Pluralsight

Pluralsight SecureReady

Stop Chasing Unicorns

How to Build Elite, Battle-Ready Security Talent From Within

Introduction

The margin for error in cybersecurity has vanished. With breach costs hitting $10.22 million per incident[1] and 91% of organizations lacking Zero Trust maturity,[2] the stakes have never been higher. But you can't buy your way out of this risk—you have to build your way out.

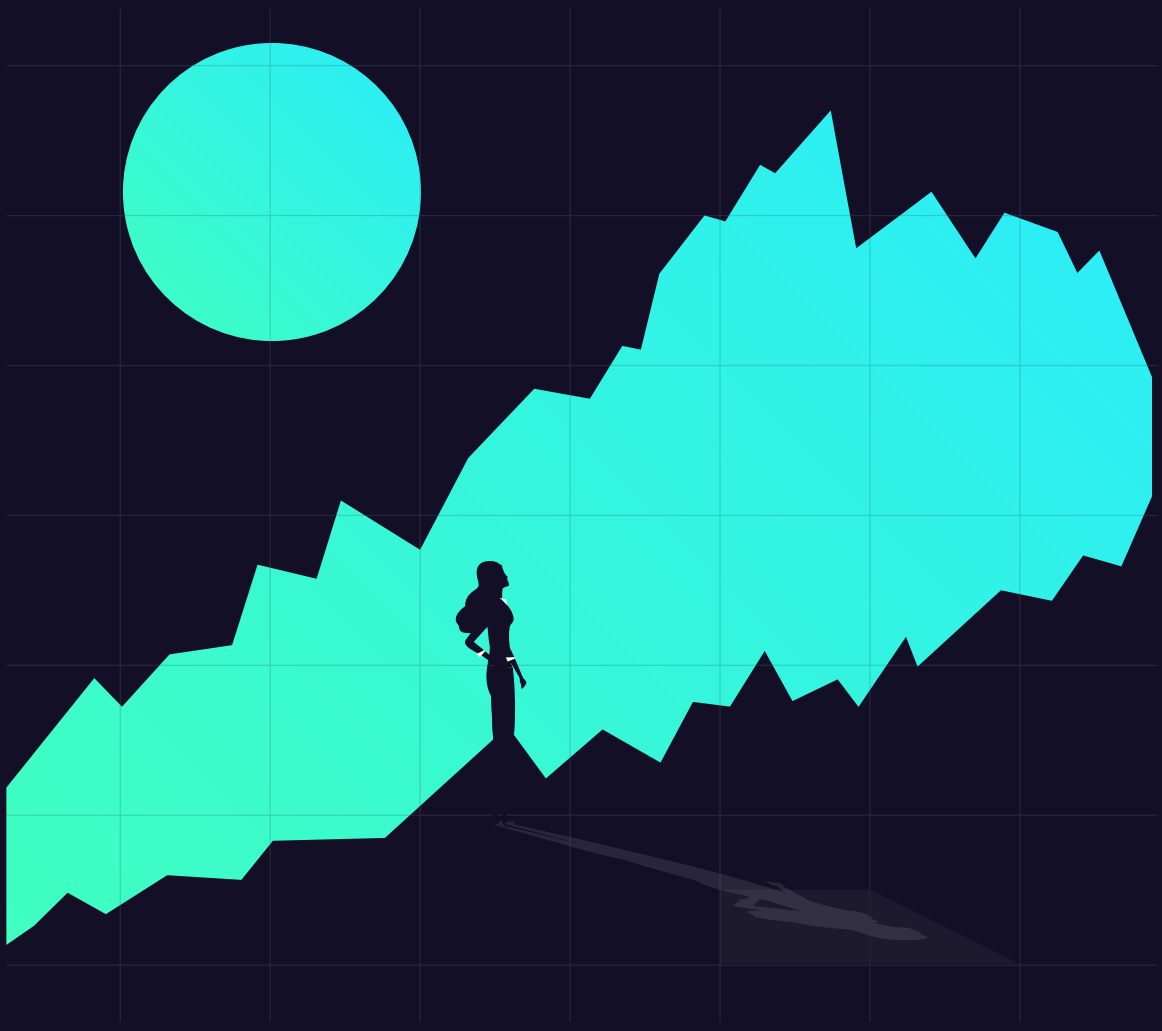
With Gartner citing the talent shortage as the #1 challenge for CISOs,[3] the only sustainable path to a protected security posture is building advanced experience from within. Security leaders must stop searching for unicorns and start developing battle-tested practitioners internally.

