Scale Threat Response, From One to Thousands

Unmask adversary-threat infrastructure, anywhere on-demand

Cybercriminals, hacktivists, and nation-state threats all evolve tactics, techniques, and procedures (TTPs) to improve their malicious capabilities. However, adversary behaviors change continuously—malware variants, distribution and alliances, zero-day leaks, and tooling. These ongoing changes prevent long-lasting protection that can scale to cover the enterprise's digital footprint.

Sustainable, scalable cyber defense comes from fingerprinting adversary-threat infrastructure and observing malicious systems relevant to the enterprise's digital attack surface.

Whether threat infrastructure is associated with one threat actor or used by thousands of adversaries (e.g., kits, C2, leaked tools), security teams require high-fidelity security intelligence to find and eliminate threats with confidence.

Highlights | RiskIQ Illuminate®

- 10+ years of digital history and tracking the global attack surface.
- Dynamic risk and reputation scoring based on real-world observations.
- Multi-factor threat fingerprinting via crawling, registry, history, and OSINT.
- Automate downstream playbooks with easy reputation APIs and on-demand threat observations..
- Elastic defense for continuous change: external threats and your attack surface.

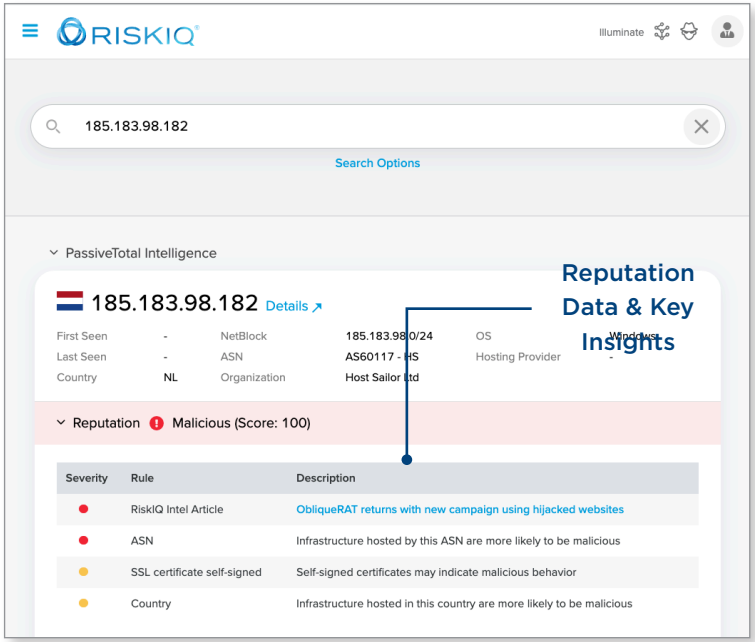
SCENARIO: From One to Many

Active and historical, real-world observations

Simply gathering intelligence from open sources or network telemetry and antimalware is not enough to solve the current security challenge to unravel what is you from what is another, what's good from what's malicious, and adversaries from allies. Relevant, actionable intelligence lets you personalize real and vital threats to you.

With the rise of remote workforces, digital supply chains, and global networks, the time could not be more advantageous for threat actors to create and distribute remote access trojan (RAT) malware.

Digital growth and change have allowed RATs to proliferate while hiding in plain sight.



https://community.riskiq.com/research?query=185.183.98.182

THREAT: ObliqueRAT

Fingerprint Adversaries, Digital Trace Analysis

You discover a machine infected with a redesigned malicious remote access trojan (RAT) named ObliqueRAT, likely related to a new campaign cited by Talos. However, the new RAT variant is delivered via adversary-controlled websites.

These websites, created for RAT development and distribution, are packed with privacy controls and have no known history on the internet. Cisco Talso published four indicators, one IP address, and three domains:

- 185[.]183.98.182
- Larsentobro[.]com
- Micrsoft[.]ddns.net
- yepp[.]ddns.net

INVESTIGATE: Remote Access Trojan (ObliqueRAT)

Dynamic reputation scoring for rapid triage and impact analysis

Quickly determine paths of investigation via dynamic reputation scoring and priorities based on the global attack surface.

ObliqueRAT was reported to be associated with the IP address 185[.]183.98.182 (seen above).

Search the IP address to see the most current reputation. The reputation for the IP address related to ObliqueRAT, 185[.]183.98.182, results as ***Malicious*** with high confidence of 100.

