immersive

eBook - Be Ready for GenAI

Building Cyber Resilience in an Age of AI Threats

Version: 01 | Published: 04 2025

POWERED BY C7

www.immersivelabs.com

CONTAINER 7

Introducing the Container 7 Team

This eBook was developed by our new Container 7 Team— a group of cybersecurity experts dedicated to tackling the evolving challenges of AI-driven threats. Made up of red teamers, threat researchers, cyber drill architects, and the minds behind our Immersive Labs, the team brings deep expertise in offensive security, incident response, and resilience engineering.

Container 7 represents more than just a name; it's where Immersive's first cyber exercises were built and where we continue to push the boundaries of cyber readiness. This eBook reflects that approach—grounded in real-world threats, practical defense strategies, and the need for continuous improvement. AI is changing the game.

Contents

immersive

Introduction: The Dual Nature of GenAI

78%

of CISOs agree that AI-assisted cyber threats are having a significant impact on their organization.

Generative AI (GenAI) is revolutionizing industries with tools that emulate human creativity, intelligence, and output. Yet, as these systems become embedded in virtually all aspects of our digital infrastructure and interactions, they expose organizations to novel threats—from prompt injection attacks to advanced social engineering.

According to new research, 78% of CISOs agree that AI-assisted cyber threats are having a significant impact on their organization, and 45% of cybersecurity professionals do not feel prepared for the reality of AI-powered cyber-threats.*

To safeguard their organizations, cyber leaders need to simultaneously prepare their workforces for rapidly changing GenAI risk, while implementing risk-reduction protocols that keep humans in the loop.

This e-book outlines how combining time-tested security practices with cutting-edge cyber drills and a secure-by-design culture builds lasting cyber resilience for an age of rapidly evolving GenAI threats.

*Source: Darktrace: The State of AI Cybersecurity

Promise & Peril

Risk in 2025

Evolving GenAI Cyber Threats

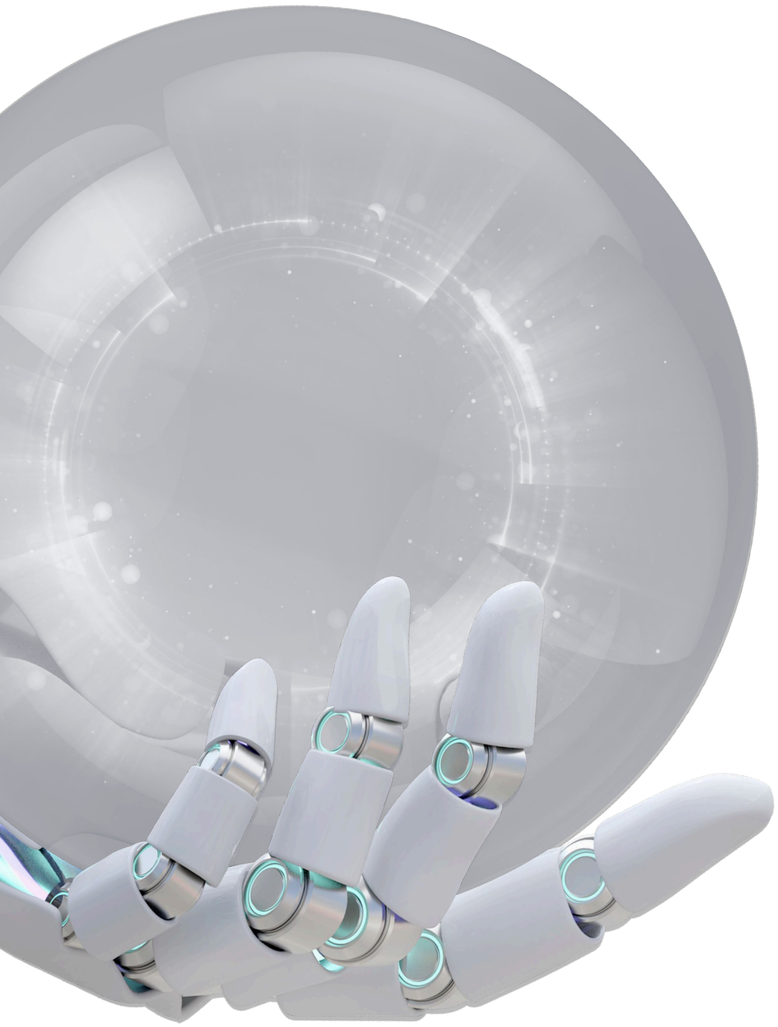
Cybersecurity risk is growing as GenAI becomes ubiquitous. Threat actors are increasingly using GenAI to improve the effectiveness of their social engineering attacks.

