RISKIQ® partnered with splunk>

RiskIQ PassiveTotal® App for Splunk

Enhancing your Security Operations with Petabytes of Internet Intelligence

Challenges: Staying Ahead of Digital Sprawl

Today, security teams require a full 360-degree view of their digital attack surface to better detect threats and defend their enterprise. This means having a continuous visibility of their organization's internal network, their presence outside the firewall, and awareness of which systems and entities your users and systems are interacting with. All enterprises are in various stages of digital transformation—moving workloads to the cloud, adopting SaaS applications, automating development operations, utilizing microservices, and switching to a serverless architecture—making monitoring and managing an enterprise's digital attack surface increasingly difficult. This digital sprawl further reinforces the need for a 360-degree visibility and context as the key to every enterprise security team's ability to timely detect, investigate, and respond to threats.

Solution: Accelerate Investigations, Eliminate Threats

RiskIQ PassiveTotal® App for Splunk seamlessly combines and enriches Splunk's data-to-everything -platform with petabytes of external Internet security intelligence collected by RiskIQ over more than a decade. Layering RiskIQ's internet Intelligence Graph on top of Splunk data in one location provides crucial external context to internal IOC's and incidents. This context helps security teams understand how internal assets interact with external infrastructure so they can block or prevent attacks and know if they've been breached.

Integrating Splunk and RiskIQ intelligence into a single platform accelerates and enriches incident response via automation and team collaboration, and opens new avenues of research. Security teams can identify and block new threat infrastructure that's part of attacks against their organization that they wouldn't otherwise know existed. This added visibility helps them identify gaps between the internet infrastructure they can see connected to their endpoints, and what they can't, which gives them a detailed picture of their attack surface—just as attackers see it.

Use Cases / Business Value:

- **Accelerate Threat Detection and Investigations.** RiskIQ PassiveTotal App for Spunk brings the most comprehensive internet security intelligence data set and automatically correlates and enriches Splunk data and Splunk Enterprise Security insights and dashboards.

Key Take-aways:

- Seamlessly aggregate, correlate and enrich Splunk data with RiskIQ's Internet Intelligence Graph
- Accelerate investigations and incident response with unparalleled context and intelligence
- Upload indicators of compromise for targeted or bulk enrichment and save results directly within local Splunk indexes.
- Collaborate with peers regardless of their location or interface by following the TeamStream
- Maintain a local index source of enrichment data from investigations for future triage or evidence preservation

Search, Correlate, and Enrich Splunk with the following Data Sets:

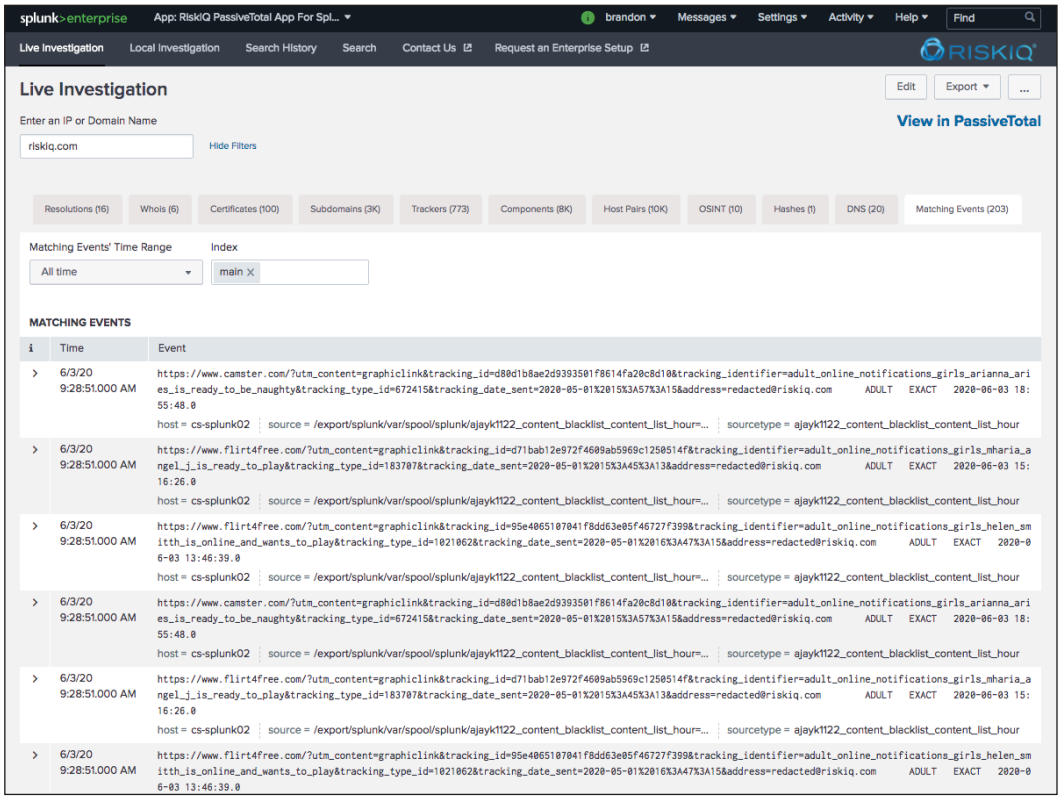
- Passive DNS
- WHOIS
- SSL Certificates
- Web and Social Trackers
- Host Pairs
- Cookies
- DNS Records & Types
- Open Ports & Services

