# **RiskIQ Illuminate for CrowdStrike**

January 11th, 2021

Summary	1
Requirements	1
Pricing	2
Integration Details	2
RiskIQ Illuminate Setup	2
RiskIQ Components within CrowdStrike Falcon	4
Search Result Card	4
RiskIQ Detection Icon	5
Testing Considerations (PoC)	6
Technical Limitations	6
Support	6
Resources	7

# 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 <u>sales@riskiq.net</u> 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.

	Managed Assets Drive Encryption	CrowdStrike Store > Illuminate	
	Account Monitoring Account Search Failed Logon Attempts Amazon Web Services	• Active Risklo Illuminate	
	Spotlight Overview Prioritized Remediation Vulnerabilities List Vulnerable Hosts List	Gein a 360-degree view of your attack surface to better detect       Image: Comparison of the surface	
	Vulnerability Search Missing Patch Search Installed Patch Search Host Search	Overview Today, security teams require a full 360-degree view of their attack surface, which encompasses both their organization's internal network and its presence outside the firewall. Riskla automatically exgregates and correlates the most comprehensive	
	Spotlight (New) Dashboard Vulnerabilities Reports	internet data sets available, including passive DNS, email, SSL certificates, host pairs, web trackers, and WHOIS data to deliver insights about the ownership, use, and activity of specific assets involved in an event or attack. When automatically cerrelated with CrowdStrike Intelligence, this data boosts incident response by	
	Intelligence Actors Indicators Sandbox	enabling researchers to quickly search across organization endpoints for indicators of compromise or find activity related to suspicious indicators they observe on an endpoint. • Search across organization endpoints for the presence of specific domains or IP addresses to speed up threat investigations.	
	Users User Management	<ul> <li>Access device information associated with a given machine to display related external data within the RiskUp platform.</li> <li>Sarch against CrowdStrike Falcon X intel data to view matching information</li> </ul>	
	CrowdStrike Store All Apps	alongside RiskIQ Internet data. • Gearches for devices with an agent that was active within the past year to discover gas in producing coverage.	
	Support News Docs Tool Downloads API Clients and Keys Sitemap Support Portal Privacy Policy Terms and Conditions	Details CATEGORIES Threat Intelligence Digital Risk Management	
		FALCON X REQUIREMENTS Falcon X PERMISSIONS Jan. 30, 2020	
	brandon.dixon@riskiq.net	APP VERSION 1.0	
9	Log Out	SALES calae@diskin.com	

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.

	0	Tours Enterprise 🕜 👤
First Seen 2019-10-23 Registrar PDR Ltd. d/b/a Publi Last Seen 2020-02-20 Registrant -	Calegoria	
Query Results		
▼ ANALYST INSIGHTS		
Not Blacklisted Resolving IP Blacklisted Registered 4 months ago	Updated 17 days ago 21Ps forsubdomains New subdomain 16 days ago Registered Resolves to IP Not Alexa 100c 449 domains share whole record 450 domains share nameserver Crawled By RokQ a more	Not an International Domain
* HEATMAP		
Su		
Mo		
Tu		
We		
Th		
Fr		
50	Sep Oct Nev Dec jan Feb	
DATA		
	2 2 7 5 1 4 1 0 10 4 0 0 3	
	Resolutions Whois Certificates Subdomains Trackers Components Host Pairs OSINT Hashes DNS Projects Cookies CrowdStrike	
Endpoints Intelligence		
ENDPOINTS Ø		
Device ID	Device Name Device MAC Address Interactions	
04272dbd0e284c9e46cb626fc341ba92	unknown unknown -	
ee421174702048e746a222050ed74369	DESKTOP-ATP83OC 00.0c 29-94-c5.b6 2020.02-19	
47e33a395a0346156769fbae3214b37b	DESKTOP-82MVVJS 00-0c-29-29-6a-5b 2020-02-19	

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.

🛰 : 🔍 Search 🛛		Q riskiq.com	×	RiskiQ - NFR 🗸 😫 💄 🕓
Filter results	Results			
All results 0	Exact result for riskiq.com			
Actors 0	Domain riskiq.com			
Detections 0	Activity Intelligence RiskIQ			
Domains 0	See more on Riskiq.com			Store app
Hashes 0	Resolutions Certificates Art	icles Projects	Components Host Pairs	
IP addresses 0	15 100 51 Trackers Cookies	10	8127 13895	
Docs 0	934 3485865			
Hosts 0				
Incidents 0				
Reports 0				
Quarantined files 0				
Sandbox 0				
Reorder results				

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.

🍡 : 👼 Activity - Detections 🛙	i i ki iii		Q Search	• ] •			RMID - NPR -	. # 1
Detections								
Gelect All III Update & Analys		No grouping	· 5	et by newest detec	ttime - 2			
Madum Techo & Technold	O DETECT TIME HOST	UNE	IR NAME	A0010400 - 514	na 🔬 🦉	User Details		
Falcon Intel via Intell.	Jul. 8, 2020 13:04:55 DESK	TOP-82MVVJS ner	na	Unassi Net	- ···	Hust Details		
High Technologie High	0 DETIGET TIME HOST Jul. 8, 2020 T14110 DESK	TOP-82MVVJS ner	IR NUMBER	ASSIGNED	** A			
						Related Intelligence		
High Falcon Intel via Intelli.	- 0 Jul. 8, 2020 1136-02 DESK	TOP-82MVVJS ner	na susati	UnassiNet	- A	Network Operations		
·	ponasa (1971)					Disk Operation		0 •
						DN3 Requests		0 *
						NS Request.		•
· · · · · · · · · · · · · · · · ·	••••• Y :		1 2 4			ongin		0.
- C shree	•••• IY)					rl/laritinel.net		0.
chrom	9488 IYO		1.12.1			lentservices.googleepis.com		0.
O Chron	ына (Y)	12	1.12.4	133 4 134		12.dropbox-download-eu.com	0 Y	•
11V08	rr • High					gs.google.com		•
OUUSTIVE Falcon Detection Method					-	cosunts geogle.com		1.
tatte a titoenout     Falcon Intel via Intelligence Indicator - Domain     second to the second tatte intelligence Indicator that has previously been used					used fo	onts.googleepis.com		1 *
Denie	In targeted attacks					onts-gatatic.com		۵ (
	dl2.dropbox-dow	nload-eu.com				ww.google.com		۰ (
						ww.gstatic.com		1 4
High Technolue     High Technolue     Falcon Intel via Intell.	TOP-82MVVJS ner	It houst	Unassi	- A 📑	No Registry Operations			
	DETECT TIME HOST		Il hututi	A00 0400 - 514	2			
High Falcon Intel via Intell.	May 27, 2020 20.05.16 DESK	TOP-82MVVJS ner	na	Unassi_ Net	- A	*		

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 <u>contact us</u> 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
    - <u>GitHub</u>

- Demo of installing the script
- Install PSRiskIQ
  - <u>GitHub</u>
  - Demo of installing the script
- Install GetArtifacts
  - <u>GitHub</u>
- 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 <u>video</u>, 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 <u>video</u>, we demonstrate how to go from a RiskIQ Threat intelligence Article to Crowdstrike Falcon IoCs to generate new detections in Crowdstrike Falcon.
  - In this <u>video</u>, we demonstrate how to go from a PassiveTotal Project back to CrowdStrike Falcon to generate new detections in CrowdStrike Falcon.