We see cyber criminals using these tools in much the same way most of us do: rapidly automating complex or monotonous tasks, which for malicious actors includes generating more effective phishing and smishing messages.

But, among the most concerning GenAI risks are prompt injection attacks, where a malicious actor tricks Large Language Models (LLM) into revealing sensitive information. Immersive's research shows that 88% of participants successfully tricked a GenAI bot into giving away sensitive information in at least one level of an increasingly difficult challenge.

This attack vector underscores a broader challenge: GenAI systems can be manipulated in ways that security teams have yet to fully anticipate.

Another threat vector is organizations' own use (or misuse) of GenAI tools, such as AI-assisted coding tools, which can inadvertently create vulnerabilities that can be exploited by attackers if proper protocols are not in place. In this environment, static security postures are no longer viable; organizations must adopt continuous, adaptive cyber resilience frameworks.



Predictions for the Next Wave of GenAI-Driven Attacks

Our experts and many industry analysts anticipate a dramatic escalation in GenAI-assisted attacks.

Adversarial Arms Race:

We have seen threat actors engage with LLMs to perform vulnerability research, either to better understand publicly reported CVEs and exploits, or to use their code review capabilities to compare patches and generate exploits.

Supply Chain Compromise at Scale:

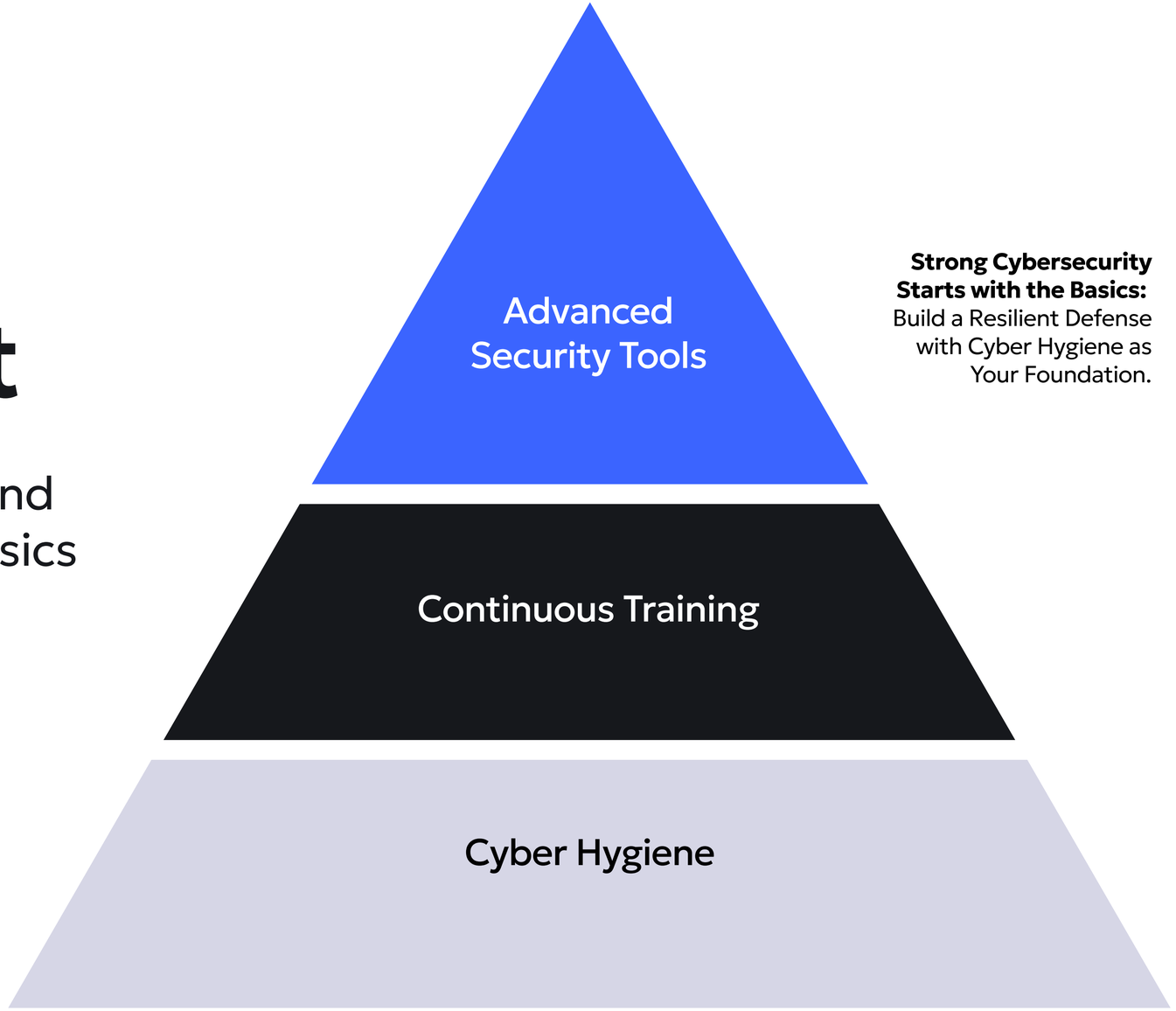
Threat actors use LLMs to perform reconnaissance against organizations, including researching technologies, platforms, and associations, and use this intelligence to craft social engineering attacks leveraging known vulnerabilities.

