



# DARKTRACE QRADAR INTEGRATION

Darktrace Threat Visualizer 6.1

Last Updated: March 12 2024

# DARKTRACE QRADAR INTEGRATION

## Darktrace Threat Visualizer 6.1

Darktrace Integration with QRadar	3
Introduction	3
About this guide	3
Requirements	3
Darktrace configuration	3
QRadar configuration	6
Darktrace QRadar DSM	9
Introduction	9
Types of Alert	9
Darktrace QRadar DSM custom content	9
Frequently Asked Questions	15



# DARKTRACE INTEGRATION WITH QRADAR

## Introduction

Darktrace provides a fundamentally unique approach to cyber defense. With a detailed understanding of what is normal within the business, Darktrace DETECT™ can identify and contain emerging threats that have bypassed traditional defenses and are active within the network. To keep security teams informed on-the-go and to integrate with a full range of security tools, model breach alerts can be issued to external systems in a wide range of formats.

## About this guide

This guide describes how to configure event collection from a Darktrace environment to the QRadar platform.

The Darktrace Device Support Module (DSM) uses streamlined JSON-format model breach alerts which are pre-mapped to custom (Darktrace-specific) and default QRadar fields for at-a-glance triage and analysis.

There are two log sources in the Darktrace DSM that send events to QRadar.

1. *Darktrace* of type *DarktraceLogSource*
2. *Darktrace AI Analyst* of type *Darktrace AI Analyst*.

To collect events from Darktrace in QRadar, you need to complete installation and configuration steps on both Darktrace and QRadar.

## Requirements

- A Darktrace instance running the most recent Darktrace Threat Visualizer software version (*minimum 6.1*)
- Configure firewall exceptions to allow communication from the Darktrace instance to the QRadar instance.
- Darktrace QRadar DSM from IBM X-Force Exchange. (*If you don't have it, follow the steps below*).
- Darktrace user with *Configuration* permissions.

## Darktrace configuration

This section explains how to configure Darktrace Threat Visualizer to send alerts to QRadar through syslog.

1. Login to Darktrace Threat Visualizer.
2. Go to **Admin > System Config**.
3. From **System Config**  
Go to **Modules > Workflow Integrations > QRadar**

4. Open **Settings**.
  - a. Enter the **Server** IP address or hostname of the syslog server.
  - b. Enter the QRadar **Server Port** details.
5. Turn on **Show Advanced Options**.

## Configure how alerts are sent to QRadar

From **QRadar Settings > Advanced Options**

1. Select your preferred configuration.
2. Configure **Advanced Options** as below.

### NOTE

Darktrace recommends the use of TCP Alerts due to the larger payload size supported by QRadar. Both UDP and TCP are supported.

FIELD NAME	APPLIES TO	DESCRIPTION
Send Alerts Using TCP	All alerts	Turn on to send alerts over TCP. TCP allows for a longer message and additional fields, such as destination hostname (dhost). Turn off to send alerts over UDP
Use TLS	All alerts	Turn on to send TCP traffic with TLS encryption. Requires "Send Alerts Using TCP": On.
TLS Verify Certificate	All alerts	Turn on to ensure that the server certificate is signed by a trusted root certificate authority. Requires "Send Alerts Using TCP": On, "Use TLS": On.
TLS Server Certificate Fingerprints	All alerts	Turn on to ensure syslog will only be sent to TLS servers that present certificates with fingerprints in this comma separated list. Requires "Send Alerts Using TCP": On, "Use TLS": On.
Time Offset	All alerts	Adjust the syslog timestamp by a given number of hours from UTC. The value can be negative or positive but it must be an integer.
Time Zone	All alerts	Adjust the syslog timestamp to a specific timezone. Takes priority over "Time Offset", if configured.

## Configure AI Analyst alerts to send to QRadar

From **QRadar Settings > Advanced Options**

1. Turn on **Send AI Analyst Alerts**.
2. Configure **Advanced Options** as below:

### NOTE

One or many *AI Analyst Incident Events* constitute an *AI Analyst Incident*.


