The Importance of Cyber Fitness:

A Vital Checkup for Your Organization

Author
Marc Brown
VP - Product & Sales - SCYTHE

Contributions by:
David Kennedy, Founder of Binary Defense and TrustedSec
Bryson Bort, Founder & CEO of SCYTHE
Trey Bilbrey, Lead Adversary Emulation Engineer at SCYTHE Labs

SCYTHE.IO

Introduction

Just as our bodies are susceptible to illness and injury, our organizations are vulnerable to cyber threats.

In our day-to-day lives, we understand the importance of maintaining good physical health. We exercise regularly, strive for a balanced diet, try to get enough sleep, and schedule annual checkups with our doctors. These practices ensure that we remain fit, detect any underlying health issues early, and ultimately live longer, healthier lives. But, as we invest in our personal health, we often forget that our digital lives need the same care and attention. Just as our bodies are susceptible to illness and injury, our organizations are vulnerable to cyber threats.

Welcome to the age of cyber fitness, where maintaining a strong cybersecurity posture is as essential as staying physically fit. Much like your physical health, your organization's cyber health relies on continuous monitoring, preventive care, and a thoughtful balance of proactive and reactive measures.

Annual Checkups: The Foundation of Cyber Health

In physical health, annual checkups provide a snapshot of your vital signs—blood pressure, heart rate, cholesterol levels, and more. Similarly, your organization should undergo regular security posture assessments. These serve as your annual cybersecurity physical, providing insights into your organization's strengths and vulnerabilities. Just as a doctor would use lab results to diagnose potential health issues, a comprehensive security assessment helps reveal hidden cyber risks—whether they stem from misconfigured systems, outdated software, or emerging threats.

By establishing a cyber hygiene baseline, organizations can assess the current state of their security practices and evaluate their compliance with industry best practices and regulations. This not only highlights areas that need immediate attention but also sets a foundation for continuous improvement throughout the year.

Annual checkups, however, aren't enough on their own. They must be complemented with continuous monitoring—like regular exercise and sleep—to ensure that your cyber health doesn't deteriorate over time.

Monitoring Vital Signs: Real-Time Audits & Threat Detection

Imagine relying solely on a once-a-year doctor's visit to monitor your health—ignoring signs of stress, fatigue, or illness for the remaining 364 days. In cybersecurity, relying solely on periodic assessments without real-time data leaves organizations dangerously exposed. Just as wearable devices and apps help us track our heart rate, steps, and sleep patterns in real time, continuous attack surface management provides real-time visibility into known and unknown endpoints, vulnerabilities, and threats lurking within your network.

Sophisticated threat actors can move swiftly like an illness sweeping through our bodies, an understanding of these threats and how to react (rest, medicine, water, etc.) as they arise is critical to staying healthy. By continuously scanning, testing, and analyzing your infrastructure, you gain a dynamic sense of your exposure preparedness. Knowing where potential exposures lie and how they may be exploited allows you to mitigate risks before they turn into full-blown breaches. It's the equivalent of detecting an elevated cholesterol level in a blood test and taking proactive steps to improve your diet and reduce future health risks.

The Power of Metrics: Tracking Cyber Fitness Progress

Just as fitness trackers help us monitor our physical progress, cybersecurity teams need metrics to gauge their cyber fitness. These metrics should track everything from the success rate of detecting and mitigating common attack vectors (such as phishing and ransomware) to the time it takes to identify and remediate threats.

For example, your cyber fitness score could be calculated based on detection and response rates of early-stage attack tactics, such as initial access, execution, and privilege escalation. If an organization can consistently detect and block these initial footholds, it drastically reduces the chances of more serious techniques—like lateral movement, data exfiltration, and ransomware—succeeding.

By continuously measuring and tracking these key metrics, organizations can improve their cyber health over time, just as individuals work to lower their cholesterol or increase their cardiovascular endurance. Over time, these small improvements add up to create a much stronger and more resilient cyber posture.

