RiskIQ and SIEM

AUTOMATED CONTEXT YIELDS LOWER MTTR

As digital transformation drives more systems online, more information about the systems and activities of their users are available for research through security information and event management (SIEM) tools. This creates a huge burden on analysts as they now have much more data to sift through during their investigations. These tools are not intelligent by design, and most alerts and events require manual review by security analysts.

With more than 80% of attacks originating from digital threats outside the firewall, security teams need more context than just the data provided by SIEMs about the systems on their own network. External context is critical to determining if an event is a true threat or a false positive. This context is provided by RiskIQ and improves the efficiency of security and analyst teams and reduces their mean time to remediation (MTTR).

BENEFITS

Consolidate and Accelerate

Consolidate threat research data sets like passive DNS, current and historical WHOIS information, SSL certificate information, and website metadata that can connect threat infrastructure. This improves analysts' MTTR and proactive defenses.

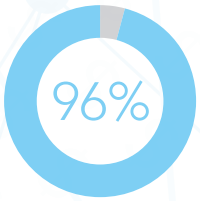
Know What You Own

On average, RiskIQ surfaces 30% more digital assets outside the firewall than what organizations think they own. That means they have a broader attack surface and higher digital risk than they might think. Unknown—and thus unmonitored—external assets are some of the most exploited attack vectors by cyber criminals.

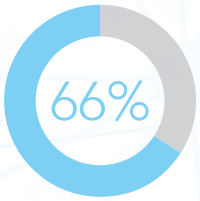
Stay Alert

RiskIQ continuously crawls your digital assets, immediately alerting on changes made to the assets, registrations, and resolutions that could indicate compromise or attack. Notifications can occur both in-platform and via alerts into your SIEM.

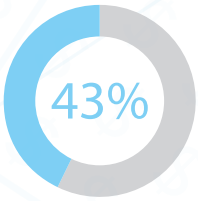
LACK OF CONTEXT RAISES RISK



The amount of malware alerts that aren't investigated.[1]



Time wasted by security analysts evaluating faulty intelligence (malware alerts)[2]



Security professionals that state that they have insufficient staffing to support the security workload[3]

1 http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf
2 http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf
3 http://info.mapr.com/rs/mapr/images/EMA-evolution-data-driven-security.pdf

1 + 1 = 3: ENRICH YOUR SIEM WITH RISKIQ TO YIELD ACTIONABLE INTELLIGENCE

The RiskIQ External Threat Management platform provides the enrichment necessary to help analysts using a SIEM to make intelligent, informed decisions about alerts and cybersecurity events.

When an alert is triggered in the SIEM, an analyst is assigned to investigate whether the event should be confirmed or dismissed as a false positive. This step requires additional data about why the system detected the anomaly, what the source was, whether the source is connected to known-malicious activity, and other infrastructure that may be related to this event.

RiskIQ PassiveTotal provides comprehensive investigation capabilities that allow analysts to pivot between the most extensive internet data sets to understand if the infrastructure flagged by an alert is related to malicious actors or threat actor groups. Once you understand the context of a single event, you can also pivot to find other, seemingly unrelated infrastructure and proactively block that, as well.

Using data sets that include passive DNS resolutions, current and historical WHOIS registrant information, SSL certificate information, as well as other web infrastructure components like analytics tracking codes, PassiveTotal provides intelligent pivots and searches that can identify threat actors, as well as uncover additional infrastructure that they may use to conduct attacks.

These data sets can be integrated into your SIEM using RiskIQ APIs, allowing for automatic enrichment of events. This improves prioritization and efficiency when investigating alerts, and allows teams to accurately address more alerts in less time.

In addition to PassiveTotal data sets, RiskIQ External Threat Detection provides additional insight into SIEM alerts through our vast databases of dangerous URLs, phishing pages, blacklisted hosts and domains, known malware hashes, and more. These are also accessible via the RiskIQ platform or API.

RISKIQ OFFERS OUT-OF-THE-BOX INTEGRATIONS AND AN EXTENSIVE API

The value of a SIEM is in its ability to ingest and correlate data from multiple data sources. That's why we provide out of the box apps for IBM QRadar and Splunk that allow direct connection to RiskIQ data sets. In addition, the platform is built on RESTful APIs for easy integration with custom-built internal systems.

QRadar®

splunk>

MALTEGO

www.riskiq.com | info@riskiq.com | +1.888.415.4447