

SCOPE CERTIFIED APPLICATION INSTALLATION AND CONFIGURATION GUIDE

Vectra Detect ServiceNow ITSM Integration (1.1.0)

Contents

1. Overview	4
1.1. Vectra ServiceNow Application	4
1.2. Application features	4
1.3. Compatibility Matrix	5
2. Vectra Detect for ITSM	5
2.1. MID Server Installation	5
2.2. Installation	5
2.3. Pre-requisites	5
2.3.1. Permissions and Roles	5
2.3.2. Application Download and Installation	6
2.3.3. Activate Scheduled Data Import	7
2.4. Configuration	7
2.4.1. Create Users	8
2.4.2. Authentication Configuration	11
2.4.3. Incident Profile	12
2.5. Entities	17
2.5.1. Accounts	17
2.5.2. Hosts	19
2.5.3. Detections	22
2.6. Process Monitor	24
2.7. Manual Actions	25
2.7.1. Download a PCAP file attached to a detection	25
2.7.2. Add a tag to a host, account, or detection on Vectra Detect.	26
2.7.3. Add a note to a host, account, or detection from SN to Vectra Detect	27
2.7.4. Mark detection as fixed	28
2.8. Incident Assignee	29
3. Uninstallation	32

4. Support, Troubleshooting, and Known Limitations	33
4.1. Support	33
4.2. Troubleshooting	33
4.2.1. Application Logs	33
4.2.2. Unable to install Vectra Detect for ITSM application from ServiceNow Store	33
4.2.3. Unable to create a new user	34
4.2.4. Unable to Collect Data	34
4.2.5. Data Collection Started and process monitor stuck on “New” state	34

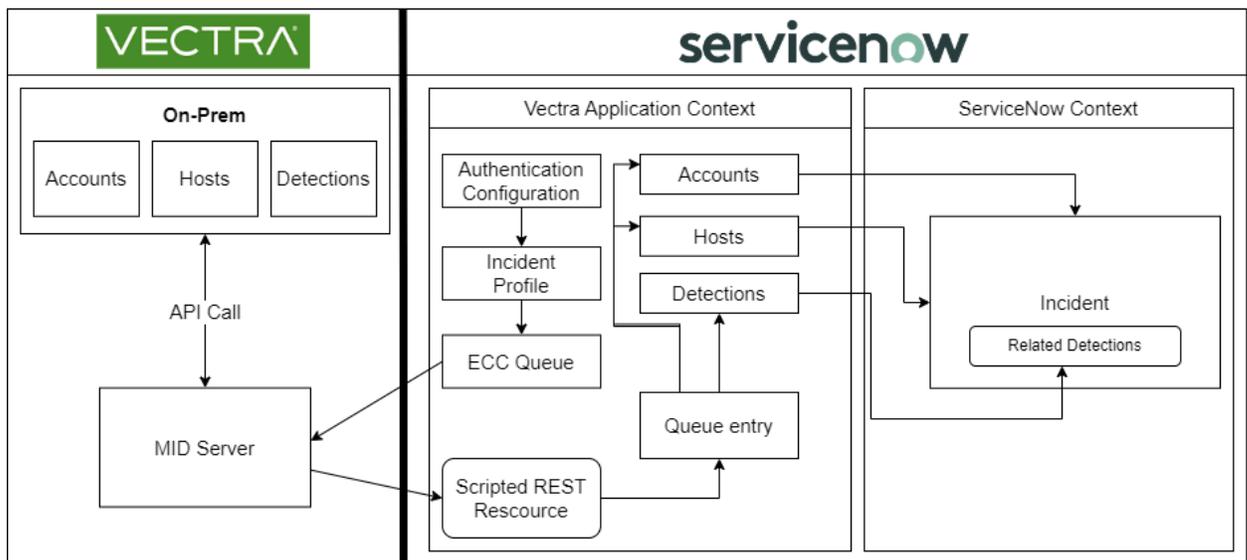
1. Overview

The Vectra threat detection and 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 ITSM application fetches all active Accounts, Hosts, and Detections from the Vectra Detect and ingests data into the ServiceNow. It provides the capability of creating “Incidents” based on the defined condition/criteria. It also provides support to perform manual actions on fetched accounts, hosts, and detections.

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 Incident creation criteria and create Incidents based on the same.
4. Ability to assign incidents to a specific user.
5. Ability to map account/host fields with Servicenow 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.

1.3. Compatibility Matrix

ServiceNow Version: Utah, Vancouver and Washington DC

Vectra API Version: 2.2

2. Vectra Detect for ITSM

2.1. MID Server Installation

This section describes how to setup 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 ITSM application from the store.

2.3. Pre-requisites

2.3.1. Permissions and Roles

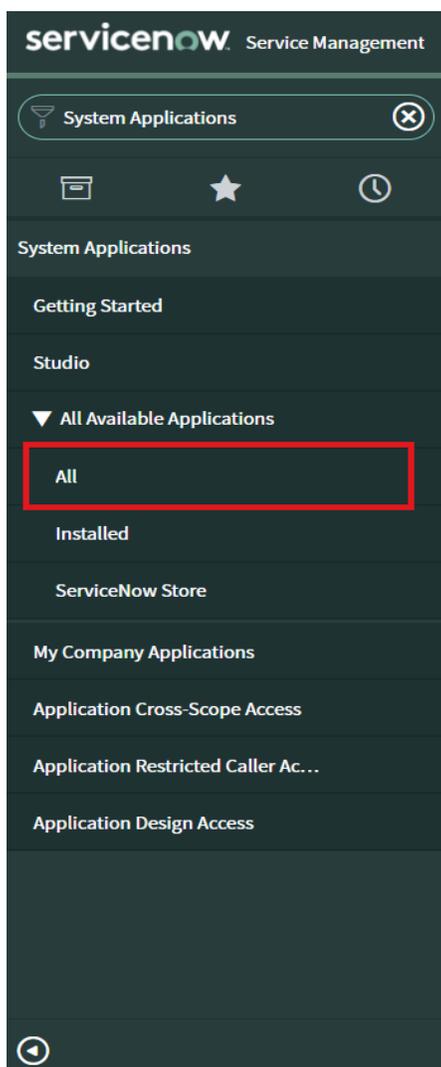
These are the ServiceNow roles and the permissions that are needed to install the application.

