

# Best Practices for Operationalization of Vectra Detect with Microsoft Sentinel

Version: May 24, 2023

## Table of Contents

<b>Introduction</b> .....	<b>2</b>
<b>Available content in Microsoft Sentinel for Vectra Detect</b> .....	<b>2</b>
<b>Recommended workflows</b> .....	<b>4</b>
<b>Overview</b> .....	<b>4</b>
Incident creation for prioritized entities .....	4
Alert creation for detections .....	4
<b>Anatomy of a Microsoft Sentinel incident for Vectra's signal</b> .....	<b>5</b>
<b>Analytic Templates logic</b> .....	<b>6</b>
Priority mapping .....	6
Frequency .....	6
<b>Alerts</b> .....	<b>6</b>
<b>Incidents</b> .....	<b>7</b>
<b>Step by step configuration of recommended workflows</b> .....	<b>7</b>
Incident creation for prioritized hosts .....	7
Alert creation for host detections .....	11
Incident creation for prioritized accounts .....	16
Alert creation for account's detections .....	18
<b>The SOC analyst journey</b> .....	<b>21</b>
<b>Best practices</b> .....	<b>23</b>
Keep the content up to date! .....	23
Create an alert when no events are received .....	24
<b>Worldwide Support Contact Information</b> .....	<b>25</b>

## Introduction

This document intends to provide guidance to operationalize Vectra Detect in Microsoft Sentinel to get the most out of the Vectra Platform and its AI prioritization technology. We recommend following these guidelines as a starting point and then making adjustments that are specific to your environment and desired workflows.

Vectra Attack Signal Intelligence has 3 core components:

- ▼ AI Detection
- ▼ AI Triage
- ▼ Ai Prioritization

Those technologies work hand in hand to provide the best signal to the SOC and focus on what matters. In the scenario where Microsoft Sentinel is used as the primary tool by the SOC to manage security incidents across their Security solutions, it is key to bring this signal into Microsoft's Sentinel workflow. This guide relies on Analytic templates provided by Vectra to implement an effective approach.

This guide is for the Vectra Classic UX (syslog based using the Vectra appliance platform). An update will be released for the Vectra Respond UX (Vectra cloud platform) in the near future.

## Available content in Microsoft Sentinel for Vectra Detect

The below table represents what is currently available and maintained by Vectra if you deploy our Detect solution from the content hub (or [Marketplace](#)):

MS Sentinel Data Point	Vectra Detect Solution
Package Version	2.0.5
Data Connector	1 (version 1.1.1)
Workbooks	1
Analytic Templates	7

- ▼ This document is an attachment to the [Sending Vectra Detect Events to Microsoft Sentinel](#) KB article on the Vectra support site.
  - That KB article details how to send data from Vectra Detect to Microsoft Sentinel while this document covers best practices around the operationalization of that data in Sentinel.

The most common mistake we are seeing is configuring and enabling all our Analytic templates. We strongly discourage doing this! Our analytic templates have been developed to cover different use cases and for implementing the best integration, we recommend following the guidelines shared in this document:

Template Name	Description	Version	Guideline	Incident	Severity
<b>Vectra AI Detect - Suspected Compromised Account</b>	Create an incident when an Account is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.	1.0.5	Highly Recommended	Yes	Dynamic
<b>Vectra Account's Behaviors</b>	This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on account's detections.	1.0.1	Recommended	No	Dynamic
<b>Vectra AI Detect - Suspected Compromised Host</b>	Create an incident when a Host is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.	1.0.5	Highly Recommended	Yes	Dynamic
<b>Vectra Host's Behaviors</b>	This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on host's detections.	1.0.1	Recommended	No	Dynamic
Vectra AI Detect - Detections with High Severity	Create an incident for high severity malicious behavior detected by Vectra AI (Threat score superior to 7.0). The Severity is a mapping with the Threat score assigned to a detection. It ranges between 0 and 10. The <i>severity_threshold</i> variable can be adjusted as desired.	1.0.6	Optional	Optional	High
Vectra AI Detect - New Campaign Detected	Identifies when a new Campaign has been detected. This occurs when multiple Detections across different Hosts are suspected to be part of the same Attack Campaign.	1.1.5	Optional	Optional	Medium
Vectra AI Detect - Suspicious Behaviors	Create an incident for each new malicious behavior detected by Vectra Detect. By default, it looks through all tactics. This can be modified to create incident only for a subset of tactics. Example of a common use case: " <i>Create an incident when a detection in the category Exfiltration is triggered</i> "	1.0.7	Optional	Optional	Dynamic

## Recommended workflows

### Overview

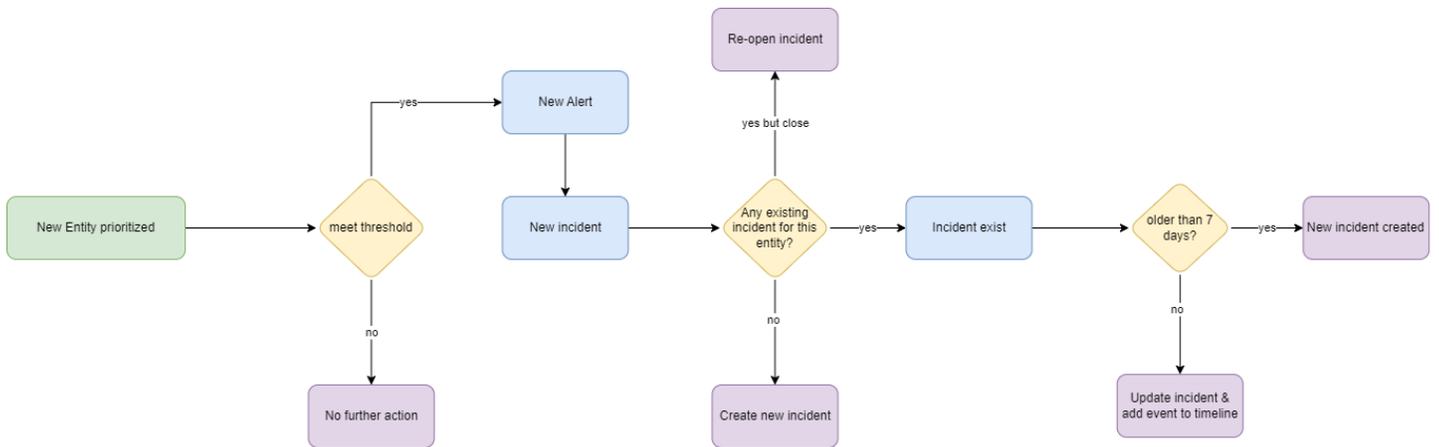
The Vectra philosophy is to focus on prioritized entities versus individual detections. The recommended configuration and workflow follow that same logic.