The malicious IP address had privacy controls concealing information from registries, such as WHOIS. However, the malicious IP shows relationships to other threat indicators found in open-source intelligence (OSINT), including system-generated certificates and host country.

Insights

Privacy controls prevent tracking IP address details via registries (e.g., WHOIS).

RAT malware is a widely distributed threat utility, nearly certain to be found within other IP addresses and domains.

Common names and system-generated SSL certificates are effective sub-IP threat indicators.

Actions

Leverage reputation scoring based on identifiers below the IP-layer, such as SSL certificates and history.

Track and trace malicious infrastructure changes, capabilities, and activity.

Extract related infrastructure and digital fingerprints embedded in internet telemetry.

Apply expanded threat intelligence to global defenses.

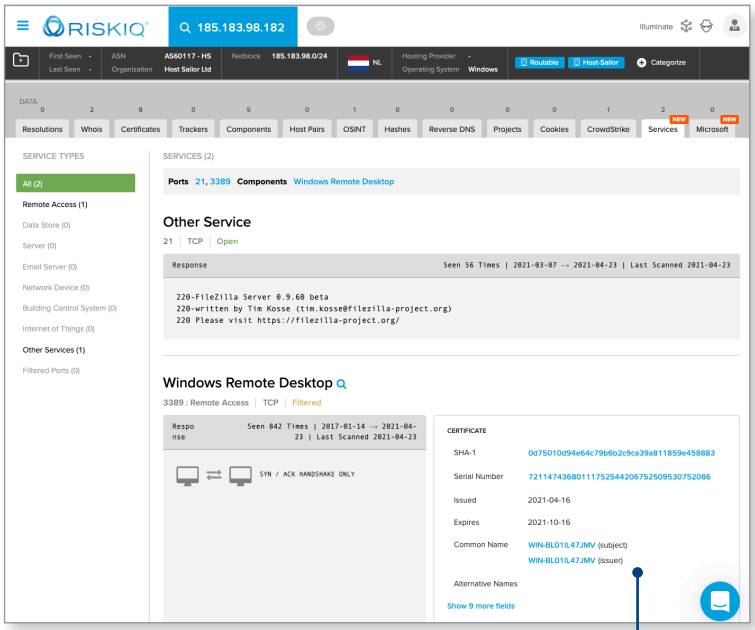
Automate downstream playbooks and workflows for elastic protection coverage—from a single threat actor to thousands.

Observations showed IP address 185[.]183.98.182 running Windows Remote Desktop Service along with a system-generated certificate containing the hostname WIN-BL01IL47JMV.

The hostname was then found to be related to dozens of malicious IP addresses and hundreds of domains. Enterprise security teams can uncover adversary-threat infrastructure for high-impact investigations and response from a single alert and indicator.

AUTOMATE: Threat Indicators, Protection

Examining the SSL Certificate History on the IP address, we can see two different several self-signed certificates and two unique hostnames WIN-BL01IL47JMV and WIN-UNIEC1PV56D, demonstrating an infrastructure overlap and a lead to new related indicators.



Services
Key Insights
Issue Date & Hostname

https://community.riskiq.com/search/185.183.98.182/services

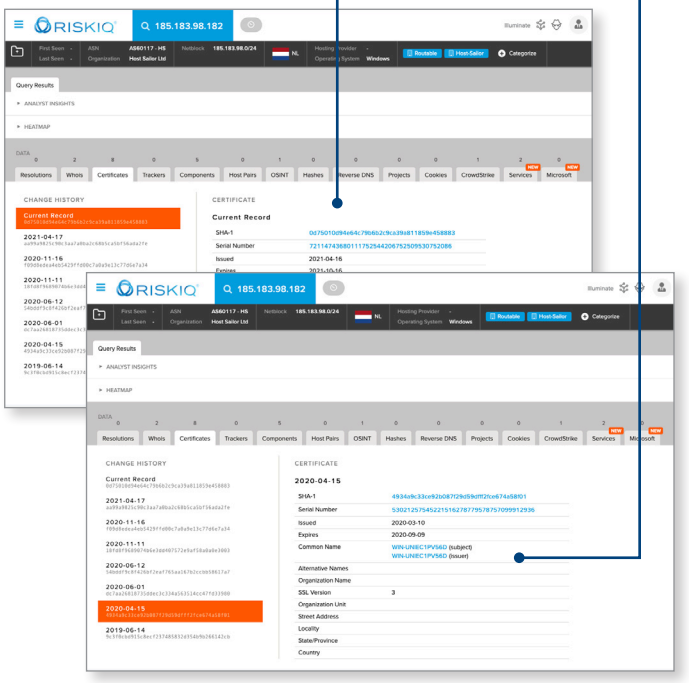
RELEVANCE: Attack Surface Intelligence

Active and historical discovery for complete visibility

Attack surface intelligence identifies and distinguishes resources and digital systems across the open and closed web

Security intelligence that combines attack surface insights with real-world observations of RAT malware enables a more impactful response.

