RiskIQ Illuminate for CrowdStrike

January 11th, 2021

Summary

RiskIQ Illuminate integrates with Falcon to give security teams a 360° view of their attack surface to better detect threats and defend their enterprise. RiskIQ Illuminate seamlessly combines Falcon's internal endpoint telemetry with petabytes of external Internet data collected for over a decade. With RiskIQ Illuminate security teams will accelerate their investigations, increase their visibility, respond more effectively to threats, and maximize the impact of their existing security solutions.

Requirements

- Administrator access to the Falcon platform in order to install the application
- Licensed for one or both of the following
    - Falcon X
    - Falcon Insight EDR

Pricing

The RiskIQ Illuminate Application for CrowdStrike is priced as an additional fee per user within the RiskIQ PassiveTotal enterprise organization. Users can conduct a free 30-day trial of the application by visiting the CrowdStrike store and clicking install. For an exact quote, please reach out to your RiskIQ account representative or sales@riskiq.net if you are not yet working with an account representative.

Integration Details

RiskIQ Illuminate brings CrowdStrike Falcon data from licensed products directly into the RiskIQ PassiveTotal product. Users conducting an investigation within RiskIQ PassiveTotal can immediately see CrowdStrike Falcon X intelligence and endpoints who have communicated with the infrastructure, all without leaving the platform.

RiskIQ Illuminate Setup

Go to the CrowdStrike Store and click on the RiskIQ application.

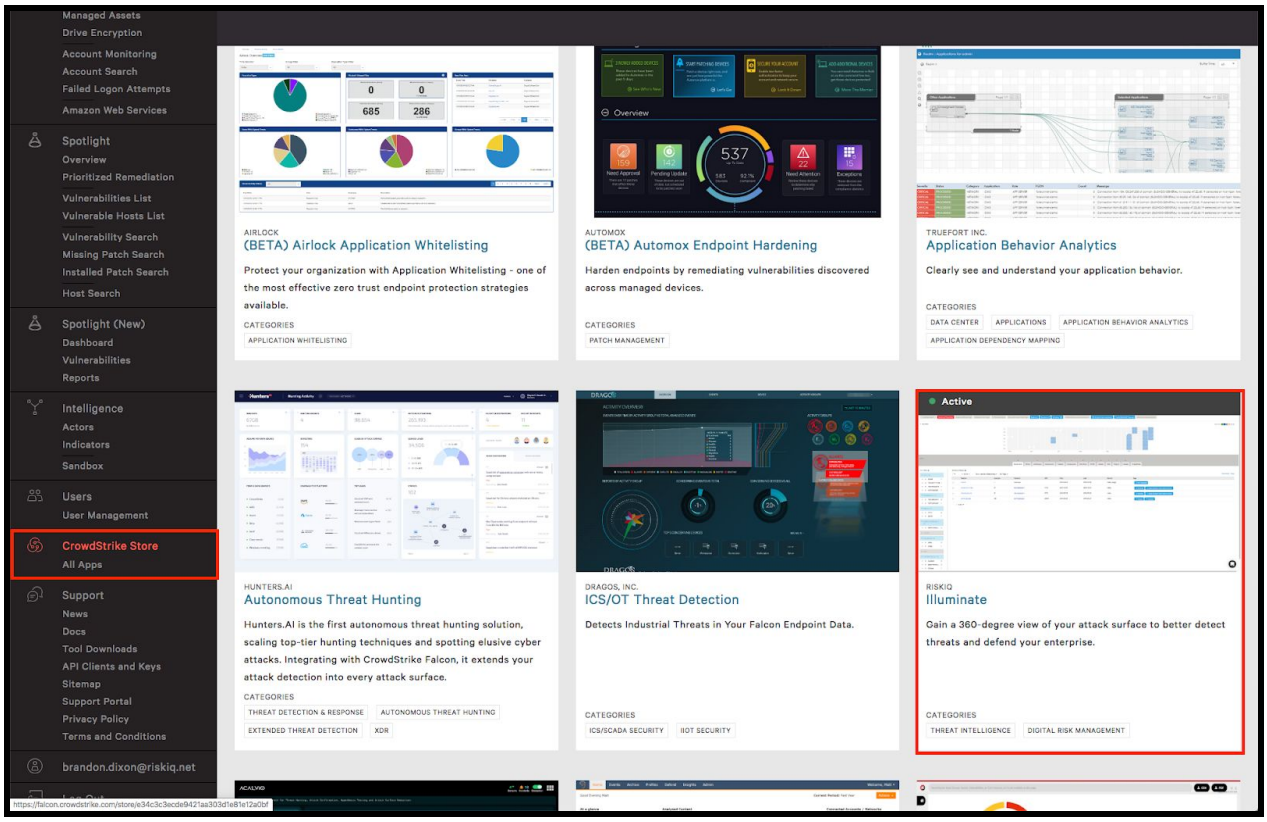

Figure-1: CrowdStrike Store showing available applications.