FIELD NAME	APPLIES TO	DEFAULT	DESCRIPTION
AI Analyst Behavior Filter	AI Analyst Alerts	Critical	Behavior categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational. Select the categories to filter alerts to.
Minimum AI Analyst Incident Event Score	AI Analyst Alerts	0	Restricts incident events sent as external alerts to those with an individual event score above the threshold.
Minimum AI Analyst Incident Score	AI Analyst Alerts	20	Incident events are part of a larger incident. Restricts incident events sent as external alerts to those with an overall incident score above the threshold. Incident scores are expected to use the full range of scores from 0-100.

## Configure model breach alerts to send to QRadar

From **QRadar Settings > Advanced Options**

1. Turn on **Send Model Breach Alerts**.
2. Configure **Advanced Options** as below:

### NOTE

1. Filters control whether alerts are sent or suppressed.
2. An alert **must pass through all relevant filters** to be created.
3. An alert **must meet all filter criteria** that are relevant to it. For example, a model breach must meet all thresholds, regular expressions and device restrictions applied.
4. Not all criteria are applicable to all alert types.
5. Some filters and settings may not appear unless "send alerts" for the relevant alert type has been turned on.
6. Global settings can override settings made here. Global Settings can be accessed by clicking the  **Config** icon to the right of **Workflow Integrations** on the **System Config** page, and changes can be made to individual modules by turning on **Enable Modular Alert Thresholds**.

FIELD NAME	APPLIES TO	DEFAULT	DESCRIPTION
Minimum Breach Score <sup>1</sup>	Model Breach Alerts	50	Enter a value to restrict the sending of alerts to those with a Breach Score that exceeds that value.
Minimum Breach Priority <sup>1</sup>	Model Breach Alerts	0	Enter a value to restrict the sending of alerts to those with a Breach priority that exceeds that value (0-5). "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.

FIELD NAME	APPLIES TO	DEFAULT	DESCRIPTION
Model Expression <sup>1</sup>	Model Breach Alerts	N/A	Enter a regular expression to restrict the sending of alerts to those with model names (and folder) that match the regular expression. "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.
Model Tags Expression	Model Breach Alerts	N/A	Enter a regular expression restrict the sending of alerts to models with tags matching the expression.
Device IP Addresses	Model Breach Alerts	N/A	Enter a comma separated list of IP addresses, and/or CIDR IP range(s). This restricts the sending of alerts concerning only devices with one of the listed IP addresses.
Device Tags Expression	Model Breach Alerts	N/A	Enter a regular expression restrict the sending of alerts to those for devices with tags matching the expression.

<sup>1</sup> Setting controlled by the global alert thresholds.

## Complete configuration

1. When configuration is complete, select **Save** to confirm.
2. A message appears to indicate success.

## QRadar configuration

This section explains how to configure event collection from Darktrace to QRadar to view Darktrace Alert logs.

### Download the Darktrace QRadar DSM

1. Go to IBM X-Force Exchange/App Exchange.
2. Search for 'Darktrace'.
3. Select 'Darktrace QRadar DSM'.
4. Download the DSM ( `Darktrace_dsm_1.1.0.zip` )

### Import the Darktrace DSM into QRadar

1. Login to the QRadar Console as an Administrator.
2. Go to **Admin > Extension Management**.
3. Select **Add**.
4. Browse to `Darktrace_dsm_1.1.0.zip` just downloaded.
5. Select **Install immediately** and **Add** to install the extension.
6. The QRadar Console updates with a notification to *Deploy Changes*. Continue to deploy changes and restart with the new configuration. This may take a few minutes.

7. Return to the **Admin** tab and select **Log Sources**.

**NOTE**

You may be required to download and install the *QRadar Log Source Management application*. Follow the instructions to do so.