System-generated Certificates with Related Hostname



https://community.riskiq.com/search/185.183.98.182/certificates

*Security Impact Score based on required cybersecurity expertise, investigation time, and scope of protection attained.

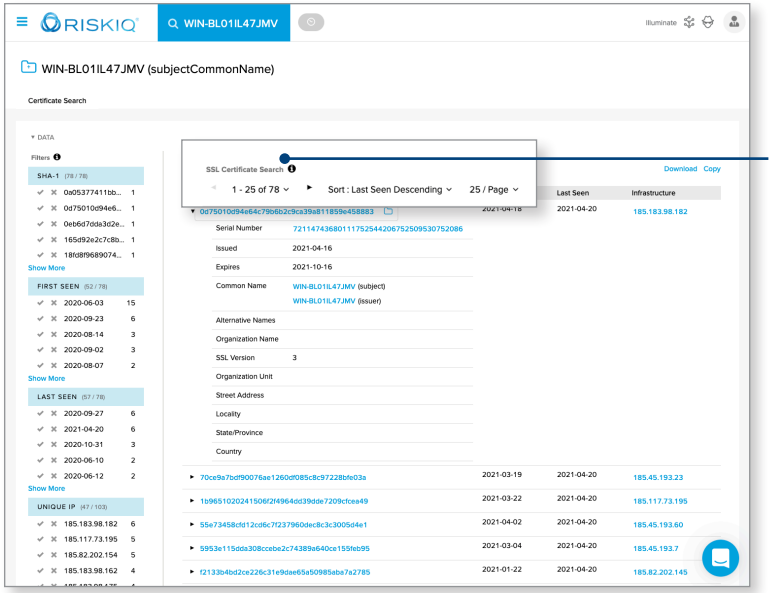
Results

Starting with a single IP address from an open-source article, uncovered:

- Adversary infrastructure, RDP
- SSL certificate-based identifiers
- 100+ additional IP addresses
- 1,000+ additional domains
- Continuously updated controls

SECURITY IMPACT SCORE

89*

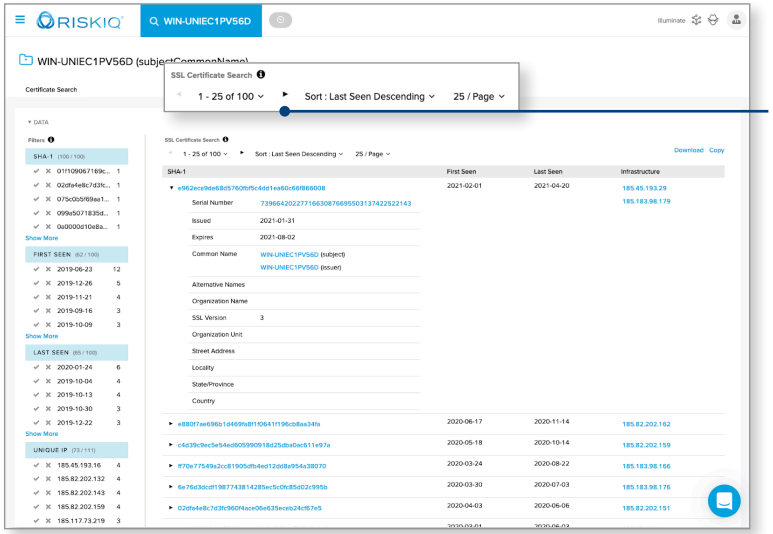


78 IP addresses are linked to hostname WIN-BL01IL47JMV. Each IP address will lead to additional hostnames and new IP addresses

https://community.riskiq.com/search/certificate/subjectCommonName/WIN-BL01IL47JMV

VISIBILITY: Finding New Related Infrastructure

Each Pivot in the self-signed certificate common name issuer hostname leads to new IP addresses. Each new IP address leads to new related self-signed certificates with new unique hostnames contained in the common name issuer.