Role	Permissions
System Administrator (admin)	<ul style="list-style-type: none"> ● Application Log
Vectra ITSM admin (x_cdsp_vectra_itsm.Vectra_admin, itil_admin, itil, export_set_scheduler)	<ul style="list-style-type: none"> ● Authentication Configuration ● Incident Profile Configuration ● IncidentAssignee ● Manual Action ● Process Monitor
Vectra ITSM user (x_cdsp_vectra_itsm.Vectra_user, itil, export_set_sc)	<ul style="list-style-type: none"> ● View and manage Vectra Accounts, Hosts, Detections, and Incidents

heduler)	<ul style="list-style-type: none"> ● Manual actions
mid_server	<ul style="list-style-type: none"> ● 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”.

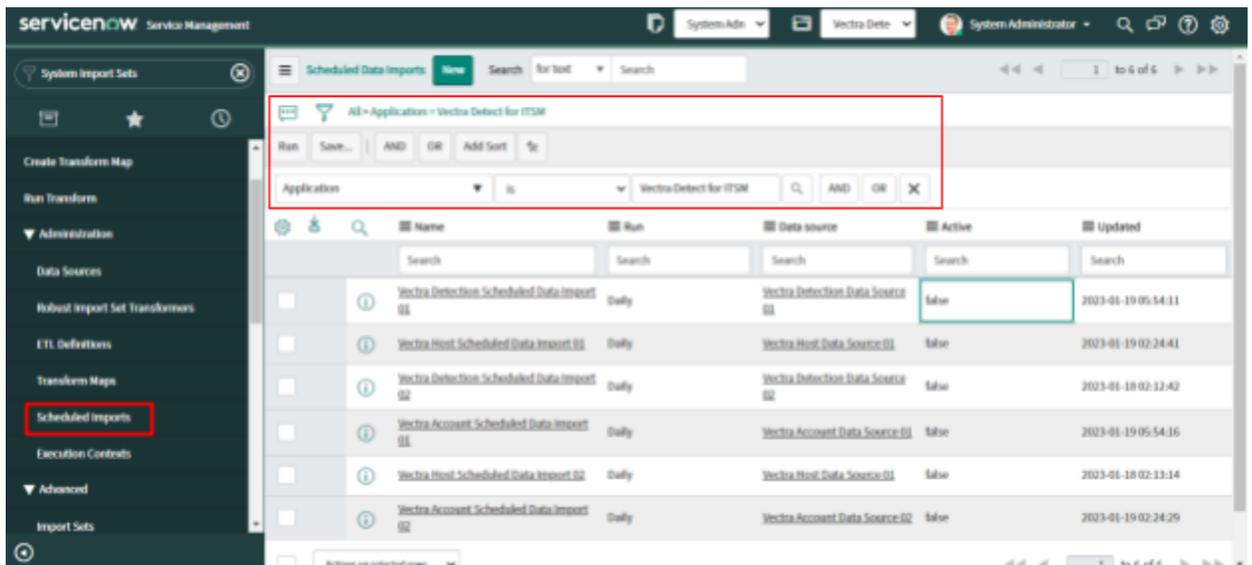


- Mark Check the “Not Installed” checkbox. A list of applications available for installation is displayed.

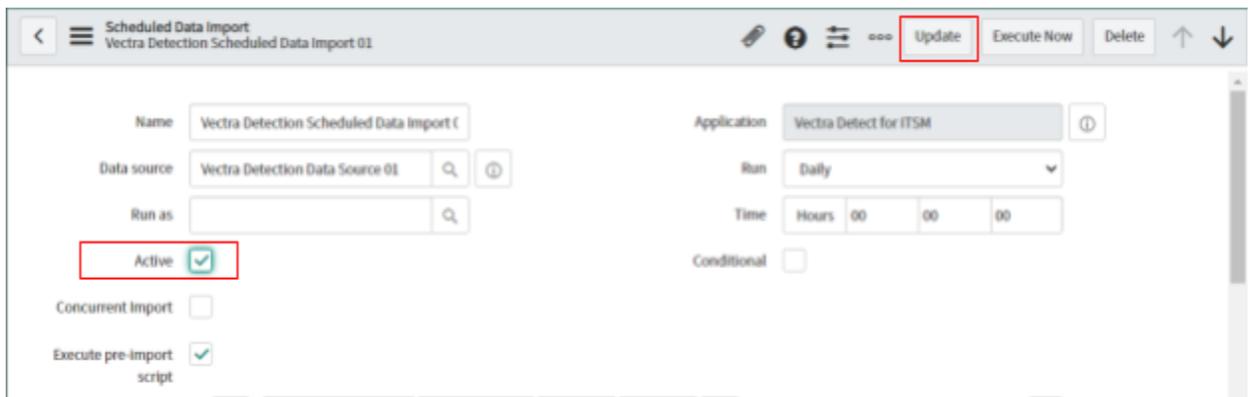
- Locate the Vectra Detect for ITSM application, select it, and click “Install”.
- The application will be installed into your instance.

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”.
3. Filter the Scheduled Data Imports by Application “Vectra Detect for ITSM”.



4. Activate all Records by Marking “Active” as true and clicking on “Update”.



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 ITSM admin	<ul style="list-style-type: none">• x_cdsp_vectra_itsm.Vectra_admin• ltil_admin• ltil• export_set_scheduler
Vectra ITSM user	<ul style="list-style-type: none">• x_cdsp_vectra_itsm.Vectra_user• ltil• export_set_scheduler
MID Server user	<ul style="list-style-type: none">• x_cdsp_vectra_itsm.Vectra_admin• mid_server

