloway141
Assigned Date	2022-12-14 06:58:53	Entity Type	Detections
Is Targeting Key Asset	false	Filtered By AI	false
Is Triaged	false	Filtered By Rule	false
Summary	{"dst_ports" : [22], "protocols" : ["tcp"], "bytes_sent" : 3313282732, "dst_ips" : ["10.250.20.141"]}	Filtered By User	false
		Vectra Detection URL	https://10.253.255.11/detections/8136

5. The user will be able to add/remove the tags and these tags will be synced back to the Vectra Detect.
6. The user will be able to add notes for the detections and these notes will be posted on Vectra Detect.



Notes

Notes: Notes

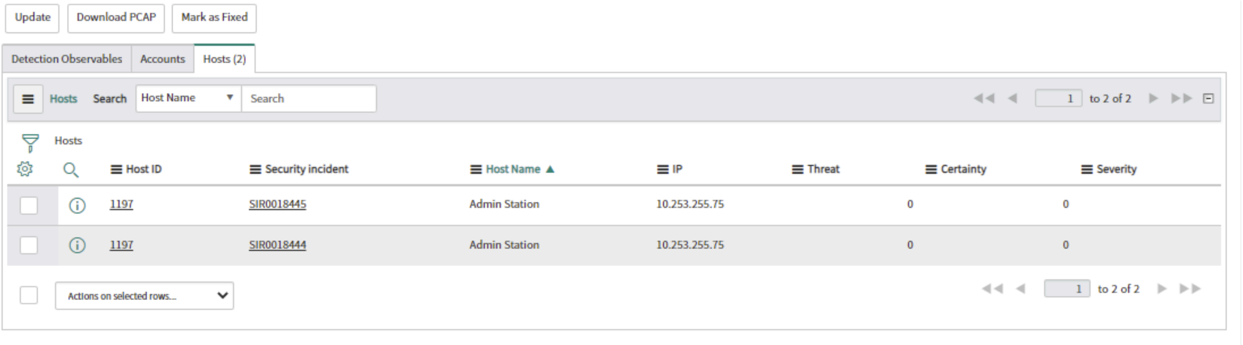
Activities: 19

System Administrator — Notes • 2022-11-30 13:05:34
Successfully removed tag testaccount322 on the Vectra platform. Response: 200

System Administrator — Notes • 2022-11-30 13:05:00
uyuyuy

System — Notes • 2022-11-30 13:04:35
Download PCAP file failed.

7. The user will be able to mark a detection as fixed by clicking on Mark as Fixed button.
8. A related list of Detection Observables, Hosts, and Accounts will be populated at the bottom of the form view.



Hosts

Host ID	Security incident	Host Name ▲	IP	Threat	Certainty	Severity
1197	SIR0018445	Admin Station	10.253.255.75		0	0
1197	SIR0018444	Admin Station	10.253.255.75		0	0

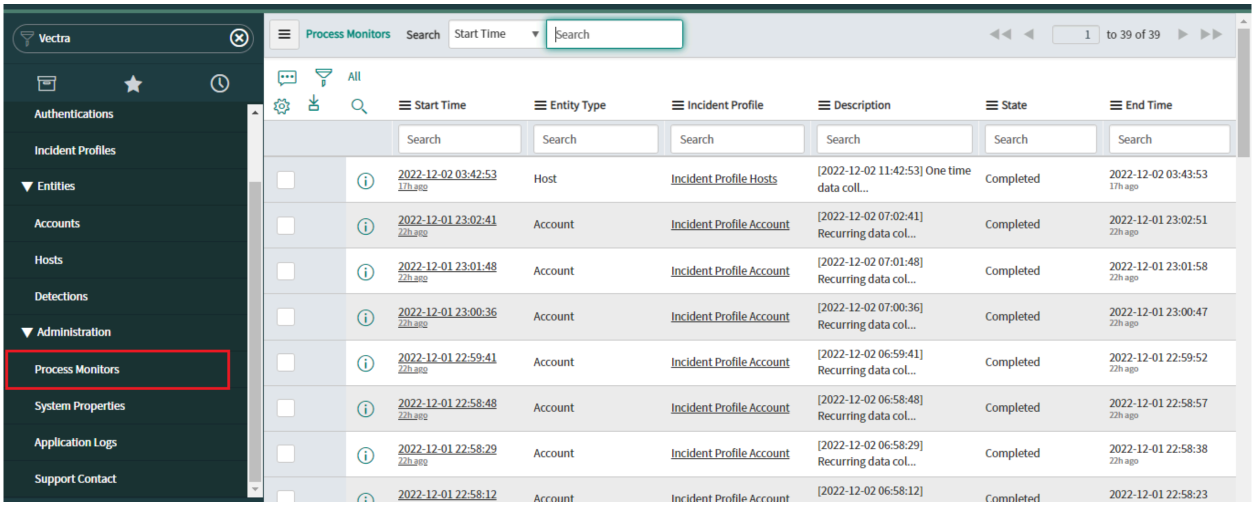
2.6. Process Monitor

This section describes how to monitor the ongoing data ingestion process.

Role Required: x_cdsp_vectra_sir.admin

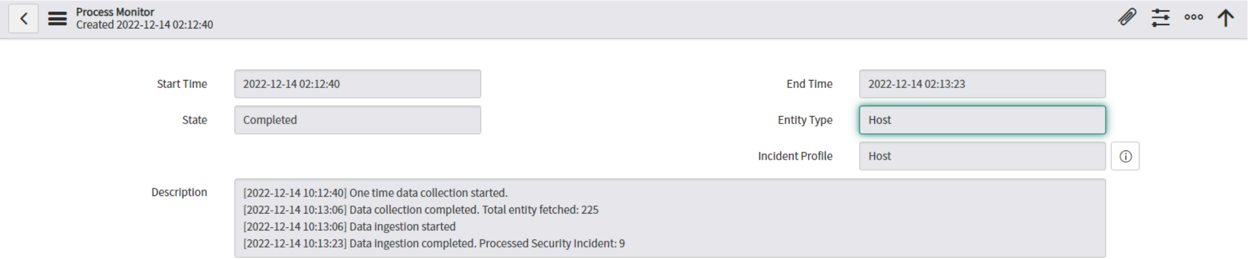
Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR” -> “Administration”
3. Click on “Process Monitor” to open all Records.



Start Time	Entity Type	Incident Profile	Description	State	End Time
2022-12-02 03:42:53 17h ago	Host	Incident Profile Hosts	[2022-12-02 11:42:53] One time data coll...	Completed	2022-12-02 03:43:53 17h ago
2022-12-01 23:02:41 22h ago	Account	Incident Profile Account	[2022-12-02 07:02:41] Recurring data col...	Completed	2022-12-01 23:02:51 22h ago
2022-12-01 23:01:48 22h ago	Account	Incident Profile Account	[2022-12-02 07:01:48] Recurring data col...	Completed	2022-12-01 23:01:58 22h ago
2022-12-01 23:00:36 22h ago	Account	Incident Profile Account	[2022-12-02 07:00:36] Recurring data col...	Completed	2022-12-01 23:00:47 22h ago
2022-12-01 22:59:41 22h ago	Account	Incident Profile Account	[2022-12-02 06:59:41] Recurring data col...	Completed	2022-12-01 22:59:52 22h ago
2022-12-01 22:58:48 22h ago	Account	Incident Profile Account	[2022-12-02 06:58:48] Recurring data col...	Completed	2022-12-01 22:58:57 22h ago
2022-12-01 22:58:29 22h ago	Account	Incident Profile Account	[2022-12-02 06:58:29] Recurring data col...	Completed	2022-12-01 22:58:38 22h ago
2022-12-01 22:58:12	Account	Incident Profile Account	[2022-12-02 06:58:12]	Completed	2022-12-01 22:58:23