A Balanced Cybersecurity Diet: Offensive and Defensive Strategies

Measurement aside, a well-balanced lifestyle requires proper nutrition, exercise, and rest. Similarly, a healthy cybersecurity posture requires a balance between offensive and defensive strategies. Too many organizations focus solely on defense—installing firewalls, patching vulnerabilities, and deploying endpoint security systems—without putting enough effort into proactive measures that expose weaknesses before attackers can exploit them.

In the same way that strength training helps build resilience in muscles, adversarial threat emulation serves as the cybersecurity equivalent of stress-testing your defenses. Offensive security strategies—like simulated real-world attacks—allow you to see how well your organization can respond under pressure. This isn't just about finding exposures; it's about understanding how attackers move, where your defenses are weak, and how you can strengthen your response mechanisms. These insights are crucial for planning and prioritizing future security investments.

A holistic cybersecurity fitness plan also includes continuous security control validation—ensuring that your existing security controls, such as MFA, EDR, SIEM, and firewalls, are actually working as intended. It's not enough to deploy these controls; you need to ensure they can stand up against evolving threats, as well as environmental and exception drift. Regularly validating their performance is akin to ensuring your exercise routine is still effective for maintaining your physical health.

Defining A Cyber Training Plan: Quarterly Activities, Tests, and Measurements

Just as a fitness trainer provides a plan with prescribed exercises, nutrition guidelines, and regular checkups, a cyber fitness plan should be structured around regular assessments, activities, and metrics to measure progress. By breaking down the year into quarterly cycles, organizations can steadily improve their security posture while ensuring they stay responsive to emerging threats. Here are my recommendations for creating your cyber fitness plan:

Step 1: Baseline Security Posture

The first step in developing an annual cyber fitness plan is to baseline your security posture. This involves evaluating your current defenses, identifying existing gaps, and understanding your organization's risk vectors.

Activities:

1. **Cyber Risk Preparedness Index:** Execute an initial set of hygiene and exposure tests to assess your current level of compliance and defense efficacy against commonly used adversarial behaviors known to target your industry. These tests provide a realistic starting point for understanding your organization's exposures and the level of risk and probability of a successful cyber attack across your infrastructure.
2. **Security Control Validation:** Conduct a comprehensive audit of your current security controls, including endpoint detection and response (EDR), SIEM, firewall, MFA, and other deployed security technologies. Evaluate their coverage and effectiveness against real-world adversarial behaviors such as phishing, ransomware, and insider threats.

Outcome:

A detailed security posture report outlining your current strengths, weaknesses, and exposure preparedness index (EPI), including identifying high-risk adversarial techniques that could compromise your environment.

Step 2: Define Priorities Based on Risk Vectors

With a clear understanding of your baseline, the next step is to define priorities for the year based on your risk landscape, business objectives, and available resources.

Key Inputs:

1. Adversarial Group Targeting: Focus on the threat actors and adversarial groups that target your industry. These groups may have specific behaviors (TTPs) that should drive your security priorities.
2. Security Initiatives and Business Goals: Align your security priorities with the business initiatives funded for the year. Whether it's securing a new cloud deployment, protecting intellectual property, or complying with regulations, ensure your cyber initiatives support overall business goals.
3. Kill Chain Exposure: Prioritize defenses against the most vulnerable stages of the kill chain. If your organization is weak in early stages (e.g., Initial Access or Privilege Escalation), these should be top priorities for improvement.

Outcome:

A strategic priority list for the year, broken down by risk areas, business objectives, and areas of exposure.

Step 3: Implement a Quarterly Cadence of Testing & Improvements

Achieving and maintaining cyber fitness requires a structured plan of continuous testing and incremental improvements. By following a quarterly cadence, your team can consistently work toward mitigating risks while staying adaptive to emerging threats.