To achieve an elevated security posture, organizations must drive this shift, moving from reactive hiring to proactive, validated skill building. This guide outlines the strategic shift required to transform your existing workforce into a validated line of defense.

1 IBM, Cost of a Data Breach (2025)

2 RSA, ID IQ Report (2025)

3 Gartner, CIO and Technology Executive Survey (2024)



Audit internal potential, readiness, and skills

You can’t build what you can’t measure. To create elite talent from within, organizations must first understand the raw potential of their existing workforce and align it to their strategic defense goals.

Step 1: Conduct a security readiness review

Stop guessing. Start architecting. Building advanced capabilities requires strategic orchestration, not ad hoc course assignments. Best-in-class security organizations utilize a structured approach to map existing roles and launch team-wide assessments to establish a baseline.

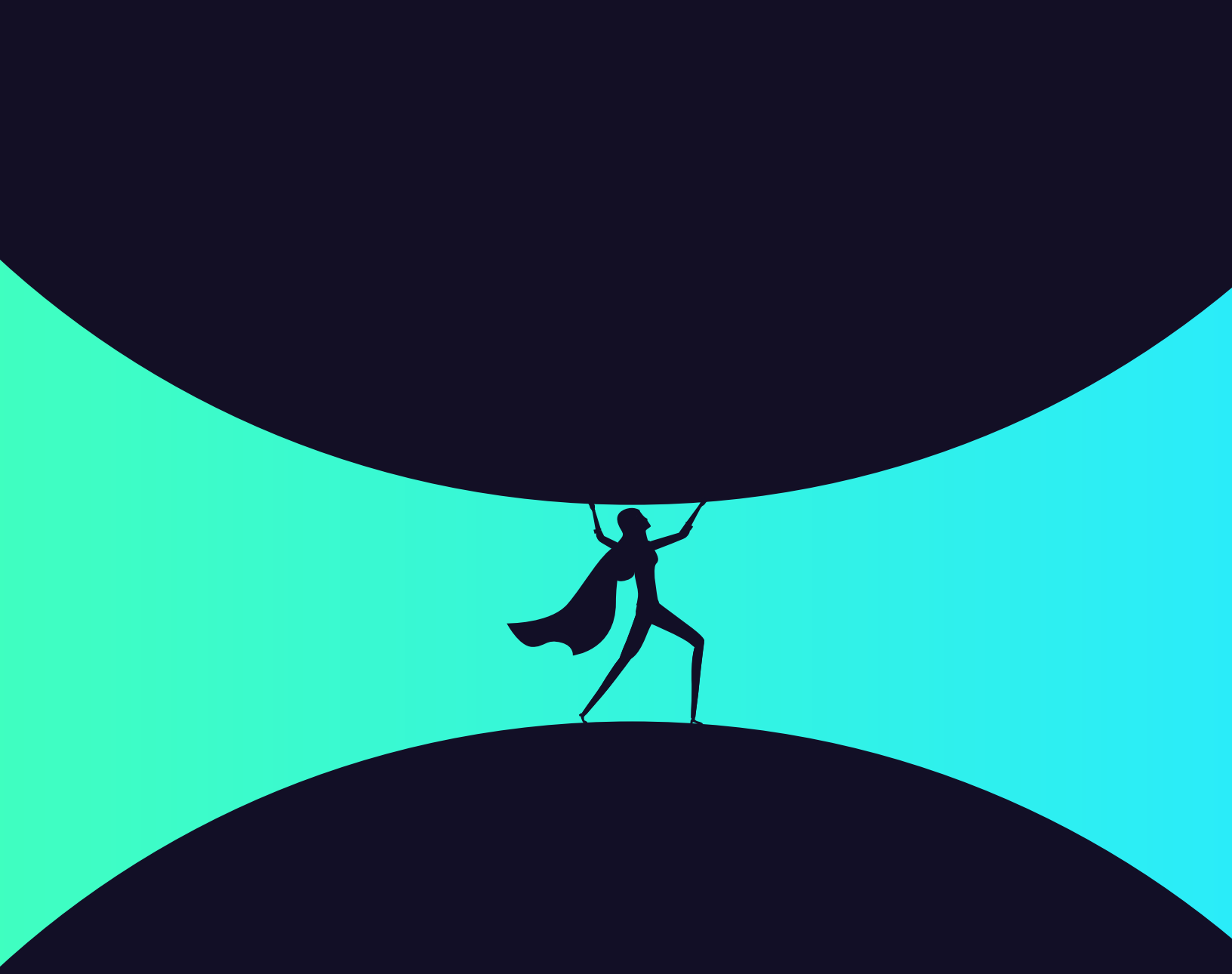
The necessity of alignment. Successful programs require a centralized program owner responsible for strategic alignment rather than leaving learning up to individual employees. This architect must identify specific readiness gaps by surveying both security practitioners and leadership to expose critical misalignment.

