Whitepaper

Reducing Risk with Continuous Cybersecurity Readiness

How to apply a data-driven framework to improve cybersecurity performance

SightGain

The Status Quo:

Cybersecurity Is Not Working

Every year, organizations are pouring more money into cybersecurity — spending millions of dollars on solutions and training. As new threat vectors emerge, the security solutions ecosystem keeps expanding, making security increasingly complex and expensive.

Yet those growing investments don't seem to be working. The cost of cybercrime and data breaches is climbing even faster, estimated to reach $945 billion in 2020.[1] And organizations are still not discovering 53% of attacks before a breach takes place.[2]

If cybersecurity leaders understand that they need to invest in the right tools and talent to protect their organizations, then why are those efforts failing?

$145 billion

spent on cybersecurity in 2020[3]

67% increase

in cybercrime in the last five years[4]

10% increase

in average cost of a data breach, 2020-2021, to a record high of $4.24 million[5]

42% of organizations

experienced a ransomware attack in FY21[6]

287 days

to identify and contain a data breach on average in 2021[7]

Sources:

1 Center for Strategic and International Studies and McAfee, "The Hidden Costs of Cybercrime," December 2020

2 Mandiant, "Deep Dive Into Reality: Security Effectiveness Report," 2020

3 Center for Strategic and International Studies and McAfee, "The Hidden Costs of Cybercrime," December 2020

4 Accenture/Ponemon, "The Cost of Cybercrime," 2019

5 IBM Security, "Cost of a Data Breach Report," 2021

6 Ponemon/Experian, "Eighth Annual Study: Is Your Company Ready for a Big Data Breach?" April 2021

7 IBM Security, "Cost of a Data Breach Report," 2021

Disconnect Between Expectations and Results

One of the many challenges of cybersecurity is metrics. Traditionally, objectively measuring the effectiveness of cybersecurity has been no easy task, and many organizations have been relying on indicators like compliance checklists for guiding their security strategies.

While regulatory compliance is an important part of minimizing overall risk, however, compliance doesn't equal protection. You only need to look as far as the daily headlines about data breaches — or your pen test report — to see proof.

Compliance metrics are incomplete and provide a false sense of security. Checking all those compliance boxes is not enough to defend your organization against today's adversaries. As long as this false sense of safety persists, the gap between cybersecurity spending and compromises will remain.

62%

of IT and IT security professionals believe security incidents will increase in the future.

Source: Ponemon/Experian, "Eighth Annual Study: Is Your Company Ready for a Big Data Breach?" April 2021

Tunnel Vision:

Focusing on the Wrong Priorities

Much of the cyber risk industry is focused on vulnerability-based risk assessments. Not surprisingly then, organizations are overwhelmed by an ever-increasing list of vulnerabilities and associated patching. To keep up with everything they need to do, they prioritize — conducting risk assessments to identify the most critical issues.

But only 1% of vulnerabilities are ever exploited.[1] The current approach to patching simply keeps security teams busier every year — and farther behind the actual threats every day.

Common Cybersecurity Challenges

Skills gap shortage

The estimated cybersecurity talent gap globally is 3.1 million, with 64% of surveyed organizations reporting shortages.[2]

Cybersecurity tools proliferation

Among organizations that suffer from cybersecurity fatigue, 96% say that managing a multi-vendor environment is challenging, indicating that complexity is a major burnout cause.[3]

Alert fatigue

The average SOC team receives 11,000 daily alerts.[4]

Sources:

1 Kenna Security, "A Decade of Insights," 2020

2 (ISC)2, Cybersecurity Workforce Study, 2020

3 Cisco, CISO Benchmark Report, 2020

4 Forrester Consulting, "The 2020 State Of Security Operations," April 2020

The Shortcomings of Vulnerability Patching

Firewalls, antivirus solutions, collaboration software, operating systems. There's no shortage of systems that require constant patching and configurations that need to be corrected. The number of vulnerabilities is growing 15% every year[1], making it harder and harder to keep up with all the exploits that are out in the wild.

