Automated Enrichment with Petabytes of Internet Intelligence

Cybercriminals are ever-increasing the scale and sophistication of their attacks making it harder to detect and block their activity. Now more than ever, it is important that your security solutions and programs have access to up-to-date, internet-scale intelligence to counteract this trend. Having programmatic access to internet intelligence and data allows security teams to streamline enrichment and security teams have the data and context to better protect their enterprises, customers, and data.

RiskIQ PassiveTotal pack for Cortex XSOAR enables security teams to scale and automate their threat detection and response programs. RiskIQ's Internet Intelligence Graph provides crucial external context to all internal IOC's and incidents. This context helps security teams understand how internal assets interact with external infrastructure so they can better detect and prevent attacks. With these insights, security teams can also proactively detect and block the new threat infrastructure that's part of attacks against their organization that they wouldn't otherwise know existed.

Integration Features

- Enrich Cortex XSOAR incidents and indicators with Passive DNS, WHOIS, SSL Certificates, Web & Social Trackers, Host Pairs, DNS Records, Open Ports and Services
- Visualize Internet data alongside existing security telemetry to accelerate triage efforts and provide confidence to analysts or responders
- Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security functions based on insights from RiskIQ PassiveTotal
- Run 100s of commands interactively via a ChatOps interface while collaborating with other analysts and Cortex XSOAR's chatbot

Benefits

- Seamlessly enrich Cortex XSOAR alerts, incidents and indicators with RiskIQ's Internet Intelligence Graph
- Accelerate investigations and incident response with unparalleled context and intelligence
- Streamline collaboration on threat investigations or incident response engagements by merging and linking internal and external telemetry
- Proactively defend your organizations from attackers with threat hunting exercises

Compatibility

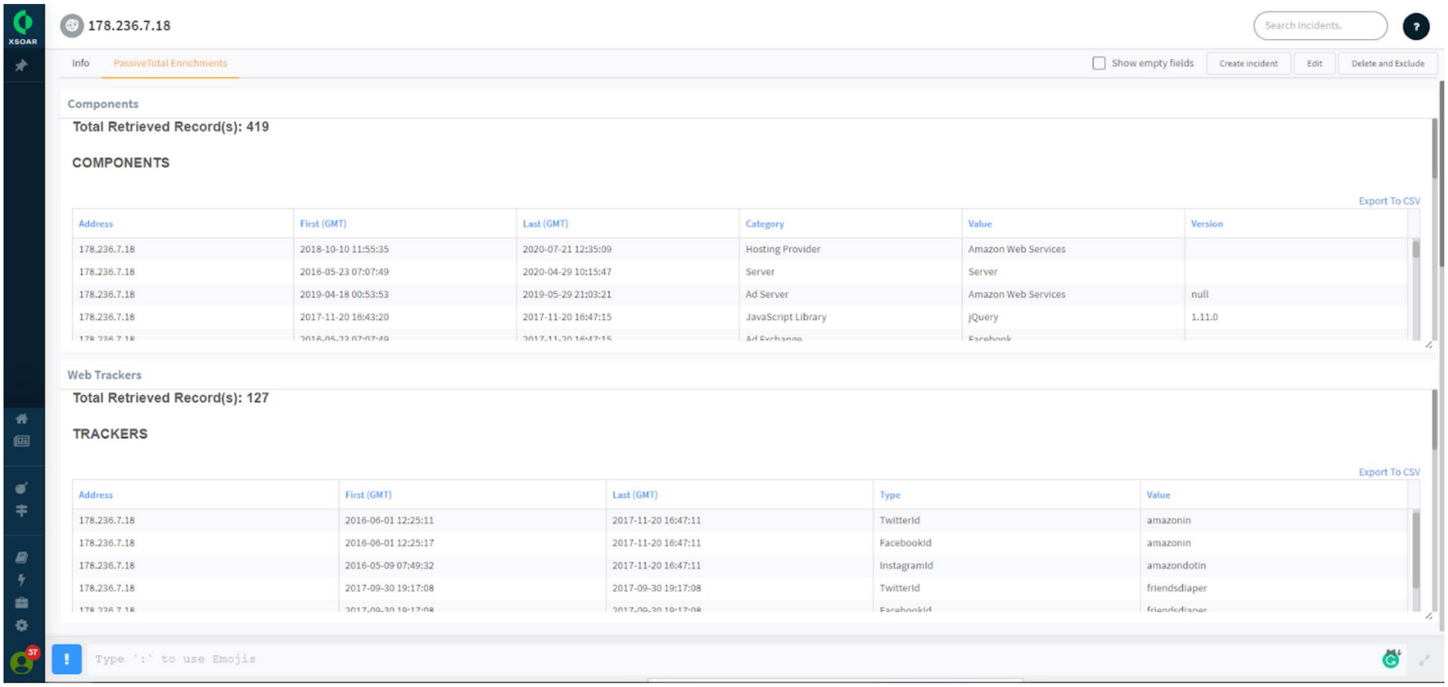
Products: RiskIQ PassiveTotal
Cortex XSOAR + RiskIQ PassiveTotal

Use Case #1
Automated Incident Enrichment and Response

Challenge: Security teams are inundated with a broad array of indicators from their security controls and infrastructure. These indicators need to be enriched and correlated with external attacker intelligence so that they can be prioritized, actioned and closed. Meanwhile, attackers are continuously shifting their infrastructure, techniques, and processes to evade detection. Real-time Internet scaled intelligence combined with machine-powered security automation is and orchestration is required in today's environment.