Once opened, click on the install button for RiskIQ. You must be an administrator in order to perform this action.

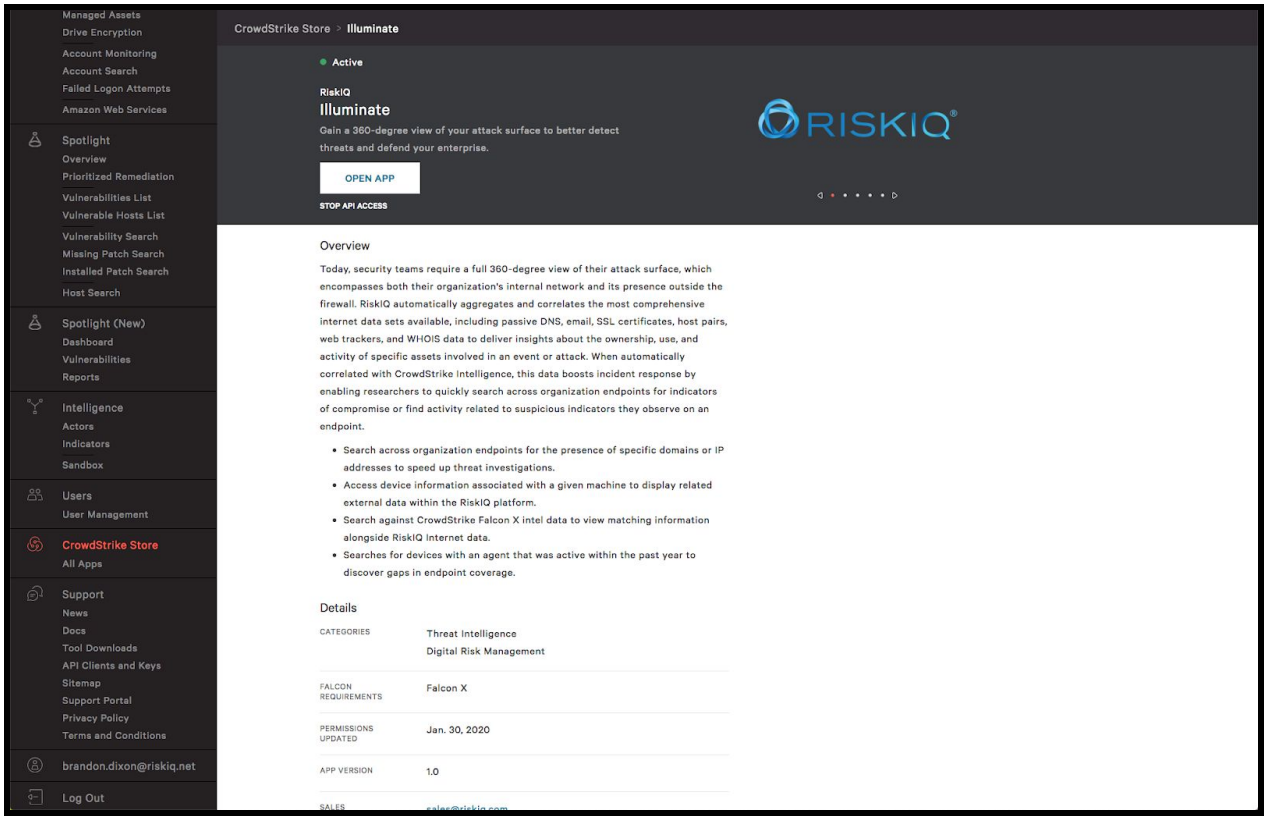

Figure-2: RiskIQ Illuminate Application within the CrowdStrike store.

Once clicked, the Falcon platform will perform the appropriate setup. If you are an existing RiskIQ PassiveTotal enterprise client, your organization will now be able to see CrowdStrike data. If you are new to the RiskIQ PassiveTotal platform, an enterprise organization will be created with the Falcon administrator set as the enterprise administrator. If you need to add additional users or make adjustments to this account, please contact the administrator or your RiskIQ representative.