Yet 99% of those vulnerabilities are never exploited. Most importantly, patching only addresses the potential efficacy of your software. You need to not only test the software (and associated patches) but also the efficacy of:

- **Configurations**
- **Hardware**
- **Data flows**
- **Automation**
- **Alerting**
- **Personnel**

This is the only way to move beyond the current ineffective approach — and to prevent, detect and alert against the malicious activity that threat actors are carrying out in your environment.

Source:

1 Kenna Security, "A Decade of Insights," 2020

?

Questions to Ask

Consider your security strategy:

- Are you adding more money to the budget every year?
- How are you measuring your return on investment (ROI)?
- Is the ROI based on assumptions (e.g., "We've never detected an attack, so security must be working.")?

Why You Need a Paradigm Shift

For the last two decades, the cybersecurity conversation has centered around technical issues like vulnerabilities, threats, technology and budgets. But despite investing more money into security technologies, spending more time everyday patching vulnerabilities and checking compliance boxes, organizations continue to fall behind threat actors.

The main reason cybersecurity is failing? Security leaders are relying on assumptions of performance instead of the proven performance of their technology, people and processes.

Assumptions vs. Reality

You assume that:

- Your staff is trained, capable and focused on the right priorities.
- Your people effectively manage processes — including events, workflows and changes.
- Your technology is deployed and configured properly.

But how do you actually know that:

- Your processes are effective?
- Your people are following those processes?
- Your technology is performing as vendors claim?

The reality is:

- ✓ Compliance can't tell you if you are stopping malicious traffic.
- ✓ Trained employees are not necessarily proficient.
- ✓ Operational technology doesn't equal effective protection.

At a Glance:

Cybersecurity Readiness Definition

Cybersecurity readiness ensures that your people, processes and technology are ready in the event of a cyberattack. Your readiness posture is measured by assessing your security strengths and weaknesses in your live environment, against real threats.

If you're spending a majority of your time patching vulnerabilities that have a small likelihood of being exploited, you're not focusing on the threats to your organization. The only way to know how your defenses will stand up to your adversaries' tactics is by testing actual exploits against your production security system. This provides you the accurate metrics that measure your readiness to stop threats when they arrive at your door.

By measuring cybersecurity readiness, you gain true understanding of your business risk exposure. Only then do you have the data to guide the implementation of effective strategies that will optimize your cybersecurity investments and improve outcomes.

To measure your readiness, you need data-driven insights into how your defenses are performing in your live environment — across people, processes and technology. This intelligence will help you confidently answer these important questions:

- How well is your organization protected against a threat?
- What isn't working?
- Where are the gaps?
- What do you need to improve?
- What do you need to invest in?

The remainder of this ebook guides you through the steps to assess readiness in your organizations and to take the corrective actions that will elevate your readiness posture.

?

Questions to Consider

Is your risk exposure — including business outcomes such as downtime, financial impact and data loss — based on best estimates?

Your decisions are only as good as your data, and to make strategic security decisions, best estimates are simply not enough.

U.S. Air Force Takes Readiness Evaluation from Assumptions to Accuracy

Sophisticated threat actors constantly target the U.S. military's technology assets, which range from weapon systems to classified data. As part of a well-funded project, the U.S. Air Force launched new Mission Defense Teams (MDTs) to protect its systems. The teams had the latest technology, a fully compliant system and highly trained and confident personnel. Consequently, the leaders believed the MDTs were ready to defend against cyber threats.

To validate their readiness, the Air Force engaged SightGain's team to conduct live testing in the organization's environment. Simulated attacks were launched to evaluate the Air Force teams' prevention, detection, response and remediation capabilities. Surprisingly, the Air Force cybersecurity analysts and tools did not detect any of the 125 malicious techniques during the live tests.

The empirical data enabled the Air Force to move from assumptions to an accurate measurement of readiness. With these insights, the team implemented a new game plan, starting with correcting configuration issues in the intrusion detection system.

Continuous testing helped further tune and improve the results. Within days, the MDTs showed significant performance gains, including 68% improvement in detection and 89% faster threat identification.

What Is Cybersecurity Readiness?

The idea of readiness is inspired by the U.S. military.
The Department of Defense defines readiness as "the ability of military forces to fight and meet the demands of assigned missions." Likewise, cybersecurity is a system designed to do a mission.

