RELIAQUEST

The CISO's Guide to Metrics That Matter in 2022

WHITEPAPER

What's in the guide?

- Examples of the most effective cybersecurity metrics to track
- How to derive meaning from metrics in order to show ROI, identify program gaps, and build budget
- Communication frameworks to enable support across the business

TABLE OF CONTENTS

How can security metrics help to strengthen your security program and communicate its value across the organization?

INTRODUCTION

Security teams, boards, and other functional departments often speak to each other in very different languages – and when there's no translator, communication gaps can arise. As threats grow in complexity, so do security teams' technologies and responsibilities. It's become increasingly critical for CISOs to distill this complexity into simple, meaningful metrics—and master the art of tailored communication for their technical teams, peers, and boards.

In meetings with security leaders, boards regularly ask questions like:

- What are our greatest cyber security risks, and what are we doing about them?
- Is our business data protected?
- Where and how are we most vulnerable to cyber-attacks?
- What returns are we receiving on the investments we've already made?
- Should our investment levels in security change, and if so, how?
- I just read about this latest breach; how well are we protected against that attack?

These are good questions that highlight board and business perspectives on linking security investments to impact on risk levels in order to enable business success.

The problem is that the data typically provided by CISOs and their security teams doesn't answer these questions, leaving CISOs struggling to explain the value of their investments and teams.

In addition, most executives wrestle with the idea that security is largely a cost center for the business – something that closely resembles an insurance policy.

Most of today's security leaders tend to talk about metrics they have on hand, limited to what is generated by tools like vulnerability scanners, antivirus solutions, SIEM (security information and event management), and their security ticketing systems, including:

Number of vulnerabilities and patches applied

Number of alarms per day or events per second

Host infections to date

Ratio of open/ closed alarms

To demonstrate security's value to the business, security teams should focus on "metrics that matter" – ones that span people, processes, and technology.

Measurements such as visibility across security controls, efficacies, and coverage gaps, help business leaders better understand the state of their security program and how to improve it. They're also essential for CISOs to demonstrate risk, ROI, and a roadmap for maturity and investment in support of necessary budget.

66%

of senior security leaders said executives and/or the Board don't understand the value of the new security technologies purchased.

Source: Making Security Possible, 2021, Ponemon Institute

IN THIS PAPER, YOU'LL LEARN:

WHY traditional metrics fall short of telling the security story

WHICH metrics to track for strategic decision-making

HOW to tailor communications to advance initiatives with boards, peers, and technical teams

Instead of delivering metrics that don't demonstrate business value, security teams should focus on "metrics that matter" – ones that span people, processes, and technology.

[1]ESG Master Survey Results, 2021 Technology Spending Intentions Survey, December 2020.

WHY TRADITIONAL METRICS FALL SHORT

1. They're centered on tools.

Security measurements have traditionally been centered on tools. These metrics tell security teams how the tools are being used, but not what the results mean. In most organizations, measurements and modeling have formed organically based on what's readily available. These measurements also have limitations in that they only provide visibility into the usage of a given tool or silo, versus a holistic view across the enterprise's entire security tool stack and program.

2. They're not actionable.

Does a metric about the number of daily phishing alerts provide context—that is, indicate that security is effective, or that it is failing? That depends on more than just the numbers, which don't highlight other complex factors like overall security operations effectiveness or performance of team members. The numbers also lack context for answering questions like, "Is this good or bad? How do we compare to other enterprises in our industry? Are our resources focused on the right areas?"

What might be a promising data point in one organization might be an indicator of serious problems in another. No two organizations are the same. Should you hire more people? Revisit investigative processes? Swap one technology solution out for another? Because boards don't know how to interpret such metrics, the path to action—such as changing processes or product configurations or implementing automation—can be murky.

3. They don't address people, processes, and technology.

People, processes, and technology make up the three pillars of any security operations framework and are dependent on each other. If you're only measuring one or two of these elements, you're not getting a holistic view of how your security model is performing. Given that security teams default to tools-based metrics, they miss out on gauging the impact of people and processes on security.