4. Open the top record to monitor the ongoing process.



Start Time	2022-12-14 02:12:40	End Time	2022-12-14 02:13:23
State	Completed	Entity Type	Host
		Incident Profile	Host

Description
[2022-12-14 10:12:40] One time data collection started.
[2022-12-14 10:13:06] Data collection completed. Total entity fetched: 225
[2022-12-14 10:13:06] Data ingestion started
[2022-12-14 10:13:23] Data ingestion completed. Processed Security Incident: 9

2.7. Manual Actions

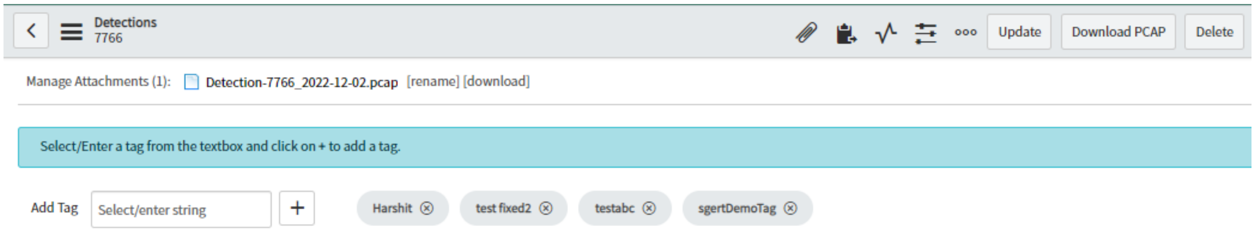
2.7.1. Download a PCAP file attached to a detection

This section describes how to download a PCAP file attached to a detection on the Vectra Detect for the “Vectra Detect for SIR” application.

Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

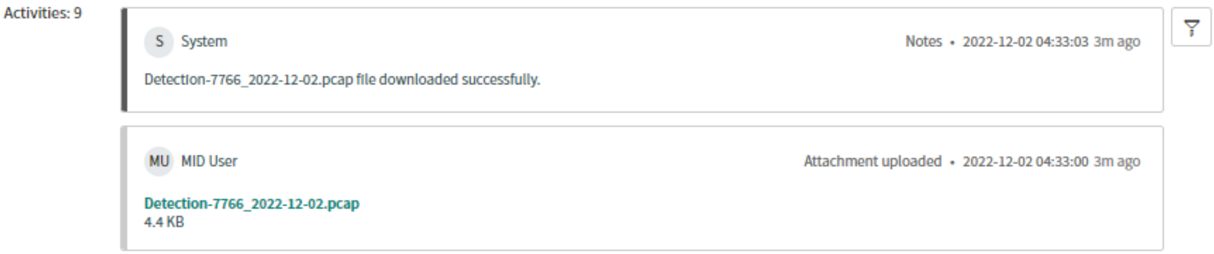
1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR”.
3. Click on “Detections” under the “Entities” separator.
4. Click on any detection record for which you want to download a PCAP file.
5. Click on the “Download PCAP” button which is available on the detection from view.



Manage Attachments (1): Detection-7766_2022-12-02.pcap [rename] [download]

Select/Enter a tag from the textbox and click on + to add a tag.

6. On successful download users can see the PCAP file in the attachment.
7. Users can also see notes for the success or failure of downloading a file.


Activities: 9

S System
Notes • 2022-12-02 04:33:03 3m ago

Detection-7766_2022-12-02.pcap file downloaded successfully.

MU MID User
Attachment uploaded • 2022-12-02 04:33:00 3m ago

Detection-7766_2022-12-02.pcap
4.4 KB

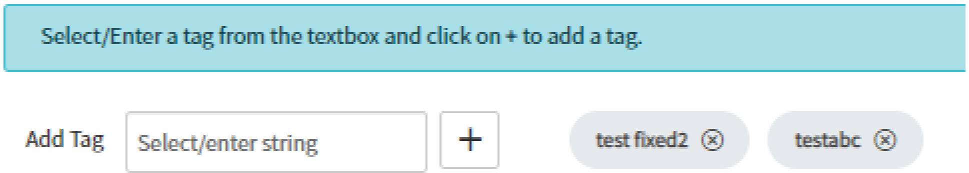
2.7.2. Add a tag to a host, account, or detection on Vectra Detect.

This section describes how to add a tag to an entity or detection from ServiceNow and sync to Vectra Detect.

Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR”.
3. Open any entity or detection.
4. The section to add a tag is shown at the top of the form view.
5. From the drop-down list select any existing tag, or create a new tag by typing the tag name and click “+” to add the tag to an entity or detection, and Vectra Detect.
6. To remove a tag from an entity or detection, and Vectra Detect, click on “x” on the tag pill.


Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag
Select/enter string

2.7.3. Add a note to a host, account, or detection to a Vectra Detect.

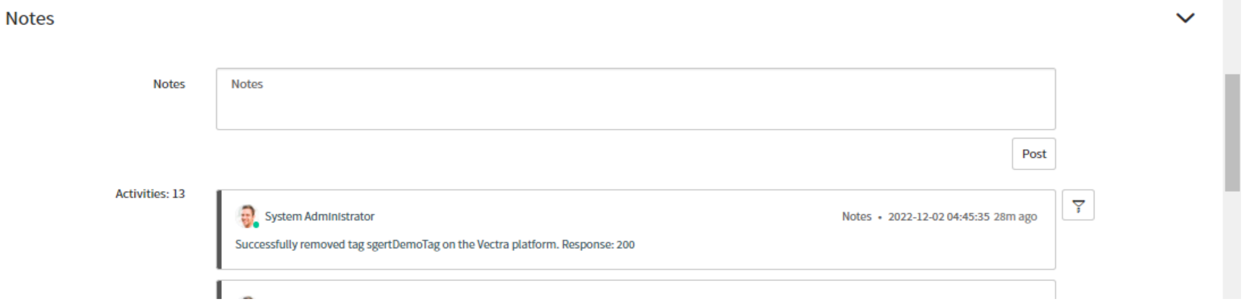
This section describes how to add a note to an entity or detection in ServiceNow, and this will reflect the changes to Vectra Detect.

Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

1. log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR”.

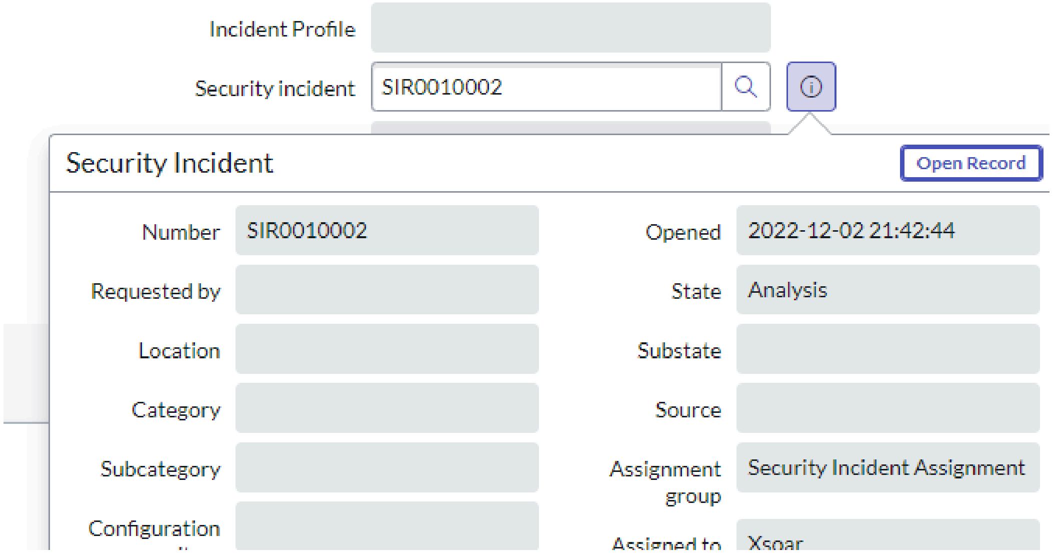
3. Open any entity or detection.
4. The section to add a note to detection is shown at the bottom of the form view.