After successfully installing the application, you should see CrowdStrike data within analyst alert tags.

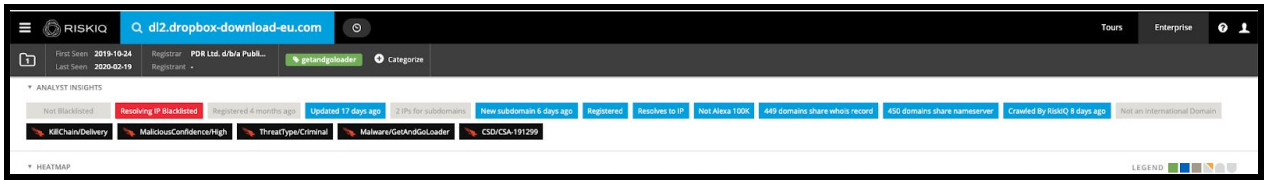

Figure-3: CrowdStrike tags from Falcon X displayed within Analyst Insights section

Additionally, you will see a CrowdStrike tab within the data sources.

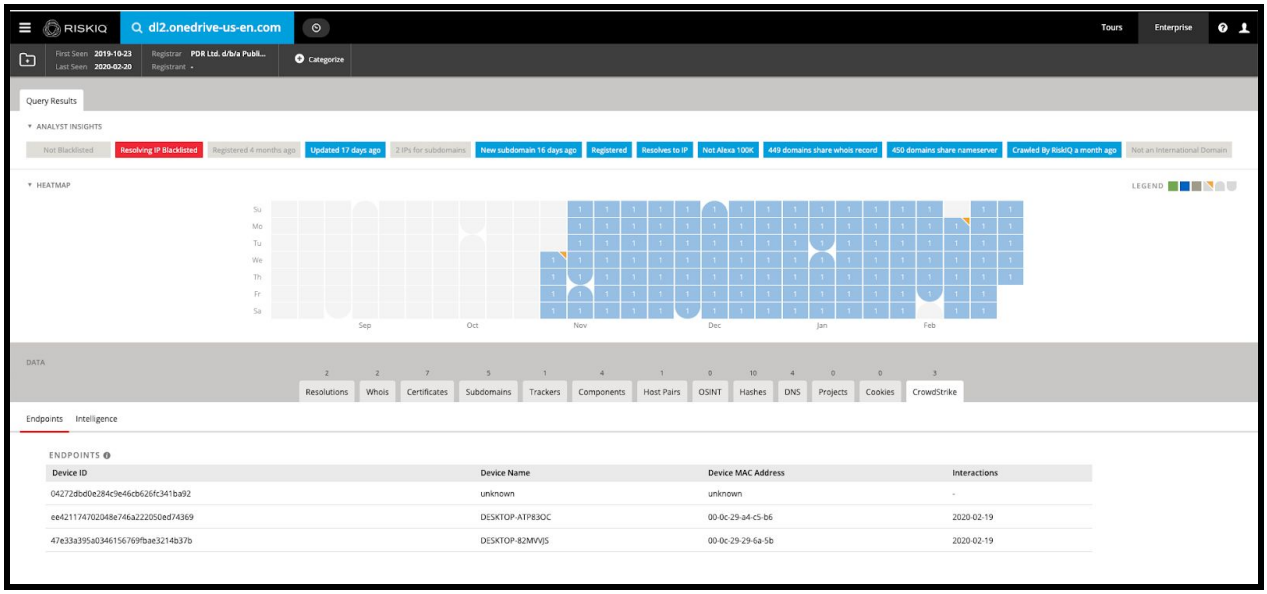

Figure-4: Endpoint matches from Falcon Insight EDR data

RiskIQ Components within CrowdStrike Falcon

Beyond the RiskIQ Illuminate Application, RiskIQ has a couple other components available within the Falcon platform. These include a search result card and a data icon.

Search Result Card

When searching for an indicator within the Falcon platform, a card interface will return with relevant information. Included within these cards will be a RiskIQ tab that will give summary information. This card is bundled with the RiskIQ Illuminate Application in the CrowdStrike Store.

