CARBON BLACK PROTECTION INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Carbon Black Protection to test the efficacy and configuration of the security control using Security Validation jobs.

API Calls

API	Usage
`/event`	Collect events from Carbon Black
`/serverConfig`	Used to test connectivity between Mandiant and Carbon Black

Supported Versions

bit9platform API v1

Before You Begin

To configure this integration, you need:

- The hostname of your Carbon Black Protection instance
- An API Token

Generate a API Token

Each Carbon Black user has a personal API key. That API key provides all permissions assigned to that user to anyone possessing the API key. It is recommended that you create a separate Carbon Black user for this integration. The user should be assigned the minimum set of permissions required to return events.

See the Carbon Black App Control User Guide for more information on how to set up **User Groups** and **Role Based Access Control** in the Carbon Black console.

To find an API key corresponding to a given Carbon Black user account,

1. Log into the Carbon Black console as an administrator.
2. Select **Administration -> Login Accounts**.
3. Find the user in the list then click the **Edit** button on the left hand side of the row containing their username.
4. The details for the selected user are displayed.
5. At the bottom of the **details** page, click the checkbox next to **Show API Token** in the API section.
6. The API token associated with the given user is displayed.
7. If no API token is displayed, click the **Generate** button and then click **Save**.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Carbon Black Protection**.

   

   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. Optional: Change the **Protocol** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **Host** value (hostname or IP address) for the Carbon Black Protection instance.
7. Enter a **Port** value. The default is **443.**
8. Enter the **Api Token** value that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Add or remove value for **Queries**. A default **IP Query** is provided.
12. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
13. 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.

14. 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. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. 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.

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

15. 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)**.