Notes

Notes	Notes
Activities: 13	System Administrator · Notes • 2022-12-02 04:45:35 28m ago Successfully removed tag sgertDemoTag on the Vectra platform. Response: 200

5. To add a note in the account or host a Security Incident should be attached to that entity.
6. Open Security Incident from the Security Incident reference field.

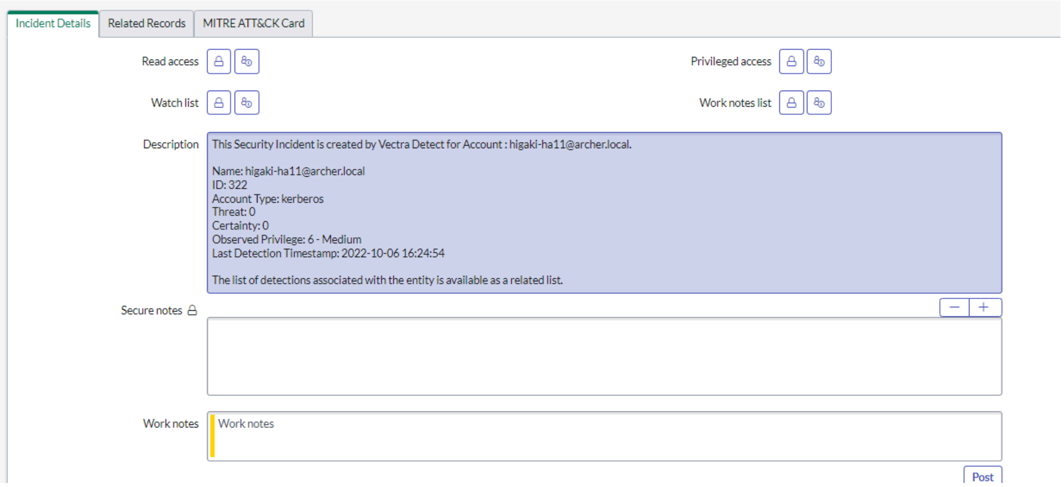


Incident Profile	
Security incident	SIR0010002

Security Incident

Number	SIR0010002	Opened	2022-12-02 21:42:44
Requested by		State	Analysis
Location		Substate	
Category		Source	
Subcategory		Assignment group	Security Incident Assignment
Configuration		Assigned to	Xsoar

7. In the form view of a Security Incident, the user can see the notes in the "Incident Details" tab.



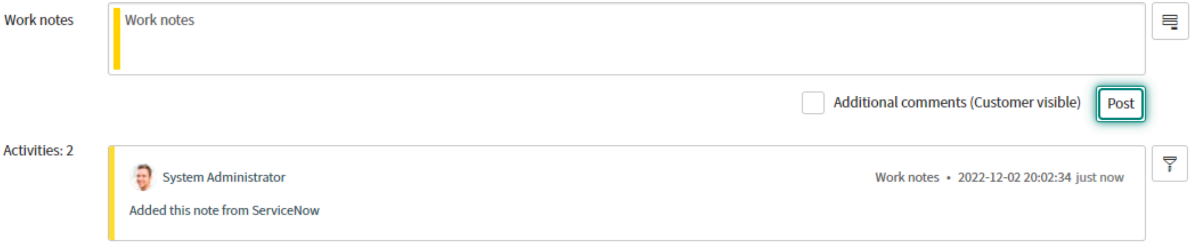
Description: This Security Incident is created by Vectra Detect for Account : higaki-ha11@archer.local.

Name: higaki-ha11@archer.local
ID: 322
Account Type: kerberos
Threat: 0
Certainty: 0
Observed Privilege: 6 - Medium
Last Detection Timestamp: 2022-10-06 16:24:54

The list of detections associated with the entity is available as a related list.

Work notes: Work notes

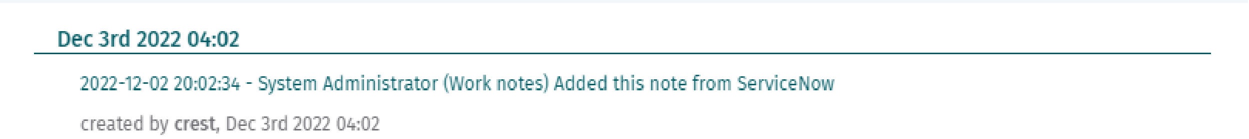
8. After writing the note click on the “Post” button.



System Administrator — Work notes • 2022-12-02 20:02:34 just now

Added this note from ServiceNow

9. This note will be synced to Vectra Detect.



Dec 3rd 2022 04:02

2022-12-02 20:02:34 - System Administrator (Work notes) Added this note from ServiceNow

created by crest, Dec 3rd 2022 04:02

2.7.4. Mark detection as fixed.

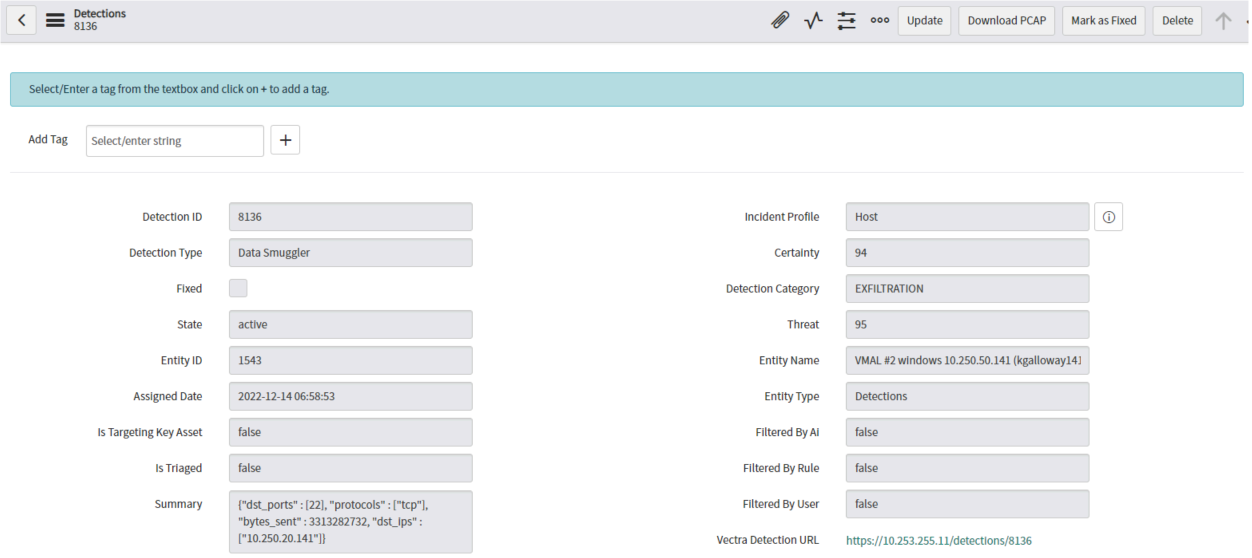
This section describes how to fix a detection in ServiceNow, and this will reflect the changes to Vectra Detect.