Your cybersecurity mission depends on what's most critical for your organization to protect. Think of it as the objective or purpose of your cybersecurity strategy: **At the end of the day, what do you expect your cybersecurity to do?**

While the mission is different for each organization, it typically centers on three main areas:

- ✓ **Intellectual property**, such as proprietary information that sets you apart from the competition
- ✓ **Personally identifiable information** (PII) that customers and employees trust you to keep private
- ✓ **Business continuity**, or operational uptime, which impacts not only revenues but also brand reputation

Readiness, in turn, evaluates how well your three pillars — people, processes and technology — can carry out the mission of defending your organization against threats. Readiness is not simply about having those three pillars in place. You need to ensure that each of those pieces, and the system as a whole, can stand up against the adversary.

Setting Up Your Three Pillars for Success

3

People, processes and technology are intertwined, and each component contributes to your overall readiness.

People

To set up cybersecurity or security operations center (SOC) analysts for success, ensure your technology and processes are serving your people so they can make the right decisions and meet the expectations of the organization.

Processes

Your processes help your people respond to threats quickly and effectively, facilitating automation and providing the framework for how all the activities, procedures and roles should work together.

Technology

Security solutions rarely come out of the box ready to deploy in your environment. They must be tuned consistently to ensure they work as designed across your infrastructure. If your people aren't spending the time tuning the technology, they will not detect the threats.

Action Step

Review your cybersecurity mission. What are the objectives of your strategy and what outcomes do you expect? These expectations will help you measure your readiness in the next steps.

Evaluating Your Readiness

You don’t know how well your cybersecurity is performing unless you see it in action. Without testing, you’ll continue to miss attacks while assuming your systems are protected because your technology is operational, you’re getting alerts, you’re current on patching and personnel are responding to activity. That’s like assuming you’re healthy just because you’re taking a multivitamin, whereas many other factors, from your lifestyle to your environment, impact your health and physical performance.

The best way to assess readiness it by analyzing your security operations under “live-fire” scenarios — emulating attacks in your production environment. These simulations are designed to test against specific threats and provide empirical data without any detrimental effects to your systems.

Many organizations rely on breach-and-attack solutions for these kinds of evaluations. These tools do a great job at evaluating technology and some of the processes. However, they lack the people context because they don’t look at the human response — essentially, only giving you a part of the picture.

To evaluate your readiness, you need to test all three pillars in unison: not only how well the technology works but also how the analyst respond, along with the processes that connect the two.

Core Questions to Ask When Evaluating Readiness

People

1. Does your team have the right level of talent and skills?
2. How does your team respond under the pressure of a serious attack?
3. How well do people recognize threats?
4. When threats are discovered, do people react quickly and accurately?
5. Are you getting a good ROI on your staff investment?

Processes

1. Are the technologies properly configured to stop the most likely tactics?
2. Is the right log data flowing throughout your security stack?
3. Do your processes generate accurate alerts?
4. Are automated response processes effective?
5. Are you getting a good ROI on your process investments?

Technology

1. What technologies are preventing, detecting and alerting the most?
2. Do you have the right portfolio of technologies and are there redundancies?
3. Where should you invest next to fill security gaps?
4. How do you know what's marketing hype and what works in your environment?
5. Are you getting a good ROI on your technology investments?

Action Step

To help measure your readiness posture and risk exposure, map threat techniques across the MITRE ATT&CK framework and score performance based on emulation of those threats.

The Principles of

Cybersecurity Readiness

In the U.S. military, readiness is a continuous improvement process that focuses on field-trained forces and proper equipment that are evaluated against their ability to accomplish the mission: to fight and win anywhere and at any time. Measurements must be used to know how well the military forces are meeting the mission demands, and the evaluation of current capabilities must be ongoing as the environment and personnel change.

Core to the military framework are three ideas:

Mission

Missions change as adversaries take new approaches, but there's always the core mission, which dictates the necessary capability and performance requirements for the unit.

Capability

Capability is the specific equipment and type of personnel needed to successfully accomplish the mission as well as quantity and type of personnel.

Continuous assessment

Measurements must be used to know how well the military forces are meeting the mission demands, and the evaluation of current capabilities must be ongoing as the environment and personnel change.