Without understandable metrics that align with business objectives, security teams and boards can experience these negative results:

- Gaps in meeting security objectives
- Inability to get budget
- Misaligned expectations
- False sense of confidence in security preparedness
- Increased risk because security is not included in strategic business decisions

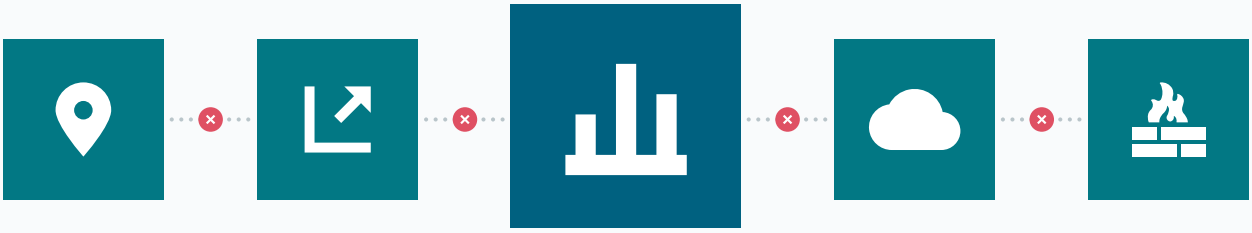
4. They don't take risk scenarios into account.

Many security leaders are concerned about specific types of cyber risks like ransomware and phishing. But decision makers don't always have the means to measure progress of their security program or impact of their security investments towards mitigating those risks. This prevents them from communicating cyber risk to the business and approaching security in a holistic way.

EXAMPLES OF COMMON SECURITY METRICS – AND WHY THEY'RE INEFFECTIVE

1. Consumption-based metrics:

Metrics like events per second or alarms per day are easy to pull in from security tools. But they mean little to your leadership, as they don't tell you if you're meeting or falling short of business or security objectives. Consumption metrics don't account for the diversity/existence of log sources or the extent of different environments. They don't capture changes in visibility that correlate to threat activity. Nor do they provide context around the impact on systems or shed light on the bigger picture.



2. Ratio of open to closed alarms:

Many ticket management and security orchestration, automation, and response (SOAR) products deliver metrics about alarm closure rates. If the open alarm rate is high, the logic goes, your security team may not have enough people to respond adequately, whereas if the alarm close rate is high, it's good news. But this is an oversimplification of the state of the security environment, and it doesn't offer action items.

These metrics address the amount of time a threat was in your environment before someone detected it and the mean time to respond following detection. They don't mean much to leadership without context. In fact, they raise more questions than answers. For example, are elongated detection times due to gaps in visibility? Gaps in threat coverage? Too many false positives? Reducing the detection and response time of one type of threat does not directly reduce times for other threats, either.

3. Number of vulnerabilities and patches:

Understanding the vulnerabilities you have and the number you patch is important, but does not convey a sense of your overall security posture without additional context. The number of patches applied by itself, for example, does not indicate that you are better off than before since you don't know how many are not yet patched, the value of the assets being patched, etc.

THE METRICS THAT MATTER

To measure the impact of people, processes, and technology on enterprise risk posture, security teams have to measure the full impact of their security models – which means gauging the ability of the security model holistically to meet business objectives. The results also need to be consumable by many stakeholders, beyond security operations.

To generate metrics that matter to leadership and provide insights for decision-making, metrics need to:

- Quantify the visibility your enterprise has into its entire environment, including on-premises and cloud, to identify and prioritize areas of risk.
- Understand coverage across known risk management frameworks and prioritize areas to close gaps
- Measure the team's effectiveness in securing your organization
- Benchmark improvement against previous periods as well as industry peers

The following metrics address these needs.

1. Visibility

In a world where everyone wants to measure number of events or vulnerabilities, there's a critical question being missed:

Do you have the right level of visibility into your environment?

60%

of respondents believe lack of visibility is a major barrier to implementing effective threat detection and investigation practices.