Solution: RiskIQ's PassiveTotal delivers comprehensive, real-time security intelligence to Cortex XSOAR. RiskIQ global discovery network that continuously extracts terabytes of internet infrastructure data. RiskIQ's Internet Intelligence Graph then maps and maintains the relationships between this data. RiskIQ's XSOAR pack provides automated enrichment to inform and power Cortex XSOAR AI and orchestration capabilities.

Benefit: RiskIQ's PassiveTotal pack for Cortex XSOAR enables security teams to rapidly scale and automate their threat detection, incident response and threat investigation programs. Security teams can automate and customize their response efforts using a robust set of playbooks.



Components

Total Retrieved Record(s): 419

COMPONENTS

Address	First (GMT)	Last (GMT)	Category	Value	Version
178.236.7.18	2018-10-10 11:55:35	2020-07-21 12:35:09	Hosting Provider	Amazon Web Services	
178.236.7.18	2016-05-23 07:07:49	2020-04-29 10:15:47	Server	Server	
178.236.7.18	2019-04-18 00:53:53	2019-05-29 21:03:21	Ad Server	Amazon Web Services	null
178.236.7.18	2017-11-20 16:43:20	2017-11-20 16:47:15	JavaScript Library	jQuery	1.11.0
178.236.7.18	2016-05-23 07:07:49	2017-11-20 16:47:15	Ad Exchange	Facebook	

Web Trackers

Total Retrieved Record(s): 127

TRACKERS

Address	First (GMT)	Last (GMT)	Type	Value
178.236.7.18	2016-06-01 12:25:11	2017-11-20 16:47:11	TwitterId	amazonin
178.236.7.18	2016-06-01 12:25:17	2017-11-20 16:47:11	FacebookId	amazonin
178.236.7.18	2016-05-09 07:49:32	2017-11-20 16:47:11	InstagramId	amazondotin
178.236.7.18	2017-09-30 19:17:08	2017-09-30 19:17:08	TwitterId	friendsdiaper
178.236.7.18	2017-09-30 19:17:08	2017-09-30 19:17:08	FacebookId	friendsdiaper

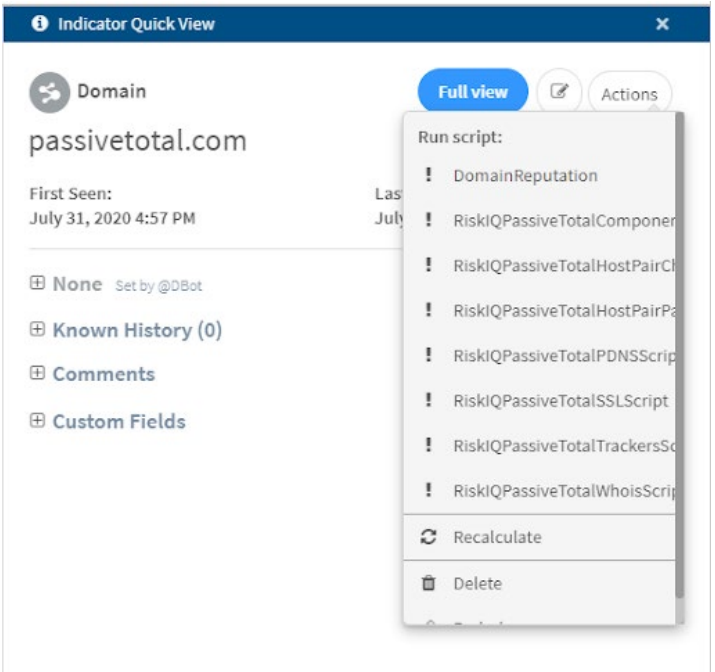
Use Case #2

Accelerate Threat Investigation and Proactively Defend Your Organization

Challenge: Transformation initiatives, which have been accelerated by COVID-19, are producing an ever-expanding and dynamic digital presence for all companies. Threat actors are taking advantage of this with increasingly sophisticated and agile attacks and campaigns. Successful investigations require security teams to identify and monitor all an attacker's infrastructure to effectively protect their organization.

Solution: The RiskIQ PassiveTotal pack, powered by our Internet Intelligence Graph, enables security teams to understand how internal assets interact with external infrastructure and explore how an attacker's infrastructure is linked. PassiveTotal allows threat hunters to easily pivot off from one data point to research and identify how an attacker's related infrastructure is linked and leveraged. Uncovering these hidden facets of an attacker's infrastructure, enables security teams to more effective monitor, alert, and block attacks.

Benefit: RiskIQ's PassiveTotal pack for Cortex XSOAR enables security teams to detect, investigate, and prevent attacks faster and more effectively than ever before. Our global internet security intelligence and Internet Intelligence Graph provide unparalleled context to detect, investigate, and remediate IoC's and security events


Domain
passivetotal.com
First Seen:
July 31, 2020 4:57 PM
Indicator Quick View
×
Full view
Actions
Run script:
DomainReputation
RiskIQPassiveTotalComponer
RiskIQPassiveTotalHostPairCl
RiskIQPassiveTotalHostPairPa
RiskIQPassiveTotalPDNSScrip
RiskIQPassiveTotalSSLScript
RiskIQPassiveTotalTrackersSc
RiskIQPassiveTotalWhoisScrip
Recalculate
Delete
Las
July
⊞ None Set by @DBot
⊞ Known History (0)
⊞ Comments
⊞ Custom Fields

About RiskIQ

RiskIQ is the leader in digital attack surface management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams, and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

About Cortex XSOAR

Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/xsoar.