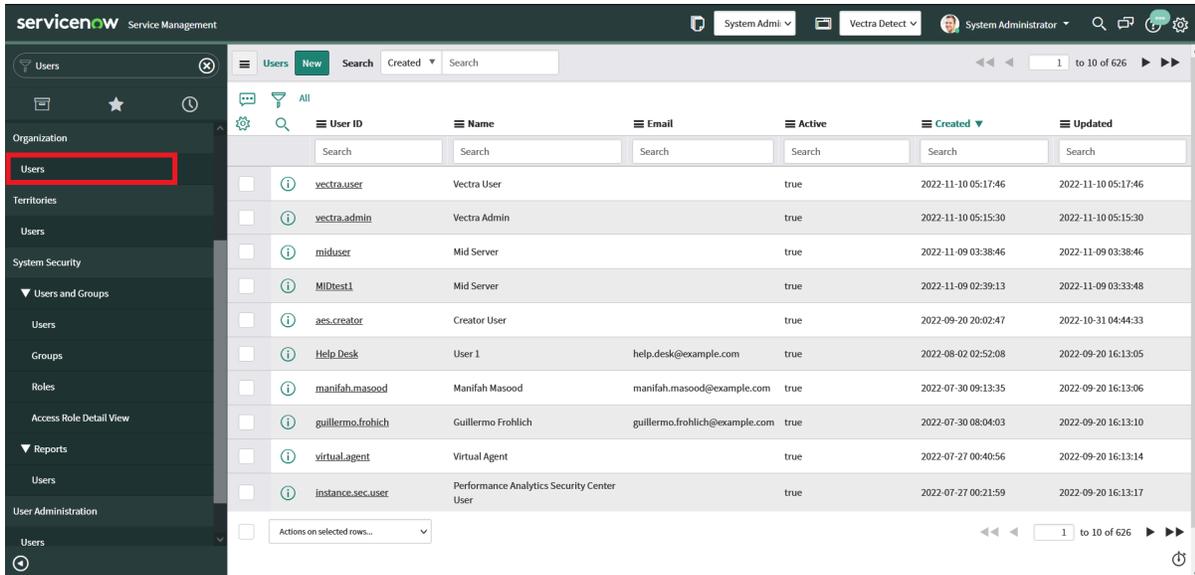
Note: MID Server user should have x_cdsp_vectra_itsm.Vectra_admin role for Vectra Detect for ITSM data ingestion.

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

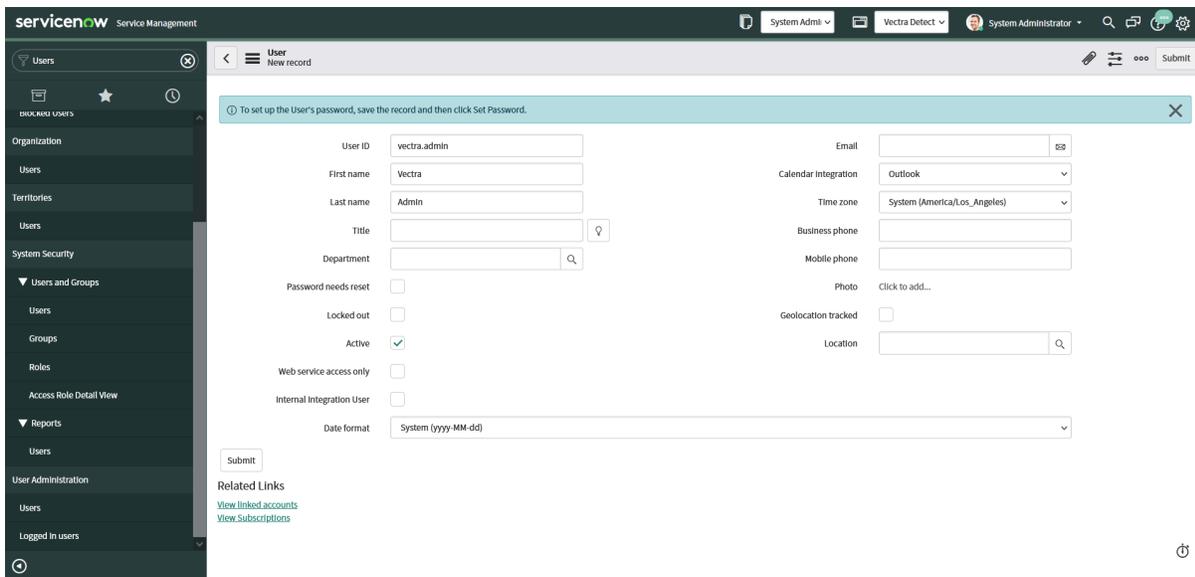
Role Required: System Administrator (admin)

Procedure:

- 1 Navigate to "Organization" -> "Users".
- 2 Click the "Users" module.



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



4 Fill in the form.

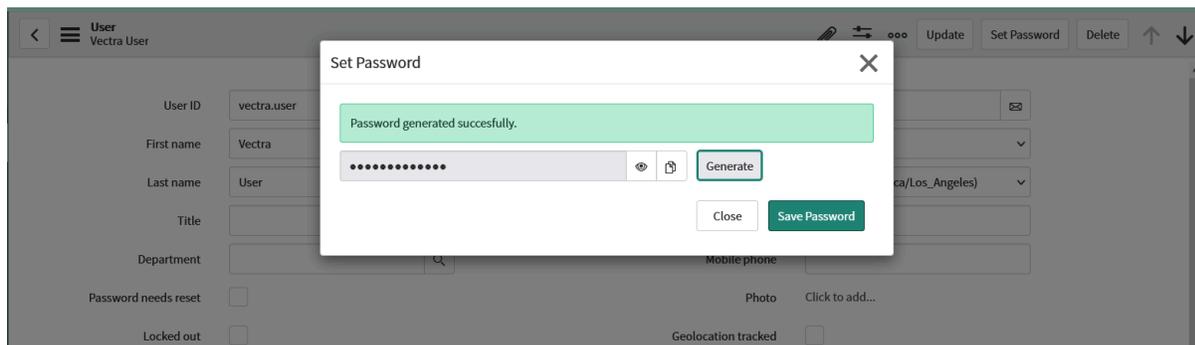
Note: The values for the user ID, title, and email address shown in the following table and figure are example values.

Field	Description
User ID	Unique User ID for the role in your ServiceNow Platform instance. An example is Vectra_itsm_admin.

