RELIAQUEST

The CISO's Guide to Metrics that Matter in 2020

How to Apply Metrics to Strengthen Security Programs and Articulate Value to Leadership

How can security metrics be applied to both strengthen your security program and communicate the value of this program to leadership?

Introduction

Security teams and boards often speak to each other in very different languages – and like any situation where there's no translator, communication gaps are in abundance.

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 from breaches?
- Where and how are we most vulnerable to cyber-attacks?
- What return are we receiving on the investments we've already made?
- Should our investment levels in security change, and if so, how?
- Are we better protected today than yesterday?

These are good questions that highlight board 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 board members wrestle with the idea that security is largely a cost center for the business – something that closely resembles an insurance policy.

Security professionals tend to talk about metrics they have on hand, often generated by tools like vulnerability scanners, antivirus solutions, SIEM (security information and event management), and their security ticketing systems, including:

- The number of alarms-per-day or events-per-second
- Critical and high vulnerabilities
- Host infections to date
- Ratio of open/closed alarms

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. Measurements such as visibility across security controls, or the efficacy of system performance, provide context that helps business leaders better understand the state of their security program and how to improve it.

100%

of large enterprises will be asked to report to their boards on cybersecurity risk **at least annually by the end of 2020**, according to Gartner.

The likelihood of your security team being grilled by the board is growing. According to Gartner[1], by the end of 2020, 100% of large enterprises will be asked to report to their boards on cybersecurity and technology risk at least annually, up from 40% of organizations in 2018. There are many reasons for boards' renewed interest in security, starting with the near-daily drumbeat of news about breaches and the financial and brand equity repercussions for businesses. Also, as security budgets have been allowed to expand, boards want to see value for these investments.

In this paper, you'll learn:

WHY traditional metrics fall short of telling the security story

WHICH metrics have meaning for both boards and security teams

HOW the right metrics can benefit the business

> **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]Gartner, "Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer," July 2019.

Why traditional metrics fall short

1. 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 system performance or the effectiveness of team members. The numbers also lack context for answering questions like, "Is this good? Is this bad? How do we compare to other enterprises in our industry?"

In one organization, 3,000 daily phishing alerts might be a promising data point, while in others, it might indicate serious problems. Should you hire more people? Investigate 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 – is murky.

2. THEY'RE CENTERED ON TOOLS.

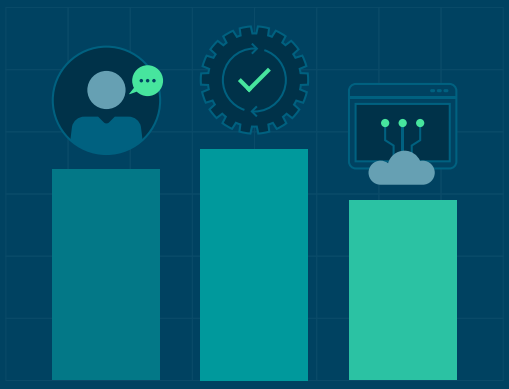
Security measurements have traditionally been centered on tools that tell security teams how the tools are being used, not what the results mean. In most organizations, measurements and modeling have formed organically, based on what's easily available. They're the low-hanging fruit of the security metrics world, and easily available – yet not easily interpreted or actionable.

3. THEY DON'T ADDRESS PEOPLE, PROCESSES, AND TECHNOLOGY.

These three pillars make up the security model of an organization 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 needed budget
- Misalignment of expectations
- False sense of confidence in security preparedness
- Increased risk because security is not included in strategic business decisions