## Log source management

From the *QRadar Log Source Management* console:

### Edit Darktrace log source

1. From **Data Sources > Log Sources** select the *Darktrace Log Source*.
2. Select **Edit**
3. Select **Protocol** tab
4. Modify the default value of **Log Source Identifier** to the fully qualified domain name (FQDN) or the IP address of the Darktrace instance that you want to send logs from.

**NOTE**

- Select FQDN or IP address to enable syslog alerts to use this value as an identifier of the instance.
- Choose a value that is compatible with your overall Darktrace alert configuration.
- If you are unsure, you can retrieve an uncategorized Darktrace alert from QRadar and confirm which value is located between the syslog prefix/date `<165>1 2021-04-07T18:42:21+09:00` and the string `darktrace` .
- Use this as the Log Source Identifier. For example, `10.15.3.39` , for `<165>1 2021-04-07T18:42:21+09:00 10.15.3.39 darktrace` .

5. Select **Save** and **Close**

### Edit Darktrace AI Analyst log source

In **Log Sources**

1. Select *Darktrace AI Analyst*.
2. Select **Edit**
3. Select the **Protocol** tab

4. Modify the default value of **Log Source Identifier** to the FQDN or the IP address of the Darktrace instance that you want to send logs from.

**NOTE**

- Select FQDN or IP address to enable syslog alerts to use this value as an identifier of the instance.
- Choose a value that is compatible with your overall Darktrace alert configuration.
- If you are unsure, you can retrieve an uncategorized Darktrace alert from QRadar and confirm which value is located between the syslog prefix/date `<165>1 2021-04-07T18:42:21+09:00` and the string `darktrace`.
- Use this as the Log Source Identifier. For example, `10.15.3.39`, for `<165>1 2021-04-07T18:42:21+09:00 10.15.3.39 darktrace`.

5. Select **Save** and **Close**.

## Confirm Log Activity

### Send Test Alert from Darktrace

From **Threat Visualizer System Configuration**:

1. Select **Verify alert settings** to send a test alert to QRadar.
2. Select **Status** to view the success of the test alert.

### View Test Alert in QRadar

From the **QRadar Console**:

1. Go to **Log Activity**
2. Select **New > Search > Top Darktrace Breaches**
3. Set **View > Real-time stream** to confirm you are receiving alerts as soon as a test alert is sent from Darktrace.
4. To view test alerts sent earlier adjust the view time period.

**NOTE**

The payload size for Darktrace QRadar alerts should be less than the default maximum length (4k). If you experience issues with payload truncation, increase the **Maximum Syslog Payload Length** in QRadar may resolve this issue. These settings are located in **System Settings > Advanced > Max UDP Syslog Payload Length** and **Max TCP Syslog Payload Length**.



# DARKTRACE QRADAR DSM

The Darktrace QRadar Workflow Integration brings Darktrace alerts directly into QRadar SIEM tool.

AI Analyst and Model Breach alerts include information about the source device, the unusual activity and a link to view the alert in the Threat Visualizer. Darktrace RESPOND action alerts notify users of pending or changed Darktrace RESPOND actions. System Status alerts contain information about errors on system components and external integrations. All alerts include links back to the Darktrace Threat Visualizer platform for further investigation.

## Introduction

The Darktrace Device Support Module (DSM) uses streamlined JSON-format model breach alerts which are pre-mapped to custom (Darktrace-specific) and default QRadar fields for at-a-glance triage and analysis.

There are two log sources in the Darktrace DSM that send events to QRadar.

1. *Darktrace of type DarktraceLogSource*
2. *Darktrace AI Analyst of type Darktrace AI Analyst.*

## Types of Alert

### AI Analyst

Darktrace Cyber AI Analyst incidents are created from AI-powered investigations into anomalies across your digital environment. Every time the conditions for a model are met and a model breach is created, AI Analyst investigates the activity and concludes whether it needs to be surfaced for human analysts to review.