Source: Making Security Possible, 2021, Ponemon Institute

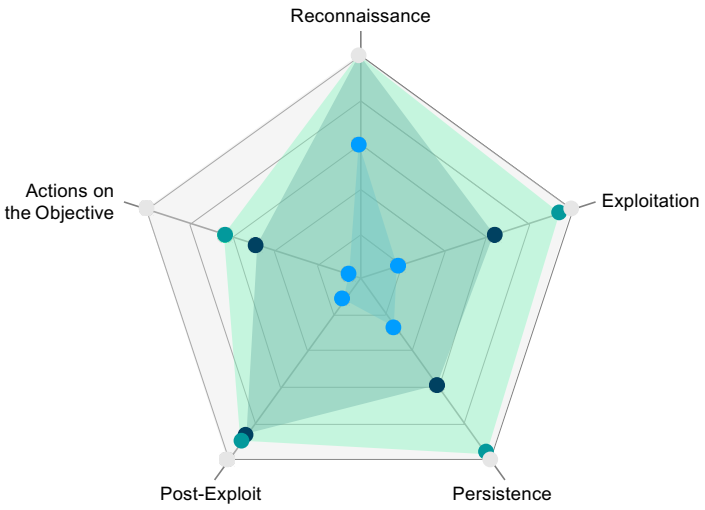
While, at the surface, this seems a simple question, many organizations struggle to answer this. In fact, respondents to a recent survey on **Making Security Possible** from the Ponemon Institute and sponsored by ReliaQuest, only 36% agree that the level of visibility into their IT environment, including on-premises and cloud, is optimized to deliver real-time status of their risk posture. And only 13% said they had over 75% visibility across their security tools, including on-premises and cloud. Without visibility or situational awareness, it would be difficult for security teams to focus on any level of threat detection or investigations.

How much of your environment can you see?

Determining how many of your log sources (such as DLP, A/V, firewall, etc.) actually perform logging is the most important step in measuring and identifying visibility gaps. Look at:

- ✔ The number of systems you have, not the number of systems from which you collect and analyze logs
- ✔ The number of machines installed with your advanced endpoint solution

Perform the same calculations in all your environment types. For instance, if you have multiple cloud environments, do you have the same level of visibility into those environments as you do in your on-premises data centers?



Sample visibility coverage mapped to the kill chain.

WHAT'S NEXT?

By first identifying gaps in logging coverage and then framework coverage, you can build a prioritized roadmap for log source integration and new detection content to improve visibility.

2. Team performance

For many CISOs, this is the most challenging category to measure. However, it's an important component to gauge in order to identify any resource gaps or process improvements that could help your team perform better. Below are a few helpful metrics to look at:

Where is your team spending its time?

- ✔ False-positive rate

False positives should be defined as a flaw in tools' rule logic or ability to detect a threat. They indicate that a rule needs to be tuned to prevent alert fatigue and to expose true positives.

How well does your team understand your environment?

Many security tools come with a variety of features and functionality. To determine if you are taking full advantage of your tools' capabilities, you can look at:

- ✔ Anomalous safe rate

Often confused with false positives, these alerts successfully detect anomalous activity judged as safe, although the same activity could be malicious. This metric is often indicative of IT hygiene issues and potential risky behaviors. Tracking this type of activity can be helpful when talking to IT business leaders about changes to policy.

- ✔ True-positive rate

True positives are alerts determined to be real. To gauge the severity of these alerts, weigh these alerts based on their individual impact to the business.

How fast is your team resolving issues? Are there any shortfalls in your team's analysis capabilities?

- ✔ Mean time to resolve (MTTR)

The above metrics provide the appropriate context to begin measuring MTTR and using it to make decisions around your team's performance. MTTR can be calculated from the time an alert is escalated to the time it's closed. Using this method, you can start to understand if you are properly staffed, if your team needs training, and/or if the problem is getting the business to act.

WHAT'S NEXT?

By analyzing the above metrics, you can determine where your team's greatest challenges are, prioritize improvements, and reduce risk. This could involve tuning noisy rules, increasing headcount, or facilitating training and improving your team's understanding of your environment.

3. Detection Coverage

While log source coverage is important for visibility, detection coverage helps you gauge how well you are protected against industry standard stages of an attack cycle.

Do you have the controls in place for visibility into critical threats?

Looking at NIST, MITRE ATT&CK®, CSF, or other industry frameworks, you can determine if you have the controls you need to get critical visibility into the types of threats that are of concern to the business. From there, you can map your use cases across your major detection controls (SIEM, EDR, UEBA) to these industry frameworks to understand the types of attack techniques into which you have visibility.

How well do you understand cyber risk?

