DATASHEET

SECURITY INTELLIGENCE SERVICES

Real-Time Access to Critical Security Data Sets

RISKIQ®

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 their environment.

PASSIVE DNS

Enhance your understanding of an attack with historical resolution data

What is it?

DNS works like a contact application for the internet. Instead of having to remember IP addresses for all the websites you wish to access, DNS makes them available using domain names, which are easier to remember and less likely to change.

Passive DNS 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.

How it can help

Passive DNS data can provide analysts insight into how a particular domain name or IP address changes over time and enables them to identify other related domains/IP addresses. When researching a suspicious or malicious event, PDNS data can provide context to an attack or additional malicious domains/IP addresses.

How to use it

- Indicator of Compromise correlation
- Historical resolution lookups
- Time-based analysis
- Fully qualified domain name lookups
- SIEM event enrichment
- Domain or IP enrichment to proactively hunt for threats

WHOIS

Registration-based correlation expands knowledge of the adversary

What is it?

Thousands of times a day, domains are bought and transferred between individuals, and domain registrants must provide information about themselves when registering one. This information gets stored in a WHOIS record associated with the domain.

WHOIS is a protocol that lets anyone query for 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.

How it can help

Attackers need to establish infrastructure to conduct their attack from and communicate with their malware. WHOIS data can provide an organization with insight into who is behind an attack campaign. Using domain registration information, an organization can unmask an attacker's infrastructure by linking a suspicious domain to other domains registered using the same or similar information.

How to use it

- Identify additional domains registered using similar information
- Determine the maliciousness of a given domain or IP address based on ownership records
- SIEM event enrichment
- Domain enrichment to proactively hunt for threats

SSL CERTIFICATES

Uncover new attack infrastructure using certificate hash and facet overlap

What is It?

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 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.

How it can help

Threat actors often use similar information across different SSL certificates for their various infrastructure. RiskIQ collects SSL certificate data as we crawl the internet, and we can correlate malicious certificates we find with their signatures.

How to use it

- Determine if a domain or IP address is legitimate based on certificate
- Identify self-signed certificates vs. third-party certificate authority
- Identify IP clusters based on shared certificates
- Identifying additional certificates of interest based on shared properties
- Surface connections among subject alternate names for certificates

NEWLY OBSERVED DOMAINS

Identify malicious domains as soon as they appear

What is It?

Newly Observed Domains, the first of our attack analytics feeds, is a proprietary enriched RiskIQ dataset containing newly resolving domains.

RiskIQ's continually updated Newly Observed Domains provides customers with near real-time intelligence of domains seen for the first time in our passive DNS repository.

How it can help

Threat actors often programmatically use different domains for their attack campaigns. These domains could be hosting phishing sites, distributing malware, or acting as part of a larger malicious campaign, therefore newly active domains can serve as a guide to whether a domain is legitimate or not.

Organizations can proactively defend their enterprise against emerging cyber threats by blocking newly observed domains for a specified time period based on policy and risk tolerance.

How to use it

- Proactive blocking of domains

ABOUT RISKIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 80 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, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures. Visit RiskIQ.com or follow @RiskIQ on Twitter.