



ORCHID BANK

Executive Readiness Pack

H1 2025

© Immersive - All Rights Reserved



Executive Summary

- Introduction
- Resilience Score

Benchmarking

Threat Response

Technical Skills

Compliance

Secure Code

C7 Insights

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

01

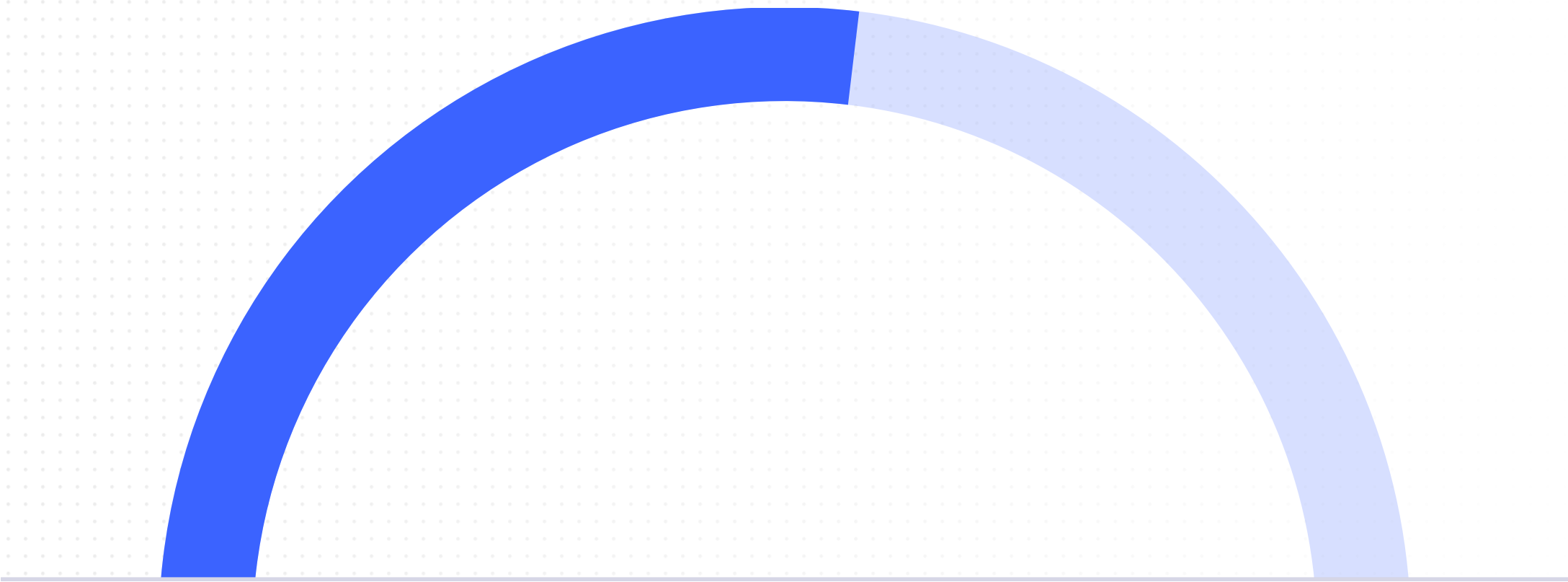
Executive Summary

The Executive Readiness Pack has been specifically designed to enable you to prove, improve, benchmark, and report cyber resilience across your organization.

Driven specifically by the outcomes your organization wants to achieve, this pack transforms exercising data into clear, evidence-based insights that show how effectively your teams are performing, progressing, and where to focus next - with specific, tailored recommendations for the CISO. It captures how readiness is evolving across your workforce, from demonstrating real-world performance and regulatory alignment to building confidence in emerging areas like AI and modern attack surfaces.

This pack gives you defensible evidence for boards, auditors, and regulators, combining benchmarking, expert analysis, and real-world performance data to track progress over time and against peers. It moves you from assumptions to assurance - from “we think we’re ready” to “we can prove it.”