Using this framework as inspiration, follow these three core principles when you assess your cybersecurity readiness:

Objective

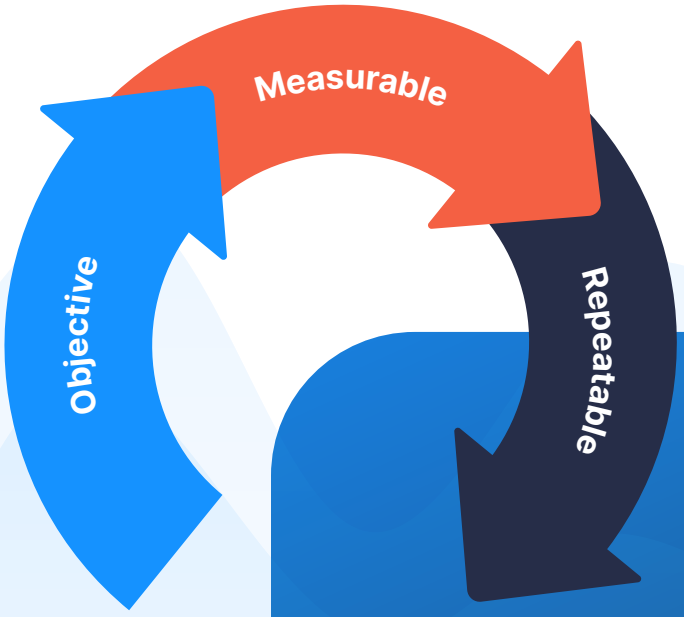
Readiness is agnostic of solution. It doesn't matter what kind of firewall you're using or the adversary's latest tactics. Readiness must be objective and based on the outcomes you expect for your organization's mission.

Measurable

You need hard data to analyze readiness, and this is where live-fire testing comes in. Without these empirical insights, you're only guessing about performance, and that's been shown to be inaccurate and is a risk you don't need to take. Further, measurable results enable you to make adjustments and documented improvements.

Repeatable

Readiness is not a "one and done" activity. The process needs to be repeatable so you can continue tuning your technology, refining your processes and training your people — all in a meaningful, ongoing way — using the same steps and metrics to evaluate progress.



Another important component of mission readiness is reporting to executive leadership. The military requires accurate, objective and timely reporting to oversight bodies such as the Joint Chiefs of Staff and U.S. Congress. In a business, this body is likely the board of directors or the executive suite. Objective, quantitative and timely reports enable your executive decision makers to:

- **Analyze the business risk exposure**
- **Understand your security investments' ROI**
- **Identify opportunities for reducing risk**
- **Update your strategic plans to reflect appropriate security priorities**
- **Allocate necessary resources to help you fill the readiness gaps**
- **Compare cost and performance of different solutions**

Questions to Ask

- How are you currently identifying your security strengths and weaknesses?
- What metrics do you use to report security ROI to your leadership?

How to Establish a

Continuous Cybersecurity Readiness Lifecyle

Readiness is a journey, not a destination. Your environment will evolve, the attack surface will expand and threats will change. That's why readiness is a continuous, iterative practice. You are testing consistently, tuning and optimizing, and investing where there are gaps. The readiness maturity framework has three main phases:

Baseline:

Establish your initial cybersecurity readiness.

Tuning:

Increase readiness to meet mission requirements.

Sustaining:

Ensure readiness over time.

Each of these phases comprises a series of repeatable steps focused on people, processes and technology to evaluate your cybersecurity system. To follow these steps, first you must determine your mission standards (or expectations) so you can evaluate your organization's ability to meet that mission in light of the threats it faces. These standards may include metrics such as percentage of threats missed (effectiveness), mean time to detect (MTTD), mean time to respond (MTTR) and other key performance indicators (KPIs) that you've established for your security program.

Those kinds of metrics are only one component of readiness. For a holistic view of readiness, you need to understand not only your desired outcomes but also all the dependencies that go into achieving the mission — and how your people, technology and processes interact and function together to protect your organization.

As you measure your readiness posture, you'll be able to:

- ✓ Understand your security strengths and weaknesses across your environment
- ✓ Identify the best opportunities for reducing security risks
- ✓ Optimize your resources and investments for the best ROI
- ✓ Pinpoint the gaps that can benefit the most from improvements
- ✓ Create an action plan for improving your readiness

The Advantages of Live-Fire Scenarios

In addition to evaluating your security in your production environment, live-fire testing has an advantage that most other methods don't offer: a signal injection.

