Integrate Reveal(x) 360 with CrowdStrike Falcon LogScale

This integration enables you to export security detections from Reveal(x) 360 to LogScale to view detection data in a centralized system, enhancing context around detections and decreasing the time to confirm threats.

System Requirements

ExtraHop Reveal(x) 360

- Your user account must have privileges on Reveal(x) 360 for System and Access Administration or Cloud Setup.
- Your Reveal(x) 360 system must be connected to an ExtraHop sensor with firmware version 9.3 or later.
- Your Reveal(x) 360 system must be connected to ExtraHop Cloud Services ⧉.

CrowdStrike Falcon LogScale

- You must have CrowdStrike Falcon LogScale version 1.92.0 or later.
- You must configure the LogScale HTTP Event Collector API ⧉ for data ingest.

Configure the CrowdStrike Falcon LogScale integration

1. Log in to the Reveal(x) 360 system.
2. Click the System Settings icon ⚙ and then click **Integrations**.
3. Click the **CrowdStrike Falcon LogScale** tile.
4. From the **LogScale Host** drop-down list, select the hostname of your LogScale endpoint.
5. Optional: If you selected a CrowdStrike Datacenter as your host, type your customer subdomain in the **Customer Prefix** field. The prefix is added to the hostname and displayed in the LogScale Ingest Host field, similar to the following example:

6. In the **Ingest Token** field, type the ingest token you configured for the LogScale HTTP Event Collector.
7. Click **Send Test Event**, and then check that the event was received by your LogScale endpoint. It might take several minutes for the test event to arrive.
8. Optional: Configure the following integration options:
    a) Click **Export Reveal(x) 360 security detections**.
    b) Click **Add Criteria** to configure the filter that determines which security detections are exported to your LogScale endpoint.
9. Optional: Click **Change Credentials** to update the LogScale hostname or the HEC token.
10. Optional: Click **Disable Integration** to keep the current credentials and options, but disable the LogScale integration.
11. Click **Save**.