### Model Breaches

A model is used to define a set of conditions which, when met, will alert the system to the occurrence of a particular event or chain of anomalous behavior. Default Darktrace models are focused on "pattern of life" anomaly detection, potentially malicious behavior and optional compliance issues, though organizations can create additional models to mirror internal policy or an existing SOC playbook. When triggered, model breach details can be sent as alerts to external platforms, reviewed in the Darktrace mobile app, or investigated in the Darktrace Threat Visualizer platform.

## Darktrace QRadar DSM custom content

The following custom properties, searches and events are included in the Darktrace QRadar DSM.

## Custom properties

### Darktrace properties

CUSTOM PROPERTY	DATA TYPE	SOURCE FIELD IN DARKTRACE INPUT	DESCRIPTION
Breach Details	Text	<code>triggeredComponents</code>	A selection of relevant details about the breach derived from the triggered components of the model.
Breach URL	Text	<code>breachUrl</code>	A direct link to the Darktrace appliance and the relevant model breach.
Description	Text	<code>modelName</code>	The name of the model that was breached.
Destination Hostname	Text	<code>destHost</code>	The hostname of the destination device or entity involved in the model breach.
Policy Breach ID	Number	<code>pbid</code>	The Policy Breach ID - <code>pbid</code> - unique identifier for the Model Breach event.
Policy ID	Number	<code>pid</code>	The Policy ID - <code>pid</code> - unique identifier for the model.
Score	Number	<code>score</code>	The breach score associated with the model breach.

For more information about default properties utilized, please see the [FAQs](#).

### AI Analyst properties

CUSTOM PROPERTY	DATA TYPE	SOURCE FIELD IN DARKTRACE INPUT	DESCRIPTION
Breach Device Hostname	Text	<code>dvchost</code>	The hostname associated with a breached device.
Breach Device IP	IP Address	<code>dvc</code>	The IP address associated with a breached device.
Current Group	Text	<code>currentGroup</code>	The UUID of the current incident this event belongs to.
Group Previous Groups	Text	<code>groupPreviousGroups</code>	If the event was part of an incident which was later merged with another. This field lists the UUIDs of the incidents before they were merged. Used for v5.2+ incident construction.
Group Score	Number	<code>groupScore</code>	The current overall score of the incident this event is part of. Relevant for v5.2+ incident construction only.
Group Category	text	<code>groupCategory</code>	The overall behavior category associated with the incident overall. Relevant for v5.2+ incident construction only.
Incident Event ID	text	<code>externalId</code>	A unique id of the incident.

CUSTOM PROPERTY	DATA TYPE	SOURCE FIELD IN DARKTRACE INPUT	DESCRIPTION
Incident Event Title	text	<b>title</b>	The title of the event. e.g. Unusual Internal Upload
Incident Score	text	<b>aiascore</b>	The current overall score of this incident.
Incident Message	text	<b>message</b>	Text added as a comment to the AI Analyst incident event.
Incident URL	text	<b>incidentEventUrl</b>	The url of the event.

## Model breach qid records

EVENT NAME	HIGH LEVEL CATEGORY	LOW LEVEL CATEGORY	SEVERITY
Darktrace Antigena	Sense	Sense Offense	5
Darktrace Asset Identified	Asset Profiler	Asset Observed	1
Darktrace Compliance	Policy	Network Threshold Policy Violation	2
Darktrace Device	Control System	Suspicious Behavior	1
Darktrace Malware Infection	Malware	Malware Infection	10
Darktrace Suspicious Activity	Suspicious Activity	Suspicious Activity	3
Darktrace Suspicious File Name	Suspicious Activity	Suspicious File Name	3
Darktrace Suspicious Pattern	Suspicious Activity	Suspicious Pattern Detected	3
Darktrace System Change	System	System Configuration	1
Darktrace Unknown Malware	Malware	Unknown Malware	4
Darktrace User	Suspicious Activity	User Activity	7
Darktrace User Defined Tag Applied	User Defined	Custom User Low	3