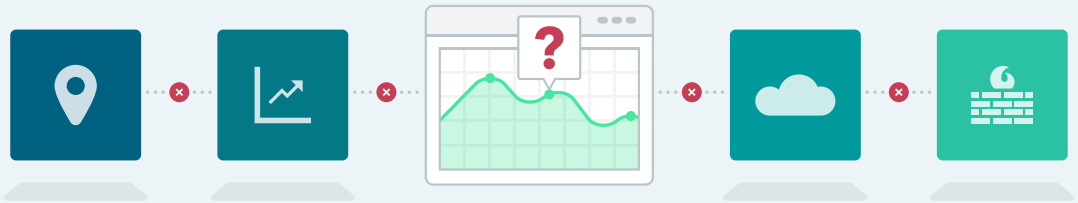


Examples of common security metrics – and why they're ineffective

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, since 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 (or lack thereof) of log sources, or the extent of geographic, cloud, or SaaS environments – nor do they capture increases and decreases in visibility that correlate to threat activity. The metrics don't provide context around the impact on systems, nor do they shed light on the bigger picture: Can businesses see everything going on in their most important systems? And what are businesses not seeing?



2. MEAN TIME TO DETECT (MTTD) AND MEAN TIME TO RESPOND (MTTR):

These metrics, which address the amount of time a threat was in your environment before it was detected, and the mean time to respond once detected, also don't mean much to leadership without context. Everyone wants to reduce these metrics, but how does this correlate to security team effectiveness? For example, are elongated detection times due to gaps in visibility or gaps in threat coverage – or lost in too many false positives?

While retrospectives are important, sharing mean time to detect and mean time to respond with board members raises more questions than answers. In addition, reducing the detection and response time of one type of threat does not directly correlate to reduced times for other threats.

3. RATIO OF ALARMS, OPEN TO CLOSED:

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

The metrics that matter

To measure the impact of people, processes, and technology, 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 for many stakeholders.

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

- Quantify the amount of visibility your enterprise has into its entire environment, in order to identify and prioritize areas of risk
- Highlight the effectiveness of your current tool set, so you can understand ROI and performance of current investments
- 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 MTTR of their teams, there's a critical question being missed:

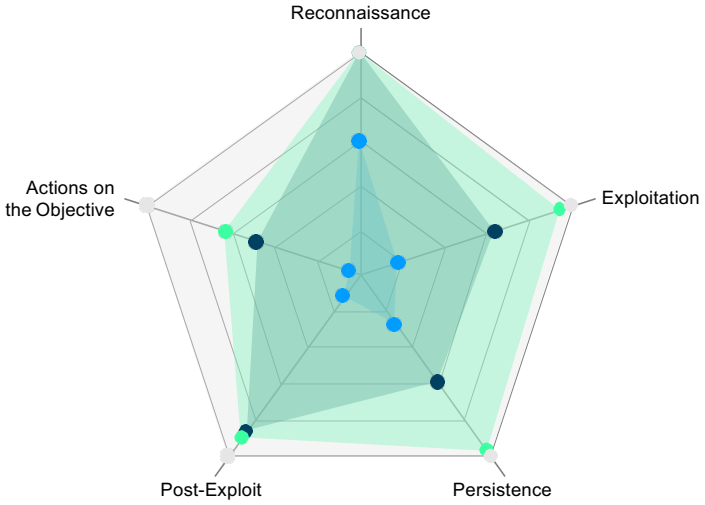
Do you have the right level of visibility into your environment?

Although this is a simple question, it can be very difficult to answer; the common response is, "I don't know," or "No." You must be able to answer this question first before looking at any other metrics. If you're only seeing 50% of your environment or are unsure of what percent of your environment you can see, your energy shouldn't be centered around tuning your team or building funnel metrics. Instead, focus your energy on metrics that can answer the following questions.

In a world where everyone wants to measure number of events or MTTR of their teams, there's a critical question being missed: Do you have the right level of visibility into your environment?

How much of your environment can you see?
This is a simple numerator and denominator calculation, but very difficult for most enterprises that don't have accurate Configuration Management Databases (CMDBs). Start broad; if you think you have about 30,000 Windows machines, look at:

- ✔ Number of systems you have, versus number of systems from which you collect and analyze logs
- ✔ Number of machines that are 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-premise data centers?