### Incident creation for prioritized entities

Analytic templates to enable:

- ▼ Vectra AI Detect - Suspected Compromised Host
- ▼ Vectra AI Detect - Suspected Compromised Account

High level view:

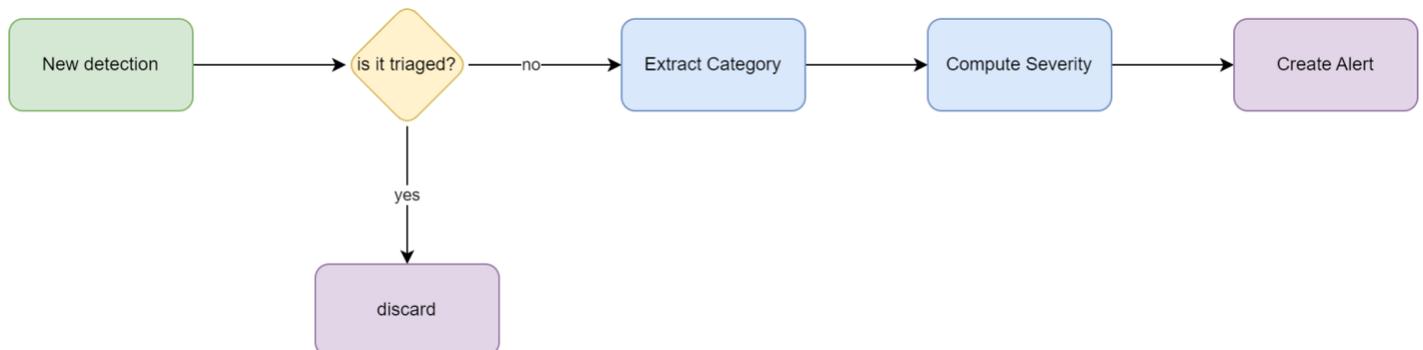


### Alert creation for detections

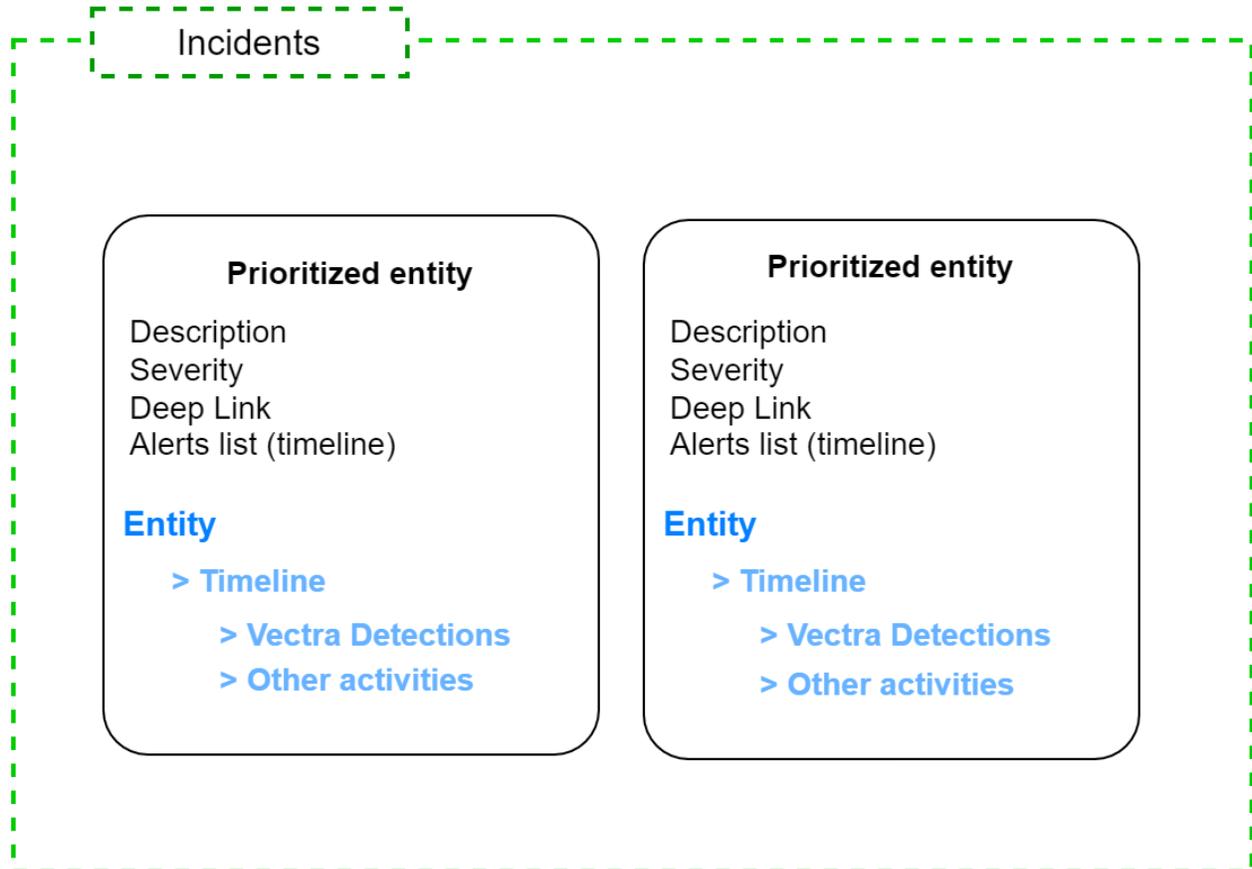
Analytic templates to enable:

- ▼ Vectra Host's Behaviors
- ▼ Vectra Account's Behaviors

The recommended workflow to handle detections associated to entities would be:



## Anatomy of a Microsoft Sentinel incident for Vectra's signal



The creation of the incident is driven by Analytic rules (created from Vectra's provided Analytic templates) per entity type:

- ▼ Description shows the Threat and Certainty scores for this entity.
- ▼ Deep link is provided to pivot to the Vectra UI.
- ▼ Incident's severity is dynamically computed based on Vectra's severity score.
- ▼ Map the incident to one Entity (Host or account)
  - Note that it would be unlikely to be attached to multiple entities.
- ▼ The Entity's timeline also shows activities, including the behaviors (detections) generated by the Vectra Platform.
  - The analyst can decide to add them to the incident timeline.

**!! Please Note:** Vectra's detections are written to the *SecurityAlert* table but are not promoted to be incidents (created from Vectra's provided Analytic templates). The entity mapping allows correlation of detections to the entity. Alerts are visible in the timeline view of the entity. An alternative approach would be to use some automation to automatically add those alerts to the incident timeline. This is not done automatically today but is a potential for future development. Please contact your Vectra account team with feedback.

## Analytic Templates logic

### Priority mapping

The severity level in Vectra's classic UX is slightly different than the one in Sentinel. This is mapping that is applied in our Analytic Templates:

Vectra Severity	Sentinel Severity
Informational	Informational
Low	Low
Medium	Medium
High	High
Critical	High

Our analytic templates have a default severity of "Informational". The correct severity is set dynamically according to the above mapping. The severity of the Alert or the Incident is automatically mapped to Vectra's severity.

### Frequency

This defines when a threat is identified and prioritized. Time to investigate is critical. Our analytic templates use the following parameters:

- ▼ Run every 5 minutes.
- ▼ Look at the events from last 5 minutes.

#### Query scheduling

Run query every \*

Lookup data from the last \* ⓘ

Start running ⓘ

Automatically  At specific time (Preview)

**i** Starting automatically, the rule will run every 5 minutes, looking up data from last 5 minutes.

### Alerts

Alert (Event) grouping must be disabled (this is set by default in our Analytics Templates). The Kusto query is already grouping by entities or detection and takes care of duplicates. A single alert or incident must be created for each entry of the result table.