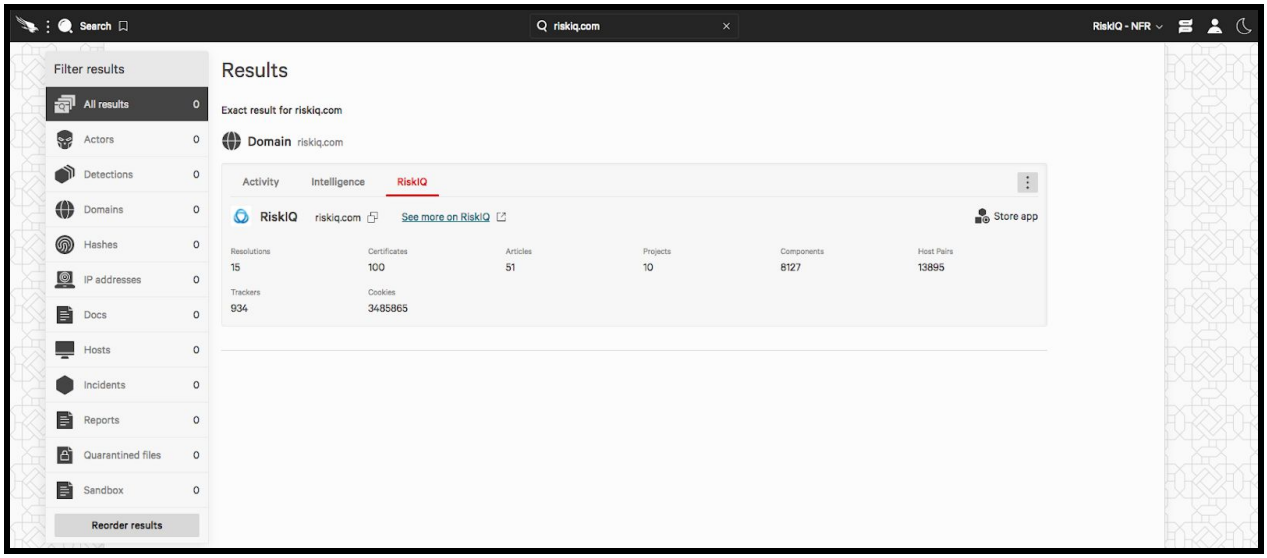

Figure-5: RiskIQ indicator card with summary information.

RiskIQ Detection Icon

Within the Falcon Detections interfaced, there's a number of side panels with metadata and enrichment information. Located within the DNS Requests and Network Connections sections are small RiskIQ icons next to each indicator. Clicking on this icon will automatically send the user to search results within RiskIQ PassiveTotal. This icon is available to all Falcon users, regardless of if they use the RiskIQ application, however, non-application users are limited in their ability to perform additional investigating and the data sets they can see.