Role Required: x_cdsp_vectra_sir.admin, x_cdsp_vectra_sir.user

Procedure:

1. log in to the ServiceNow instance.

2. Navigate to “Vectra Detect for SIR”.
3. Open a detection form “Vectra Detect for SIR” - > “Entities” - > “Detection”.To fix the detection from Vectra, click on the “Mark as Fixed” button available in the header of the form.



Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag: Select/enter string

Detection ID	8136	Incident Profile	Host
Detection Type	Data Smuggler	Certainty	94
Fixed	□	Detection Category	EXFILTRATION
State	active	Threat	95
Entity ID	1543	Entity Name	VMAL #2 windows 10.250.50.141 (kgalloway14]
Assigned Date	2022-12-14 06:58:53	Entity Type	Detections
Is Targeting Key Asset	false	Filtered By AI	false
Is Triaged	false	Filtered By Rule	false
Summary	{"dst_ports" : [22], "protocols" : ["tcp"], "bytes_sent" : 3313282732, "dst_ips" : ["10.250.20.141"]}	Filtered By User	false
		Vectra Detection URL	https://10.253.255.11/detections/8136

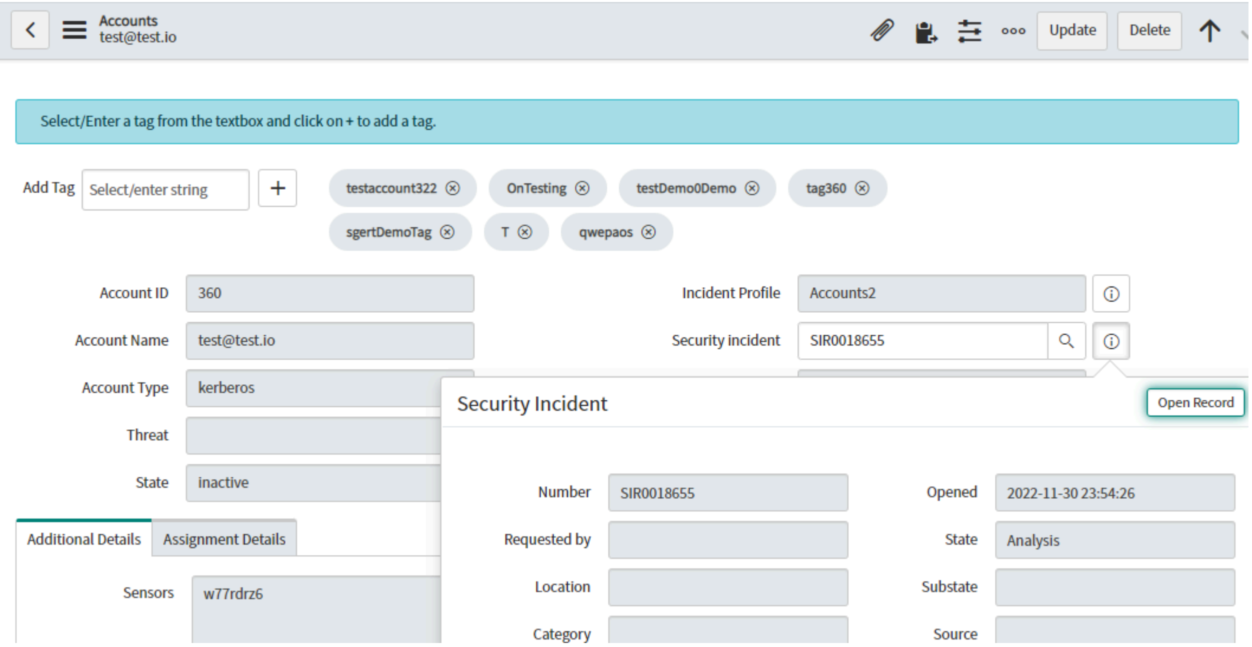
2.8. Incident Assignee

This section describes how to assign a user to an unassigned entity in the Vectra Detect from ServiceNow.

Role Required: x_cdsp_vectra_sir.admin,x_cdsp_vectra_sir.user

Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for SIR”.
3. Open any security Incident created for an account or host.



Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag Select/enter string +

testaccount322 ⊗ OnTesting ⊗ testDemo0Demo ⊗ tag360 ⊗ sgertDemoTag ⊗ T ⊗ qwepaos ⊗

Account ID	360
Account Name	test@test.io
Account Type	kerberos
Threat	
State	inactive

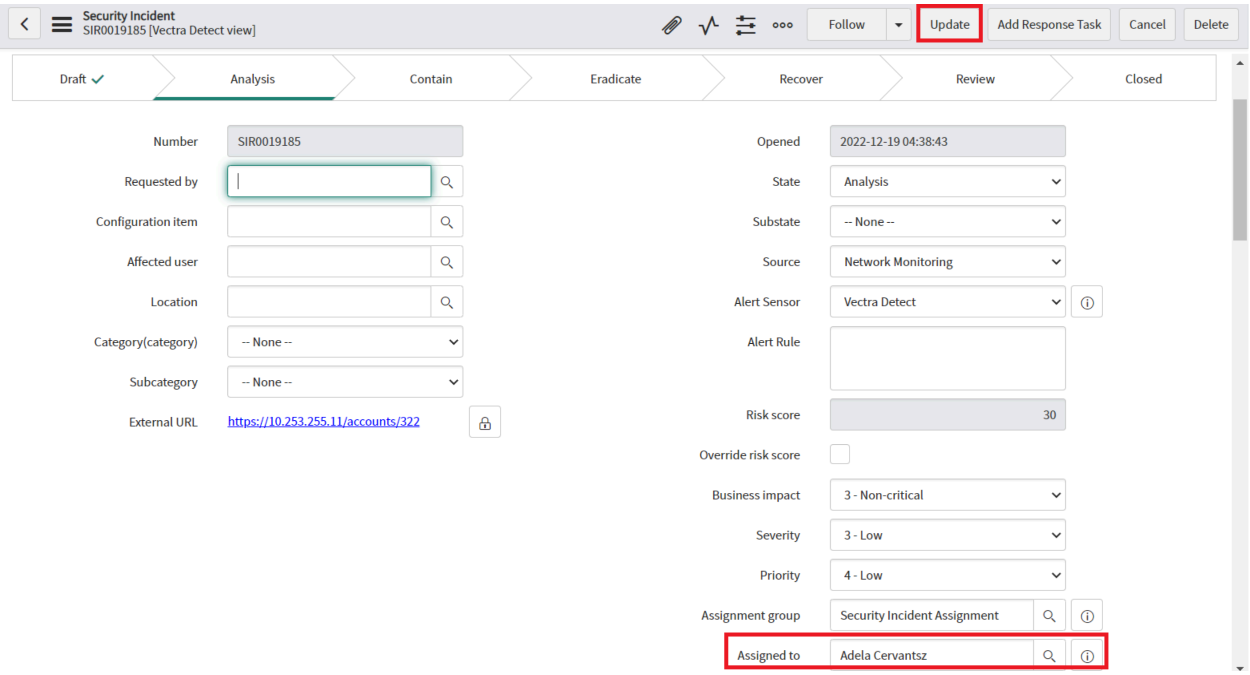
Incident Profile	Accounts2
Security incident	SIR0018655