Cyber Hygiene

The Importance of Cyber Hygiene and Continuous Skills Development

In an era of headline-grabbing GenAI tools and threats, it’s easy to overlook the timeless basics that remain the cornerstone of effective cybersecurity.

Cyber hygiene isn’t about chasing the newest technology—it’s about ensuring that the cyber fundamentals of an organization are strong and pervasive throughout the workforce. In this chapter, we explore why these basics matter, how to bridge the gap between technology investments and human upskilling, and the critical importance of continuous training in a rapidly evolving threat landscape.



Strong Cybersecurity Starts with the Basics: Build a Resilient Defense with Cyber Hygiene as Your Foundation.

Why Cyber Hygiene Remains Critical for Defense

Prioritize

Despite the allure of advanced GenAI tools, the basics of cybersecurity remain unchanged. Regular patching, secure configuration, and stringent access controls remain a vital line of defense.

Even as attackers leverage new technology, many breaches still occur because organizations and their leaders overlook or fail to prioritize these fundamental practices.

Start:

- Implement automated patch management systems.
- Regularly audit system configurations and access controls.
- Schedule routine vulnerability assessments.

Stop:

- Relying solely on advanced security tools without maintaining basic controls.
- Delaying updates due to operational inertia.

Continue:

- Enforcing strict access policies and user permissions.
- Maintaining a proactive incident response plan.

Exercising for a Cyber Ready Workforce

Improve

Far too many organizations invest heavily in new security technologies, while underinvesting in cyber exercising for their teams. This is a critical mistake and one that creates an imbalance that leaves the human element - the very core of an organization's defense - vulnerable.

Savvy leaders know they must continuously prove and improve cyber capabilities across, and at all levels, of the organization to guard against emerging threats - especially in light of new threats posed by GenAI.

Start:

- Allocate a dedicated budget for regular cybersecurity training, exercising, and drills.
- Incorporate hands-on, scenario-based exercises into your training programs.
- Foster a culture of continuous learning through mentorship and peer reviews.

Stop:

- Overemphasizing tech stacks at the expense of workforce development.
- Assuming that advanced tools eliminate the need for ongoing training.

Continue:

- Investing in innovative security technology.
- Conducting periodic skills assessments to identify training gaps.

Building a Continuous-Learning Culture

Educate

A culture of continuous learning is essential. As AI-related threats evolve, training programs must be updated to cover new attack techniques such as prompt injection.

This ongoing education helps your teams remain agile, ensuring they can adapt quickly to emerging risks while reinforcing the fundamentals of cyber hygiene.

Start:

- Implement regular micro-training sessions that address the latest threat trends.
- Simulate real-world scenarios and reinforce learning.
- Measure training outcomes using performance metrics and feedback loops.

Stop:

- Relying on one-off training sessions that quickly become outdated.
- Using static, lecture-based training methods that do not engage learners.

Continue:

- Encouraging cross-departmental collaboration and sharing of best practices.
- Updating training materials as new vulnerabilities and attack techniques are identified.


Resilience

Cyber Drills and the Future of Resilience

Legacy cyber training methods have become obsolete because they tend to be check-box exercises that leave teams overconfident and underprepared, often without any data to prove one's actual cyber capabilities. They also seldom keep pace with rapidly emerging threats, such as AI-assisted attacks.