#### Event grouping

Configure how rule query results are grouped into alerts

- Group all events into a single alert
- Trigger an alert for each event

**i** A single analytics rule can generate up to 150 alerts. If you choose "Trigger an alert for each event" and the rule query returns more than 150 events, the rule will generate 150 alerts, and the last alert will include a summary of all the events. [Learn more >](#)

## Incidents

There are a few things we tried to avoid:

- ▼ Creating duplicate incidents.
- ▼ Creating too many incidents.
- ▼ Creating incidents every time a detection shows up.

The table below provides a mapping between our Analytics templates and what we recommend:

Analytic Template Name	Type	Grouping settings
Vectra AI Detect - Suspected Compromised Host	Incident	7 days (per entity)
Vectra Host Behaviors	Alert	None
Vectra AI Detect - Suspected Compromised Account	Incident	7 days (per entity)
Vectra Account Behaviors	Alert	None

We do not include other analytic templates as their configuration would depend on the use case that needs to be addressed. We do not recommend enabling them by default as they could generate too many incidents if not properly tuned.

## Step by step configuration of recommended workflows

### Incident creation for prioritized hosts

First, we want to create Incidents when Hosts are prioritized in the Vectra appliance platform. To do so, we are going to modify the analytic template named: Vectra AI Detect - Suspected Compromised Host.

- ▼ Menu: Configuration > Analytics > Rule templates.
- ▼ Search for Vectra and select the template name **Vectra AI Detect - Suspected Compromised Host**.
- ▼ Click "Create rule".

The screenshot shows the Microsoft Sentinel Analytics interface. On the left is a navigation pane with categories like Threat management, Content management, and Configuration. The main area displays a list of rule templates under the 'Rule templates' tab, filtered by 'Vectra'. The 'Vectra AI Detect - Suspected Compromised Host' template is selected and highlighted. A detailed view of this template is shown on the right, including its description, data sources (CommonSecurityLog (AI/VectraDetect)), and tactics and techniques (Collection, Command And Control, Credential Access, Discovery, Exfiltration, Impact, Lateral Movement). At the bottom, there is a 'Rule query' section with a note: 'You haven't used this template yet; you can use it to create analytics rules.' and a 'Create rule' button.

- ▼ Set the status to **Enabled** and make sure than Severity is set to **Informational** (it should be default).

Microsoft Azure

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

## Analytics rule wizard - Create new rule from template

Vectra AI Detect - Suspected Compromised Host

**General** Set rule logic Incident settings Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

### Analytics rule details

Name \*

Vectra AI Detect - Suspected Compromised Host

Description

Create an incident when a Host is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical). Recommended configuration

Tactics and techniques

7 selected

Severity

Informational

Status

**Enabled** Disabled

On the next page, the **rule logic** settings are all preconfigured:

- ▼ The query (use the view query results to validate if it returns any results).
- ▼ An incident is created when a host is in the High or Critical quadrant.
- ▼ The Alert enrichment:
  - Entity mapping.
  - Custom details.
  - Alert details.
- ▼ The scheduling of the query and the threshold.
- ▼ Event grouping.

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

## Analytics rule wizard - Create new rule from template

Vectra AI Detect - Suspected Compromised Host

Define the logic for your new analytics rule.

### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
// Edit this variable to only keep the Severity level where an incident needs to be created (Defaults are: "High", "Critical" ). Possible values are: "Low", "Medium", "High", "Critical"
let configured_level = dynamic(["High", "Critical"]);
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X Series"
```

[View query results >](#)

### Alert enrichment

#### Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis.

For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

<input type="text" value="Host"/>	<input type="text" value="HostName"/>	<input type="text" value="SourceHostName"/>	<input type="button" value="+ Add identifier"/>
<input type="button" value="+ Add new entity"/>			

#### Custom details

Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. [Learn more >](#)

<input type="text" value="ScoreDecrease"/>	<input type="text" value="score_decreases"/>	<input type="button" value="+ Add new"/>
--	--	--

#### Alert details

Here you can select parameters in your alert that can be represented in the name or description of each instance of the alert, or that can contain the tactics and severity assigned to that instance of the alert. Enter free text in the fields below, and to insert a parameter, type a column name from the query results, surrounded by double curly brackets. Example: {{columnName}}. If the parameter has no value (or an invalid value in the case of tactics and severity), the alert details will revert to the defaults specified in the first page of the wizard. [Learn more >](#)

Alert Name Format

Alert Description Format

<input type="text" value="AlertLink"/>	<input type="text" value="vectra_URL"/>	<input type="button" value="🗑"/>
<input type="text" value="ProductName"/>	<input type="text" value="DeviceProduct"/>	<input type="button" value="🗑"/>
<input type="text" value="ProviderName"/>	<input type="text" value="DeviceVendor"/>	<input type="button" value="🗑"/>
<input type="text" value="ConfidenceScore"/>	<input type="text" value="certainty_score"/>	<input type="button" value="🗑"/>

- Next, the Incident settings should all be preconfigured as well but please check them for incident creation as well as the grouping:

The screenshot shows the 'Incident settings' tab in the 'Analytics rule wizard - Create new rule from template' interface. The page is for a rule named 'Vectra AI Detect - Suspected Compromised Host'. It includes sections for 'Incident settings', 'Alert grouping', and 'Re-open closed matching incidents'. The 'Incident settings' section has a toggle for 'Create incidents from alerts triggered by this analytics rule' set to 'Enabled'. The 'Alert grouping' section has a toggle for 'Group related alerts, triggered by this analytics rule, into incidents' set to 'Enabled'. Below this, there is a dropdown for 'Limit the group to alerts created within the selected time frame' set to '7' and 'Days'. There are three radio button options for grouping alerts into a single incident, with the first option 'Grouping alerts into a single incident if all the entities match (recommended)' selected. There are also dropdowns for 'Select entities' and 'Select details'. A warning icon indicates that entity-based alert grouping only works with entities mapped using the new version. At the bottom, there are 'Previous' and 'Next: Automated response >' buttons.

- ▼ The **automated response** depends on your environment and does not have anything configured by default.
- ▼ Click **Review** then **Create**.

The screenshot shows the 'Review and create' tab in the 'Analytics rule wizard - Create new rule from template' interface. A green banner at the top indicates 'Validation passed'. The 'Automated response' tab is selected. The page displays 'Analytics rule details' and 'Analytics rule settings'. The 'Analytics rule details' section includes: Name (Vectra AI Detect - Suspected Compromised Host), Description (Create an incident when a Host is suspected to be compromised...), Tactics and techniques (Credentialed Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact), Severity (Informational), and Status (Enabled). The 'Analytics rule settings' section shows the 'Rule query' with a KQL script that filters for specific device events and sets a severity level based on threat and certainty scores. The 'Rule frequency' is set to 'Run query every 5 minutes' and the 'Rule period' is 'Last 5 minutes data'. At the bottom, there are 'Previous' and 'Create' buttons.

- ▼ Once deployed, you should see the analytic rule in the Active rules list:

The screenshot shows the Microsoft Sentinel Analytics interface. On the left is a navigation pane with categories like General, Threat management, Content management, and Configuration. The main area displays 'Active rules' with a search filter set to 'Vectra'. A table lists the active rules:

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last modified
Informational	Vectra AI Detect - Susj	Scheduled	Enabled	+		Vectra AI Detect	4/11/2023

On the right, a detailed view of the rule 'Vectra AI Detect - Suspected Compromised Host' is shown. It includes the following information:

- Informational Severity**, **Content hub Content Source**, **Enabled Status**
- Description:** Create an incident when a Host is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical. Recommended configuration is to trigger an alert for at least High and Critical.
- Tactics and techniques:** Collection (0), Command and Control (0), Credential Access (0), Discovery (0), Exfiltration (0), Impact (0), Lateral Movement (0)
- Rule query:**

