RISKIQ®

Think Outside the Firewall™

# RiskIQ SIS™ (Security Intelligence Services)

## Real-time Access to Critical Security Data Sets

### Features

- Programmatic access to petabytes of internet-scale data from RiskIQ
- Diverse data set offering to bring context to incident response and investigations
- Extensible API to enrich security tools and support high volume queries

### Benefits

- Accelerate time-to-response to threats with automated enrichment
- Access RiskIQ data & intelligence from inside other security tools

As cyberattacks against your organization increase, it's more important than ever to have a security program built on robust and reliable data to enrich your analysis and inform your decision-making process. RiskIQ offers our world-class intelligence and vast, internet-scale data sets to organizations for integration directly into the security systems already in use, whether they're commercial SIEM solutions or custom-built platforms. Having direct, high-volume access to this intelligence and data allows for programmatic defense against threats to your environment.

Using RiskIQ SIS™ (Security Intelligence Services), security teams can automatically enrich security alerts and events, and automatically provide information to orchestration platforms for proactive blocking of digital threats.

## Internet Data

As attacks against your organization increase, it's more important than ever to have a security program built on robust and reliable data to enrich your analysis and inform your decision-making process. RiskIQ offers the ability to ingest critical security data at scale programmatically


### PDNS

Passive DNS (PDNS) is a system of record that stores DNS resolution data for a given domain or IP address. This historical resolution data set allows analysts to view which domains resolved to an IP address and vice versa.

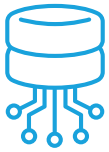
RiskIQ offers API access to our passive DNS repository in multiple ways to provide analysts with the ability to correlate domain and IP address overlap.

### SSL Certificates

SSL certificates are files that digitally bind a cryptographic key to a set of user-provided details and assist in providing security when transmitting information over the internet. These certificates should be self-signed by a third-party to verify their authenticity, but they can be self signed by malicious actors. Beyond just securing data, certificates can be used to encrypt data sent between command and control servers and machines infected with malware.

### WHOIS

WHOIS is a protocol that lets anyone query ownership information about a domain, IP address, or subnet. RiskIQ has a vast repository of WHOIS data which is available to query for registrant information.



### Derived Crawling Data

Our derived data sets provide customers with insight into web page attributes and associations based on RiskIQ's vast crawling infrastructure and can provide security analysts with new data sets through which to investigate and track attacks to their organizations. These data sets include:

- Website attributes and component metadata
- Host pair associations
- Cookie names

## Attack Analytics

RiskIQ Attack Analytics, a proprietary RiskIQ data set, is based on malicious observations inside of real-time internet data sets. As attacks evolve and propagate outside of your network, RiskIQ behavioral analytics identifies cyber threats and provides customers with filtered lists of known bad hosts, domains, IPs, and URLs.


### Newly Observed Domains and Hosts

Threat actors often use different domains and hosts for their attack campaigns programatically. These entities could be hosting phishing sites, distributing malware, or acting as part of a larger malicious campaign. Therefore, newly observed data sets can serve as a guide to whether a domain or host is legitimate or not.

RiskIQ provides customers with domain and host intelligence in the form of a list of domains and host observed resolving to an IP address for the very first time in our Passive DNS repository.

### Blacklist Intelligence

RiskIQ ingests and aggregates blacklist feeds from internet service providers, phishing solutions, fraud prevention, and other internet security organizations to consolidate and further enrich our proprietary blacklists.

Our blacklist intelligence is built off of this ingestion and analysis delivering curated lists of known bad URLs, Domains, and IP addresses associated with malware, phishing, and scam events.

Additionally, our content blacklists offer customers an easy way to block employees from visiting undesirable sites on the internet.

## Common Use Cases for RiskIQ's Security Intelligence Service

### Enrichment

Enriching data from security incidents, events, or research projects to gain a deeper understanding or context of a threat.

### Proactive Blocking

Ingestion of content into blocking systems such as firewalls, DNS servers, or proxies to inform detection.

### Threat Hunting

Filtering down a large set of data to known malicious activity or that which is associated with something known as bad.

### Custom Integrations

Bringing Internet and attack analytics data into existing security solutions through integrations or custom development.

RISKIQ®

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

**Learn how the RiskIQ could help protect your digital presence by scheduling a demo today.**

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ

Copyright © 2018 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 11_18

The only warranties for RiskIQ products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. RiskIQ shall not be liable for technical or editorial errors or omissions contained herein.