For instance, according to the Pluralsight Tech Skills Report (2025), 38% of technologists say their leaders are not aware of existing skills gaps. Furthermore, strategic priorities often differ: while executives rank data as a top-three priority for 2026, IT professionals prioritize AI/ML. The process should culminate in a detailed report that bridges these perspectives, informing a customized development roadmap for the next 12 months.

Step 2: Map roles and inventory skills

Defining elite standards. To cultivate specialists, leadership must define what “elite” looks like for their specific technology stack. While best practices involve referencing industry-standard frameworks like NIST/NICE, DoD/DCWF, or ENISA, organizations don’t have to mirror them exactly. Instead, mapping role expectations directly to your org chart is what transforms generic job titles into clear, achievable technical milestones.

Baselines that matter. Organizations should use quantitative skill assessments to gauge practitioner capabilities across the entire department. This allows leaders to measure the progression gap—identifying exactly how far internal candidates are from the mission-critical standards required for defense.



The training ground: How to forge elite capabilities

Once you've identified the potential of your teams, the focus shifts to transformation. The goal goes beyond upskilling. It's about forging practitioners into battle-tested specialists who deliver continuous, proactive defense.

Step 3: Set learners on high-velocity learning paths

Specialized tracks for critical outcomes. General awareness training is insufficient for security professionals. If you can't hire for skills like pen testing or incident response, you need a way to build that expertise from within—giving your team access to targeted, high-impact learning paths that develop hard-to-find capabilities.

The speed of relevance. Elite talent must move faster than the market. A modern workforce strategy requires rapid-response mechanisms that ensure teams are trained on "breaking headline" threats immediately. Programs should provide CVE emulation content within hours or days of a major disclosure, ensuring internal teams gain the experience to detect and mitigate new threats before they impact the live environment.

Certification that supports readiness. For many organizations, certifications are more than credentials. They are tied to compliance requirements and critical role eligibility. Certifications like CISSP, CompTIA Security+, and SC-900 are often required for practitioners to advance or meet organizational standards. But preparing an entire team to certify on a deadline is difficult to scale. While self-paced prep works for individuals, instructor-led training accelerates team-wide progress. Intensive, multi-day sessions provide the structure and focus needed to certify faster, with higher confidence and better alignment to your security goals.

Step 4: Battle-test teams in immersive live-fire experiences

Battle-testing the build. To validate readiness across security operations, GRC, and engineering, organizations must utilize labs that replicate the full friction of a genuine breach.

- **Full-spectrum adversary emulation:** Real readiness requires executing complete kill chains, not just "tool tours" or simulations. Learners emulate workflows from attack-surface mapping (Amass) to Active Directory takeover. Advanced scenarios like Windows Defender evasion and OT/ICS security ensure teams train against the exact tradecraft used by actors like Volt Typhoon and LockBit.
- **Integrated attack-and-defend validation:** Best-in-class labs pivot immediately from exploitation to investigation. Teams must analyze investigation-grade artifacts—packet captures, disk forensics (Autopsy/FTK), and memory forensics (Volatility)—to validate their ability to catch the very exploits they just deployed.
- **Enterprise SOC simulation:** To find the signal in the static, operations teams must work with SIEM-relevant, multi-source data (Zeek, Splunk, or Windows telemetry) rather than toy logs. Training requires writing custom detections and managing false positives to identify genuine threats amidst realistic operational noise.