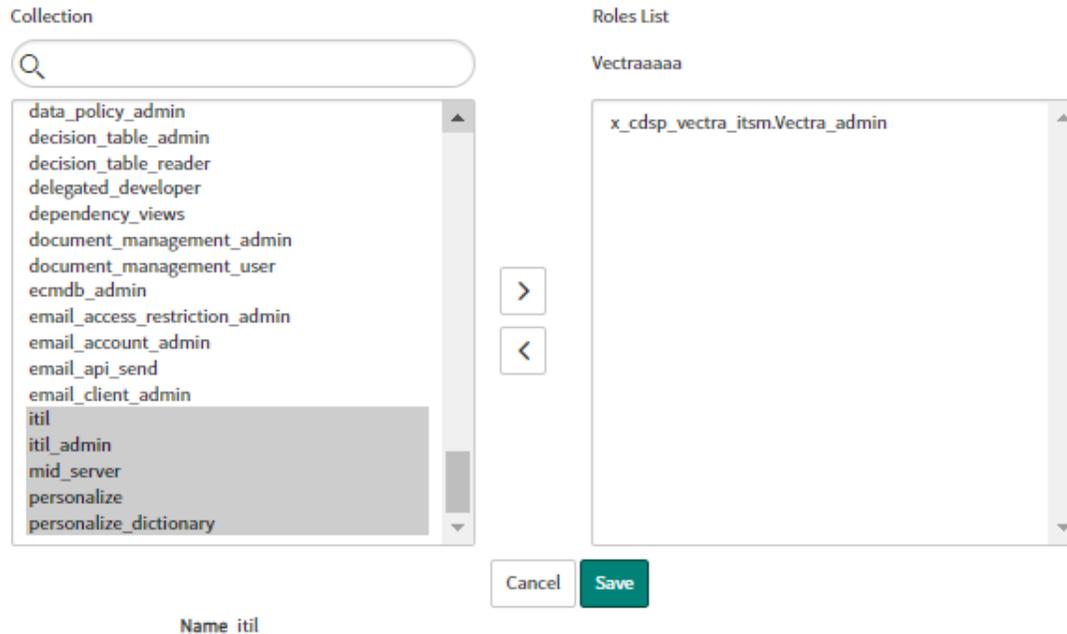
First Name	First Name of the user you are assigning
Last Name	Last Name of the user you are assigning
Title	Job Title, for example, Vectra Admin
Password	Unique password created for this role
Email	Unique email address

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

- 5 Click on "Submit" Once submitted, you can assign the role.
- 6 On the Users list, in the User ID column, click on the name of the new user you created, Vectra_itsm_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.



- 9 One pop-up will be displayed by clicking on "Generate." This will generate a unique password for the newly 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 required role in the Collection field.
- 13 In the Collection column, select and move required roles to the Roles List.



14 Click “Save”.

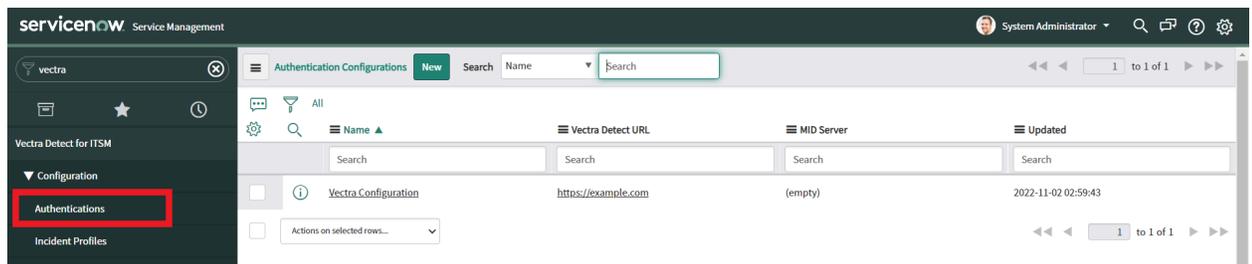
2.4.2. Authentication Configuration

This section describes how to configure authentication, which is used to populate ServiceNow with incidents from Vectra and perform manual actions.

Role Required: x_cdsp_vectra_itsm.Vectra_admin

Procedure:

1. log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for ITSM” -> “Configuration”.
3. Click on “Authentications”.



4. Enter the Name, Vectra Detect URL, API Token and Select the MID Server for communication with the Vectra Detect.

Authentication Configuration
New record

This authentication configuration record is used to connect to the Vectra Detect platform

- Name: Unique name to identify the Authentication Configuration
- Vectra Detect URL: Provide the URL of the Vectra Detect platform
- Token: Provide the API Token generated from platform
- MID Server: Provide the MID Server to communicate with the Vectra Detect Platform

Note: Vectra Detect URL should be in `https://{vectra-instance-url}` format

* Name: Vectra Detect Config

* MID Server: MID Server Vectra

* Vectra Detect URL: https://example.com

* API Token:

Submit

5. Click on “Submit” to authenticate.

6. On success “Authentication configuration saved successfully” message is shown.

Authentication Configurations **New** Search Name Search

Authentication configuration saved successfully.

	Name	Vectra Detect URL	MID Server	Updated
<input type="checkbox"/>	Vectra Detect Config	https://10.253.255.11	dev115052.mid	2022-12-01 20:35:47 just now

Actions on selected rows...

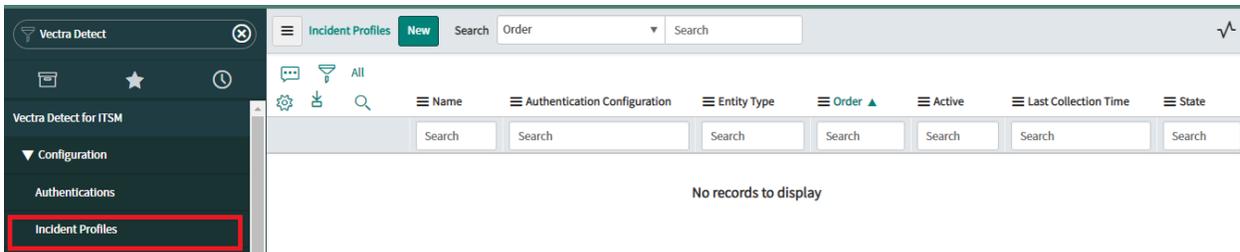
2.4.3. Incident Profile

This section describes how to configure the Incident profile for receiving the Accounts, Hosts, and Detections for the “Vectra Detect for ITSM” application, which is used to populate ServiceNow with incidents.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, itil

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to “Vectra Detect for ITSM” -> “Configuration”
3. Click on “Incident Profiles”



4. Click on New. It will open a new Incident profile view.
5. In the “Basic Information” section Select Authentication Configuration 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.

6. In the “Incident Creation” section users can provide IncidentCreation Criteria and Fallback User.
 - 6.1. Incidents will be created as per the conditions specified in the Creation Criteria.
 - 6.2. There will be two criteria: Incident Creation Criteria and Detection Criteria. The incident will be created if even one of the requirements is met.
 - 6.3. “Incident Creation Criteria” will be applied on the Account/Host and incident will be created for those Account/Host who satisfy the criteria.
 - 6.4. “Detection Criteria” will be applied on detection, and if they match, an incident for the Account/Host associated with the detection will be created.