Security programs don't operate in a vacuum. There are distinct cyber risk scenarios CISOs are interested in measuring against. By identifying those risk scenarios and mapping coverage against them, CISOs can ensure their security programs align with the organization's evolving business requirements.

There are four dimensions of cyber risk confronting organizations. These are as follows:

Exploitation involves malicious actors attempting to get into an organization's systems by exploiting a particular path. Common exploitation vectors include phishing, remote access, and weaknesses in the supply chain.

Infiltration is when attackers use an initial compromise to move to high-value targets located elsewhere in the network. This phase typically relies on stolen credentials and/or movement across different systems and network segments.

Exfiltration amounts to the theft of data. Those details can take on various forms including payment card information (PCI), protected health information (PHI), intellectual property (IP), and personally identifiable information (PII).

Disruption refers to the use of ransomware or other methods to undermine the functionality of a service or application.

Can you detect the risk scenarios that matter to you?

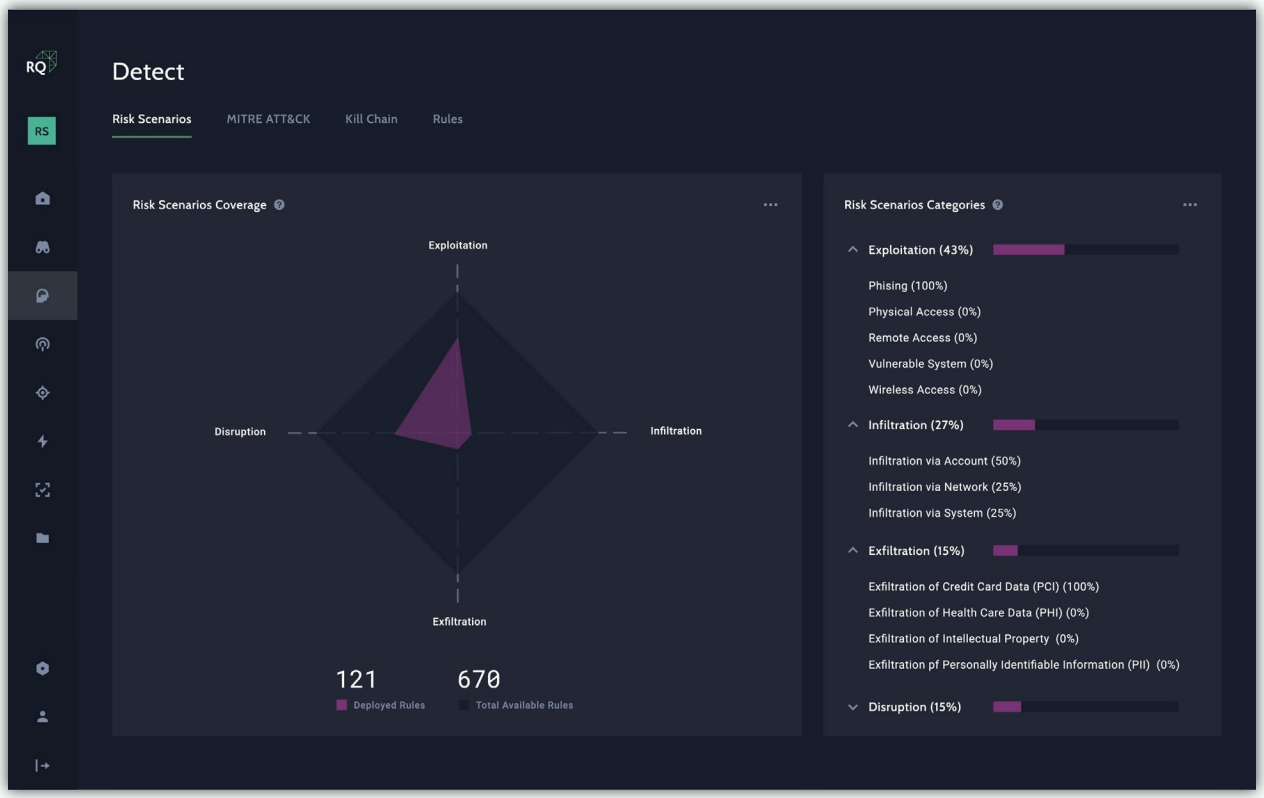
Go and ask a CISO, "What are the risks you're worried about?" Some say, "phishing." Some say, "ransomware." Some say, "disruption to critical apps and services." Every security leader is concerned about a few risk scenarios and the threats that can manifest or exacerbate them. They also want to understand the elements that need to be in place to help them track and stay ahead of these threats. But their ability to do so depends on certain elements:

