5-Questions Security Intelligence Must Answer:

How to Build Security Resilience in a New Age of Cyber Threats

2020 | October

Organizations have been growing their digital presence online and migrating their infrastructure to the cloud, outside the friendly confines of their firewall and other network security controls. This digital transformation has grown the enterprise digital attack surface and dramatically broadened the spectrum of threats and vulnerabilities that can affect the average organization.

Sophisticated APTs and low-level cybercriminals alike threaten businesses' safety, targeting their data, IP, systems, and people. Today, 375 new threats emerge each minute. Security teams must have the intelligence necessary to defend their organizations from a vast universe of threats, some of which traverse their network, many that don't.

Unfortunately, this digital complexity makes informed security decision-making an immense challenge. To able to defend their business successfully, the enterprise must be able to proactively address this changing threat landscape, using intelligence to answer the following questions:

1. Where are the weaknesses in my attack surface?
2. Where should I focus my resources to keep pace with digital growth?
3. Which threats are relevant to my organization?
4. Where is an active attack coming from?
5. How can my security programs be more resilient?

In this whitepaper, we'll frame the challenges of effective threat intelligence and focus on answering these five questions.

Security Intelligence: A Unique Challenge

The modern threat landscape can be overwhelming for security teams, most of which lack the security intelligence they need to make informed decisions about protecting their organizations. This intelligence exists and is readily available, but it's hidden amid a deluge of confusing, irrelevant intelligence - seemingly infinite static with no discernible relevance, uniformity, or consistency to any individual organization.

To successfully find what they need and get value from security intelligence, there are three main challenges security teams must overcome:

1. A LACK OF RELEVANCE AND AN ADEQUATE UNDERSTANDING OF THREATS AND ATTACKERS

Every organization is unique. The type of business they are, the infrastructure they use, and how they interact with the internet affect how they may be vulnerable and how actors will target them.

Becoming an expert in the motives, tactics, and tools threat actors use against organizations similar to yours will help counter them. Further, having quick, immediate access to the IOCs from attacks against similar organizations can help you block attacks against yours.

2. NEARLY INFINITE BREADTH AND DEPTH OF ATTACK PATHS, WEAKNESSES, AND RELATIONSHIPS

Every organization is unique, with a unique, complex, and sophisticated digital footprint that's susceptible to particular vulnerabilities and attacks. These enterprise-specific attributes—geographic locations, asset mixes (people, technology, and third-parties), alert volume, and team composition—are not easily accounted for. Worse, they can result in significant enterprise security and compliance gaps.

3. COMPLEX SECURITY AND RESPONSE DECISIONS AND PROCESSES WITH MANY PERSONAS AND GROUPS

Security decisions are complex within the enterprise organization, requiring multiple constituencies, including but not limited to boards of directors, shareholders, c-level executives, security leadership, business unit and brand leadership, general IT and systems management staff, and more.

Achieving risk-based standards for threat investigation and response processes is critical. Yet, there is a lack of relevant intelligence and evidence to inform and unify decision making with objectively appropriate actions. What's more, the most relevant cyber threat information is compartmentalized in different data silos and sources across a typical organization—teams, logs, OSINT, and various feeds—creating significant enterprise security and compliance gaps.

Five Questions Leading to Security Intelligence Mastery

Question 1: Where are the weaknesses in my attack surface?

Every threat program must consider the likely outcomes of dramatically different cybersecurity situations. Understanding their wide-ranging exposures and knowing which threat actors are most likely to affect them are difficult tasks, but foundational to cybersecurity success.

SOLUTION: QUESTION, ANSWERED

Knowing what makes up your organization's attack surface—all the internet-facing assets outside the firewall and in the cloud—is step one to keeping it safe. This visibility is vital for the whole enterprise and should inform all strategic goals and initiatives.

However, knowing how attackers could target your organization, and others like it, provides the additional context needed to eliminate blind spots and prevent exposures from being exploited. Having a handle on exposures, attack paths, reputations, and access controls across an organization's attack surface puts the enterprise in the driver's seat, especially as their digital presence grows to meet business demands. This knowledge is also the basis for supercharged incident response and vulnerability management.