6.5. If both criteria are empty then incidents will be created for all the entities (Account/Host) fetched.

6.6. An entity will be allocated to a Fallback user on Vectra Detect in the scenario that the Incident created for an unassigned entity is assigned to a user in ServiceNow who is unavailable on Vectra Detect.

The screenshot shows the 'Incident Profiles' configuration page for an 'Account' entity, specifically the 'Incident Creation' tab. The page has a breadcrumb trail: Basic Information > Incident Creation > Field Mapping > Scheduling. The 'Incident Creation Criteria' section includes a light blue informational box with the following text: 'Define what kind of entities should be converted to Incident. Filter conditions are case-sensitive.' It lists: '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.', and 'If both are present, they will apply as an "OR" condition. For ex:'. Below this, two examples are provided: 'Entity Criteria: Threat > 50 AND Certainty > 25' and 'Detection Criteria: Detection Category = COMMAND & CONTROL'. The final condition is '(Threat > 50 AND Certainty > 25) OR (Detection Category = COMMAND & CONTROL)'. The configuration area has two sections: 'Entity Criteria' and 'Detection Criteria'. 'Entity Criteria' has 'Add Filter Condition' and 'Add "OR" Clause' buttons. Below, it shows 'All of these conditions must be met' with two conditions: 'Threat' greater than '50' and 'Certainty' greater than '25', both connected by 'AND'. 'Detection Criteria' also has 'Add Filter Condition' and 'Add "OR" Clause' buttons, but the fields are currently empty, showing '-- choose field --', '-- oper --', and '-- value --'. The 'Fallback User' section has a light blue box explaining that the default 'Assigned to' field will be used to assign entities to a user on Vectra Detect, or the fallback user if the user doesn't exist. Below this is a text input field for the 'Fallback User' with a red asterisk icon. At the bottom right are 'Previous' and 'Next' buttons.

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.

The screenshot shows two error messages in a red box at the top of the configuration page. The first message is 'Fallback user fallback_user does not exist on Vectra Detect platform' with a close button (X). The second message is 'Invalid update'. Below the error messages is the breadcrumb trail: Basic Information > Incident Creation > Field Mapping > Scheduling.

7. After Configuring the Incident Creation 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 Incidents fields.

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

7.3. After applying mapping fields the user can click on “Next” to go to “Scheduling” for configuring.

8. In the “Scheduling” tab user has to configure data ingestion for Recurring Data Collection and One Time Data Collection.
 - 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.

Incident Profiles
test account

Update Delete

Basic Information Incident Creation Field Mapping Scheduling

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

Recurring Data Collection

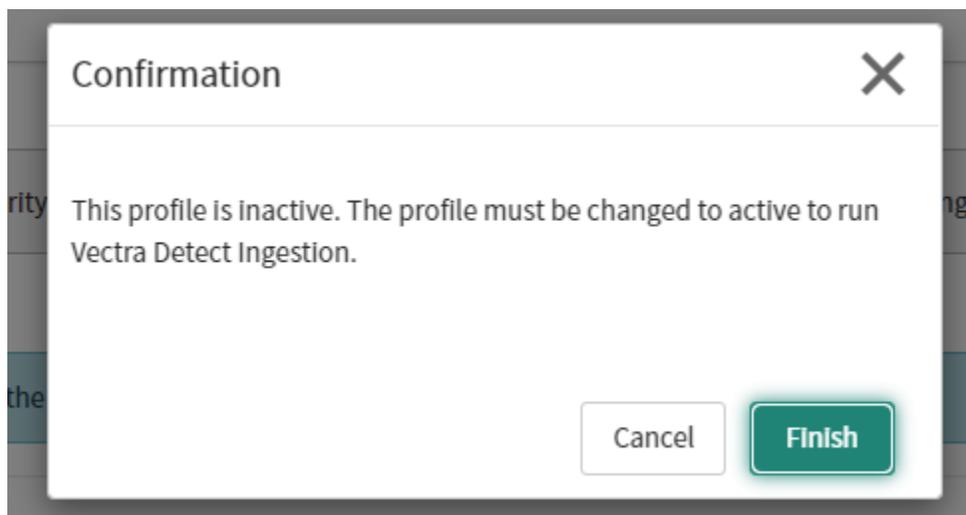
Recurring Data Collection

One-Time Data Collection

One-Time Data Collection

Previous Finish

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.



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 Incidents (Account/Host) and also provides a detailed view of the selected entity record that is fetched through data collection.

Prerequisite: Authentication configuration. (See [Authentication Configuration](#)).

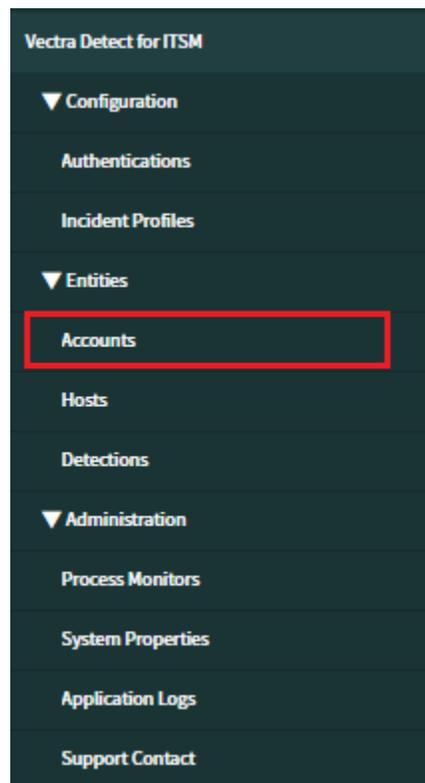
2.5.1. Accounts

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

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

1. Login to the ServiceNow instance.
2. Navigate "Vectra detect for ITSM" -> "Entities" -> "Accounts".



Accounts Search Incident Profile Search							
Account ID	Incident	Account Name	Threat	Certainty	Severity	Incident Profile	
360	INC0016209	test@test.io	0	0	Low	Incident Profile Account	
322	INC0016210	higaki-ha11@archer.local	0	0	Low	Incident Profile Account	

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 "IncidentField" will be read-only.