- ✔ Detection rules that map to each threat and risk scenario to understand coverage
- ✔ An understanding of coverage gaps to help determine the next course of action

It's important for CISOs to know where they stand in defending against cyber risks. But they also need to understand what additional measures they need to have to protect against the threats that pose those risks. This approach not only provides a CISO the state of their security posture but an actionable roadmap to execute against to mature their program.

WHAT'S NEXT?

By analyzing the above metrics, you can determine where your team's greatest challenges are and prioritize improvements to help them and therefore reduce risk, whether that be tuning noisy rules, increasing headcount, or facilitating training and your team's understanding of your environment.



BOARD QUESTIONS, AND METRICS THAT DELIVER THE ANSWERS

The metrics described above will arm you with the talking points you need to communicate the value of your security program – as well as answer the following questions in board meetings:

BOARD QUESTIONS	ACTIONABLE METRICS	BENEFITS
Where and how are we most vulnerable to attacks?	Visibility	Measuring visibility across spectrums by environment, diversity, attack surfaces, and context provides a greater understanding of vulnerabilities, and better captures improvements from onboarding new data sources and analytics in a scoring that the board can understand.
Are we protected from breaches?	Visibility	While you can never answer this question with "yes," you can provide a quantitative response around what you have visibility into vs. where your gaps are. You can then prioritize a roadmap to close these gaps with new data sources or content.
What are our greatest risks?	Visibility	To understand your greatest risks, you must first understand your "crown jewels"—this could be patient data, IP, etc. Then, research threats custom to your industry and environment, and using the kill chain or MITRE ATT&CK® framework, you can show your current level of protection and critical gaps that need addressing.
Should our investment levels in security change, and if so, how?	Visibility & Detection Coverage	Visibility metrics expose gaps in the security program, while detection coverage determines what gaps need to be filled to increase detection of techniques by either optimizing existing tools, or if a new investment is needed.

BOARD QUESTIONS	ACTIONABLE METRICS	BENEFITS
How well can we detect against attacks?	Detection Coverage	Looking at the use of security investments and security tool performance provides a realistic understanding of ROI.
Are we adequately staffed to address risk? **How long is it taking to detect threats and respond?**	Team Performance	Looking at response rates in light of false positives and innocuous activities provides greater context for influences that negatively impact individuals' performance.
Are we better protected today than yesterday? **Is security keeping up with the business?**	Visibility, Team Performance	By reviewing trends for visibility and team performance scores, enterprises can better understand if they are more protected or why they aren't. Teams can then drill down into specific coverage areas or risk scenarios to explain if protection meets risk tolerance levels.

THE THREE TIERS OF SUCCESSFUL COMMUNICATION

Collecting the right metrics isn't enough to advance your security initiatives. To truly close gaps, increase efficiencies, and reduce risk, you need to understand whose buy-in is needed and how you can effectively package your metrics to obtain this support.

First, it's important to note that the buy-in you need extends beyond the board. While board communication is top of mind for advancing budget, CISOs must also establish rapport with their peers and technical teams to secure the business.

Each of these stakeholders has different goals, concerns, and challenges. To influence different groups to act, you must understand what exactly they care about and adjust the story you tell. This is an ongoing challenge for many CISOs.

Below, we'll take a closer look at what each stakeholder cares about so that you can adjust your communication style accordingly.

Board-level communication

When addressing board members, the goal is to not only be prepared to answer the questions we discussed above but also to proactively communicate what's being measured, why it's being measured, and how these metrics align to the business's strategic priorities.

Boards care about the business impact of risk, resource levels, threat trends, and how your organization stacks up to similar organizations—primarily using maturity measures.

- Show trends over time and use benchmarks to facilitate an understanding of whether a metric is "good" or "bad."
- Discuss coverage you have against each of the risk/threat scenarios you are most concerned about and your roadmap to address them.
- Be prepared to discuss the implications on consumer trust, service reliability, reputation, and legal exposure when discussing the highest risks to the business.
- Set realistic expectations around the impact of new investments based on your current security posture and environment.