```
// Edit this variable to only keep the Severity Id
let configured_level = dynamic(["High", "Critical"]);
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X Series"
| where DeviceEventClassID == "hsc"
```
- Rule frequency:** Run query every 5 minutes
- Rule period:** Last 5 minutes data
- Rule threshold:** (empty)

## Alert creation for host detections

The intent is to create alerts for every host detection triggered by Vectra's Attack Signal Intelligence. Alerts go to the *SecurityAlert* table. To do so, we are going to modify the analytic template named: Vectra AI Detect - Vectra Host's Behaviors.

- ▼ Menu: Configuration > Analytics > Rule templates.
- ▼ Search for Vectra and select the template name **Vectra AI Detect - Vectra Host's Behaviors**.
- ▼ Click "Create rule"

The screenshot shows the Microsoft Sentinel Analytics console. On the left is a navigation menu with categories like General, Threat management, Content management, and Configuration. The main area displays a list of active rules. A table shows one rule: 'Vectra Host's Behaviors' with a severity of 'Informational', a rule type of 'Scheduled', and a source name of 'Vectra AI Detect'. On the right, a detailed view of this rule is shown, including its description, data sources (CommonSecurityLog), tactics and techniques (Collection, Command And Control, Credential Access, Discovery, Exfiltration, Impact, Lateral Movement), a KQL query, and rule frequency/threshold settings. A 'Create rule' button is visible at the bottom of the rule details pane.

▼ Set the status to **Enabled** and make sure than Severity is set to **Informational** (it should be default).

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Analytics](#) >

## Analytics rule wizard - Create new rule from template

Vectra Host's Behaviors

**general** | [Set rule logic](#) | [Incident settings](#) | [Automated response](#) | [Review and create](#)

Create an analytics rule that will run on your data to detect threats.

### Analytics rule details

Name \*

Vectra Host's Behaviors

Description

This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on host's detections.

Tactics and techniques

7 selected

Severity

Informational

Status

**Enabled** Disabled

On the next page, the **rule logic** settings are all preconfigured:

- ▼ The query (use the view query results to validate if it returns any results)
  - An alert would be created for every detection that is not triaged.
- ▼ The Alert enrichment:
  - Entity mapping
  - Custom details
  - Alert details
- ▼ The scheduling of the query and the threshold
- ▼ Event grouping

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

### Analytics rule wizard - Create new rule from template ...

Vectra Host's Behaviors

General Set rule logic Incident settings Automated response Review and create

Define the logic for your new analytics rule.

#### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```

threat_score >= 50 and certainty_score <= 50, "High",
threat_score >= 50 and certainty_score >= 50, "Critical",
"UNKNOWN")
| extend Severity = case(level == "Info", "Informational", level == "Critical", "High", level)
| summarize arg_max(threat_score, *) by source_entity, Activity
| sort by TimeGenerated
    
```

[View query results >](#)

#### Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Host

HostName SourceHostName + Add identifier

+ Add new entity

Custom details

Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. [Learn more >](#)

Activity Category

+ Add new

Alert details

Here you can select parameters in your alert that can be represented in the name or description of each instance of the alert, or that can contain the tactics and severity assigned to that instance of the alert. Enter free text in the fields below, and to insert a parameter, type a column name from the query results, surrounded by double curly brackets. Example: {{columnName}}. If the parameter has no value (or an invalid value in the case of tactics and severity), the alert details will revert to the defaults specified in the first page of the wizard. [Learn more >](#)

Alert Name Format

Vectra AI - {{Activity}} Detected

Alert Description Format

Entity is a host. Category is {{Category}}. Threat score is {{threat\_score}} and certainty score is {{certainty\_score}}.

AlertLink vectra\_URL

Severity Severity

ProductName DeviceProduct

Previous [Next: Incident settings >](#)

- ▼ Next, the **Incident settings** must **disabled**. We want to create only alerts.

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel | Analytics](#) >

## Analytics rule wizard - Create new rule from template ...

Vectra Host's Behaviors

General Set rule logic **Incident settings** Automated response Review and create

### Incident settings

Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled **Disabled**

### Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled Disabled

Limit the group to alerts created within the selected time frame

5 Hours

Group alerts triggered by this analytics rule into a single incident by

- Grouping alerts into a single incident if all the entities match (recommended)
- Grouping all alerts triggered by this rule into a single incident
- Grouping alerts into a single incident if the selected entity types and details match:

Select entities

Select details

**⚠** Entity-based alert grouping can make use **only** of entities mapped using the new version, if any exist. Entities mapped with the old version (that appear in the query code) will be available for grouping **only** if there are no mappings defined using the new version.

Re-open closed matching incidents

Enabled Disabled

Previous

Next : Automated response >

- ▼ The **automated response** depends on your environment and does not have anything configured by default.
- ▼ Click "**Review**" and then "**Create**".

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >  
**Analytics rule wizard - Create new rule from template** ...  
 Vectra Host's Behaviors

Validation passed.

General Set rule logic Incident settings Automated response **Review and create**

**Analytics rule details**

Name: Vectra Host's Behaviors  
 Description: This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on host's detections.  
 Tactics and techniques:
 

- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Severity: Informational  
 Status: Enabled

**Analytics rule settings**

Rule query

```
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X Series"
| where DeviceEventClassID != "campaigns"
  and DeviceEventClassID != "hsc"
  and DeviceEventClassID != "audit"
  and DeviceEventClassID != "health"
  and DeviceEventClassID != "asc"
| extend Category = coalesce(
  column_if_exists("DeviceEventCategory", ""),
  extract("cat=(.+?)(?=$)", 1, AdditionalExtensions),
  ""
)
| project-rename threat_score = FlexNumber1
| project-rename certainty_score = FlexNumber2
| project-rename vectra_URL = DeviceCustomString4
| project-rename detection_name = DeviceEventClassID
| project-rename triaged = DeviceCustomString5
| where triaged != "True" and AdditionalExtensions !has "account"
| extend source_entity = case(isnotempty(SourceHostName), SourceHostName,
"UNKNOWN")
| extend level = case(threat_score == 0 and certainty_score == 0, "Info",
threat_score < 50 and certainty_score < 50, "Low",
threat_score < 50 and certainty_score >= 50, "Medium",
threat_score >= 50 and certainty_score <= 50, "High",
threat_score >= 50 and certainty_score >= 50, "Critical",
"UNKNOWN")
| extend Severity = case(level == "Info", "Informational", level == "Critical", "High", level == "Low", "Low", level == "Medium", "Medium", level == "High", "High", level == "Critical", "Critical")
| project Severity, level, threat_score, certainty_score, vectra_URL, detection_name, triaged, source_entity, Category
```

Previous Create

▼ Once deployed, you should see the analytic rule in the Active rules list:

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics ...