Accounts test@test.io
Update Delete

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

Add Tag +

Account ID:

Account Name:

Account Type:

Threat:

State:

Incident Profile:

Incident:

Severity:

Certainty:

Vectra Account URL: <https://10.253.255.11/accounts/360>

Additional Details

Assignment Details

Sensor(s):

Privilege Category:

Last Detection Timestamp:

Privilege Level:

Update
Delete

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

Sensor(s) w7Trdrz6 Last Detection Timestamp 2022-10-20 19:26:53

Privilege Category Privilege Level

Update Create Incident Delete

Detections Search Entity Name Search 1 to 2 of 2

Detections

	Detection ID	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State
<input type="checkbox"/>	7270	Privilege Anomaly: Unusual Service	LATERAL MOVEMENT	360	test@test.io	0	0	false	fixed
<input type="checkbox"/>	7817	Privilege Anomaly: Unusual Service	LATERAL MOVEMENT	360	test@test.io	0	0	false	fixed

- A user may create an Incident for a given account if the Incident associated with it is either closed or blank by clicking on "Create Incident".
- When an Incident is created, a message with the phrase "Incident <INCIDENT-NUMBER> created successfully" is displayed to the user.

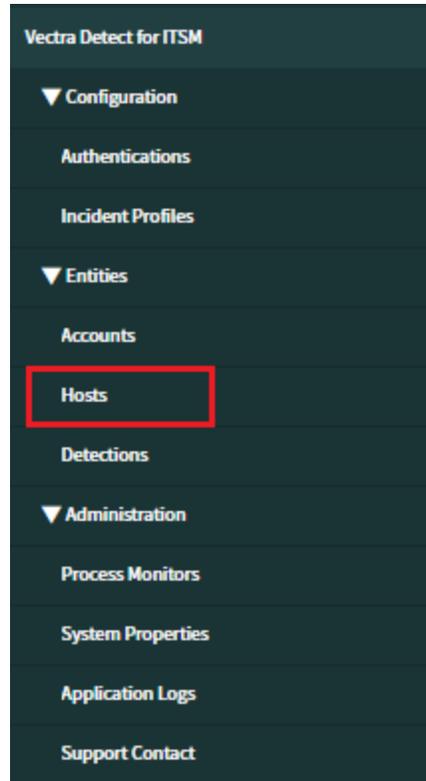
2.5.2. Hosts

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 an Incident for a specific host.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

- Login to the ServiceNow instance.
- Navigate to "Vectra detect for ITSM" -> "Entities" -> "Hosts"



Hosts								Search
Severity								Search
All								
Host ID	Incident	Host Name	IP	Threat	Certainty	Severity		
Search	Search	Search	Search	Search	Search	Search	Search	
<input type="checkbox"/>	369	INC0016214	VMAL #2 - Jump station ICS	10.250.100.150	18	57	medium	
<input type="checkbox"/>	872	INC0016212	VMAL #2 windows 10.250.50.111 (higaki-ha11)	10.250.50.111	4	37	low	
<input type="checkbox"/>	1383	(empty)	Lab #6_conti - 10.230.50.120 (l6-user120)	10.230.50.120	31	11	low	
<input type="checkbox"/>	873	(empty)	VMAL #2 windows 10.250.50.112 (endo-ka012)	10.250.50.112	4	46	low	
<input type="checkbox"/>	1396	(empty)	Lab #6_conti - 10.230.50.131 (l6-user131)	10.230.50.131	26	34	low	

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

Hosts
VMAL #2 windows 10.250.50.111 (higaki-ha11)

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

Add Tag +

Host ID	872	Incident Profile	Host
Host Name	VMAL #2 windows 10.250.50.111 (higaki-	Incident	INC0034605
IP	10.250.50.111	Severity	low
Threat	4	Certainty	35
Host Type	yaSHk3l-	Probable Owner	higaki-ha11@archer.local
State	active	Vectra Host URL	https://10.253.255.11/hosts/872

Additional Details | Assignment Details

Sensor(s)	eti2pc2s	Sensor Name	Vec2c610896a947c5b5102c466a28f49a
Privilege Category	Medium	Last Detection Timestamp	2022-12-10 14:29:01
Privilege Level	4	Host Artifact Set	
Is Key Asset	false		

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

Privilege Level	4	Host Artifact Set	
Is Key Asset	false	Previous IPs	
Is Targeting Key Asset	false	Last Source	10.250.50.111
Has Active Traffic	true		

Update Delete

Detections Search Entity Name Search 1 to 99 of 99

Detections

	Detection ID	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State
<input type="checkbox"/>	7918	SMB Brute-Force	LATERAL MOVEMENT	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	70	72	false	fixed
<input type="checkbox"/>	7789	Novel External Destination Port	INFO	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	0	0	false	fixed
<input type="checkbox"/>	7392	File Share Enumeration	RECONNAISSANCE	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	57	95	false	fixed
<input type="checkbox"/>	7331	RPC Recon	RECONNAISSANCE	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	70	94	false	fixed
<input type="checkbox"/>	7250	Hidden HTTPS Tunnel	COMMAND & CONTROL	872	VMAL #2 windows 10.250.50.111 (higaki-ha11)	0	0	false	fixed

- A user may create an Incident for a given host if the Incident associated with it is either closed or blank by clicking on "Create Incident".
- When an Incident is created, a message with the phrase "Incident <INCIDENT-NUMBER> created successfully" is displayed to the user.

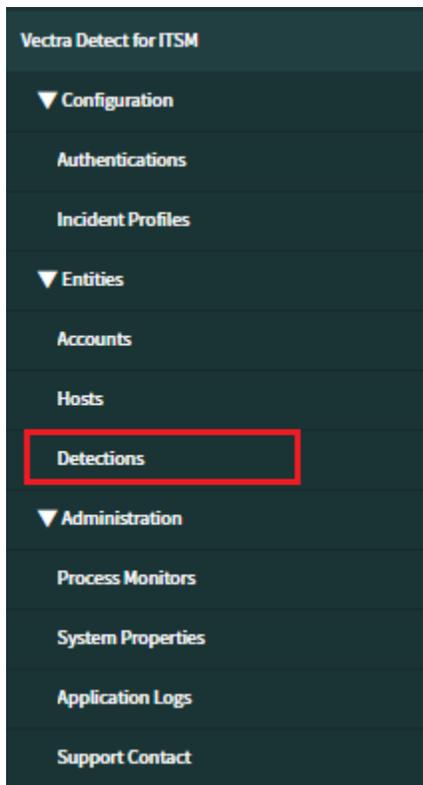
2.5.3. Detections

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. Add and remove tags. Users can also add notes that will be reflected back to the Vectra Detect.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Vectra detect for ITSM" -> "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.