100 IP addresses are linked to hostname WIN-UNIEC1PV56D. Each IP address will lead to additional hostnames and new IP addresses

https://community.riskiq.com/search/certificate/subjectCommonName/WIN-UNIEC1PV56D

SCENARIO: From One to Many

Scaling Threat Investigations

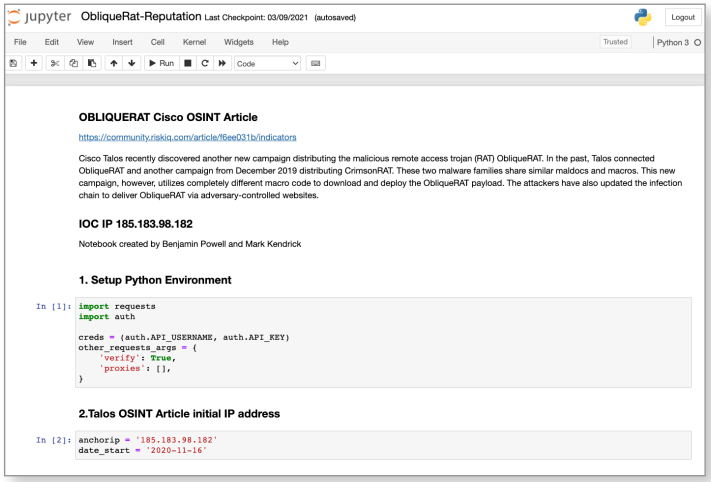
Speed and repeatability are key to investigations. Many Cyber Threat Investigators utilize scripts and API to perform multiple tasks in series to get accurate, repeatable results.

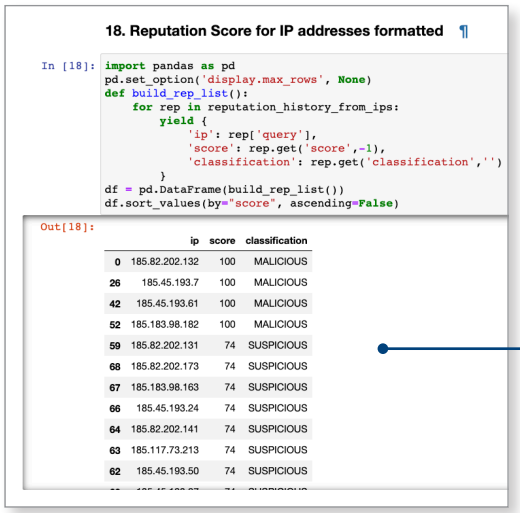
AUTOMATE: Threat Indicators, Protection

By understanding the manual process of this investigation script can automate the investigation.

Steps:

1. Start with IP address
2. Find all self-signed Certificate
3. Search on the common name issuer hostnames
4. Find all IP addresses associated with common name issuer.
5. Repeat until no new unique IP address or Common Name issuer hostnames appear.
6. Then determine the reputation score for each unique IP address and unique domain.





Over 90 Unique IP addresses were discovered all had a dynamic reputation score of Malicious or Suspicious

After just 3 degrees of separation from the initial IP address, these hostnames were found in self-signed certificates:

WIN-BL01IL47JMV
WIN-UNIEC1PV56D
WIN-BVLRV1JQS28
WIN-U2QBNCSEVVG
WIN-MJPCIGVK17I
WIN-BJ8C2GA1PMK
WIN-host2000-95
WIN-FKLITKTLLT2
WIN-4KL5DI6AHGP
WIN-VL36D5H5VCA
WIN-6O9C3GCCMMI
WIN-0VAE1841EL4
WIN-UNIEC1PV56E

Over 1900 Unique domains were discovered over 576 had a dynamic reputation score of Malicious or Suspicious

Scripts can be run any time to find new up-to-date indicators that can be used in your organization's SIEM to SOAR, EDR to MSSP.

RiskIQ Illuminate SecOps Intelligence—API Based Module

RiskIQ's SecOps Intelligence module provides unique insights and security information suited for easy integration with SIEMs and other security unified management platforms. Security professionals using SecOps Intelligence integrated into their single pane of glass system use RiskIQ reputation information to distinguish friend from foe and identify items to be escalated for further investigation.