Selected workspace: 'demolab-loganalytics'

Search

General: Overview (Preview), Logs, News & guides, Threat management: Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), Content management: Content hub (Preview), Repositories (Preview), Community, Configuration: Data connectors, Analytics, Watchlist, Automation, Settings

Rules by severity: High (11), Medium (30), Low (7), Informational (2)

Active rules

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last
Informational	Vectra Host's Behavior	Scheduled	Enabled	+	+	Vectra AI Detect	4/11/
Informational	Vectra AI Detect - Susj	Scheduled	Enabled	+	+	Vectra AI Detect	4/11/

**Vectra Host's Behaviors**

Informational Severity, Content hub Content Source, Enabled Status

ID: 85a8fbee-7124-412f-a30d-eb03c9d1d72f

Description: This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on host's detections.

Tactics and techniques:
 

- Collection (0)
- Command and Control (0)
- Credential Access (0)
- Discovery (0)
- Exfiltration (0)
- Impact (0)
- Lateral Movement (0)

Rule query

```
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X Series"
| where DeviceEventClassID != "campaigns"
  and DeviceEventClassID != "hsc"
  and DeviceEventClassID != "audit"
```

Rule frequency: Run query every 5 minutes  
 Rule period: Last 5 minutes data  
 Rule threshold: Trigger alert if query returns more than 0 results  
 Event grouping: Trigger an alert for each event

Edit Compare with template

## Incident creation for prioritized accounts

The same logic is being applied to accounts.

- ▼ Menu: Configuration > Analytics > Rule templates.
- ▼ Search for Vectra and select the template name **Vectra AI Detect - Suspected Compromised Account**.
- ▼ Click "Create rule".

The screenshot shows the Microsoft Sentinel Analytics interface. On the left is a navigation menu with categories like General, Threat management, and Configuration. The main area displays a list of active rules under the 'Rule templates' tab. A search filter 'vectra' is applied. The table lists several rules, with 'Vectra AI Detect - Suspected Compromised Account' selected. The right-hand pane provides details for this rule, including its severity (Informational), description, data sources (CommonSecurityLog), and a list of tactics and techniques (Collection, Command And Control, Credential Access, Discovery, Exfiltration, Impact, Lateral Movement). A 'Create rule' button is visible at the bottom of the details pane.

- ▼ Set the status to **Enabled** and make sure that Severity is set to **Informational** (it should be the default).

The screenshot shows the 'Analytics rule wizard - Create new rule from template' in Microsoft Azure. The breadcrumb path is Home > Microsoft Sentinel > Microsoft Sentinel | Analytics. The title is 'Analytics rule wizard - Create new rule from template' and the subtitle is 'Vectra AI Detect - Suspected Compromised Account'. The 'General' tab is active, showing the following configuration:

- Name \***: Vectra AI Detect - Suspected Compromised Account
- Description**: Create an incident when an Account is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical). Recommended configuration
- Tactics and techniques**: 7 selected
- Severity**: Informational
- Status**: Enabled (radio button selected)

- ▼ In the next screen: *Set rule logic*, everything is preconfigured and should be left with default values (An incident would be created when an account is in the High or Critical quadrant).

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

## Analytics rule wizard - Create new rule from template

Vectra AI Detect - Suspected Compromised Account

General **Set rule logic** Incident settings Automated response Review and create

Define the logic for your new analytics rule.

### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
// Edit this variable to only keep the Severity level where an incident needs to be created.
//Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.'
let configured_level = dynamic(["High", "Critical"]);
let upn_has_prefix = ":";
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
```

[View query results >](#)

### Alert enrichment

#### Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis.

For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Account			
Name	name	+ Add identifier	
UPNSuffix	upn_suffix		

+ Add new entity

### Results simulation

This chart shows the results of the last 50 evaluations of the defi that point in time.

🔄 Test with current data

Define a valid analytics rule configuration and click 'Test'

- ▼ In the Incident settings page, make sure that:

- Incident settings is enabled.
- Alert grouping is enabled with 7 days (Grouping alerts into a single incident if all the entities match).
- Re-open closed matching incidents is enabled.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

## Analytics rule wizard - Create new rule from template

Vectra AI Detect - Suspected Compromised Account

General **Set rule logic** **Incident settings** Automated response Review and create

### Incident settings

Microsoft Sentinel alerts can be grouped together into an incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

**Enabled** Disabled

---

### Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

**Enabled** Disabled

ⓘ Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

Limit the group to alerts created within the selected time frame \*

7 Days

Group alerts triggered by this analytics rule into a single incident by

Grouping alerts into a single incident if all the entities match (recommended)

Grouping all alerts triggered by this rule into a single incident

Grouping alerts into a single incident if the selected entity types and details match:

Select entities

Select details

⚠ Entity-based alert grouping can make use **only** of entities mapped using the new version, if any exist. Entities mapped with the old version (that appear in the query code) will be available for grouping **only** if there are no mappings defined using the new version.

Re-open closed matching incidents

**Enabled** Disabled

- ▼ Review and create. The rule is now listed as active:

6 Active rules

More content at Content hub

Rules by severity: High (11) Medium (30) Low (7) Informational (3)

Active rules | Rule templates | Anomalies

Search: vectra Add filter

Severity	Name	Rule type	Status	Tactics	Tech
<input checked="" type="checkbox"/>	Informational	Vectra AI Detect - Suspected Compromised Account	Scheduled	Enabled	+3
<input type="checkbox"/>	Informational	Vectra Host's Behaviors	Scheduled	Enabled	+3
<input type="checkbox"/>	Informational	Vectra AI Detect - Suspected Compromised Host	Scheduled	Enabled	+3

## Alert creation for account's detections

The intent is to create alerts for every account's detection triggered by the Vectra Attack Signal Intelligence. Alerts go to the *SecurityAlert* table. To do so, we are going the analytic template named: Vectra AI Detect - Vectra Account's Behaviors.

- ▼ Menu: Configuration > Analytics > Rule templates.
- ▼ Search for Vectra and select the template name **Vectra AI Detect - Vectra Account's Behaviors**.
- ▼ Click "create rule"

Microsoft Azure | Microsoft Sentinel | Microsoft Sentinel

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'demolab-logs-analytics'

Search resources, services, and docs (G+)

6 Active rules

More content at Content hub

Rules by severity: High (11) Medium (30) Low (7) Informational (3)

Active rules | Rule templates | Anomalies

Search: vectra Add filter

Severity	Name	Rule type	Data sources	Tactics	Techniques	Source name
Informational	<b>IN USE</b> Vectra AI Detect - Suspected Compromised Account	Scheduled	Vectra AI Detect	+3		Vectra AI Detect
Informational	<b>IN USE</b> Vectra Host's Behaviors	Scheduled	Vectra AI Detect	+3		Vectra AI Detect
High	Vectra AI Detect - Detections with High Severity	Scheduled	Vectra AI Detect	+3		Vectra AI Detect
Informational	<b>IN USE</b> Vectra AI Detect - Suspected Compromised Host	Scheduled	Vectra AI Detect	+3		Vectra AI Detect
Informational	Vectra AI Detect - Suspicious Behaviors by Category	Scheduled	Vectra AI Detect	+3		Vectra AI Detect
Medium	Vectra AI Detect - New Campaign Detected	Scheduled	Vectra AI Detect			Vectra AI Detect
Informational	Vectra Account's Behaviors	Scheduled	Vectra AI Detect	+3		Vectra AI Detect

**Vectra Account's Behaviors**

Informational Severity | Gallery Content Content Source | Scheduled Rule Type

Description: This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on account's detections.

Data sources: Vectra AI Detect, CommonSecurityLog (AVectraDetect) 5/1/2023, 12:27:03 PM

Tactics and techniques: Collection (0), Command And Control (0), Credential Access (0), Discovery (0), Exfiltration (0), Impact (0), Lateral Movement (0)

Rule query: 