Sensors w77rdrz6

Security Incident

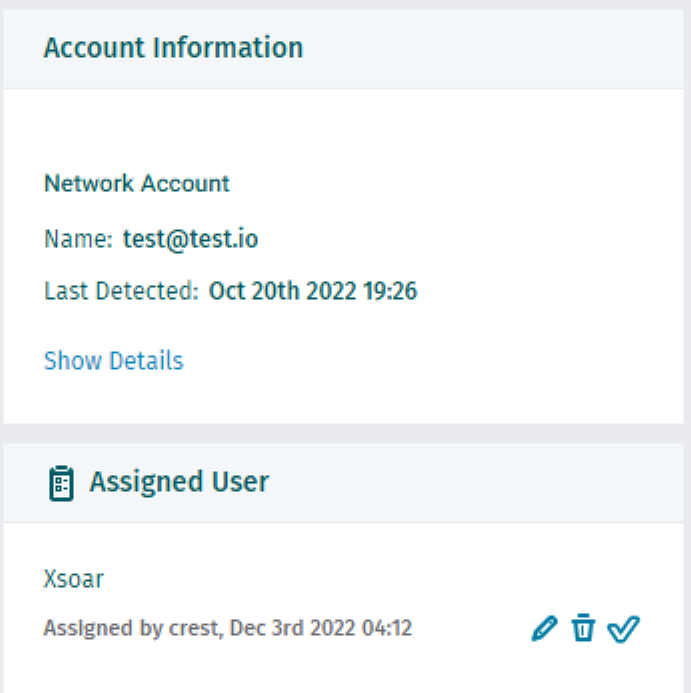
Number	SIR0018655	Opened	2022-11-30 23:54:26
Requested by		State	Analysis
Location		Substate	
Category		Source	

4. In the Security Incident form view user can see the “Assigned To” Entity.
5. Select a ServiceNow user who is present in the Vectra Detect and click on “Update”.



Number	SIR0019185	Opened	2022-12-19 04:38:43
Requested by		State	Analysis
Configuration item		Substate	-- None --
Affected user		Source	Network Monitoring
Location		Alert Sensor	Vectra Detect
Category(category)	-- None --	Alert Rule	
Subcategory	-- None --	Risk score	30
External URL	https://10.253.255.11/accounts/322	Override risk score	□
		Business impact	3 - Non-critical
		Severity	3 - Low
		Priority	4 - Low
		Assignment group	Security Incident Assignment
		Assigned to	Adela Cervantsz

6. Assigned User will be reflected back to Vectra Detect and a successful assignment will post a note in the work note of the ServiceNow Security Incident.



Account Information

Network Account

Name: test@test.io

Last Detected: Oct 20th 2022 19:26

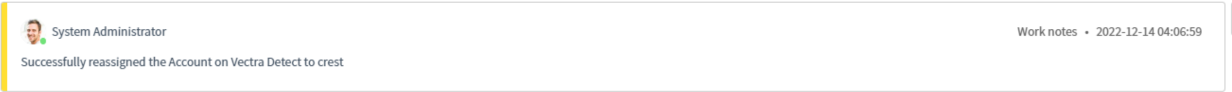
Show Details

Assigned User

Xsoar

Assigned by crest, Dec 3rd 2022 04:12

7. If an entity is already assigned to a user in Vectra and we try to reassign it to some other user then the security incident will be assigned to the user in ServiceNow as well as on the Vectra Detect.



System Administrator

Work notes • 2022-12-14 04:06:59

Successfully reassigned the Account on Vectra Detect to crest

8. If the assigned user is not present on Vectra Detect, the fallback user which is configured in the Incident profile will be assigned to the entity on Vectra Detect.

2.9. SOAR Action: Observable Enrichment

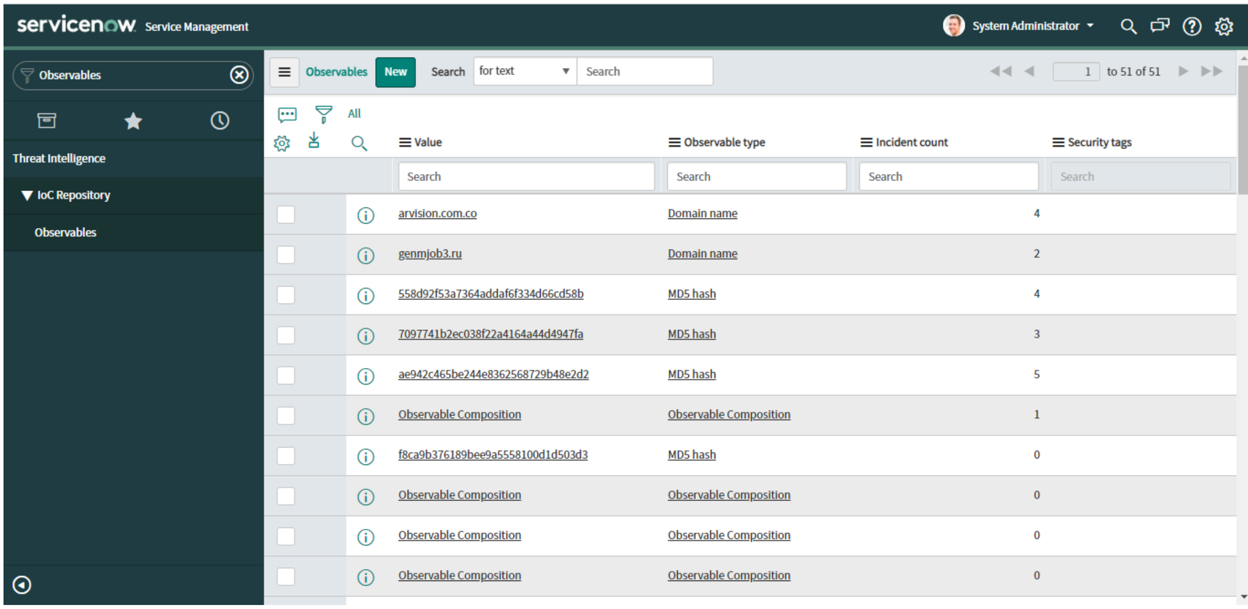
This section describes how to enrich the observables for specified IP. Whenever any new observable is added to the Security Incident the observable enrichment should be done for that observable.