Are you prepared to address newsworthy threats?

When board members see a headline about a new threat, their next questions will likely be, "What are we doing to ensure that doesn't happen to us?" For instance, in 2020 security teams saw an uptick in authentication attacks, insider threats, and phishing scams related to COVID-19 and a remote workforce. As a result, CISOs were questioned on whether or not these attacks were occurring in their environment, and what controls and measures were put in place to protect the organization.

#COVID19 Drives Phishing Emails Up 667% in Under a Month

Source: InfoSecurity Magazine

When new threats are in the news, proactively anticipate the board's questions and be prepared with answers by following this story telling formula:

Step 1:
Summarize what the threat is by looking at related indicators of compromise.

Step 2:
Address what you're seeing in your environment and explain how the threat could affect the organization.

Step 3:
Highlight the investments you've already made that would provide protection.

Step 4:
Explain what additional action you're taking to address the threat.

Peer communication

Peer groups can sometimes constitute one of the most undervalued relationships to security leaders. Without support from IT, application development, and business, however, CISOs run the risk of being seen as a roadblock or the "Department of 'No.'"

Peers care about their team's capacity and goals as well as how initiatives will impact them.

Quick tips for communicating with peers:

- ✔ Share your plans and understand others' priorities to build an integrated roadmap.
- ✔ Lead communications with facts and reason
- ✔ Explain how security initiatives will yield advancement, recognition, and other benefits.

> **When building your roadmap, include peers across the organization early in the process to ensure alignment and foster trust. For instance, if the Vice President of IT has plans to make the cloud more available, you would align on your plans to secure the cloud.**

Technical team communication

In a world where hiring and retaining top security talent is a persistent challenge, CISOs must place high importance on communication with their team members. A high turnover rate in your team can slow down projects or even halt them entirely. In addition to providing your team with the proper tools and training, being clear, direct, and empathetic is key to setting your team—and security program—up for success.

Technical teams care about what needs to be done and when as well as how any initiative will develop their skills and advance their career.

Quick tips for communication:

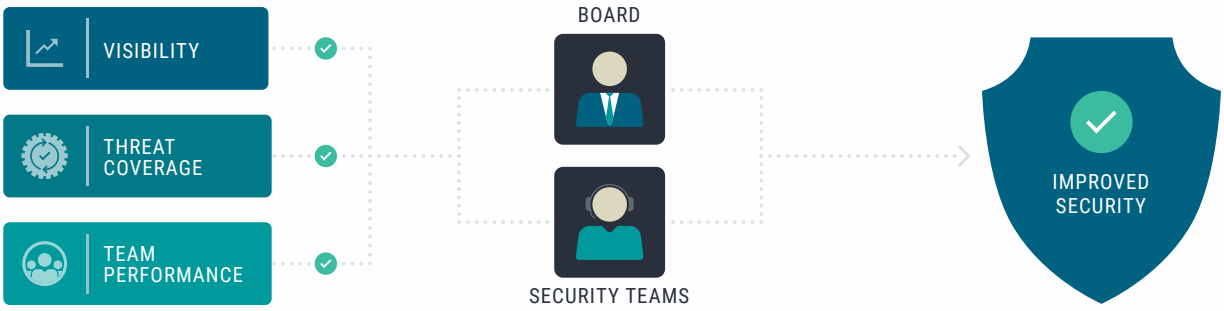
- ✔ Focus on the "why" behind your requests and how it fits into the larger picture.
- ✔ Listen to your team's ideas and input.
- ✔ Provide details on what requirements and timelines must be met.
- ✔ Understand your team's challenges and use your leverage with peers and the Board to alleviate those obstacles.

Can metrics shed light on whether the business is better protected today compared to yesterday?

When packaged with a communication strategy, relevant security metrics can be a powerful tool for CISOs to better highlight their security program and roadmap improvements. The benefits of using metrics that matter include:

- Highlighting opportunities for increased investment or reallocation of resources that would improve security
- Creating more productive conversations with boards, peers, and technical teams
- Connecting security investments to business outcomes
- Demonstrating and mitigating relevant risks to the enterprise

As a step toward better communication across the organization, security teams should start their conversations in advance of key business transformation projects. Too often, they find out about projects long after they've begun. If they can bake security into projects earlier—and speak to boards using metrics that matter—security teams can better scale the security organization while accommodating the needs of the business.