```
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X-Series"
| where DeviceEventClassID != "campaigns"
and DeviceEventClassID != "hsc"
and DeviceEventClassID != "audit"
```

Note: You haven't used this template yet; you can use it to create analytics rules.

Create rule

< Previous Page 1 of 1 Next > Showing 1 to 7 of 7 results.

- ▼ Set the status to **Enabled** and make sure than Severity is set to **Informational** (it should be default).

Microsoft Azure

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

### Analytics rule wizard - Create new rule from template

Vectra Account's Behaviors

General Set rule logic Incident settings Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

#### Analytics rule details

Name \*

Vectra Account's Behaviors

Description

This analytic rule is looking for new attacker behaviors observed by the Vectra Platform. This rule is focused on account's detections.

Tactics and techniques

7 selected

Severity

Informational

Status

Enabled Disabled

- ▼ In the next screen: *Set rule logic*, everything is preconfigured and should be left with default values (query, entity mapping, alert details, frequency, etc.)

Microsoft Azure

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

### Analytics rule wizard - Create new rule from template

Vectra Account's Behaviors

General Set rule logic Incident settings Automated response Review and create

Define the logic for your new analytics rule.

#### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
| where DeviceProduct == "X Series"
| where DeviceEventClassID != "campaigns"
  and DeviceEventClassID != "hsc"
  and DeviceEventClassID != "audit"
```

View query results >

#### Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Account

Name name

UPNSuffix upn\_suffix

+ Add new entity

Custom details

Alert details

Here you can select parameters in your alert that can be represented in the name or description of each instance of the alert, or that can contain the tactics and severity assigned to that instance of the alert. Enter free text in the fields below, and to insert a parameter, type a column name from the query results, surrounded by double curly brackets. Example: {(columnName)}. If the parameter has no value (or an invalid value in the case of tactics and severity), the alert details will revert to the defaults specified in the first page of the wizard. [Learn more >](#)

Previous Next: Incident settings >

- ▼ In the next screen, *Incident settings* must be set to **Disabled**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

### Analytics rule wizard - Create new rule from template

Vectra Account's Behaviors

General Set rule logic **Incident settings** Automated response Review and create

**Incident settings**  
Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule  
 Enabled  Disabled

**Alert grouping**  
Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents  
 Enabled  Disabled

Limit the group to alerts created within the selected time frame  
 5 Hours

Group alerts triggered by this analytics rule into a single incident by  
 Grouping alerts into a single incident if all the entities match (recommended)  
 Grouping all alerts triggered by this rule into a single incident  
 Grouping alerts into a single incident if the selected entity types and details match:

Select entities  
 Select details

⚠ Entity-based alert grouping can make use **only** of entities mapped using the new version, if any exist. Entities mapped with the old version (that appear in the query code) will be available for grouping **only** if there are no mappings defined using the new version.

Re-open closed matching incidents  
 Enabled  Disabled

Previous **Next : Automated response >**

- ▼ Click "**Review**" and then "**Create**".
- ▼ The rule is now listed as active:

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

### Microsoft Sentinel | Analytics

Selected workspace: 'demolab-loganalytics'

Search Create Refresh Analytics workbooks Enable Disable Delete Import Export Guides & Feedback

7 Active rules More content at Content hub

Rules by severity  
 High (11) Medium (30) Low (7) Informational (4)

Active rules Rule templates Anomalies

Search vectra Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last Modified ↓
<input checked="" type="checkbox"/>	Informational Vectra Account's Behaviors	Scheduled	Enabled	+3	+3	Vectra AI Detect	5/1/2023, 5:46:04 PM
<input type="checkbox"/>	Informational Vectra AI Detect - Suspected Compromised A	Scheduled	Enabled	+3	+3	Vectra AI Detect	5/1/2023, 5:17:27 PM
<input type="checkbox"/>	Informational Vectra Host's Behaviors	Scheduled	Enabled	+3	+3	Vectra AI Detect	5/1/2023, 4:58:37 PM
<input type="checkbox"/>	Informational Vectra AI Detect - Suspected Compromised H	Scheduled	Enabled	+3	+3	Vectra AI Detect	5/1/2023, 1:12:54 PM

## The SOC analyst journey

This section describes an example of the workflow for an analyst. It starts in the Incidents page where, as a SOC analyst, new and existing incidents would be picked up.

The screenshot shows the Microsoft Sentinel 'Incidents' page. A table lists several incidents, with one highlighted in orange. Annotations with green arrows point to various elements:

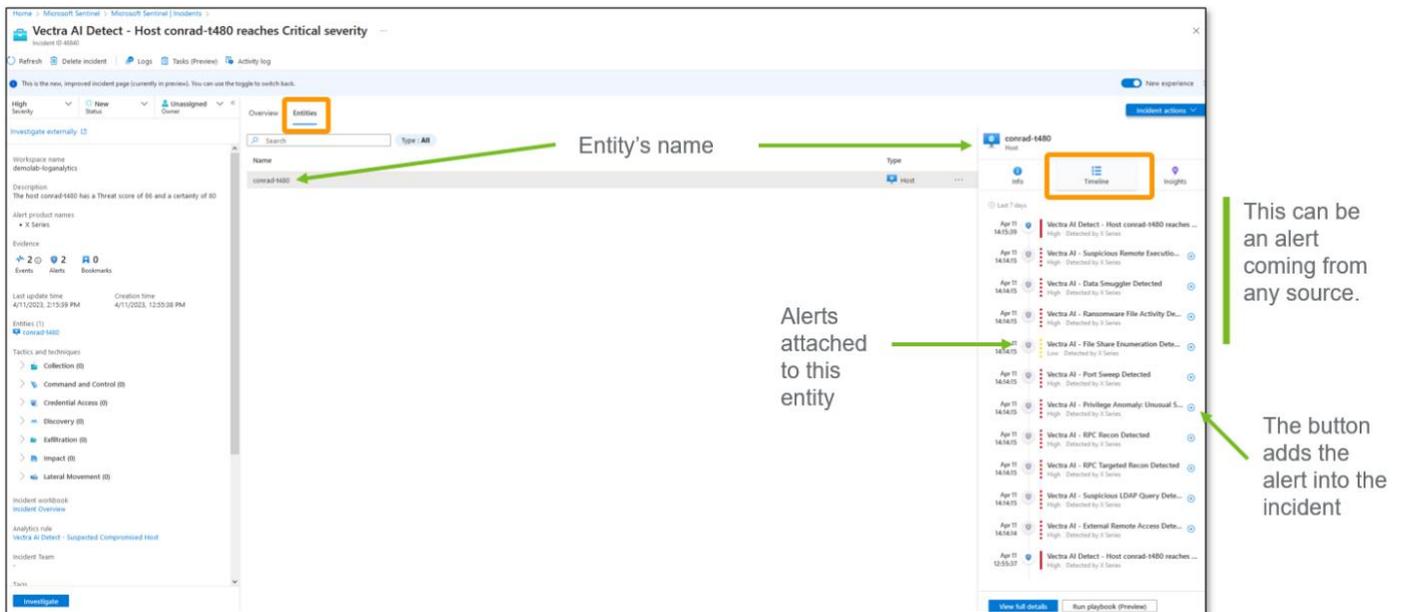
- Pivot to Vectra UI:** Points to the 'View full details' button at the bottom right of the incident table.
- Severity dynamically map to Vectra's severity:** Points to the 'High Severity' status of the selected incident.
- Reflect the latest Threat and certainty scores:** Points to the 'Threat score of 86 and a certainty of 80' in the incident description.
- Entity's name:** Points to the 'conrad-1480' entity name in the incident details pane.
- Investigate the incident:** Points to the 'View full details' button.