A growing number of leaders at the world's largest organizations are turning instead to Cyber Drills - interactive experiences that pressure-test teams' decision making against a simulated attack - as a way to build lasting cyber resilience.

Cyber Drills are beneficial because they often reveal skills or judgement gaps in even the most confident teams—areas that can be improved before it's too late.

We predict that Cyber Drills will soon become as common as fire drills because they place teams in dynamic, high-pressure scenarios that mirror actual incidents, enabling them to build the muscle memory necessary for rapid, coordinated responses.

94%

of cyber leaders have deployed Cyber Drills, or plan to, within the next three years to better prepare their people for threats.

Source: Immersive Cyber Readiness Survey, 2025

Proving and Improving Cyber Readiness

Cyber Drills are more than a preparedness exercise—they generate measurable insights that enable organizations to prove and improve their resilience. By tracking metrics such as incident response times, decision quality, and interdepartmental coordination leaders can see where their organization is strong and weak and upskill teams. The benchmarking data that comes from these exercises become a key performance indicator, reflecting how well the organization can detect, respond to, and recover from incidents.

Key Elements of Effective Cyber Drills:

Assessment and Feedback:

Detailed after-action reporting that identifies strengths and gaps.

Iterative Improvement:

Using Cyber Drill outcomes to refine playbooks, update technical controls, and improve training.

Objective Metrics:

Establishing benchmarks that can be tracked over time to demonstrate improvements in readiness.

Effective Cyber Drills must encompass the entire organization—from technical teams to executives—and even extend to the supply chain. Cyber Drills and smaller versions of these (called Micro-Drills) can provide brief, but impactful exercises to build readiness across diverse roles without disrupting daily operations and keep pace with new attacks.

How to Know You're Ready: Metrics, Benchmarks, and Continuous Improvement

Determining readiness involves more than running an exercise. It requires:

Quantitative Metrics:

Tracking response times, error rates, and the quality of decision-making.

Qualitative Feedback:

Gathering insights from participants about their confidence and clarity during drills.

Continuous Improvement:

Regularly updating your drill scenarios based on lessons learned and evolving threats, ensuring your resilience improves with each iteration.

Extending Cyber Drills to The Boardroom

Strategy

Strategies for GenAI Safeguards

Secure-by-Design for GenAI Systems

To counter AI-specific threats, security must be integrated from the ground up. A secure-by-design approach entails:

- **Embedding Security Controls Early:** Implement robust data loss prevention (DLP) and input validation as part of the AI development lifecycle.
- **Context-Aware Filtering:** Develop intelligent filters that differentiate between legitimate and malicious inputs.
- **Regular Security Audits:** Continuously evaluate your AI systems to ensure they adhere to best practices and emerging standards.

Integrating Advanced Security Controls and Continuous Feedback Loops

A comprehensive resilience strategy combines strong cyber hygiene with innovative security measures. This includes:

- **Automated Monitoring and Real-Time Analytics:** Utilize AI-driven tools to detect anomalies and monitor system behavior continuously.
- **Feedback Loops:** Leverage data from Cyber Drills to inform and update security protocols - ensuring that every drill contributes to an ever-improving defense posture.
- **Objective Measurement:** Use metrics like the Cyber Resilience Score to demonstrate improvements to regulators, insurers, and internal stakeholders.

Embedding “Prove and Improve” into Your Cyber Resilience Roadmap

Every cyber resilience program should be built on a continuous improvement cycle:

- **Assessment:** Regularly evaluate your current security posture through both drills and formal audits.
- **Training:** Update training modules to include the latest AI-driven threat scenarios.
- **Cyber Drills:** Implement a cadence of immersive, realistic exercises that cover various disruption scenarios, including supply chain and cross-functional incidents.
- **Adaptation:** Refine policies and technical controls based on drill outcomes and real-world incident data.
- **Collaboration:** Engage cross-functional teams—including IT, legal, compliance, and external partners—to ensure a holistic approach to resilience.

The Role of Regulatory and Supply Chain Assurance

Increasingly, regulators and insurers are demanding tangible proof of resilience. Incorporate supply chain exercises into your program to ensure that not only your organization, but also your key partners are prepared for cyber incidents. This comprehensive approach helps build trust with external stakeholders and meets emerging regulatory requirements.