**AI Analyst qid Records**

NAME	HIGH LEVEL CATEGORY	LOW LEVEL CATEGORY	SEVERITY
AI Analyst Accomplish Low	Suspicious Activity	Suspicious Activity	3
AI Analyst Accomplish Medium	Suspicious Activity	Suspicious Activity	5
AI Analyst Accomplish High	Suspicious Activity	Suspicious Activity	7
AI Analyst Escalation Low	Potential Exploit	Potential Misc Exploit	3
AI Analyst Escalation Medium	Potential Exploit	Potential Misc Exploit	5
AI Analyst Escalation High	Potential Exploit	Potential Misc Exploit	6
AI Analyst Foothold Low	Malware	Misc Malware	4
AI Analyst Foothold Medium	Malware	Misc Malware	6
AI Analyst Foothold High	Malware Misc	Malware	8
AI Analyst Infection Low	Malware	Misc Malware	4
AI Analyst Infection Medium	Malware	Misc Malware	6
AI Analyst Infection High	Malware	Misc Malware	8
AI Analyst Recon Low	Recon	Misc Reconnaissance Event	4
AI Analyst Recon Medium	Recon	Misc Reconnaissance Event	5
AI Analyst Recon High	Recon	Misc Reconnaissance Event	6
AI Analyst Lateral Low	Suspicious Activity	Suspicious Pattern Detected	4
AI Analyst Lateral Medium	Suspicious Activity	Suspicious Pattern Detected	5
AI Analyst Lateral High	Suspicious Activity	Suspicious Pattern Detected	6
AI Analyst Compliance	Policy	Compliance Policy Violation	2

## Custom QIDMAP

Darktrace models are mapped to QRadar *Event Names* according to the folder the model is contained in. New or custom models created in a mapped folder are automatically mapped.

DARKTRACE FOLDER	QID RECORD
Anomalous Connection	Darktrace Suspicious Activity
Anomalous File	Darktrace Suspicious File Name
Anomalous Server Activity	Darktrace Device
Antigena	Darktrace Antigena
Compliance	Darktrace Compliance
Compromise	Darktrace Unknown Malware
Device	Darktrace Device
IaaS	Darktrace Suspicious Activity
ICS	Darktrace Suspicious Activity
Infrastructure	Darktrace Asset Identified
Inoculation	Darktrace Malware Infection
Multiple Device Correlations	Darktrace Suspicious Pattern
SaaS	Darktrace Suspicious Activity
System	Darktrace System Change
Tags	Darktrace User Defined Tags Applied
Unusual Activity	Darktrace Suspicious Activity
User	Darktrace User

## Custom Search - "Top Darktrace breaches"

This custom search selects the last 24 hours of Darktrace model breaches, sorted by descending breach score. The following columns are displayed:

COLUMN	DESCRIPTION
Start Time	Default QRadar field. Time at which the event arrived at the QRadar appliance.
Event Name	One of the custom Darktrace <b>qid</b> records. "Unknown" if event is unmapped.
High Level Category	QRadar low level category of qid record Darktrace breach maps to
Low Level Category	QRadar low level category of qid record Darktrace breach maps to
Description (custom)	The name of the model that was breached.
Breach Details (custom)	A selection of relevant details about the breach derived from the triggered components of the model.
Username	The <b>did</b> of the device which triggered the model breach. A unique device identifier within Darktrace.
Breach URL (custom)	A direct link to the Darktrace appliance and the relevant model breach.
Score (custom)	The breach score associated with the model breach.
Magnitude	Default QRadar field.

# FREQUENTLY ASKED QUESTIONS

The following FAQs answer typical Darktrace QRadar integration questions.