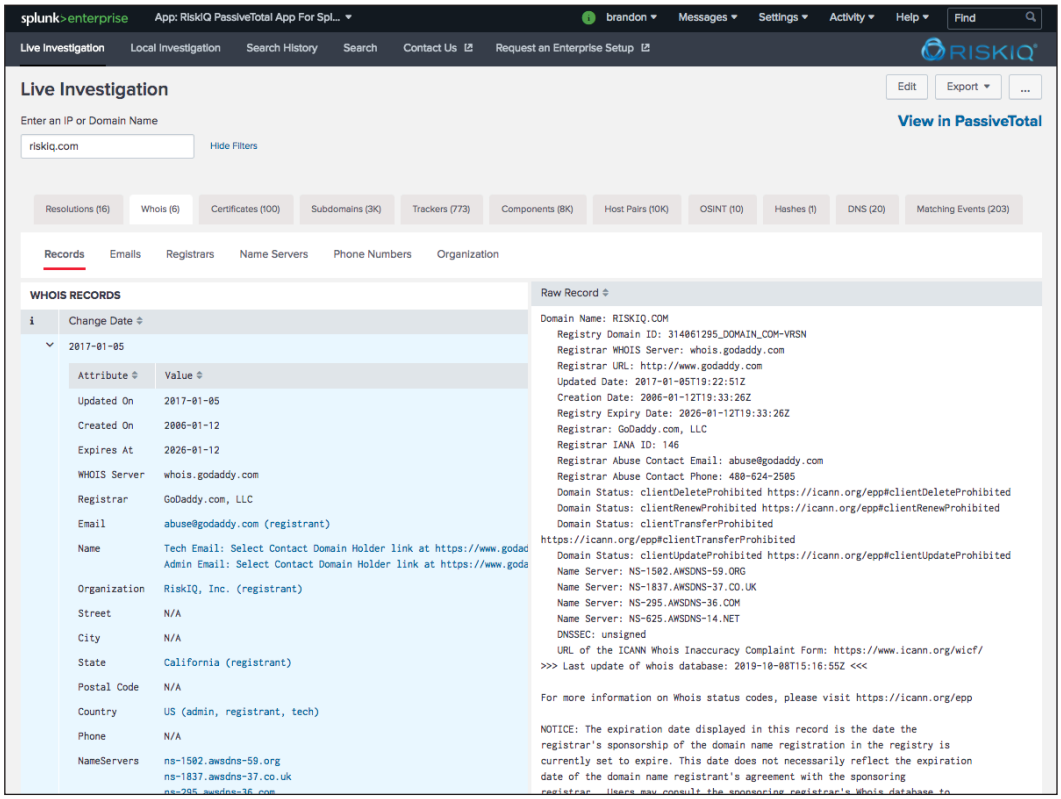
- **Empower Collaboration and Reduce Remediation Time.** RiskIQ PassiveTotal App for Spunk enables enterprise security teams to seamlessly collaborate on threat investigations or incident response engagements by merging and linking internal and external context.
- **Proactively Defend Your Organization from Attackers.** Uncover hidden facets of an attacker's infrastructure, proactively block this malicious infrastructure, and set monitors on branded terms to be alerted when elements are found that may be targeting your brand.

Better Defend Your Organization from Attackers

Threat Infrastructure Analysis is a research process that brings context to incidents and attack campaigns by identifying and linking related entities through multiple data sets, including active and passive DNS, WHOIS, SSL certificates, and other page content attributes. RiskIQ App for Splunk aggregates external threat actor intelligence with internal indicators data into a single platform, so analysts can spend their time focusing on threats, not data collection and correlation.

Screen Shots





About RiskIQ, Inc.

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.

Visit https://www.riskiq.com or follow us on Twitter. Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/

About Splunk, Inc.

Splunk Inc. (NASDAQ: SPLK) turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale. **Learn more: https://www.splunk.com**

RISKIQ

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com