RISKIQ® partnered with splunk>®

RiskIQ Security Intelligence Services Add-on for Splunk

Automated Internet Intelligence and Analytics Enrichment for Splunk

Challenges:

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

Solution: Internet Scaled Insights and Context, Delivered Locally

RiskIQ Security Intelligence Services for Splunk enables security teams to rapidly scale and automate their threat detection programs. The Security Intelligence Services Add-on will automatically ingest and store RIskIQ internet intelligence directly within Splunk, so that it can be applied against local log information.

Integrating Splunk and RiskIQ Security Intelligence Services into a single platform accelerates and automates incident response and investigations. Security teams can quickly identify and block new threat infrastructure that's part of attacks against their organization that they wouldn't otherwise know existed.

Use Cases / Business Value:

- **Automate Threat Detection, Incident Enrichment, and Prevention.** RiskIQ SIS Add-on for Spunk brings the most comprehensive internet security intelligence data set and enables programmatic enrichment of Splunk data to enable automated threat detection and blocking activities.
- **Proactively Defend Your Organization from Attackers.** Programmatically uncover hidden facets of an attacker's infrastructure at scale, proactively block this malicious infrastructure, and set monitors on branded terms to be alerted when elements are found that may be targeting your brand.
- **Generate High-Fidelity Incidents.** RiskIQ Attack Analytics identifies cyber threats and provides customers with filtered lists of known bad hosts, domains, IPs, and URLs to action. These analytics are Based on malicious observations inside of real-time petabytes of internet data sets.

Key Take-aways:

- Accelerate investigations and incident response with unparalleled context and intelligence
- Cross-reference local logs with newly registered infrastructure to identify suspicious activity.
- Identify and automate searching for trends in new, suspicious, and malicious infrastructure at scale.
- Generate high-fidelity security incidents based on blacklist, phish, and scam data.

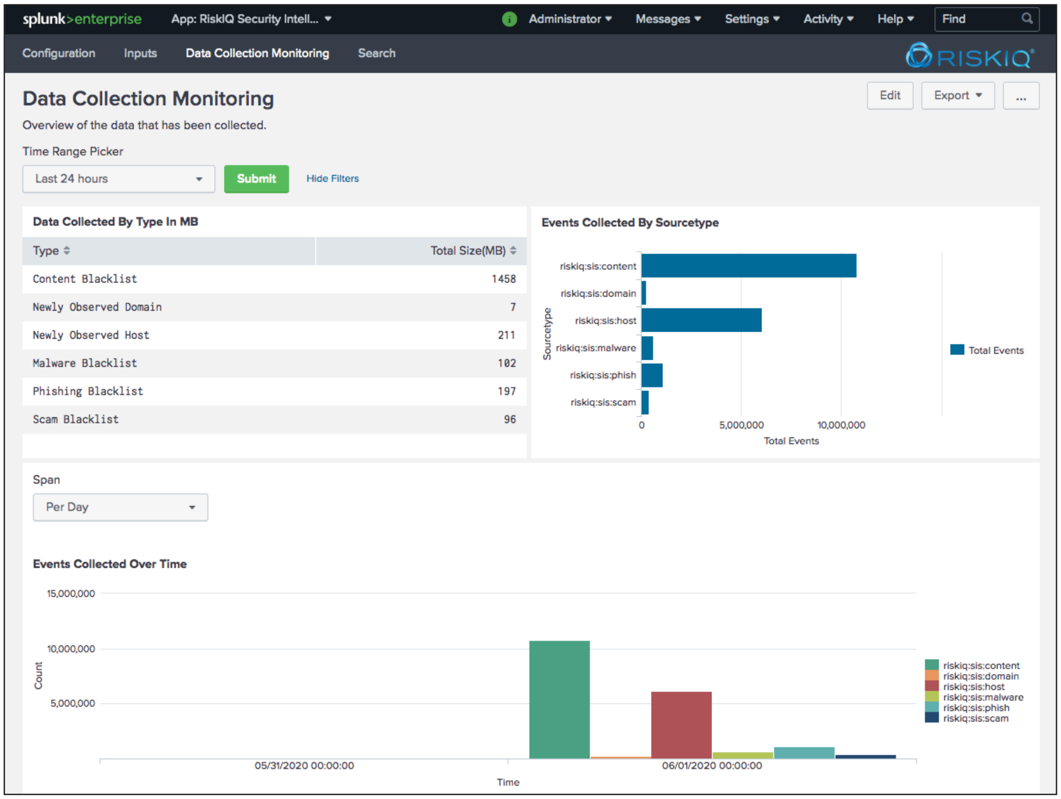
RiskIQ Attack Analytics is a proprietary RiskIQ data set based on malicious observations inside of real-time internet data sets:

- Newly Observed Domains and Hosts
- Blacklist Intelligence—curated lists of known bad URLs, Domains, and IP addresses associated with malware, phishing, and scam events.

Better Defend Your Organization from Attackers

Threat Infrastructure Analysis is the 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 SIS Add-on for Splunk aggregates and automates the enrichment of external threat actor intelligence with internal indicators data and logs, so security teams can automate detection, investigation and research activities and better protect their enterprise.

Screen Shots



Data Collection Monitoring

Overview of the data that has been collected.