The full details provide additional detail such as the timeline where you can see incidents associated to this entity. The grouping configuration of events (7 day windows) allows a view of how the score has been evolving over time which will directly impact the severity associated with that incident.

The screenshot shows the detailed view of an incident in Microsoft Sentinel. Annotations with green arrows and text describe key features:

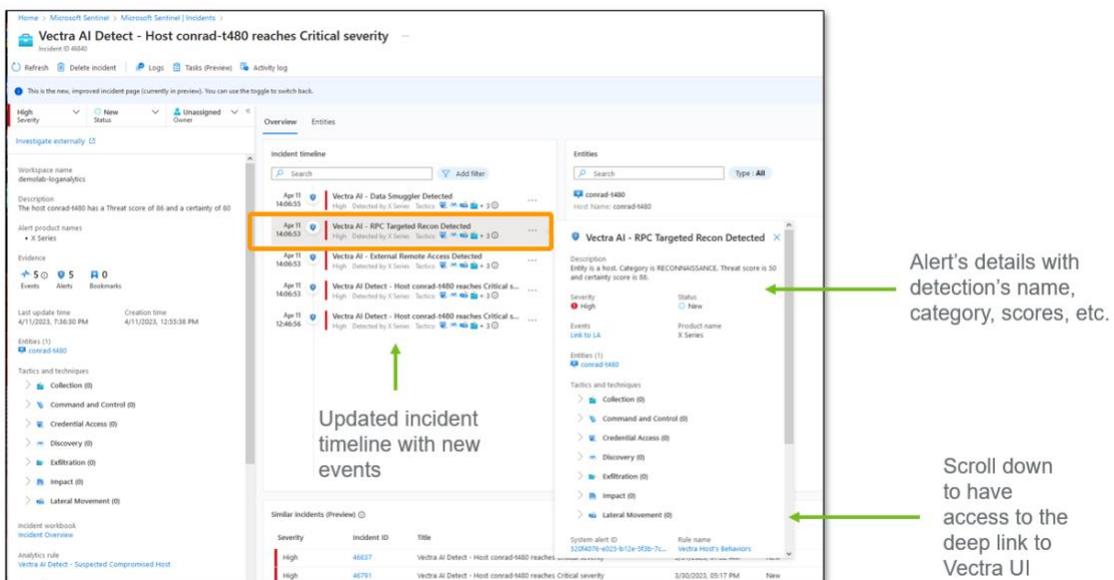
- Pivot to Vectra UI:** Points to the 'Investigate externally' button in the top left navigation bar.
- Entity's name:** Points to the 'conrad-1480' entity name in the 'Entities' pane.
- Timeline for this entity with threat and certainty scores changes:** Points to the 'Incident timeline' pane, which shows a sequence of events related to the entity.

Now, as the next step, an analyst would like to see all the different attacker's behaviors that have been observed for that entity. This can be done right in Sentinel by clicking on the entity's name, and then the timeline tab:



Alerts in the entity's timeline view can come from any source (EDR, FW, etc.). This is why the entity mapping configuration is key to successfully correlate them. Alerts of interest from this entity can be added to the incident by clicking the + button, then it shows up in the incident timeline view. Navigate back to the overview tab to see the timeline view. You can click on any new alert that you added in your incident to see additional details for each of them that allow you to continue your investigation:

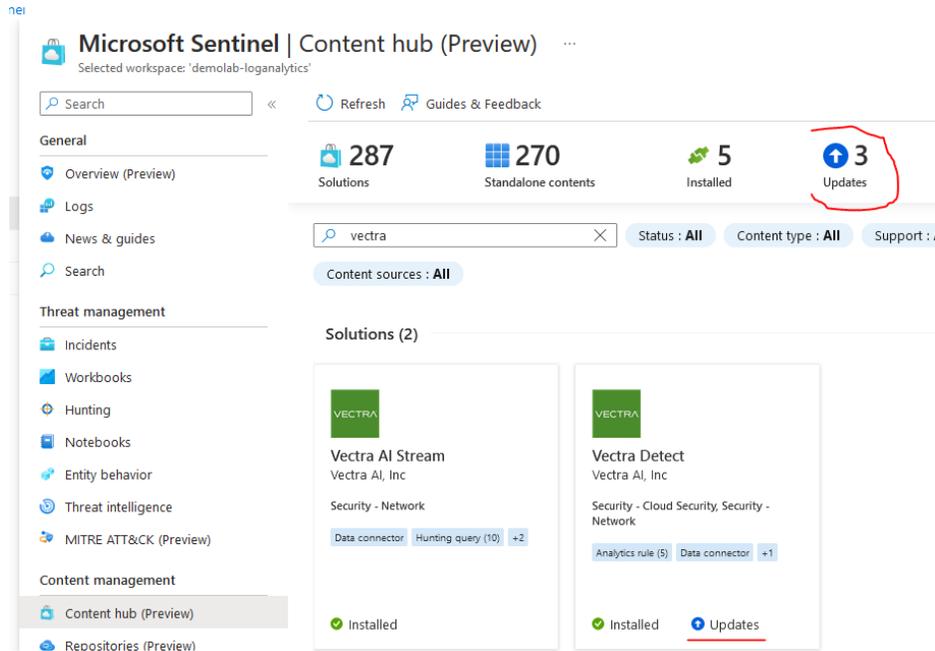
- ▼ Detection name
- ▼ Category
- ▼ Severity
- ▼ Threat and Certainty Scores
- ▼ Deep link to Vectra UI