Users have access to RiskIQ Intelligence & Reputation Data as easy-to-integrate feeds and simple APIs for use in SIEMs and other security management solutions. RiskIQ leverages our research-assisted artificial intelligence and machine learning profiling to frequently updated feeds and markers for reputation scores to deliver actionable intelligence at scale.

The use of this module significantly boosts the accuracy of a team's event review and reduces the time to either dismiss or escalate these events by leveraging our reputation scoring data. Users also have access to our PassiveTotal community platform, enabling teams to quickly pivot through 10+ years of historical data for additional investigation.

The SecOps Intelligence module enables teams running day-to-day security operations, including Operations Center and Detection & Response teams, to easily access the most up-to-date security information in the industry. It assists analysts in making fast and efficient decisions when reviewing security events.

API-Based Integrations:

The SecOps Intelligence module also provides a single API to streamline an organization's efforts across multiple platforms. RiskIQ provides a reputation score via the easily integrated API to reveal insights, including relationships to known exploits or hacker activity.

Furthermore, SecOps Intelligence users will have access to RiskIQ's Splunk application that supports our reputation data.

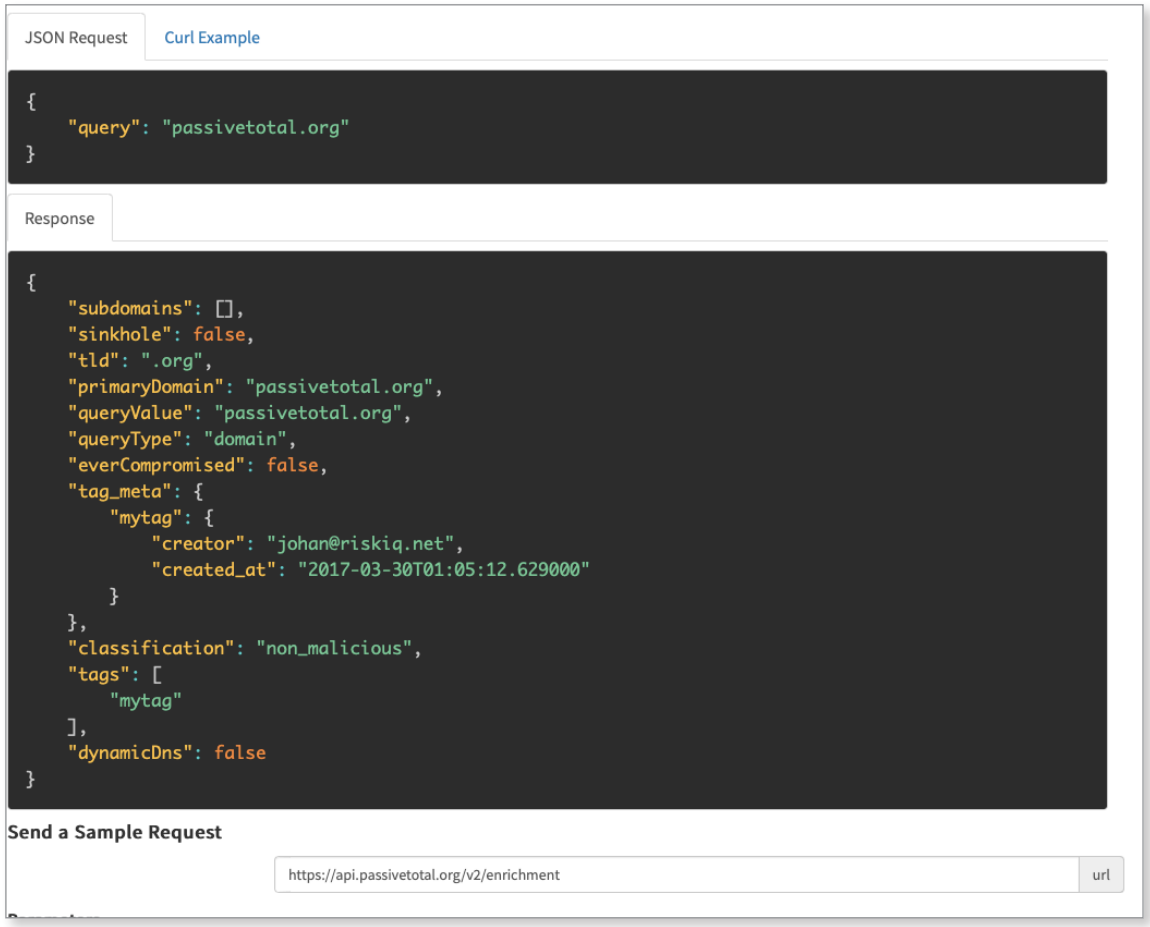
Organizations can use this alerting feature to proactively block malicious infrastructure within their environments, providing better situational awareness and reducing possible exposure to future attacks.