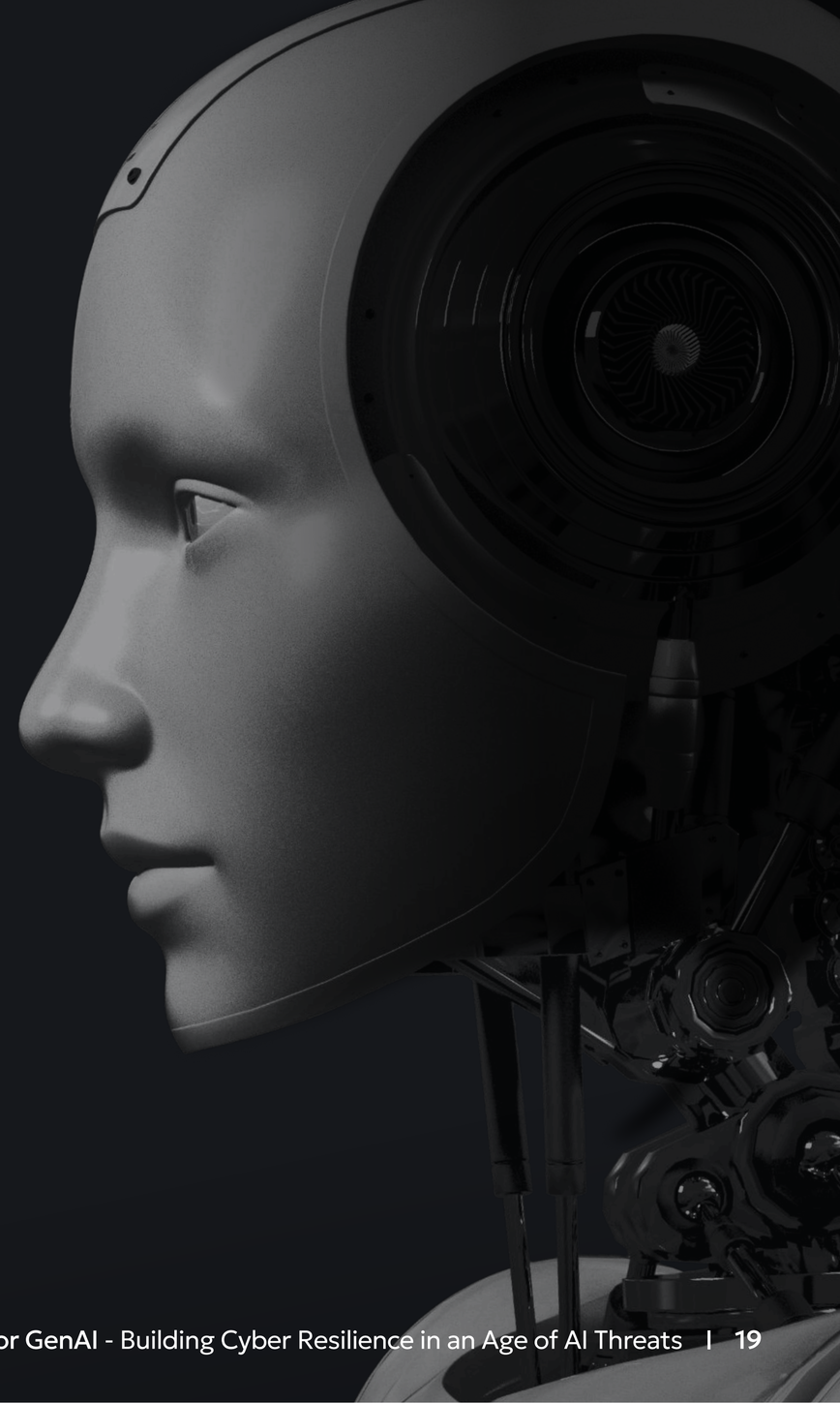
Next Steps

The convergence of GenAI and cyber - security is redefining organizational risk.

To remain resilient, organizations must integrate traditional cyber hygiene with dynamic, immersive Cyber Drills and a secure-by-design approach for GenAI systems. By adopting a “prove and improve” strategy and culture, leaders can create a continuously evolving defense strategy that is measurable, actionable, and effective.

Empower your organization with a robust, GenAI-forward resilience program. Download our Cyber Drill Best Practices Guide →

Contact the Immersive team → to learn how our solutions can help you build a future where your cyber resilience is continuously proven and improved.



Be Ready

immersive

Continuously Assess, Build, and Prove Your Cyber Resilience

Our immersive cybersecurity solutions ensure your team is prepared to tackle and defend against the evolving cyber risks of today, and tomorrow.