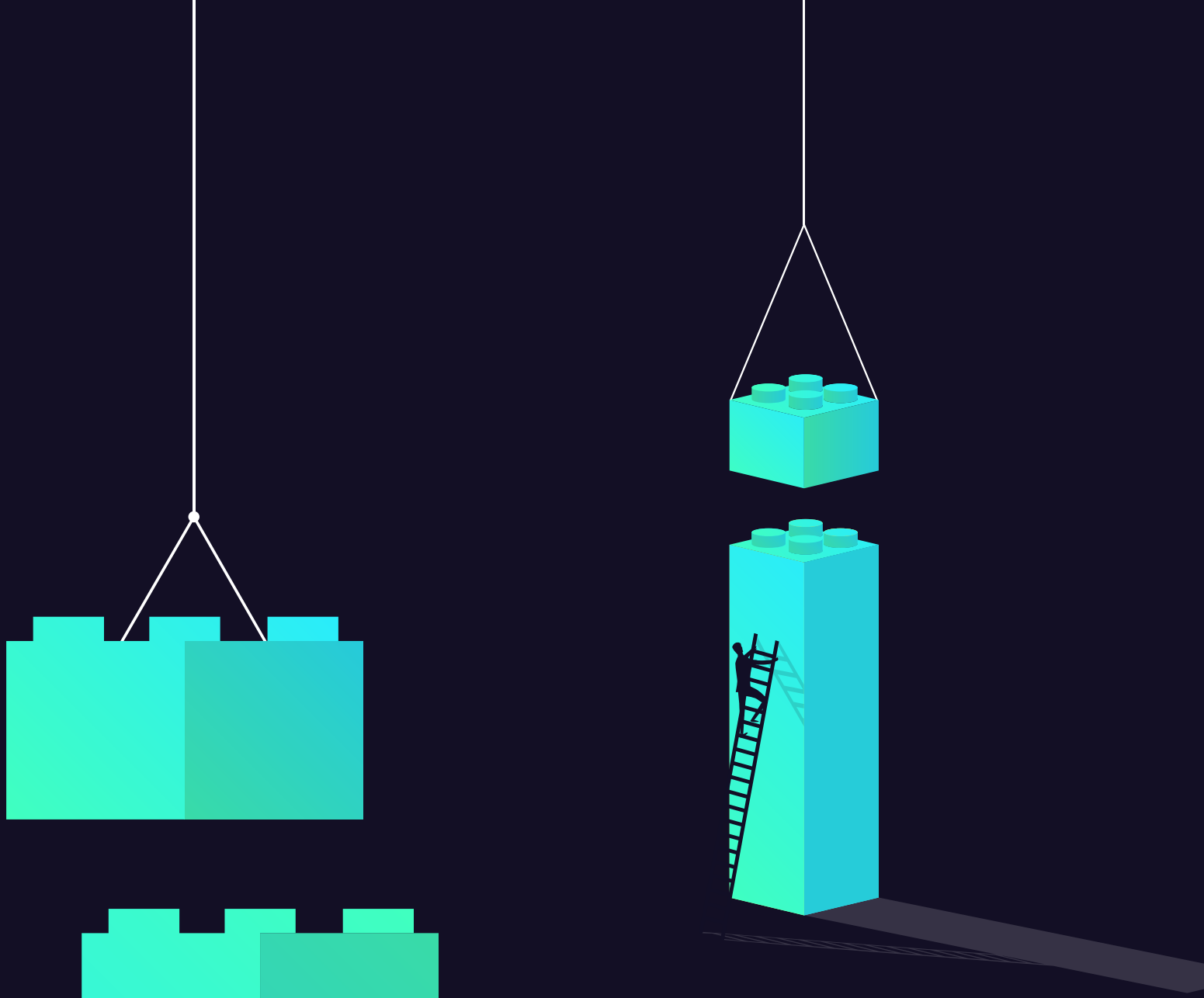
Verify your teams' readiness

The final piece is proving that the internal build was successful. Security leaders need metric-driven confidence to ensure ongoing organizational readiness.

Step 5: Measure progression and optimize

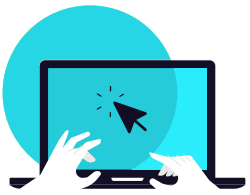
Trust, but verify. To confirm elite talent has been built, organizations must measure collective response capabilities alongside course completion rates. The most effective programs use unguided challenge labs and security sandboxes to measure skill progression in real time.

Optimization loops. These assessments must force practitioners to solve problems with zero assistance, effectively simulating specific attack techniques against defensive monitoring tools. This data provides the proof that internal candidates have officially bridged the gap and are ready for mission-critical roles.