Role Require: x_cdsp_vectra_sir.user,sn_si.analyst

Procedure:

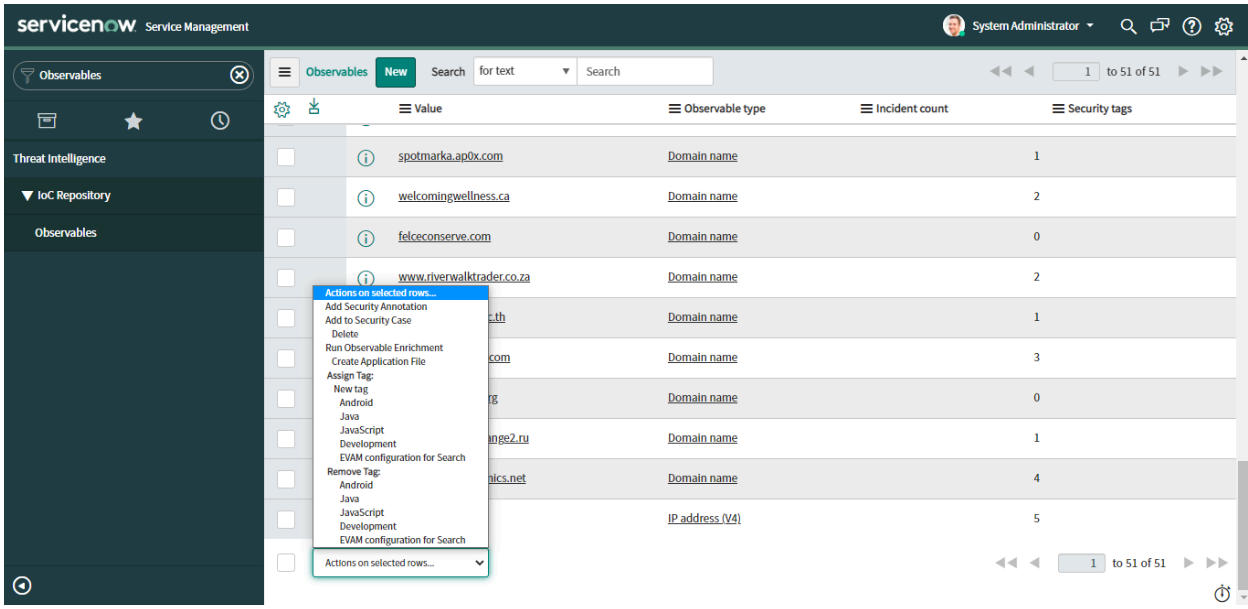
1. Log in to the ServiceNow instance,
2. Navigate to the “Vectra Detect for SIR”

3. Click on the “Host” under the “Entities” module.
4. Open any existing Security Incident associated with the Host.
5. Navigate to the related list “Associated Observables”
6. Click on the Edit button and insert IP addresses for Observable Enrichment.
7. Click on the Save button.
8. Select the available IP address(es)
9. Perform the action “Run Observable Enrichment” from the drop-down menu.
10. Users can see the observables from the related list “Host Observables” or “Detection Observables” for the respective IP address.
11. There is another way to run the observable enrichment which is from the Observables table. In the observable table, there will be various observables of the organization either populated manually or by some discovery sources.



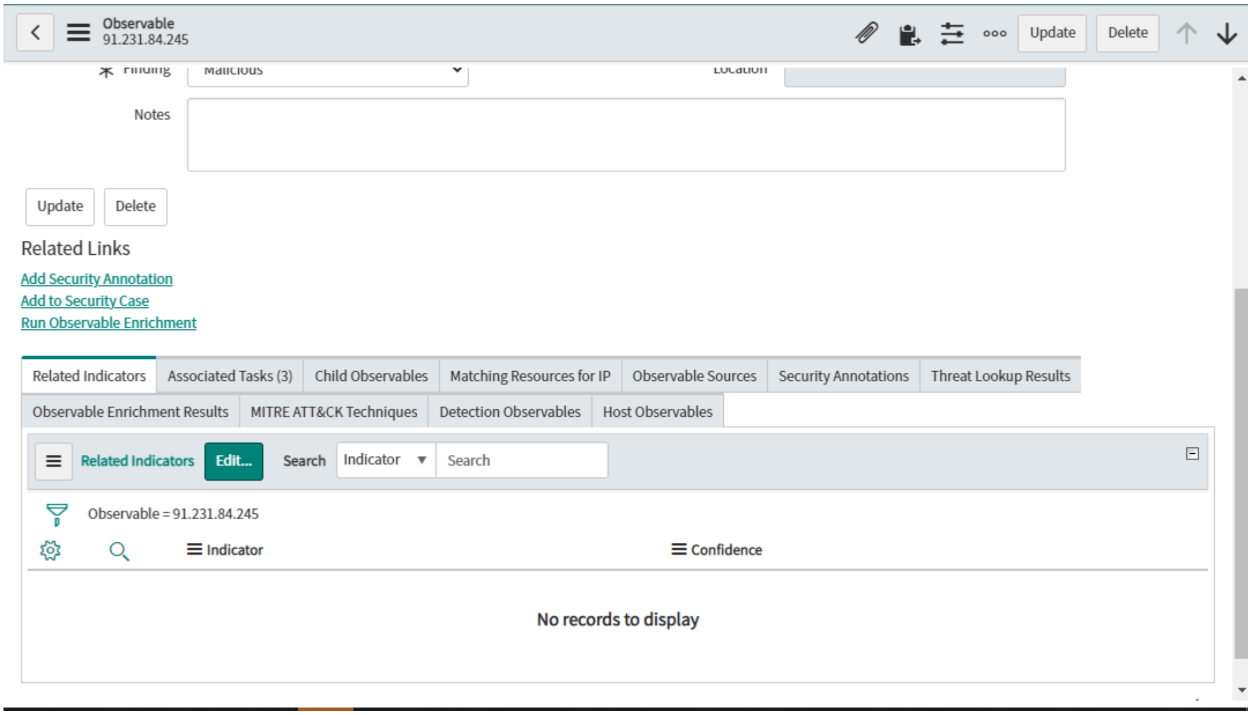
Value	Observable type	Incident count	Security tags
Search	Search	Search	Search
arvision.com.co	Domain name	4	
genmjob3.ru	Domain name	2	
558d92f53a7364addaf6f334d66cd58b	MD5 hash	4	
7097741b2ec038f22a4164a44d4947fa	MD5 hash	3	
ae942c465be244e8362568729b48e2d2	MD5 hash	5	
Observable Composition	Observable Composition	1	
f8ca9b376189bee9a5558100d1d503d3	MD5 hash	0	
Observable Composition	Observable Composition	0	
Observable Composition	Observable Composition	0	
Observable Composition	Observable Composition	0	

12. You can select multiple observables with type IP address and run observable enrichment action as shown below,



Value	Observable type	Incident count	Security tags
spotmarka.ap0x.com	Domain name	1	
welcomingwellness.ca	Domain name	2	
felceconserve.com	Domain name	0	
www.riverwalktrader.co.za	Domain name	2	
.th	Domain name	1	
com	Domain name	3	
rg	Domain name	0	
nge2.ru	Domain name	1	
nics.net	Domain name	4	
	IP address (V4)	5	

13. Or you can open any specific observable of type IP address and run observable enrichment by clicking on “Run Observable Enrichment” from the Related Links.



Finding: Malicious

Location:

Notes:

Related Links

Add Security Annotation

Add to Security Case

Run Observable Enrichment

Observable = 91.231.84.245

Indicator	Confidence

No records to display

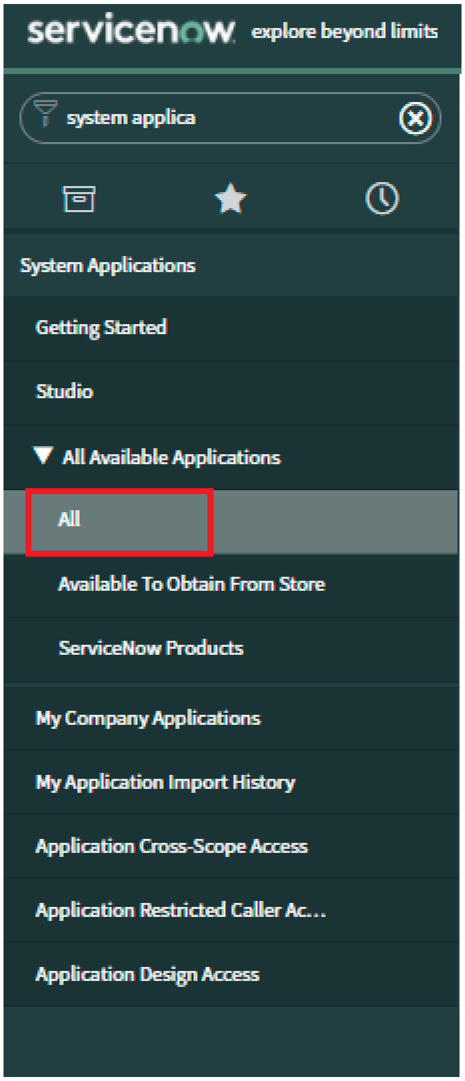
3 Uninstallation

This section describes how to uninstall the Vectra Detect SIR application from a ServiceNow instance.