RiskIQ draws from an 11-year history of the internet and its connectedness over time to deliver the security intelligence necessary to detect and respond to cyberattacks and identify your attack surface with astounding precision.

SUCCESS CRITERIA

- Identify cyber attackers and indicators of their activities.
- Pinpoint attacker tools and infrastructure and determine their targets and tactics.
- Discover attacker-exposed assets, correlate with the probability of compromise.

Question 2: Where should I focus my resources to keep pace with digital growth?

Digital transformation has accelerated over the past decade and went into hyperdrive as the COVID-19 pandemic hit. Almost overnight, workforces and business operations decentralized and dispersed worldwide, widening protection gaps and introducing scores of new remote access points, perimeter devices, and digital infrastructure. IT had to set up new systems, new access points, and new channels quickly to enable remote employees and increase online interaction with customers. Much of this new infrastructure will remain in place long after the pandemic subsides as organizations re-evaluate their policies on flexible working and address revised consumer expectations.

As a result, attackers now have far more access points to probe or exploit outside most security teams' purview. Users, apps, brands, customers, partners, employees, and infrastructure are all open to attack—and unfortunately, the protections needed for each of these digital asset classes are different for each organization.

How do you keep pace with these rapid digital changes and put the security policies and controls in place that block determined attackers that are becoming more numerous and more sophisticated each day?

SOLUTION: QUESTION, ANSWERED

With a deep and broad understanding of third-party risks, enterprises can make better decisions and reduce the uncertainty of their organization's third-party dependencies. RiskIQ embeds insights from over ten years of security intelligence on third parties—IP and non-IP resources, hosts and host-pairs, apps, pages, ports, data, transport, content, components, and code. We already mapped it all, so nothing stays hidden. RiskIQ's Community and Enterprise threat indicators give customers rapid awareness of attackers and the relevant infrastructure between them, streamlining security controls, prevention, and protections by infusing them with accurate and timely threat intelligence. RiskIQ also aggregates threat indicators and continuously enhances them with curated and corrected open-source intelligence (OSINT) and proprietary research from RiskIQ Labs.

SUCCESS CRITERIA

1. Patented Infrastructure Chaining, observations
2. Automated Data Assembly
3. Curated OSINT
4. In-Product Human Intelligence (HUMINT)
5. One-click Search, Indicator Assembly

Question 3: Which threats are relevant to my organization?

Although the future is unknown, we can make reasonable guesses and be more confident in our decisions by observing history and noting where, when, how, and how often threats occur, helping us build a probability of the same event happening again. Having threat intel that shows where similar organizations are vulnerable, how they're attacked, and by which actors spotlights the threats that are most relevant to an organization. However, this exercise requires knowing the internet's history.

Unfortunately, most enterprise security teams lack the relevant history and data artifacts to confirm suspicions or create models to predict what will happen in different scenarios. Without a clear view of past exposures, exploit tendencies, shifting infrastructure, system behavior, and targets compromised, security teams are left with an unclear view. In this case, preventative models and plans are mere guesswork.

SOLUTION: QUESTION, ANSWERED

For more than ten years, RiskIQ has been crawling and absorbing the internet to define the web's identity and composition by fingerprinting each component, connection, service, IP-connected device, and infrastructure to show customers how they—and attackers targeting them—fit within it. Our global sensor network continuously extracts, analyzes, and assembles internet data, updating each customer's unique Intelligence Graph with a current and 10-year history.

This history prevents data-stitching guesswork and provides a single, unified view of the internet that security leaders can use to inform their decisions. RiskIQ enables security teams to expand insights to find exposures, hunt threats, expand investigations, and collaborate with relevant security intelligence, so nothing remains a mystery.

Teams can also see what attackers are up to by referencing curated intelligence, instantly pivoting to RiskIQ's world-leading data sets to triage, respond, and validate protections with precision. Easily extract threat indicators and signatures for proactive detection and blocking; watchlists, firewalls, EDRs, and ACLs neutralize attackers.

SUCCESS CRITERIA

1. More than a decade of internet data history.
2. Patented infrastructure chaining.
3. Curated and corrected open-source intelligence (OSINT).
4. In-product human intelligence (HUMINT).