Key Features

- Enrichment feeds via Amazon S3 bucket
- Newly observed domains act as a layer of protection
- Newly observed hosts act as an added layer of protection against quick attack campaigns
- Malware and phishing with feed-based information
- Reputation data and key insights with rating and key contributing factors
- Easily integrated API based entity reputation score lookups

Example Illuminate API Request

https://api.passivetotal.org/index.html



Get Enrichment Data For A Query

Python wrapper for RiskIQ PassiveTotal API

https://pypi.org/project/passivetotal/

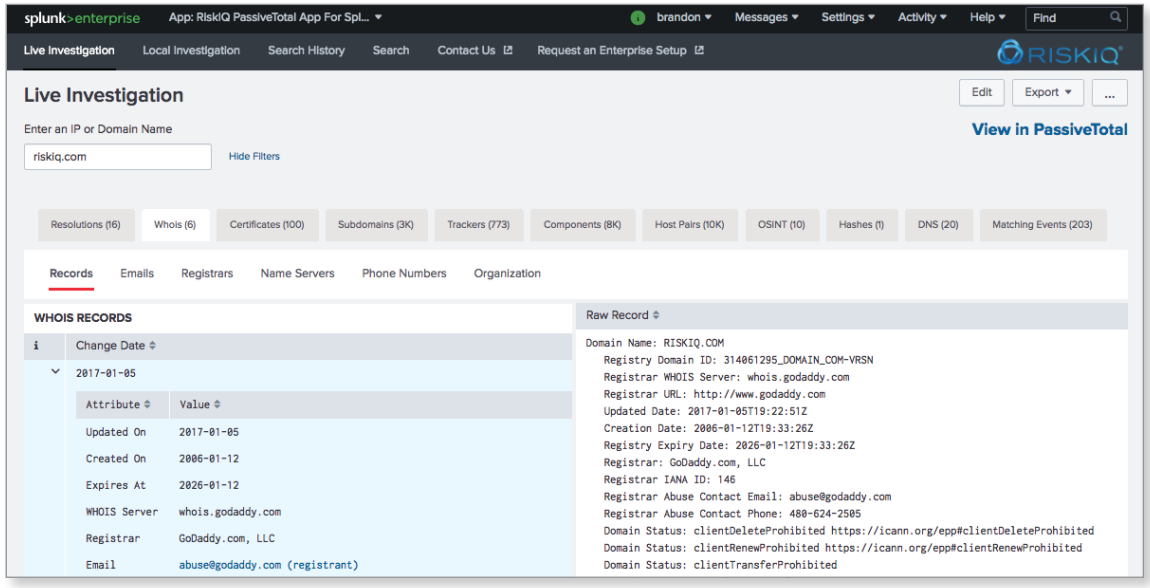
https://passivetotal.readthedocs.io/en/latest/

Key Benefits

- No new process changes or context switching, just enhanced capabilities
- No new tools, easily integrated
- Save analysts unnecessary work and scale their techniques
- Research is saved and correlated
- Turn a one-time hunt into a detection capability
- Respond proactively with precision-targeted detection logic

Vendor-agnostic flexible APIs and apps, and co-development with Interlock Partners

A web interface option with API access available to companies and their support teams is extremely handy when investigating detected events. In-app mitigation workflow, along with continuous monitoring of online resources, lets companies quickly take action, know when threats have been successfully remediated, and track event lifecycle metrics to report on threat response efficiency.



Splunk Integrations with Illuminate API

Integrations Key Benefits

- Automatically triage every indicator found within your Splunk logs to drive alert creation and further Internet enrichment using RiskIQ Illuminate SecOps Module.
- Enhance the security ecosystem—people, processes, and technologies
- Maximize investments and enable attack surface awareness throughout the security stack
- Future-proof digital risk and threat programs with intelligent systems, technologies, and partnerships

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com