Activities (Quarterly):

Q1: Cyber Hygiene and Endpoint Security Audit

- **Activities:** Perform a cyber hygiene audit across endpoints, servers, and cloud platforms. Ensure that all systems are compliant with best practices. Leverage scanning/attack surface management tools to scan and map known and unknown assets.
- **Exercises**: Conduct a broad but less deep tabletop-purple team hybrid exercise focused on response procedures for common attacks (ransomware / phishing.)
- **Outcome**: A report outlining compliance gaps and improvement areas, as well as, recommended remediation actions for endpoint security.

Q2: Attack Surface and Adversarial Threat Validation

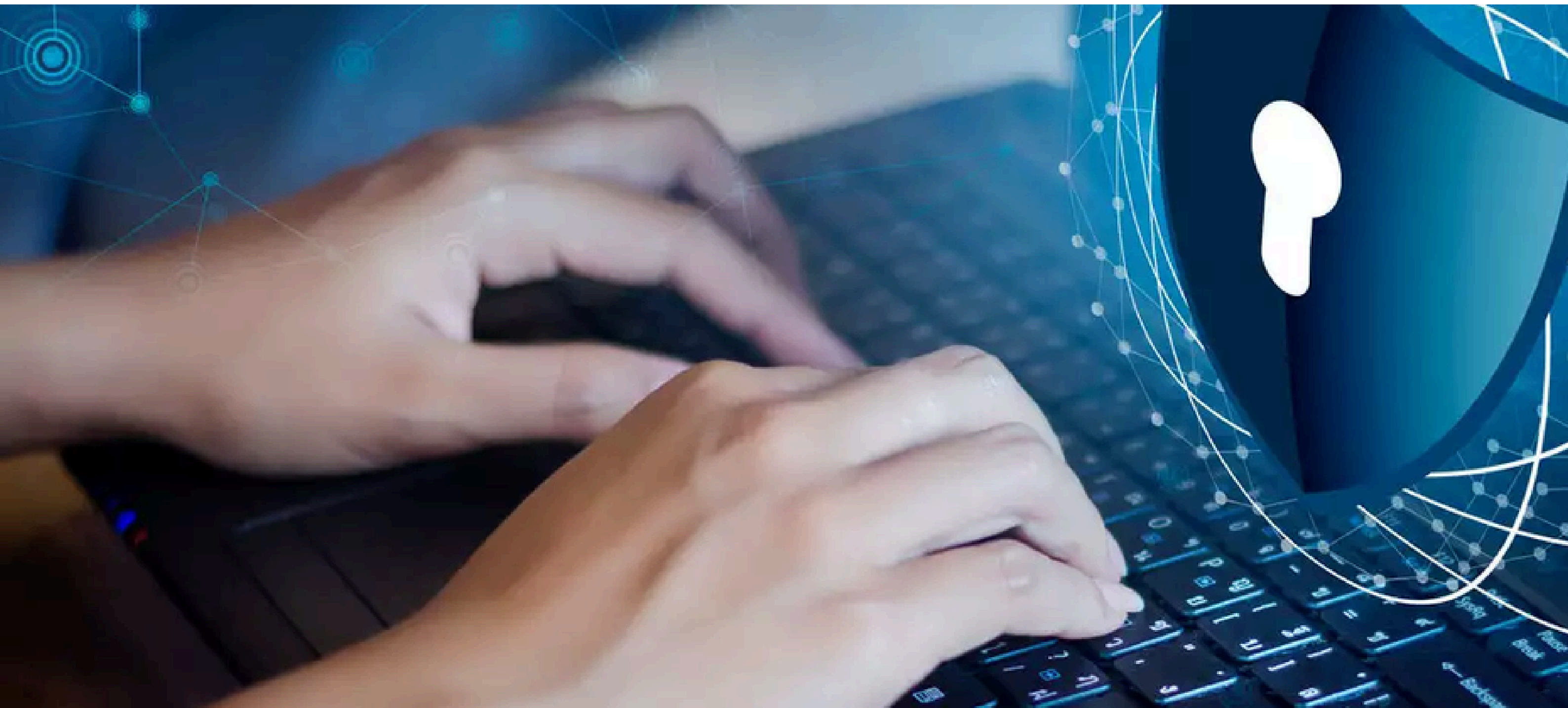
- **Activities**: Deploy adversarial threat emulation tests based on the most likely 'tier 1' attack vectors targeting your industry. Validate security controls such as EDR, SIEM, and MFA through continuous security control validation tests. Use real-world adversarial behaviors to check how well your controls mitigate threats.
- **Exercises**: Perform a purple team exercise to test collaboration between your offensive (red) and defensive (blue) teams. Test recently released threat campaigns and highest-risk threat vectors across the kill chain.
- **Outcome**: A risk exposure report highlighting the current Exposure Preparedness Index, vulnerable assets, and gaps, demonstrating the effectiveness of current defenses.