Time Range Picker: Last 24 hours

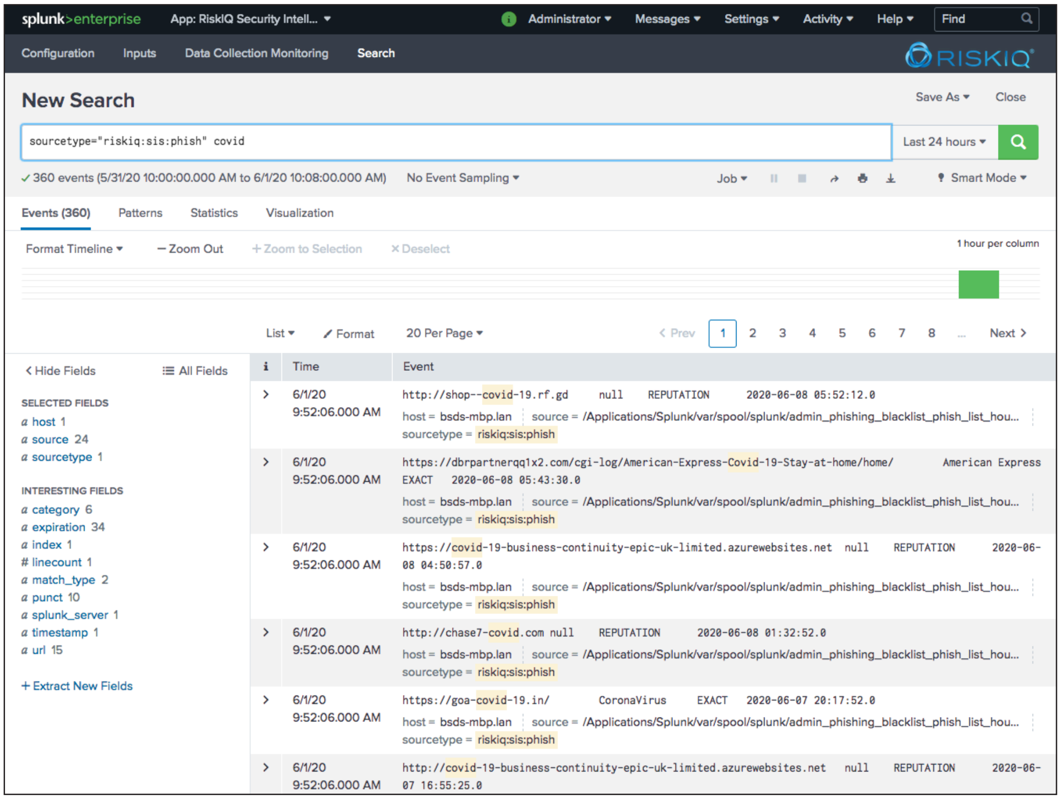
Data Collected By Type In MB

Type	Total Size(MB)
Content Blacklist	1458
Newly Observed Domain	7
Newly Observed Host	211
Malware Blacklist	102
Phishing Blacklist	197
Scam Blacklist	96

Events Collected By Sourcetype

Span: Per Day

Events Collected Over Time



New Search

```
sourcetype="riskiq:sis:phish" covid
```

✓ 360 events (5/31/20 10:00:00.000 AM to 6/1/20 10:08:00.000 AM)

SELECTED FIELDS

- a host 1
- a source 24
- a sourcetype 1

INTERESTING FIELDS

- a category 6
- a expiration 34
- a index 1
- # linecount 1
- a match_type 2
- a punct 10
- a splunk_server 1
- a timestamp 1
- a url 15

```
i  Time                  Event
>  6/1/20                http://shop--covid-19.rf.gd      null     REPUTATION      2020-06-08 05:52:12.0
   9:52:06.000 AM        host = bsds-mbp.lan   source = /Applications/Splunk/var/spool/splunk/admin_phishing_blacklist_phish_list_hou...
                         sourcetype = riskiq:sis:phish
>  6/1/20                https://dbrpartnerqq1x2.com/cgi-log/American-Express-Covid-19-Stay-at-home/home/        American Express
   9:52:06.000 AM        EXACT    2020-06-08 05:43:30.0
                         host = bsds-mbp.lan   source = /Applications/Splunk/var/spool/splunk/admin_phishing_blacklist_phish_list_hou...
                         sourcetype = riskiq:sis:phish
>  6/1/20                https://covid-19-business-continuity-epic-uk-limited.azurewebsites.net  null     REPUTATION      2020-06-
   9:52:06.000 AM        08 04:50:57.0
                         host = bsds-mbp.lan   source = /Applications/Splunk/var/spool/splunk/admin_phishing_blacklist_phish_list_hou...
                         sourcetype = riskiq:sis:phish
>  6/1/20                http://chase7-covid.com null     REPUTATION      2020-06-08 01:32:52.0
   9:52:06.000 AM        host = bsds-mbp.lan   source = /Applications/Splunk/var/spool/splunk/admin_phishing_blacklist_phish_list_hou...
                         sourcetype = riskiq:sis:phish
>  6/1/20                https://goa-covid-19.in/         CoronaVirus     EXACT    2020-06-07 20:17:52.0
   9:52:06.000 AM        host = bsds-mbp.lan   source = /Applications/Splunk/var/spool/splunk/admin_phishing_blacklist_phish_list_hou...
                         sourcetype = riskiq:sis:phish
>  6/1/20                http://covid-19-business-continuity-epic-uk-limited.azurewebsites.net   null     REPUTATION      2020-06-
   9:52:06.000 AM        07 16:55:25.0
```

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

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com