Question 4: Where is an active attack coming from?

Once you gather threat intelligence via OSINT or network traffic, you still don't have the full story. Intelligence is a living and breathing organism and must be continuously updated as things change and evolve to reflect the current threat landscape. For example, the attacker's timeline, behaviors, and new indicators of compromise must all be kept up to date to give organizations a critical situational awareness and an early warning signal that an attack may be approaching.

Relevant information is hard to come by—it's often hidden in the vast expanses of the internet and tucked away in underground forums. Even when security teams have a good grip on current threats, attack plans, and infrastructure, the threat actors on the other side continuously refine their strategies. Threat actors are also always probing the enterprise digital attack surface, hoping to find new assets and vulnerabilities before security teams do. Therefore, it's crucial to keep track of the latest in threat intelligence as well as your enterprise attack surface so you can discover new digital assets and vulnerabilities before your adversary.

SOLUTION: QUESTION, ANSWERED

Each day, RiskIQ's automated analysis and smart crawling continuously maps the internet and detects changes within the enterprise attack surface. Our collection preserves what a page looked like each time it was crawled, so we know how pages have changed, including if they've been compromised. Many webpages are fluid and may change hundreds of times after their initial load—some are just shells that only become populated after a user has requested the page. RiskIQ not only keeps the full HTML content from the crawled page, but our systems also save any dependent files used in the loading process.

On top of this historical view of the internet, our automatic systems and team of researchers continuously add indicators to give customers rapid awareness of attackers and the relevant infrastructure connecting them. This universal internet intelligence provides enterprise security teams a head-start, distilling the relationships between the enterprise and attackers simultaneously. Identifying fluctuations on both sides of the adversarial relationship provides a 360-degree view of the attack surface.

SUCCESS CRITERIA

1. More than a decade of internet data history. + (monitor and model changes through time, identify high-impact security indicators for monitoring).
2. Patented infrastructure chaining highlights the relationships between digital data—enterprise, attackers, third parties, components, and code.
3. Curated and corrected open-source intelligence (OSINT) (aggregated and linked to RiskIQ's award-winning data platform for relevance and easy watchlists).
4. In-Product Human Intelligence (HUMINT) - extra eyes, ears, and expertise with the same monitoring mandate as our customers—seek and eliminate cyber threats.

Question 5: How can my security programs be more resilient?

Cyber investigations and analysis demand a vast set of skills, including malware analysis, reverse engineering, digital forensics, and discovery techniques. Executing on these motions leads to greater digital resilience for the organization. However, threat investigations are manual, labor-intensive tasks, and much of the necessary information is hidden, inaccessible, or lacks specific guidance on putting the intelligence into action.

Analysts and response teams often do not have access to the relevant data necessary to pinpoint threats and threat infrastructure and are forced to assemble and analyze disjointed information, which only yields a small piece of the picture. Each fluctuation of the internet—new hosts, host pairs, cookies, components changes, codes, actions, scripts, pages, apps, people, and protocols—are all observable clues that point to signs of an attack. These clues should all be handy for investigators to reference to paint a complete picture of an attack and inform the appropriate response.

SOLUTION: QUESTION, ANSWERED

Imagine open-source intelligence that has been vetted, corrected, curated, and automatically served to you with recommendations for specific actions. Imagine receiving an alert from an EDR, SIEM, SOAR, or ITSM and being able to assemble all relevant data artifacts associated with it instantly—hashes, tags, indicators, chatter, attribution, history, and attack methods? With this kind of precision, investigations become a steady flow for continuous security improvement, controls, visibility, and, ultimately, enterprise digital resilience.

With this resilience, teams can scale security operations by automating data assembly to quickly find threat actors and infrastructure, fortifying group knowledge and skills across the SOC. With RiskIQ internet intelligence powered by attacker-aware machine learning, digital forensics go into hyperdrive.

SUCCESS CRITERIA

1. Continuous Passive Collection, Smart Crawling
2. Data History, Decade +
3. Patented Infrastructure Chaining
4. Curated OSINT
5. In-Product HUMINT
6. Live Watchlists and Intelligent Expiration