Role Required: System Administrator (admin)

Following steps will guide you on how to uninstall the Vectra Detect SIR App from the ServiceNow UI.

1. Navigate to “System Applications” “All Available applications” “All”.


servicenow explore beyond limits
system applica
System Applications
Getting Started
Studio
All Available Applications
All
Available To Obtain From Store
ServiceNow Products
My Company Applications
My Application Import History
Application Cross-Scope Access
Application Restricted Caller Ac...
Application Design Access

A. Mark Check the “Installed” checkbox. A list of applications installed in the instance is displayed.

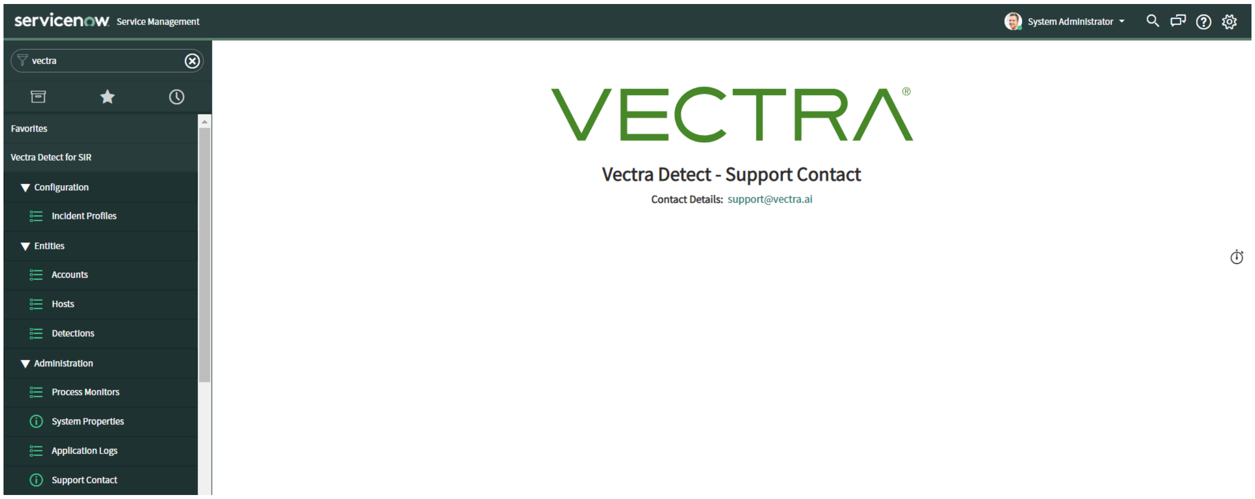
B. Locate the Vectra Detect SIR application, select it, and click “Uninstall” under the related links.

C. The application will be uninstalled from your instance.

4. Support, Troubleshooting, and Known Limitations

4.1. Support

- For any issues related to the application navigate to “Vectra Detect SIR” -> “Support Contact”.



Vectra Detect - Support Contact

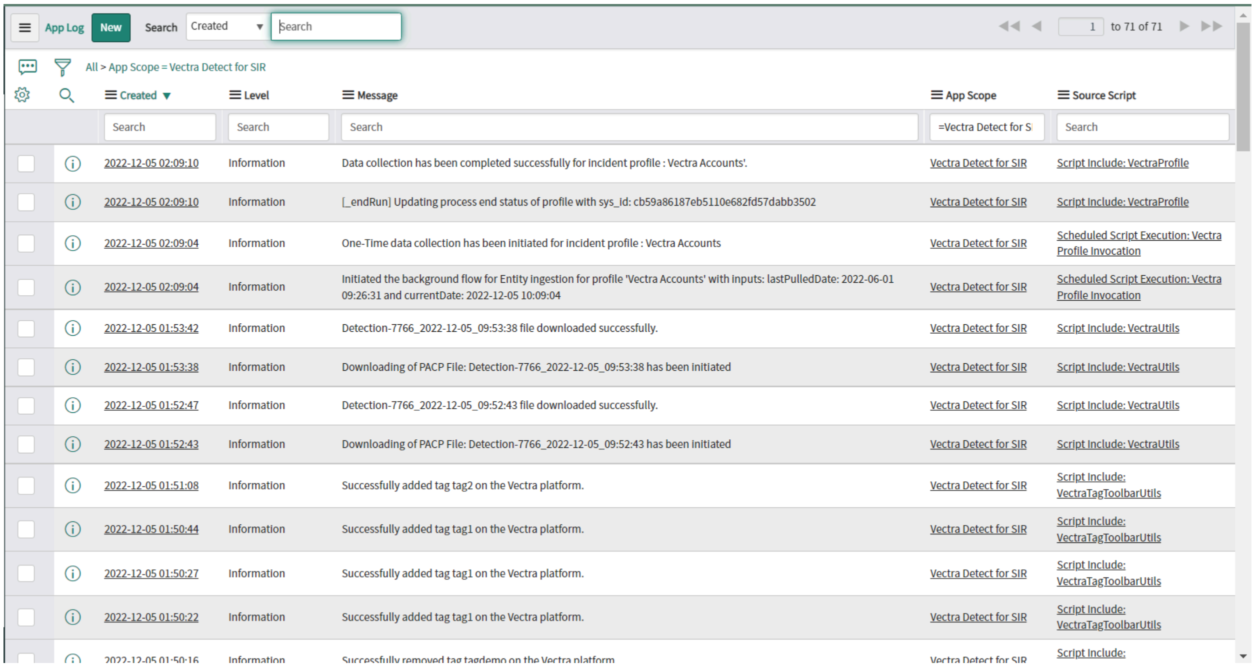
Contact Details: support@vectra.ai

4.2. Troubleshooting

4.2.1. Application Logs

Role Required: System Administrator (admin)

1. The user should check the application logs whenever he/she experiences any errors.
2. Navigate to “Vectra Detect SIR”.
3. Open “Application Logs”.