When you're flying a plane or are manufacturing equipment, your environment provides a multitude of information to a system of sensors describing physical and environmental factors that alert you when something goes wrong. The cybersecurity environment does not provide that information organically, so security does not typically generate true performance signals. If you're missing an attack, you simply don't know that you're missing it.

Readiness assessments change the cyber environment's natural dynamic. Since live threat emulation injects that signal into your production environment for readiness assessments, you know exactly what to look for in your people and technology responses — and you know with certainty if people, processes and technology missed or caught the signal.

Although you can introduce threat emulation signals through penetration testing and red team exercises, those activities are both more expensive and sporadic. The benefits of live-fire testing include not only a continuous, automated and repeatable process but also a more comprehensive and proactive assessment.

1

Baseline:

Establishing Initial Performance

People:

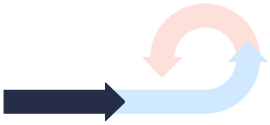
Evaluate against performance standards appropriate for individual roles, procedures and experiences.

- Did the analysts correctly identify the threat? How long did it take?
- Did they follow the right processes?
- Did they escalate the incidents as expected?
- How long did it take the incident responders to investigate and mitigate?
- Did they completely eradicate the threat?
- What steps were missed?
- Were there any duplicated processes or redundant steps?
- Did the team follow the playbooks that you have established?

Your people readiness goals are to:

- ✓ Measure how well individuals and the team perform
- ✓ Pinpoint inefficiencies in the processes they follow
- ✓ Understand if the workload is appropriate (e.g., whether analysts are overwhelmed or carry a disproportionate part of the responsibilities load)
- ✓ Identify the gaps that can be improved with training

1



Processes:

Evaluate process outputs and dataflows against expected results.

- Is threat detection data flowing where it's supposed to?
- Is data processing occurring as expected?
- What data is being logged but not forwarded (e.g., to SIEM/SOAR)?
- What automated activity should occur?
- How do your processes compare to industry standards?
- Is the process producing quality alerts for the analysts?

Your process readiness goals are to:

- ✓ Figure out what processes are not working and improving the operation
- ✓ Measure the efficiency and effectiveness of your processes
- ✓ Find inefficient and redundant processes
- ✓ Identify the gaps that can be improved with additional training, revised workflows and other tuning

Technology:

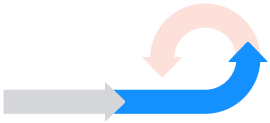
Evaluate each security solution and tool against what it's expected to do.

- Is each piece of technology blocking, logging and forwarding threat detection information as expected?
- What technology is not preventing or detecting actions that it should have?
- What technology is sending information to the SIEM/SOAR?
- Are the alerts being generated as expected?
- Which technology is the most effective and which is the least effective in stopping distinct types of attacks?

Your technology readiness goals are to:

- ✓ Measure how well your solutions are performing relative to vendor claims
- ✓ Understand which security solutions are the most effective and have the best ROI
- ✓ Figure out which technology areas you need to invest in to cover gaps

2



Tuning:

Increasing Readiness from the Baseline

Your readiness baseline testing has likely identified gaps and areas for improvement. To advance your readiness maturity, use that roadmap to improve performance across your organization before retesting. These are some of the recommended activities for increasing readiness:

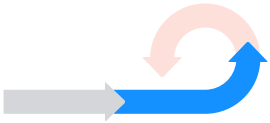
People:

The best way to improve your team's performance is by practicing against real threats. This may include training scenarios for:

- ✓ Basic threats, then building up to advanced threats
- ✓ The systems and technology that personnel are expected to use every day
- ✓ Incident escalation procedures
- ✓ Specific techniques for various threats
- ✓ Proper configuration of security tools

The results can be used to automatically assign training to individuals and teams based on areas that you identified for improvement from baseline. Use a mix of basic and advanced training, labs and self-testing modules.