Do you have the right controls in place to detect and respond to threats?
Looking at NIST, ATT&CK MITRE, 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. Start by measuring:

- ✔ Coverage mapped to industry frameworks or kill chain stages

2. TOOL EFFICACY

If you've invested money into your critical tool set – such as SIEM, EDR, and UEBA – it's important to determine if you're maximizing your ROI on these technologies. By measuring both your tool health and tool maturity, you'll be able to answer these questions:

How well are your current tools working?
- ✔ Number of issues your team is experiencing with the tool
- ✔ Number of outages or inactive services over a set timeframe
- ✔ Number of vendor tickets
- ✔ Drops in functionality

Use these metrics to identify improvements that could increase your technology's effectiveness.

How well are you optimizing your tools' capabilities?
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:

- ✔ Integration of latest features and functionalities
- ✔ Projection for environment growth and architecture recommendations

3. 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 the rule logic or tools' ability to detect a threat, and results in a change needing to be made to the rule. False positives should not be repeated.

How well does your team understand your environment?

✔ 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

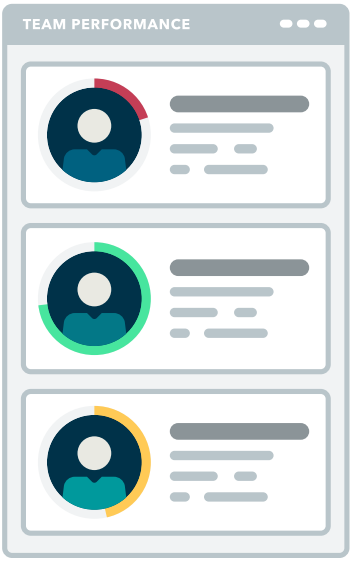
True positives are alerts your team has determined to be real. To gauge the severity of these alerts, apply a weighting to this rate based on impact to the business, as some true positives will have a more detrimental effect than others.

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

✔ Mean time to respond (MTTR)

Only after all the above metrics are measured and tuned can you start to really measure MTTR. The above metrics provide the appropriate context to use MTTR 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, or if the real problem is getting the business to take action on the found issue.



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
How much visibility do we have across our different environments?	Visibility	Measuring visibility across spectrums by environment, diversity, attack surfaces, and context provides a greater understanding of risk, and better captures improvements from onboarding new data sources and analytics in a scoring that the board can understand.
Where and how are we most vulnerable to attacks?		
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.
Are we receiving value from our existing security tool investments?	Tool Efficacy	Looking at the extent that security investments are used, in addition to security tool performance, provides a more realistic understanding of return on security investment.
Are we adequately staffed to address risk? How long do risks remain in our environment prior to detection?	Team Performance	Looking at response rates in light of false positives and innocuous activities provides greater context for influences that negatively impact individuals' performance.
Should our investment levels in security change, and if so, how?	Visibility & Tool Efficacy	Visibility metrics expose gaps in the security program, while tool efficacy metrics determine whether these gaps can be filled by optimizing existing tools, or if a new investment is needed. For example, gaps in SaaS activity often lead to investment in cloud access security brokers (CASBs) if these gaps can't be filled by optimizing existing technology.
Are we better protected today than yesterday? As the business changes, is security keeping up?	Combination of Visibility, Tool Efficacy, and Team Performance	By reviewing trends for combined visibility, tool efficacy, and team performance scores, enterprises can better understand if they are more protected – and if not, why not. Teams can also drill down to specific coverage areas or threat types to explain if protection meets risk tolerance levels.

CAN METRICS SHED LIGHT ON WHETHER THE BUSINESS IS BETTER PROTECTED TODAY COMPARED TO YESTERDAY?

Relevant security metrics help close the communications gap between boards and security teams – so both can speak the same meaningful language. The benefits of using metrics that matter include:

- ✔ Highlighting opportunities to improve security
- ✔ Creating more productive conversations with boards
- ✔ Connecting security investments to business outcomes
- ✔ Demonstrating and mitigating relevant risks to the enterprise

As a step toward better communication with boards, security teams should also make sure that conversations start in advance of key business transformation projects. Too often, security teams find out about projects long after initiation; they're only included in projects to check off boxes. If security teams help bake security into projects earlier – and speak to boards using these metrics that matter – they're in a better position to scale the security organization while accommodating the needs of the business.