Detections Search Entity Name Search										
All > State = active										
	Detection ID	Detection Type	Detection Category	Entity ID	Entity Name	Threat	Certainty	Is Triaged	State	
<input type="checkbox"/>	8113	New Host Role	INFO	1468	VMAL2windows10.250.50.107seankase107	0	0	false	active	
<input type="checkbox"/>	7982	New Host Role	INFO	820	VMAL2-Windows10pc-cherylt	0	0	false	active	
<input type="checkbox"/>	8032	New Host Role	INFO	1275	VMAL #6 - DMZ web1	0	0	false	active	
<input type="checkbox"/>	8129	New Host Role	INFO	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	0	0	false	active	
<input type="checkbox"/>	8109	Suspicious LDAP Query	RECONNAISSANCE	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	20	25	false	active	
<input type="checkbox"/>	8132	Suspicious Relay	COMMAND & CONTROL	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	32	95	false	active	
<input type="checkbox"/>	8124	RPC Targeted Recon	RECONNAISSANCE	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	58	56	false	active	
<input type="checkbox"/>	8120	Suspicious Remote Execution	LATERAL MOVEMENT	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	20	71	false	active	
<input type="checkbox"/>	8101	SQL Injection Activity	LATERAL MOVEMENT	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	63	89	false	active	
<input type="checkbox"/>	8136	Data Smuggler	EXFILTRATION	1543	VMAL #2 windows 10.250.50.141 (kgalloway...	95	94	false	active	

<
≡
Detections
8113
🔗
📄
🔍
☰
⋮
Update
Download PCAP
Mark as Fixed
Delete
↑

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

Add Tag +

Detection ID	<input type="text" value="8113"/>	Incident Profile	<input type="text" value="Host"/> ⓘ
Detection Type	<input type="text" value="New Host Role"/>	Certainty	<input type="text" value="0"/>
Fixed	<input type="checkbox"/>	Detection Category	<input type="text" value="INFO"/>
State	<input type="text" value="active"/>	Threat	<input type="text" value="0"/>
Entity ID	<input type="text" value="1468"/>	Entity Name	<input type="text" value="VMAL2windows10.250.50.107seankase1"/>
Assigned Date	<input type="text" value="2022-12-12 13:09:36"/>	Entity Type	<input type="text" value="Detections"/>
Is Targeting Key Asset	<input type="text" value="false"/>	Filtered By Ai	<input type="text" value="false"/>
Is Triaged	<input type="text" value="false"/>	Filtered By Rule	<input type="text" value="false"/>
Summary	<input type="text" value='{"roles": ["File Server"], "last_timestamp": "2022-12-06T21:10:18Z", "description": "This is the first time this host role was identified on this host:"}'/>	Filtered By User	<input type="text" value="false"/>
		Vectra Detection URL	https://10.253.255.11/detections/8113

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

Notes

Notes

Notes

Post

Activities: 2

 System Administrator
This note is added from ServiceNow

Notes • 2022-12-02 04:22:14 just now

7. A related list of Hosts, and Accounts will be populated at the bottom of the form view.

Accounts Hosts (1)

Hosts Search Severity Search

Hosts

Host ID	Incident	Host Name	IP	Threat	Certainty	Severity
1073	INC0016305	VMAL #2 windows 10.250.50.139 (wakesette...	10.250.50.139		0	0

Actions on selected rows...

2.6. Process Monitor

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

Role Required: x_cdsp_vectra_itsm.admin

Procedure:

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

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

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

Process Monitor
Created 2022-12-14 02:27:54

Start Time: 2022-12-14 02:27:54 End Time: 2022-12-14 02:28:12

State: Completed Entity Type: Account

Incident Profile: Account ⓘ

Description: [2022-12-14 10:27:54] One time data collection started.
[2022-12-14 10:28:01] Data collection completed. Total entity fetched: 2
[2022-12-14 10:28:01] Data ingestion started
[2022-12-14 10:28:12] Data ingestion completed. Processed Incidents: 2

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 ITSM” application.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

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

Add Tag + Harshit test fixed2 testabc sgertDemoTag

- 6. On successful download users can see the PCAP file in attachment.
- 7. Users can also see notes for 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 sync to Vectra Detect.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

- 1. Log in to the ServiceNow instance.
- 2. Navigate to “Vectra Detect for ITSM”.
- 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 + test fixed2 testabc

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

This section describes how to add a note to an entity or detection in ServiceNow sync to Vectra Detect.

Role Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

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

Post

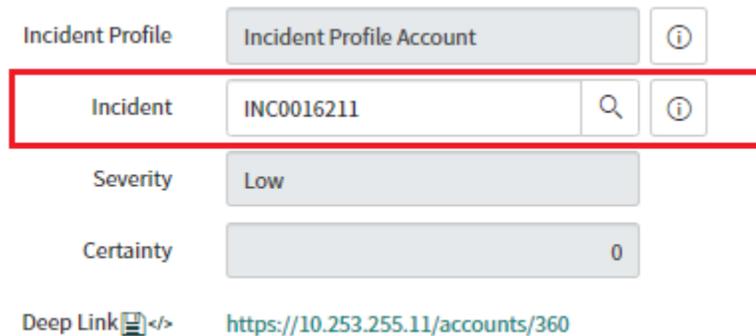
Activities: 13

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, an Incident should be attached to that entity.
6. Open Incident from the Incident reference field.



Incident Profile

Incident Profile Account

Incident

INC0016211

Severity

Low

Certainty

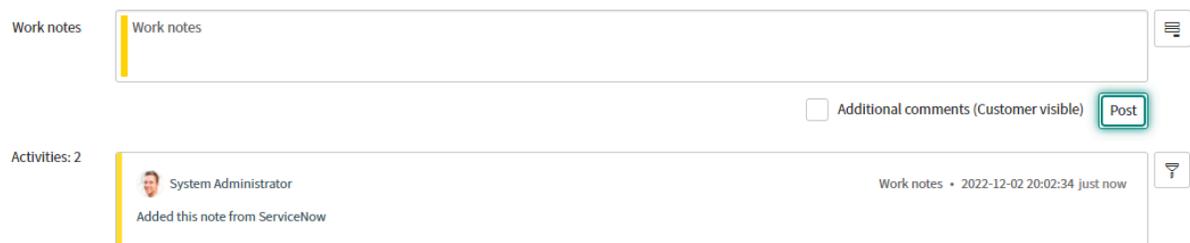
0

Deep Link  <https://10.253.255.11/accounts/360>

7. In the form view of an Incident, the user can see the notes in the “Notes” tab.



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



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, sync to Vectra Detect.

