RELIAQUEST

SOLUTION BRIEF

RELIAQUEST GREYMATTER

THE MODEL INDEX

Delivering Actionable Metrics with the ReliaQuest Model Index

Traditional Cybersecurity Metrics Fall Short

The increased volume and complexity of threats have driven enterprises to expand investment in new their security tools, such as SIEM, EDR, across multiple cloud environments, and third-party apps. Yet it is increasingly difficult to understand if these investments actually strengthen your organization's security posture. In a survey of 400 enterprises, 60% reports most of their security technologies are underutilized[1]. Equally challenging is conveying security tool effectiveness in a language your leadership understands. According to Gartner, by 2020 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually, up from 40% of organizations in 2018[2].

The variety and technical nature of tool-specific reports or compliance checklists create difficulties in accurately assessing your team's ability to use security tools for effective detection and response. Outputted metrics require interpretation without providing any guidance into practical improvements. Traditional metrics, such as rates of alarms, time-to-triage, mean-time-to-detect or respond, dwell time, and others, are difficult to interpret and action on results. Do the results capture operational or technology issues, or personnel issues? The technical statistics are often meaningless to individuals outside the security team and fail to help organizations understand their current state of security posture or their security model maturity.

Traditional Security Metrics Failures

Fast Alarm Closure Rates	A well-functioning SOC -OR- Missing critical threats from visibility gaps
High Mean time to Detect (MTTD)	Untuned analytics content -OR- Lack of visibility coverage
High Time-to-triage	Staffing issues -OR- Lack of automation -OR- Process issues

Measuring The Effectiveness of Your Security Model

Effective security metrics require CISOs and their teams to assess their full security models – the use of your technology, resources, and processes – recognizing improvements or impediments in reaching your security program objectives. The results need to be easily interpreted and in a format consumable to a variety of stakeholders.

How do you measure the effectiveness of a security model?

- Audit visibility across all attack vectors
- Monitor the health and performance of your security tools
- Measure the team's effectiveness in using your security tools
- Benchmark your team's performance against previous periods as well as your peers.

Introducing The ReliaQuest Model Index

The ReliaQuest Model Index provides ongoing assessment of your team's visibility, security tool efficacy, and team performance to drive greater consistency and evolution of your security model. The Model Index is provided through ReliaQuest GreyMatter, the industry's first platform for security model management.

[1] 2019 ReliaQuest Security Technology Sprawl Report

[2] Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer, Gartner, July 2019

The ReliaQuest Model Index

Type	Assessment	Benefit
Visibility	Log source coverage and diversity	Scores visibility and diversity of log sources cross your entire organization
	Kill chain coverage	Measures threat detection coverage across all phases of the kill chain
	Threat context	Evaluates the quality of threat intelligence and its integration and effectiveness into your threat detection and investigations
Tool Efficacy	Tool health	Assesses health indicators from your current configuration and architecture
	Tool maturity	Evaluates the depth of capabilities utilized in alignment to your environment
Team Performance	Mean time to resolve (MTTR)	Calculated from the time an alert is escalated to full resolution
	False Positive rate	% of false positive responses
	Anomalous safe rate	Activity has been adjudicated as safe, but the same activity can sometimes be malicious.
	No response rate	% of alerts not responded

The ReliaQuest Model Index Advantage

ReliaQuest customers receive their quantitative assessments compared against peers within their industries and across all others, enabling benchmarking and trending over time to quickly spotlight opportunities for improvement. As part of ongoing enablement, customer security teams, from CISOs to their key domain leaders, work together with experts to interpret results and receive individualized both tactical and strategic guidance for evolving their security model.

Examples of Guided Recommendations

Visibility

- Prioritized log sources to onboard
- Prioritized log types to filter
- Content from the ReliaQuest Content Library to increase threat coverage
- Use of provided, curated threat intelligence in analytics and investigations

Tools

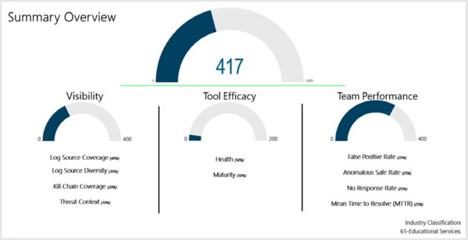
- Validated system patches and updates
- New version testing and onboarding
- Configurations, architecture improvements, and add-ons

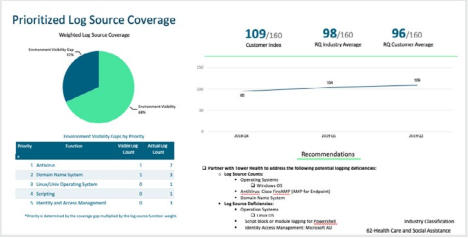
Team

- Specific tuning and content configurations to reduce false positives
- Implement automation or recommend process improvements

Strategic

- How to evolve the organization's security model to better support business priorities
- Use of Model Index results for executive team/board discussions
- Roadmap of additional investments in, and optimization of, security technology, teams, and process




Prioritized Log Source Coverage
Weighted Log Source Coverage
Environment Visibility Gap 32%
Environment Visibility 68%
109/160
Customer Index
98/160
RQ Industry Average
96/160
RQ Customer Average
150
100
50
0
95
104
109
2018Q4
2019Q1
2019Q2
Industry Classification
62-Health Care and Social Assistance

Environment Visibility Gaps by Priority

Priority	Function	Visible Log Count	Actual Log Count
1	Antivirus	1	2
2	Domain Name System	1	3
3	Linux/Unix Operating System	0	1
4	Scripting	0	1
5	Identity and Access Management	0	3

*Priority is determined by the coverage gap multiplied by the log source function weight.

Recommendations

- ❑ **Partner with Tower Health to address the following potential logging deficiencies:**
  - ○ **Log Source Counts:**
    - Operating Systems
      - ❑ Windows OS
    - AntiVirus: Cisco FireAMP (AMP for Endpoint)
    - Domain Name System
  - **Log Source Deficiencies:**
    - Operation Systems
      - ❑ Linux OS
    - Script block or module logging for Powershell
    - Identity Access Management: Microsoft AD

The ReliaQuest Model Index demonstrates return on investment of an organization's investments in people, technology, and incident response workflows with insights your leadership understand. To see learn more about the ReliaQuest Model Index or learn about security model management, please visit us at **https://www.reliaquest.com.**

RELIAQUEST

Make Security Possible™

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