If security teams help bake security into projects earlier – and speak to boards using these metrics that matter – they're in a better position to scale the security organization while accommodating the needs of the business.

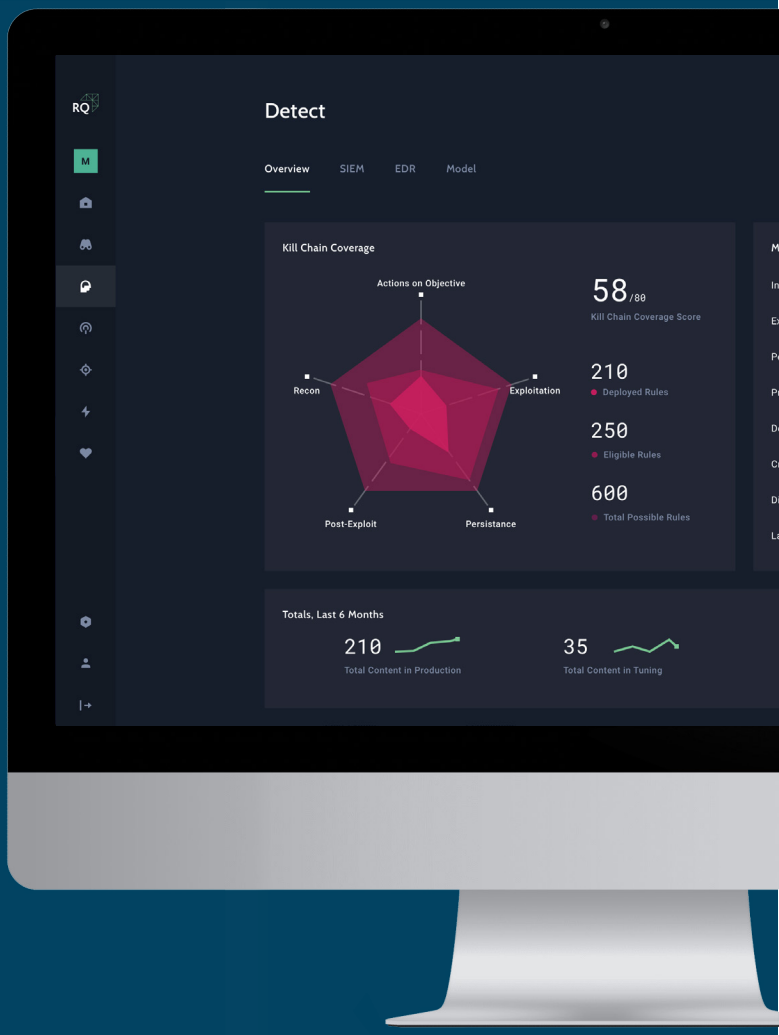
How ReliaQuest Delivers Metrics that Matter

Through ReliaQuest's Model Index, enterprises are recognizing return on investment for their people, technology, and processes, captured with insights that are understandable to leadership. The Model Index provides comprehensive metrics that recognize current level of visibility, as well as associated risks across your enterprise visibility, tool efficacy, and team performance.

The Model Index is provided through ReliaQuest GreyMatter, the platform for proactive security model management. GreyMatter increases your enterprise visibility while automating threat detection and response. It does this by unifying and integrating existing SIEM, EDR, multi-cloud, and third-party apps to deliver a centralized, transparent view across your environment.

The platform's analytics provide actionable reporting and metrics that measure ongoing improvement of the security model to recognize and communicate success across the enterprise. ReliaQuest customers receive their reporting compared against past performance and peers within their industries, enabling benchmarking and trending over time.

LEARN MORE ABOUT RELIAQUEST GREYMATTER



ReliaQuest's Model Index provides on-demand reporting focusing on visibility, tool efficacy, and team performance identifying risks and providing detailed recommendations to improve the security model.

RELIAQUEST

Make Security Possible™

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