



# **Darktrace QRadar Integration**

Threat Visualizer v5.0

## 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, the Enterprise Immune System can identify and contain emerging threats that have bypassed traditional defenses and are active within the network. For security teams who wish to leverage this learning to enhance the value of their existing security stack, the Threat Visualizer offers multiple ways to integrate.

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

Additionally, the Threat Visualizer platform provides a curated set of default models as standard, designed and constantly tuned by the specialized Darktrace analyst team. The Darktrace DSM provides pre-mapped Event Types and Event Categories for all default Darktrace model categories, allowing new models to be automatically categorized.

### Custom Entities

The following custom entities and searches are included in the Darktrace QRadar DSM.

### Custom 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 FAQ.

### Custom `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

Event Name	High Level Category	Low Level Category	Severity
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

### Custom QIDMAP

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

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
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"

Selects 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 <code>qid</code> 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 <code>did</code> 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.

## Deploying Darktrace QRadar Integration

### Requirements

- A Darktrace Appliance running the most recent Darktrace Threat Visualizer software version (*minimum v4.7*)
- Any required firewall exceptions to allow communication from the master appliance to the QRadar instance on the required port (514 by default).
- A valid copy of the Darktrace QRadar DSM retrieved from the IBM X-Force Exchange.

### Darktrace Configuration

1. Access the Threat Visualizer interface of the Darktrace appliance intended to send alerts to QRadar. From the main menu, locate the **System Config** page (**Admin > System Config**).  
  
Locate **Modules** from the left-hand menu.
2. In the **Workflow Integrations** (*previously Alert Outputs*) subsection, select **QRadar**. This alert format is tailored to work with the Darktrace DSM.
3. Complete the **Server** location and optionally modify the communication port. Ensure that the port selected is allowed by any intermediary firewalls.
4. Darktrace recommends the use of **TCP Alerts** due to the larger payload size supported by QRadar. Both UDP and TCP are supported.
5. Configure any alert thresholds, time offsets or additional settings as required. Please see the FAQ for more details.
6. Enable **Send Alerts** and save your changes.

### QRadar Configuration

1. Log into QRadar, navigate to the "**Admin**" tab and then click on "**Extension Management**".
2. Click on the **Add** button on the top right corner, a popup will open.  
  
Locate the Darktrace DSM file. Tick "**Install immediately**" and add the DSM.
3. Return to the Admin tab and click "Log Sources". Select the Darktrace entry, and in the "Protocol" tab modify the default value of **Log Source Identifier** to the hostname or the IP address of the Darktrace appliance already configured to send logs to QRadar.

In the majority of deployments, the payload size for Darktrace QRadar alerts should not exceed the default maximum length (4k). If you are experiencing issues with payload truncation, increasing the **Maximum Syslog Payload Length** within QRadar may resolve this issue. These settings can be located in **System Settings > Advanced > Max UDP Syslog Payload Length** and **Max TCP Syslog Payload Length**.

## Frequently Asked 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	destIP
Destination MAC	Text	destMac
Destination Port	Port	destPort
Event Category	Text	Extracted from modelName
Event ID	Text	Extracted from modelName
Log Source Time	Date	time
Source IP	IP Address	sourceIP
Source MAC	Text	sourceMac
Source Port	Port	sourcePort
Username	Text	deviceId

### 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.

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

Three settings are available to filter the model breaches that Darktrace sends out to external alert platforms: **Minimum Breach Priority**, **Minimum Breach Score** and **Model Expression**. These settings can be configured globally, or within each individual QRadar configuration section. If more than one alert condition is configured then a model breach **must meet all criteria** to generate an alert.

If the fields are read-only within the QRadar configuration section, it means that these thresholds are configured globally. Global Settings can be accessed from the  **Config** button to the right of **Workflow Integrations (previously Alert Outputs)**, and enabled on a per-format basis using "Enable Modular Alert Thresholds".

- **Minimum Breach Priority:** every model has a priority from 0-5 indicating the breach severity. Providing a minimum alert priority of 1 to 5 will restrict alerts to models that fire with a threshold of the priority number or greater.
- **Minimum Breach Score:** the alert score (model breach score) is displayed when hovering over the colored line to the left of a model breach. The score is a percentage representing the overall priority of a breach and can be filtered with a slider in the main Threat Visualizer.
- **Model Expression:** regular expressions can be entered to restrict alerts to model names that match a certain Regex value.