Roles Required: x_cdsp_vectra_itsm.Vectra_admin, x_cdsp_vectra_itsm.Vectra_user

Procedure:

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for ITSM”.
3. Open a detection form “Vectra Detect for ITSM” -> “Entities” -> “Detection”.

- To fix the detection from Vectra, click on “Mark as Fixed” button available in the header of the form.

The screenshot shows the Vectra Detect interface for a specific detection. At the top, there is a header bar with a back arrow, a menu icon, the text 'Detections 8113', and several action buttons: 'Update', 'Download PCAP', 'Mark as Fixed', 'Delete', and an upward arrow. Below the header is a light blue bar with the instruction 'Select/Enter a tag from the textbox and click on + to add a tag.' Underneath this is an 'Add Tag' section with a text input field containing 'Select/enter string' and a '+' button.

The main form is divided into two columns of input fields:

- Left Column:**
 - Detection ID: 8113
 - Detection Type: New Host Role
 - Fixed:
 - State: active
 - Entity ID: 1468
 - Assigned Date: 2022-12-12 13:09:36
 - Is Targeting Key Asset: false
 - Is Triaged: false
 - Summary: [{"roles": ["File Server"], "last_timestamp": "2022-12-06T21:10:18Z", "description": "This is the first time this host role was identified on this host."}]
- Right Column:**
 - Incident Profile: Host
 - Certainty: 0
 - Detection Category: INFO
 - Threat: 0
 - Entity Name: VMAL2windows10.250.50.107seankase1
 - Entity Type: Detections
 - Filtered By Ai: false
 - Filtered By Rule: false
 - Filtered By User: false
 - Vectra Detection URL: <https://10.253.255.11/detections/8113>

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_itsm.Vectra_admin,x_cdsp_vectra_itsm.Vectra_user,itsl, itil admin

Procedure:

- Log in to the ServiceNow instance.
- Navigate to “Vectra Detect for ITSM”.
- Open any Incidentcreated for an account or host.

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

Add Tag +

tag360 × sgerDemoTag × testaccount322 × T ×

qwepaos × OnTesting × testDemo0Demo ×

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

Incident Profile: Incident Profile Account

Incident: INC0016211

Open Record

Incident

Number: INC0016211
 Caller:
 Category: Inquiry / Help
 Subcategory:
 Contact type:
 State: New
 On hold reason:
 Impact: 3 - Low

Additional Details: Assignment Details

Sensor(s): w77rdz6

4. In the Incident form view user can see the “Assigned To” Entity.

Incident INC0016211

Follow Update Create Security Incident Resolve Delete

Number: INC0016211
 Caller: Abel Tuter
 Category: Inquiry / Help
 Subcategory: -- None --
 Service:
 Service offering:
 Configuration item:
 Short description: This Incident is created from Vectra Detect for Account : test@test.io
 Description: This Incident is created by Vectra Detect for Account : test@test.io. Name: test@test.io ID: 360 Account Type: kerberos Threat: 0

Contact type: -- None --
 State: New
 Impact: 3 - Low
 Urgency: 3 - Low
 Priority: 5 - Planning
 Assignment group:
 Assigned to: Xsor User

5. Select a ServiceNow user who is present in the Vectra Detect and click on “Update”.
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 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 ✎ 🗑️ ✓

Activities: 4

System Administrator

Work notes • 2022-12-02 20:12:21 1m ago

Successfully assigned the entity on Vectra Detect Platform

System Administrator

Field changes • 2022-12-02 20:12:21 1m ago

Assigned to	Xsor User
Incident state	In Progress was New

7. If an entity is already assigned to a user in Vectra and we try to reassign it to some other user then the 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.

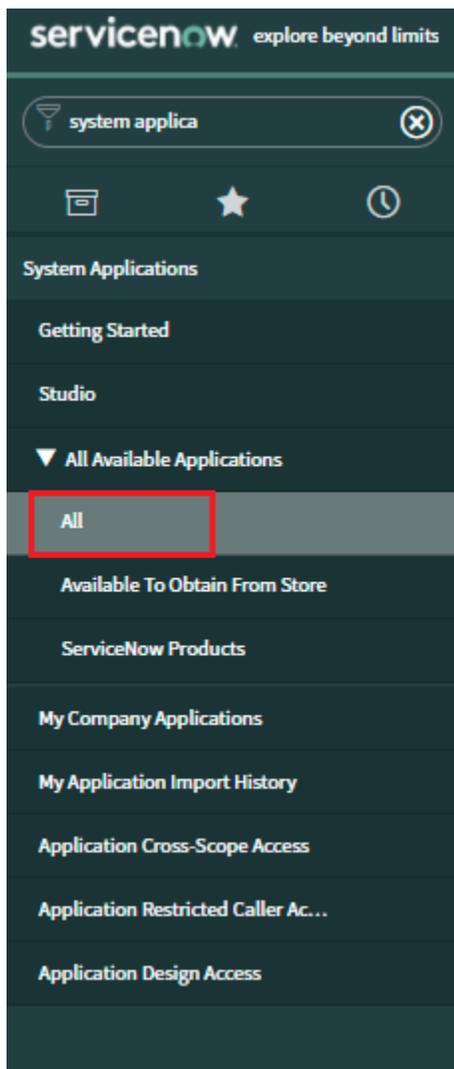
3. Uninstallation

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

Role Required: System Administrator (admin)

The following steps will guide you on how to uninstall the Vectra Detect for ITSM App from the ServiceNow UI.

Navigate to “System Applications” -> “All Available applications” -> “All”.



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

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

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 for ITSM” -> “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 for ITSM”.
3. Open “Application Logs”.

4.2.2. Unable to install Vectra Detect for ITSM 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.

4.2.3. 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

4.2.4. Unable to Collect Data

Problem Statement: Getting error while data collection.

Role Required: Vectra admin (x_cdsp_vectra_itsm.admin)

1. Log in to the ServiceNow instance.
2. Navigate to “Vectra Detect for ITSM”.
3. Check “Application Logs” for any errors.

4.2.5. 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.

END OF DOCUMENT