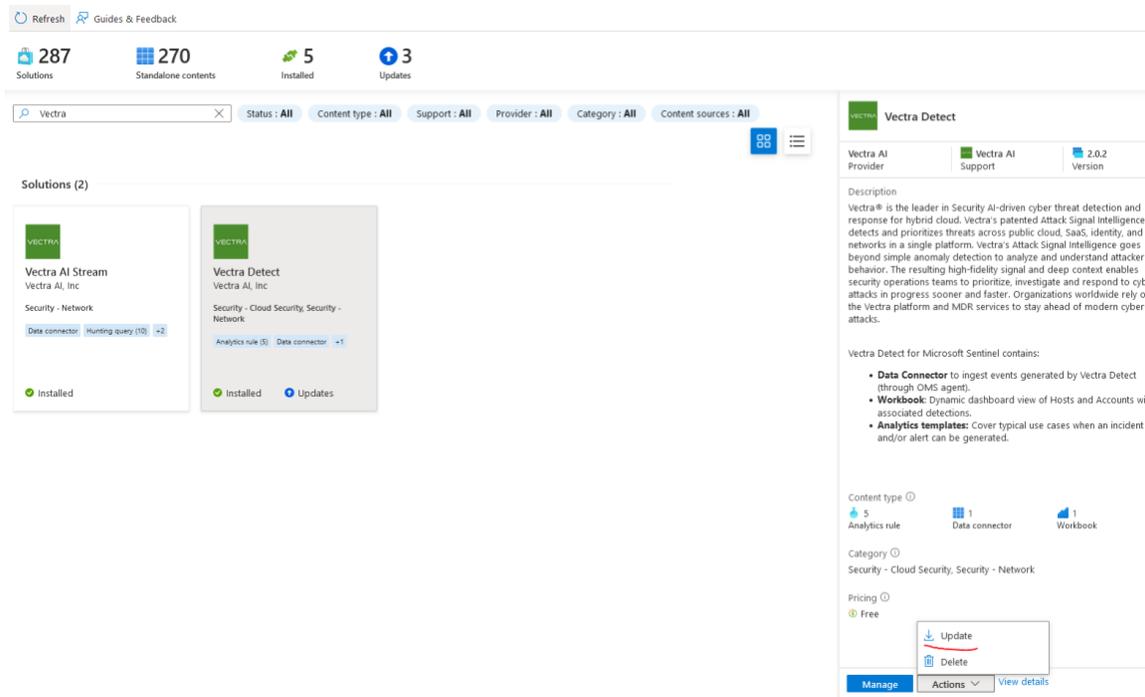
## Best practices

### Keep the content up to date!

As we continuously improve our content for Microsoft Sentinel, please make sure that you are using the latest version. New versions can include enhancements for new features as well as bug fixes. When updates are available, it can be seen in content hub:



- ▼ Once you click on the tile, on the bottom right, click on **Actions > Update** to deploy latest version of the content and follow the wizard to deploy it in the right workspace.



- ▼ Once it has been deployed, you would see that an update is available for the templates you already deployed. In the scenario of analytic templates, the tag "UPDATE AVAILABLE" is added to rules that have an update.
- ▼ To proceed, click the "Review and update" button at the bottom right of the page.

Severity	Name	Rule type	Status	Tactics	Techniques	Source
Informational	Vectra Host Behaviors	Scheduled	Enabled			Custom
Informational	UPDATE AVAILABLE Vectra Host Behaviors	Scheduled	Enabled			Vectra /
Informational	Vectra Account Behavi	Scheduled	Enabled			Custom
Informational	UPDATE AVAILABLE Vectra Account Behavi	Scheduled	Enabled			Vectra /
Medium	Vectra detections for c	Scheduled	Disabled			Custom
Medium	UPDATE AVAILABLE Vectra detections for c	Scheduled	Disabled			Vectra /
Medium	Potential DGA detecte	Scheduled	Disabled	Command And	T1568 +1	Gallery
Medium	Threat Essentials - NR	Scheduled	Disabled			Custom
Medium	Threat Essentials - Ma	Scheduled	Disabled			Custom
Medium	UPDATE AVAILABLE Susj	Scheduled	Disabled		T1098	Gallery
Medium	Threat Essentials - Tiri	Scheduled	Disabled	Exfiltration		Custom
Medium	CS562 - RDP Nesting	Scheduled	Disabled	Lateral Movem		Custom
Medium	CS591 - Rare Group h	Scheduled	Disabled			Custom
Medium	UPDATE AVAILABLE Det	Scheduled	Disabled		T1098 +1	Gallery
Medium	UPDATE AVAILABLE Offi	Scheduled	Disabled		T1098 +1	Gallery
Medium	Excessive NXDOMAIN	Scheduled	Disabled	Command And	T1568 +1	Gallery
Medium	UPDATE AVAILABLE Excl	Scheduled	Disabled	Defense Evasio	T1562	Gallery
Medium	CS575 - Possible cont	Scheduled	Disabled	Command And		Custom

Id: 54b79984-d7fa-481f-86b7-0c309cb83ea2

Description: Create an incident when a Host is suspected to be compromised. The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat. Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.

Tactics and techniques: Collection (0), Command and Control (0), Credential Access (0), Discovery (0), Exfiltration (0), Impact (0), Lateral Movement (0)

Rule query: // Edit this variable to only keep the Sev  
let configured\_level = dynamic(["High", "C  
CommonSecurityLog  
| where DeviceVendor == "Vectra Networks"  
| where DeviceProduct == "X Series"

Buttons: Edit, Review and update

## Create an alert when no event is received

As described in this [KB](#), we rely on a Microsoft agent to send Vectra's events to Sentinel. This agent is receiving events via syslog and forwards them to the correct Log Analytics Workspace within Azure. To detect any issues with the middleware component, we recommend using Azure Monitor to setup an alert when no events are received for 24 hours. It is very unlikely that the Vectra platform does not generate any events for so long. Depending of your preferences, you can go as low as 1 hour.

- ▼ In Azure Monitor, create a new alert similar to the below:

**No data from Vectra Detect the last 24 hours** ☆ ...

Log search alert rule

Search

Essentials

Resource group (move): cloud-shell-storage-westurope

Location (move): West US 2

Subscription (move): [redacted]

Subscription ID: [redacted]

Tags (edit): Click here to add tags

Severity: 1 - Error

Description: No data coming from the CEF connector

Scope

Resource	Hierarchy
demolab-loganalytics	[redacted]

Actions

Name	Contains actions
email-notification	1 Email

Conditions

Name: [redacted] Estimated monthly cost: \$0.50

Table rows = 0

Query: CommonSecurityLog  
| where DeviceVendor == "Vectra Networks"  
| where DeviceProduct == "X Series"  
| sort by TimeGenerated

KQL query used:

```
CommonSecurityLog  
| where DeviceVendor == "Vectra Networks"  
| where DeviceProduct == "X Series"  
| sort by TimeGenerated
```

In this case, we send out an email notification when the alert is triggered. You can change the action to whatever fits best in your environment.

## Worldwide Support Contact Information

- ▼ Support portal: <https://support.vectra.ai>
- ▼ Email: [support@vectra.ai](mailto:support@vectra.ai) (preferred contact method)
- ▼ Additional information: <https://www.vectra.ai/support>