2



Processes:

Process improvement connects both to people and technology and can be a mix of testing specific technology and tuning data flows and alerts. This may include activities such as:

- Fixing errors in data flows and configuration files
- Updating alerts and workflows
- Automating responses
- Identifying logs that don't add value

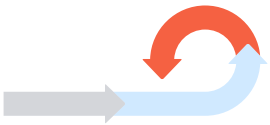
Technology:

Your improvements should focus both on optimizing your current stack and adding new solutions that are best suited for your organization to fill the gaps. Activities include:

- Comparing effectiveness of technologies to attacks and to threat groups
- Removing redundant technologies based on those that are most effective
- Evaluating alternatives based on standard tests of adversary activity and implementing those with the best fit for your organization

Depending on the gap between your baseline and your desired readiness state, this phase of the readiness lifecycle may take some time to complete. Make improvements, repeat the tests from the baseline assessment, make further improvements and test again. The idea is to continue iterating until you fix the problems and build up to the next phase, sustained readiness.

2



Sustaining Readiness

Sustained readiness means having a mature readiness approach that is built on continuous assessments and consistently tests and fine-tunes your organization's ability to fight evolving threats. As your environment, threats, technology and the team change, you will need to repeat the increased readiness activities to adjust for this evolution and to address the entropy that's unavoidable over time.

Recommendations for sustaining readiness:

- Automated testing — set up the live-fire systems to automate the testing, ensuring your security posture does not change and is reported if it does
- Unannounced live-fire attack simulations — to help keep your team on their toes, do not tell them they are experiencing an exercise
- Investments in gaps that cannot be addressed by tuning — add new technology or staff as necessary
- Automatically assigned trainings — to keep them current in their skills, assign both to individuals and teams based on new attack techniques and threat group activity
- Continuous automation improvement — to save labor and technology costs, automate responses to the greatest extent possible

Action Step

- Use your live-fire assessments to quantify the likelihood and the potential financial impact of a breach.
- Assign tailored online exercises, such as scenario-based interactive modules, to each analyst based on individual live-fire test results.
- To ensure a balanced security portfolio, optimize your current stack before you introduce new solutions for known portfolio gaps.

Improving Risk Management with

Continuous Cybersecurity Readiness

By analyzing performance results of individual technologies and people, your organization can determine the amount of risk reduction each component contributes. Combine this information with the costs of those components to analyze the ROI relative to the value those resources provide.

If the assessment process identifies gaps that can't be tuned away, evaluate the readiness of alternatives so you can present a business case. Use these insights to optimize the long-term cybersecurity portfolio and put the results in business terms that your executives and the board can readily understand so they can make data-driven decisions.

How SightGain Improves Readiness

SightGain is the only cybersecurity risk management solution focused on cybersecurity readiness. Unlike typical cybersecurity risk assessment and management tools that rely on industry benchmark data, compliance checklists and assumptions, SightGain tests and measures readiness using real-world attack emulations in your live environment to gather empirical data.

SightGain first quantifies your organization's risk exposure — including potential financial loss, downtime or data loss. Then it measures your readiness posture, identifying the specific strengths and weakness in your production environment — across people, processes and technology. Finally, the solution enables you to optimize your security stack and investments based on empirical data.

With SightGain, you get these core questions answered:

- **What's your cyber risk exposure?**
- **Which cyber capabilities are working or not working?**
- **How should you invest to optimize readiness?**

Eliminate the Guesswork

Ensure Your Team's Readiness

Stop throwing money at cybersecurity in hope of solving your security challenges. It's time for a paradigm shift.

In today's digitally driven world, you rely on data for making business decisions, innovating your business model and introducing new experiences for customers. Security should be no different. Just like you use data to make business investments, you need data-driven performance insights to make security decisions.

Improving your security readiness posture is a journey that requires ongoing assessments. Use empirical performance assessment evidence for complete clarity on how well your security is working and where you need to focus your improvement efforts.

By eliminating assumptions and changing the security conversation to readiness, you'll be in the best position to minimize your organization's risk and achieve the best security ROI.

About the SightGain Solution

SightGain's Continuous Readiness Platform is designed to find gaps and redundancies in the performance of people, processes and technology in cybersecurity systems. It uses live-fire attack simulations to measure, quantify and optimize cyber defense readiness.

SightGain

Learn more at **SightGain.com**