Sustain excellence to build business value

An elite internal workforce is a valuable asset that must be retained and leveraged to satisfy governance requirements.



Step 6: Address org-wide objectives through targeted, hands-on learning

Intensive multi-day security workshops. Use immersive, multi-day formats to upskill your security team on critical topics. Focus areas might include incident response, digital forensics, AI threat modeling, or other high-impact domains.

Security for engineering. Extend your security posture beyond the core team by helping developers and architects build baseline skills in DevSecOps, secure coding, and security architecture. Integrating security early in the development lifecycle reduces risk and improves resilience.

Rapid certification prep. Support your team's path to industry-recognized certifications—like CISSP, Security+, or SC-900—by combining on-demand prep with live, intensive training sessions. This kind of high-focus learning can ensure teams get certified faster and with greater confidence.

Conclusion

How Pluralsight SecureReady delivers an end-to-end security readiness solution

While the strategic guide above outlines the requirements for a modern defense, Pluralsight SecureReady provides the solution. We replace the guesswork of general content libraries and the isolation of niche tools with a fully managed, structured ecosystem.

We combine the depth of an exhaustive content library with the realism of enterprise-grade labs and dedicated program management orchestration to deliver a readiness program designed to achieve three critical business outcomes:

01 Elevated security posture

Move beyond check-the-box compliance to build a collective defense. Security development isn't one-size-fits-all. Unlike general providers that offer volume without verification, we work with you to map your specific organizational needs to standard capability frameworks like NIST/NICE and DoD/DCWF.

- **Strategic alignment:** Through dedicated program management, we'll conduct an Annual Security Readiness Review, evaluating team strengths across 16 key security capabilities to identify blind spots before attackers do.

- **Security role-based paths:** Master the specialized skills required for security event triage, threat hunting, and incident response. Our security role-based paths combine courses, Skill IQ assessments, and practice exams into one structured learning experience. Whether focusing on malware analysis or penetration testing, these leveled paths—beginner, intermediate, and advanced—allow you to build proficiency in the right order and at the right pace.

02 Continuous, proactive defense

Neutralize threats before they touch your production environment. The gap between a vulnerability disclosure and an exploit is shrinking. We empower your team to shift from reactive to ready by providing the how-to guide for patching and protecting systems immediately.

- **The 48-hour advantage:** When a major CVE is disclosed, our Rapid Response Content team releases training and hands-on simulation labs within 48 hours. Your team validates defense strategies against headlines in real time, ensuring your perimeter is hardened while competitors are still reading the news.

- **Realistic noise-filled labs:** We don't just test code. We test resilience. Our 350+ enterprise-grade multi-system labs simulate complex networks under siege, forcing teams to sift through operational noise to find the needle in the haystack.

03 Ongoing organizational readiness

Ensure your team is mission-ready through verified execution. CISOs lack objective data on how their teams perform under pressure. We solve this by shifting from training to testing, providing the objective data needed to measure collective response capabilities.

- **Verified capability:** Unlike guided labs that offer hints, our challenge mode labs drop practitioners into scenarios with zero assistance. This provides a binary pass/fail check that confirms a team member can execute independently before they touch production systems.

- **Orchestrated growth:** We sustain readiness through practitioner-led training delivered virtually. We validate your team's capability using security awareness, defense, and rapid-response courses tailored to your industry and tech stack. This ensures the team can neutralize the specific risks targeting your environment.

The SecureReady difference

We built this solution because security leaders told us they needed more than just access to content—they needed proven readiness. We solve the critical capability gap that general content libraries and niche tools ignore, bridging the divide between knowing a concept and executing a defense.

- **Managed execution vs. self-directed guesswork:** Unlike platforms that hand you a library card and walk away, your dedicated program manager orchestrates the entire lifecycle—from readiness reviews to scheduling live team workshops—ensuring you hit your milestones without the administrative burden.

- **Enterprise realism vs. gamified puzzles:** Our 350+ enterprise-grade security labs aren't isolated puzzles. They utilize enterprise-grade datasets, real SIEM telemetry (Splunk, ELK, or Zeek), and investigation-grade artifacts to simulate the true friction of an enterprise breach.

- **Adversary emulation vs. tool tours:** We go beyond teaching tools by emulating full kill chains. From Windows Defender evasion to OT/ICS SCADA scenarios, your team trains against the exact tradecraft used by active threat actors like Volt Typhoon and LockBit.