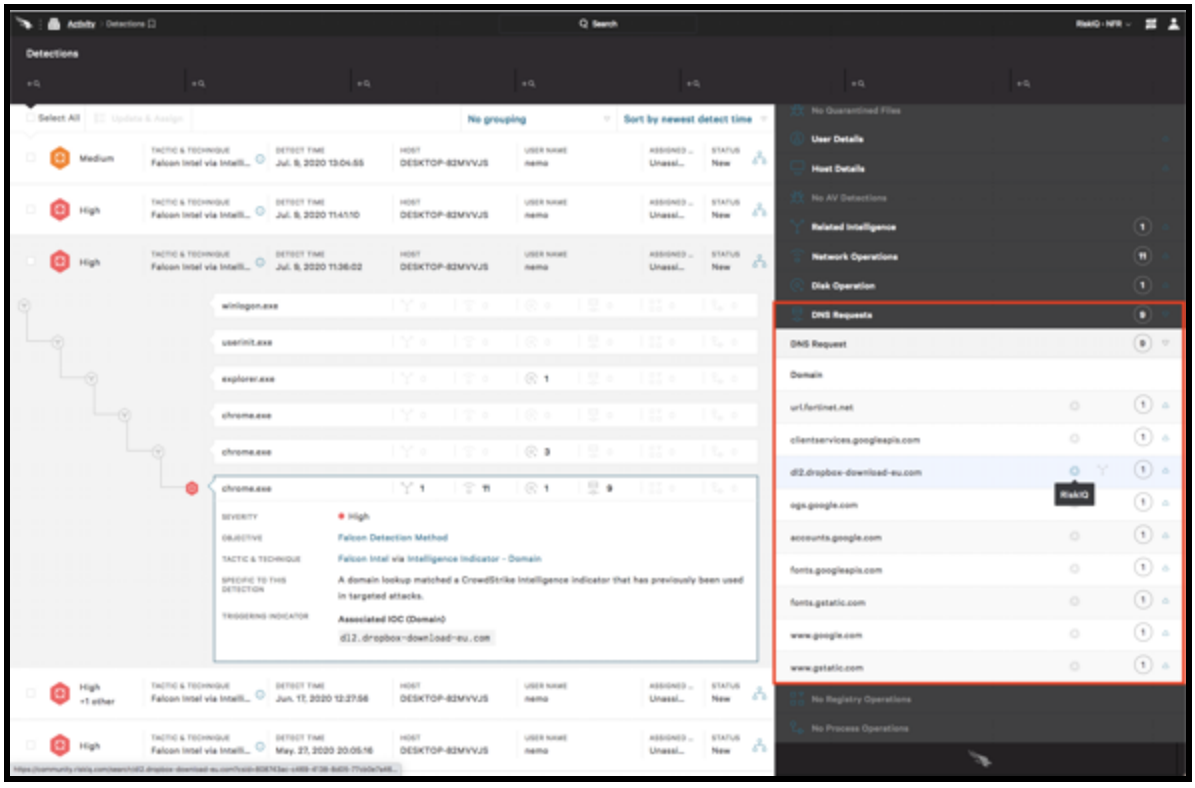

Figure-6: RiskIQ Icon located next to indicators in the Detections page of Falcon

Testing Considerations (PoC)

Once a user accesses the RiskIQ Illuminate application and clicks on the Install button, this will start the 30 day trial for all users with the same email domain. Therefore, it's important to identify the stakeholders that will be involved in the proof-of-concept, so everyone has a chance to test the integration. If you're interested in testing the integration, we advise that you reach out to sales@riskiq.net as the first step.

Technical Limitations

- 1 Crowdstrike Customer ID (CID) maps to one 1 PassiveTotal Enterprise organization (at this time).
    - Note: RiskIQ will be modifying this configuration to allow for multiple CIDs to map to one PassiveTotal organization. Timeline for this project has not been determined.
- The integration is configured at the PassiveTotal organization-level rather than the user-level (at this time).
    - Therefore, if you would like only certain users to have the integration within your PassiveTotal organization, we recommend that you work with your RiskIQ Account Executive to create a separate PassiveTotal organization for users that will not have the integration enabled. Users that are placed in separate PassiveTotal organizations will not be able to view their Team projects (by default, unless shared each time), search history, tags, and classifications with the other PassiveTotal Enterprise organization.
    - Note: RiskIQ will be modifying this configuration to allow the integration to be setup at the user-level rather than organization-level. Timeline for this project has not been determined.
- RiskIQ is able to collect up to 30 days of Crowdstrike metadata for interactions. If you notice an endpoint that flags in PassiveTotal from searching an indicator and there is no date noted under Crowdstrike > Endpoints > Interactions, please check your Crowdstrike instance for the date the endpoint specifically reached out to that indicator.

Support

RiskIQ is happy to provide support for our CrowdStrike application. If you have questions, feedback or run into issues, please contact us using support@riskiq.com. Alternatively, existing enterprise clients can reach out directly to their support representative. Please do not contact CrowdStrike support for issues related to the RiskIQ application.

Resources

Integration Overview

RiskIQ Illuminate App for Crowdstrike Falcon (Brief Demonstration)

Joint Threat Hunting Workshop - RiskIQ & Crowdstrike

- Overview of integrated use cases
- Demonstration of Powershell Scripts
    - Install PSFalcon
        - GitHub

        - Demo of installing the script
    - Install PSRiskIQ
        - GitHub
        - Demo of installing the script
    - Install GetArtifacts
        - GitHub
    - The PowerShell Scripts were created by Crowdstrike's Brendan Kremian, Sr. Sales Engineer, Public Sector/Healthcare Pacific Northwest.
    - Note: These Powershell scripts **do not come with support**. If the scripts require maintenance, the end user will be responsible for debugging the script.
- Clips from RiskIQ & Crowdstrike Joint Threat Hunting Workshop
    - In this video, we demonstrate searching an IoC inside of CrowdStrike Falcon Intelligence to expand the investigation with RiskIQ Intelligence. From there, you can quickly determine if you're affected using the CrowdScrape Chrome Plug-in.
    - In this video, we demonstrate how to go from a RiskIQ Threat intelligence Article to Crowdstrike Falcon IoCs to generate new detections in Crowdstrike Falcon.
    - In this video, we demonstrate how to go from a PassiveTotal Project back to CrowdStrike Falcon to generate new detections in CrowdStrike Falcon.