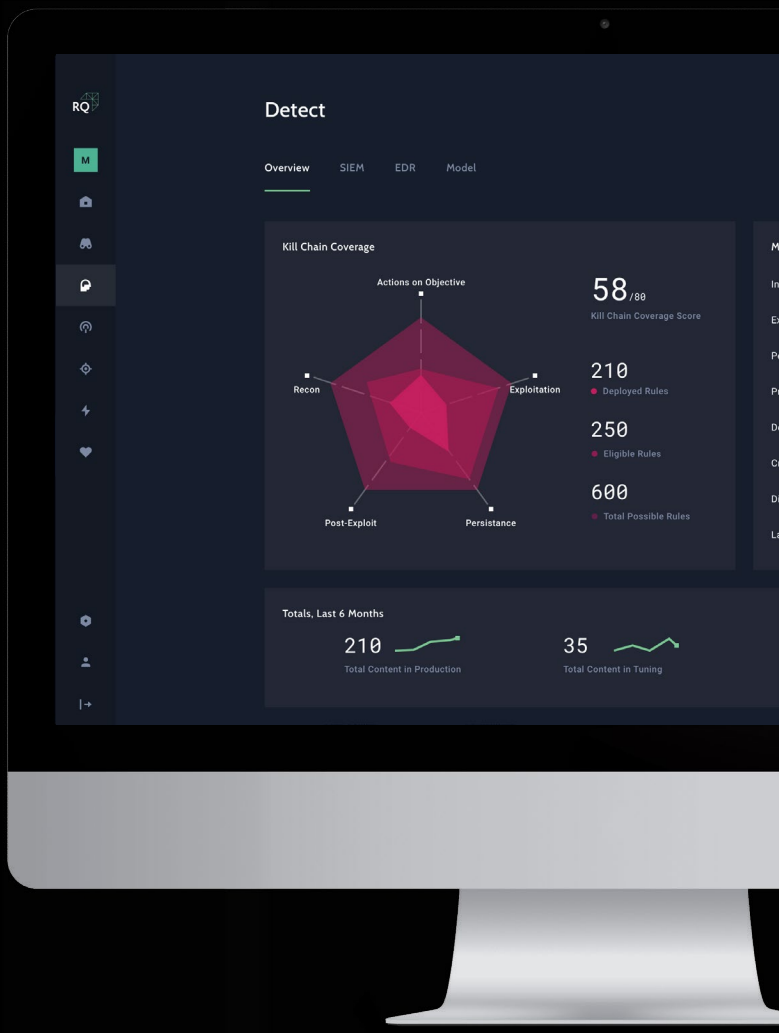
If they can bake security into projects earlier—and speak to Boards using metrics that matter—security teams can better scale the security organization while accommodating the needs of the business.

HOW RELIAQUEST DELIVERS METRICS THAT MATTER

Through ReliaQuest's Security Model Index, CISOs receive actionable metrics around visibility—mapped to frameworks like MITRE ATT&CK® and risk scenarios of concern—as well as metrics around team performance, so they can identity gaps and prioritize improvements.

ReliaQuest offers a unique combination of technology and services to meet customers where they are and help them mature their security program at their pace. The Security Model Index is delivered through GreyMatter, the unifying cloud-native technology platform. By bringing together telemetry from across an organization's security ecosystem through the platform's proprietary universal translator, and with the use of automation and artificial intelligence, GreyMatter delivers singular visibility and helps security teams take fast action and keep ahead of threats.

The platform's analytics provide actionable reporting that measures continuous improvement of security programs. ReliaQuest customers receive their reporting benchmarked against past performance and industry peers, so they can recognize trends and make improvements over time.



LEARN MORE ABOUT RELIAQUEST GREYMATTER

> **GreyMatter gives us confidence to know we are effectively reporting on our posture in real time and setting appropriate goals to mature our security program in line with objective benchmarks.**
>
> – CISO, leading research hospital

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com