Q3: Risk Reduction

- Activities: Validate security controls against 'tier 2' attack vectors using real-world adversarial behaviors to check how well your controls mitigate threats.
- Exercises: Run recent threat emulations followed by a purple team exercise to test detection and response to specified attacks and related adversarial behaviors.
- Outcome: A risk reduction report identifying control gaps and providing recommendations to improve defenses.

Q4: Insider Threat and Advanced Testing

- Activities: Focus on insider threat simulations by emulating malicious internal actors attempting to escalate privileges, access sensitive data, or move laterally through the environment.
- Exercises: Conduct a tabletop exercise to validate your incident response plan against insider threats.
- Outcome: A report detailing the effectiveness of insider threat detection and recommendations for improving privileged access management.



Step 4: Measure and Track Cyber Fitness Improvements

To ensure continuous improvement, measuring progress over time and refining your strategy is critical.

Key Metrics:

- Threat Exposure Score: Track how your organization's exposure to critical attack vectors changes over time.
- Security Control Effectiveness: Measure how often security controls detect or mitigate adversarial actions. Use metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Compliance and Remediation Rates: Measure the percentage of systems in compliance with cybersecurity best practices and the time taken to remediate identified vulnerabilities.

Outcome:

A cyber fitness scorecard that tracks progress against defined objectives and demonstrates improvements in your overall security posture.

Step 5: Improved Reporting for Stakeholders

Comprehensive, easy-to-understand reports are essential for keeping key stakeholders informed. These reports should be tailored to different audiences and provide actionable insights based on the results of your security testing and validation efforts.

Reporting Types:

1. Executive Reports: Summarize high-level findings, risk exposure, and the effectiveness of security controls in a format that communicates impact to business leaders.
2. CISO Reports: Provide a more detailed technical breakdown of findings, focusing on kill chain defense, insider threat readiness, and continuous control validation.
3. Compliance Reports: Ensure that your compliance reports meet regulatory requirements (e.g., ISO, PCI DSS) by integrating results from audits, security assessments, and remediation efforts.

Outcome:

- Well-structured reports that highlight cyber fitness improvements, identify gaps, and provide strategic recommendations for further action.

Final Thoughts: A Long-Term Approach to Cyber Fitness

Much like personal health, cybersecurity is not a one-time effort—it requires ongoing care, attention, and adjustments. Annual checkups alone won't keep you healthy; the daily habits, continuous monitoring, and proactive interventions make the difference in the long run.

In the same vein, organizations must adopt a long-term approach to cybersecurity, focusing on continuous improvement, proactive defense, and strategic offense. Incorporating technologies and practices that focus on cyber hygiene, attack surface analysis, exposure hunting, and continuous control validation ensures that your organization is prepared for today's threats and tomorrow's unknowns. Just as achieving personal fitness requires a combination of regular check-ups, exercise, and a balanced lifestyle, maintaining cyber fitness requires a balance of proactive strategies, continuous monitoring, and periodic evaluation.

With the stakes as high as they are in today's market, keeping your organization cyber fit isn't just an option—it's a necessity.

www.scythe.io | info@scythe.io