## What default QRadar properties do Darktrace Model Breach events utilize?

The Darktrace DSM utilizes the following overridden system properties:

SYSTEM PROPERTY	DATA TYPE	SOURCE FIELD IN DARKTRACE INPUT
Destination IP	IP Address	<code>destIP</code>
Destination MAC	Text	<code>destMac</code>
Destination Port	Port	<code>destPort</code>
Event Category	Text	<i>Extracted from</i> <code>modelName</code>
Event ID	Text	<i>Extracted from</i> <code>modelName</code>
Log Source Time	Date	<code>time</code>
Source IP	IP Address	<code>sourceIP</code>
Source MAC	Text	<code>sourceMac</code>
Source Port	Port	<code>sourcePort</code>
Username	Text	<code>deviceId</code>


## What protocols can alerts be sent over?

The QRadar alert output supports UDP and TCP format alerts, with optional TLS security and certificate validation for TCP. The use of TCP is recommended due to the longer payload length permitted within QRadar.

SETTING	DESCRIPTION
Send Alerts Using TCP	Turn on to send alerts over TCP. TCP allows for a longer message with greater detail. Turn off to send alerts over UDP.
Use TLS	Turn on to send TCP traffic with TLS encryption. Requires "Send Alerts Using TCP": On.
TLS Verify Certificate	Turn on to ensure that the server certificate is signed by a trusted root certificate authority. Requires "Send Alerts Using TCP": On, "Use TLS": On.
TLS Server Certificate Fingerprints	Turn on to ensure syslog will only be sent to TLS servers that present certificates with fingerprints in this comma separated list. Requires "Send Alerts Using TCP": On, "Use TLS": On.
Time Offset	Adjust the alert timestamp by a given number of hours from UTC. The value can be negative or positive but it must be an integer. As of Darktrace 6.1, this field also alters timestamps in the alert body.

### Can I filter the alerts sent to QRadar?

An alert **must meet all filter criteria** that are relevant to it. For example, a model breach must meet all thresholds, regular expressions and device restrictions applied.

If the settings fields appear to be read-only, it means that they are configured globally. Global Settings can be accessed by clicking the  **Config** icon to the right of **Workflow Integrations** on the **System Config** page, and changes can be made to individual modules by turning on **Enable Modular Alert Thresholds**.

FIELD NAME	APPLIES TO	DEFAULT	DESCRIPTION
AI Analyst Behavior Filter	AI Analyst Alerts	Critical	Behavior categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational. Select the categories to filter alerts to.
Minimum AI Analyst Incident Event Score	AI Analyst Alerts	0	Restricts incident events sent as external alerts to those with an individual event score above the threshold.
Minimum AI Analyst Incident Score	AI Analyst Alerts	20	Incident events are part of a larger incident. Restricts incident events sent as external alerts to those with an overall incident score above the threshold. Incident scores are expected to use the full range of scores from 0-100.
Model Breach Behavior Filter	Model Breach Alerts	Critical, Suspicious	Behavior categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational. Select the categories to filter alerts to.
Minimum Breach Score <sup>1</sup>	Model Breach Alerts	50	Enter a value to restrict the sending of alerts to those with a Breach Score that exceeds that value.
Minimum Breach Priority <sup>1</sup>	Model Breach Alerts	0	Enter a value to restrict the sending of alerts to those with a Breach priority that exceeds that value (0-5). "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.
Model Expression <sup>1</sup>	Model Breach Alerts	N/A	Enter a regular expression to restrict the sending of alerts to those with model names (and folder) that match the regular expression. "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.
Model Tags Expression	Model Breach Alerts	N/A	Enter a regular expression restrict the sending of alerts to models with tags matching the expression.
Device IP Addresses	Model Breach Alerts	N/A	Enter a comma separated list of IP addresses, and/or CIDR IP range(s) to restrict the sending of alerts to only those alerts concerning a device with one of the listed IP addresses.
Device Tags Expression	Model Breach Alerts	N/A	Enter a regular expression restrict the sending of alerts to those for devices with tags matching the expression.

<sup>1</sup> Setting controlled by the global alert thresholds.