	Created	Level	Message	App Scope	Source Script
	Search	Search	Search	=Vectra Detect for S	Search
☐	2022-12-05 02:09:10	Information	Data collection has been completed successfully for incident profile : Vectra Accounts'.	Vectra Detect for SIR	Script Include: VectraProfile
☐	2022-12-05 02:09:10	Information	[_endRun] Updating process end status of profile with sys_id: cb59a86187eb5110e682fd57dabb3502	Vectra Detect for SIR	Script Include: VectraProfile
☐	2022-12-05 02:09:04	Information	One-Time data collection has been initiated for incident profile : Vectra Accounts	Vectra Detect for SIR	Scheduled Script Execution: Vectra Profile Invocation
☐	2022-12-05 02:09:04	Information	Initiated the background flow for Entity ingestion for profile 'Vectra Accounts' with inputs: lastPulledDate: 2022-06-01 09:26:31 and currentDate: 2022-12-05 10:09:04	Vectra Detect for SIR	Scheduled Script Execution: Vectra Profile Invocation
☐	2022-12-05 01:53:42	Information	Detection-7766_2022-12-05_09:53:38 file downloaded successfully.	Vectra Detect for SIR	Script Include: VectraUtils
☐	2022-12-05 01:53:38	Information	Downloading of PACP File: Detection-7766_2022-12-05_09:53:38 has been initiated	Vectra Detect for SIR	Script Include: VectraUtils
☐	2022-12-05 01:52:47	Information	Detection-7766_2022-12-05_09:52:43 file downloaded successfully.	Vectra Detect for SIR	Script Include: VectraUtils
☐	2022-12-05 01:52:43	Information	Downloading of PACP File: Detection-7766_2022-12-05_09:52:43 has been initiated	Vectra Detect for SIR	Script Include: VectraUtils
☐	2022-12-05 01:51:08	Information	Successfully added tag tag2 on the Vectra platform.	Vectra Detect for SIR	Script Include: VectraTagToolbarUtils
☐	2022-12-05 01:50:44	Information	Successfully added tag tag1 on the Vectra platform.	Vectra Detect for SIR	Script Include: VectraTagToolbarUtils
☐	2022-12-05 01:50:27	Information	Successfully added tag tag1 on the Vectra platform.	Vectra Detect for SIR	Script Include: VectraTagToolbarUtils
☐	2022-12-05 01:50:22	Information	Successfully added tag tag1 on the Vectra platform.	Vectra Detect for SIR	Script Include: VectraTagToolbarUtils
☐	2022-12-05 01:50:16	Information	Successfully removed tag tagdemo on the Vectra platform	Vectra Detect for SIR	Script Include:

4.3 FAQs

i. Unable to install Vectra Detect SIR application from ServiceNow Store

Problem Statement: Unable to install the application from ServiceNow Store.

1. Verify you have the system administrator (admin) role.
2. Navigate to “System Applications” ⍰ “All Available applications” ⍰ “All”.
3. Verify the application appears under the “Installed” Tab.

ii. Unable to create a new user

Problem Statement: Unable to create a new user for Vectra.

1. Review the following link and execute the steps.

https://docs.servicenow.com/bundle/rome-platform-administration/page/administer/users-and-groups/task/t_CreateAUser.html

iii. Unable to Collect Data

Problem Statement: Getting error while data collection.

Role Required: Vectra admin (x_cdsp_vectra_sir.admin)

1. Log into the ServiceNow instance.
2. Navigate to “Vectra Detect SIR” - > “Administration” - > “Application logs”.
3. Check “Application Logs” for any errors.

iv. Data Collection Started and process monitor stuck on “New” state

Problem Statement: data ingestion started and a process is also created but is in a “New” State for a long period of time.

Role Required: admin

1. Log in to the ServiceNow instance.
2. Navigate to “System Users”
3. Open MID Server user and check roles.

Note x_cdsp_vectra_itsm.admin role should be assigned to a MID Server user.

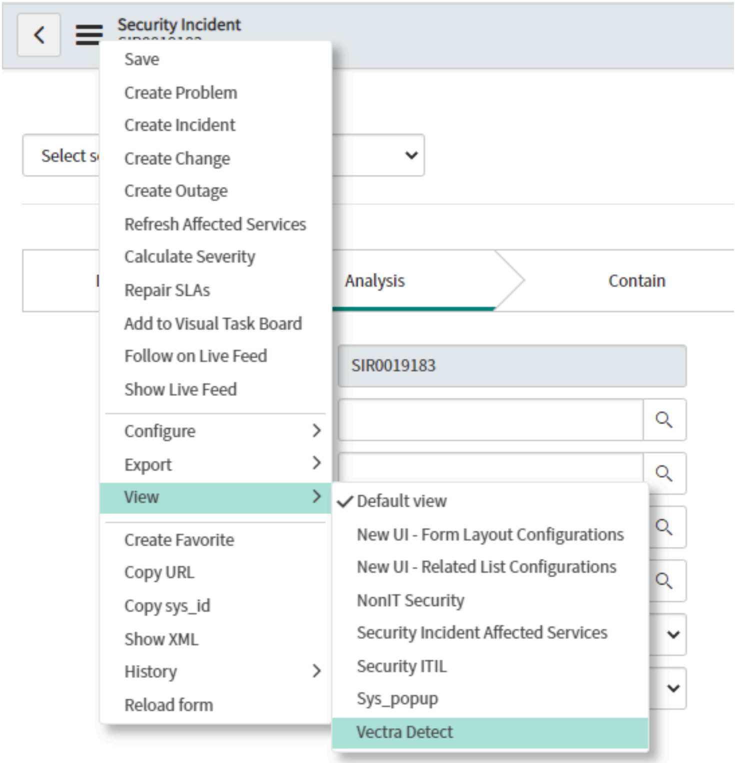
1. Restart MID Server
2. Delete the created profile and create a new profile and mark it active to start data ingestion.

v. Unable to see external link in Security Incident Form view

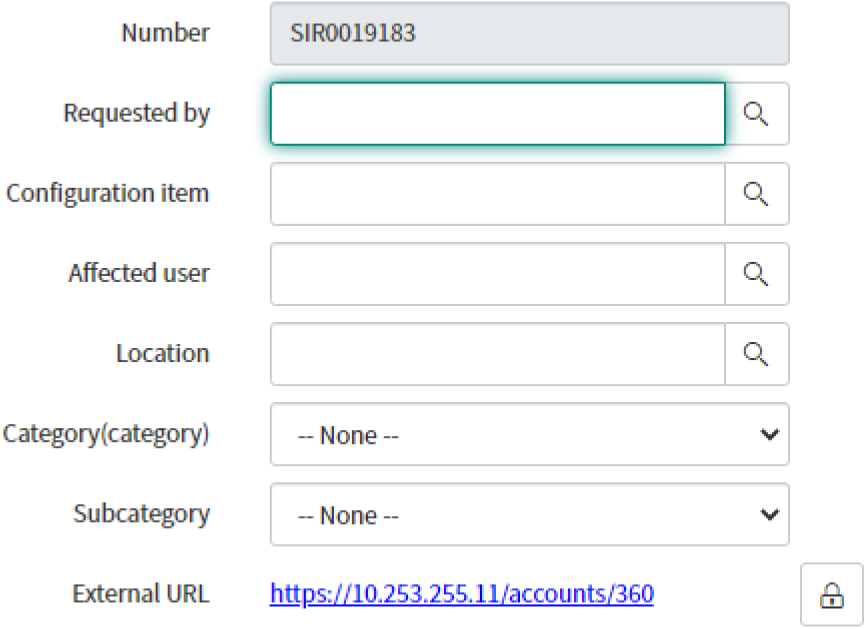
Problem Statement: The link to Vectra Detect is not visible in the form view of the Security incident.

Role Required : view_changer

1. Log in to the ServiceNow instance.
2. Navigate to “Security Incident”
3. Open a Security Incident associated with Vectra Account/Host
4. Change the view from “Default View” to “Vectra Detect”



5. User should be able to see External URL:



Number	SIR0019183
Requested by	
Configuration item	
Affected user	
Location	
Category(category)	-- None --
Subcategory	-- None --
External URL	https://10.253.255.11/accounts/360

End of Document