Mandiant

IBM QRADAR INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to IBM Qradar to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to IBM Qradar to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
`/api/ariel/searches`	Start a Search Query for Events
`/api/ariel/searches/(id)/results`	Get resultset of Events for search with `(id)`
`/api/siem/offenses`	Search Query for Offenses
`/api/ariel/databases`	Used to validate connectivity and API credentials

Supported Versions

v7.3

Before You Begin

To configure this integration, you need:

- The hostname of your IBM Qradar instance
- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- Token

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > IBQ Qradar**.

   

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your IBM Qradar instance.
7. Enter a **Port** value. The default is **443**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

8. Choose an **Auth Method**: either **Basic** or **Token**.
9. Enter the **Username** and **Password** for the user account with permissions to use API endpoints.
10. Optional: If you chose **Token** for the authentication method, enter the generated **Token** value.
11. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
12. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
13. Optional: Add or remove **Queries**, as needed. **IP Query** is provided.
14. Optional: Modify the **Offense Query Fields** and **Offense Query Filter**, if needed. Default values are provided.
15. Enter a value in the **Correlated Events Queries** and add more queries, if needed.
16. Optional: Modify the **Field Map** values, as necessary.

    

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

17. Optional: Change the value for **Page Size** (default **500**) if needed.
18. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

    

    If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. If supported by your integration, configure correlation queries:
        i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
        ii. Modify the **Correlation Query Interval**, if necessary (minutes).
    d. Select **Discover network devices automatically**, the default and recommended option.

    

    If unselected, reported events won't include product information for any matching network security technology.

    e. Select **Save Suspicious Events**.
    f. Modify the **Event Time Adjustment** (seconds). The default is **0**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

19. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

This integration is remote capable.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access QRadar.
2. Port for QRadar communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS for connections to the QRadar port (default is HTTPS).
4. Identify or create credentials to access QRadar. Admin permissions are required, at minimum.
5. Identify the timezone of the QRadar host.

Configuration

TO ADD THE QRADAR INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **QRadar**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7ddd/n/qradar-836.png)

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Select the **Credential type** and add the appropriate credentials.
5. Change the **Time zone** to match that of the QRadar host.
6. Review and update the **Query**to include instance-specific field names, sources, data types, and other customizations.

   The default queries can be viewed by clicking **Show default query.**

   The query includes information that allows event matching based on any file hashes included in an Action.

7. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d7c9cba0017c2f7dd5/n/qradar-adv.png)

QRadar Integration - Advanced section

8. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

9. (Optional) Review and update the populated query information (**Flows query**, **Offense query** fields, **Offense query** filter, **Correlated Events Query**).
10. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
11. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
12. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

> If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

13. (Optional) Select **Discover network devices automatically**.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

The QRadar integration can also include these two fields in its queries:

- `host`, which when populated will be used to indicate the source of the events.
- `url`, which when populated is used for matching events to DNS query Actions.

> The url field is not a default qradar field, so you name it yourself. For example, `select qid, qidname(qid), "DNS_Domain" as url, sourceip,`

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

TO VERIFY CONNECTIVITY TO QRADAR

Click **Test** to verify that:

- The Director can communicate with QRadar on the port and protocol specified.
- QRadar credentials are valid and working.
- Times match.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.