YOUR RESILIENCE SCORE:



540
/1000

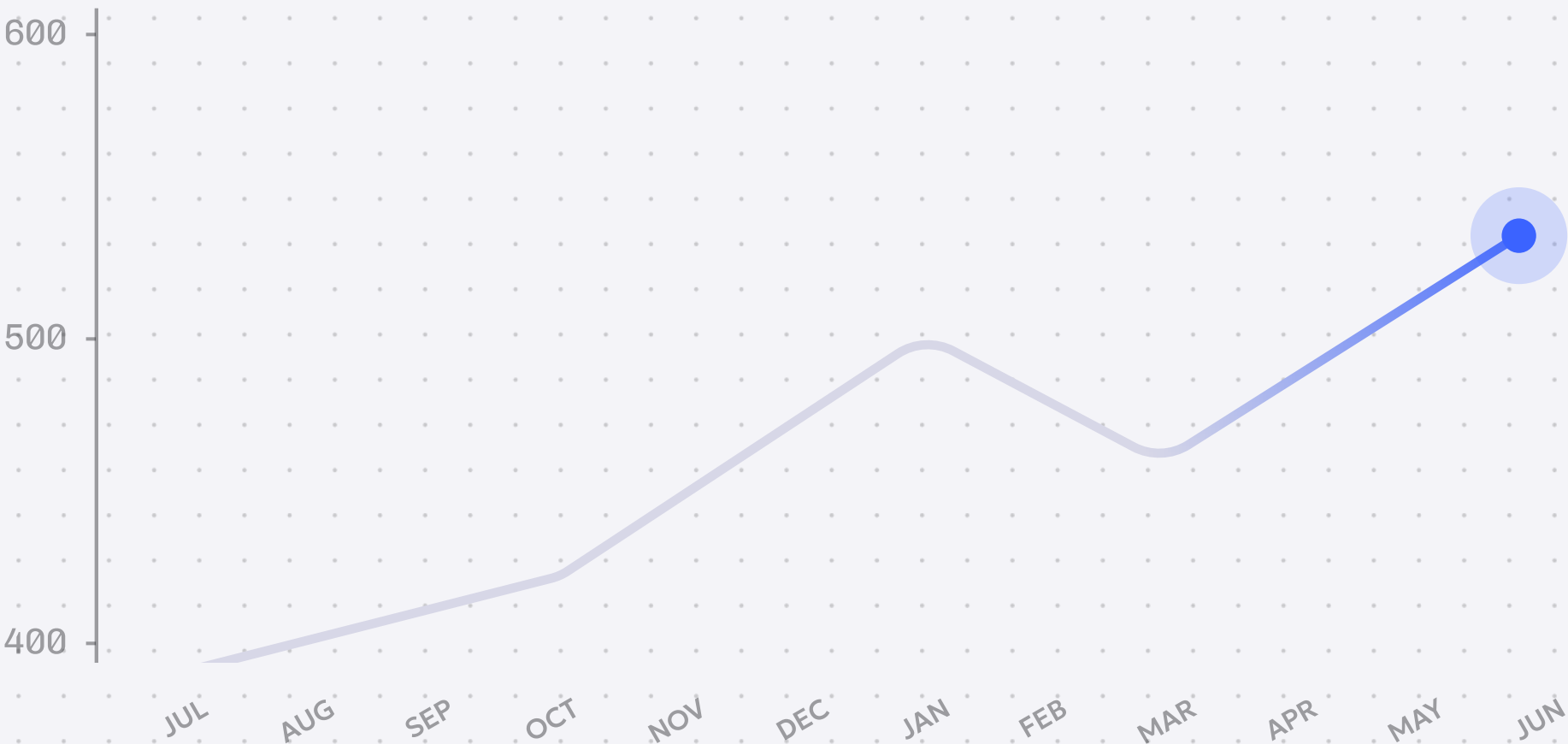
Developing Resilience
Last Updated: 30 June 2025

THE RESILIENCE SCORE IS YOUR ORGANIZATION’S MEASURE OF CYBER READINESS

It’s how Immersive evaluates your ability to take on today’s most advanced threats - translating your team’s real-world performance into a clear, actionable number. It shows exactly how effectively your staff are navigating the evolving threat landscape, how well you’re covering the MITRE ATT&CK framework, and how fast you respond when it matters most. Your Resilience Score of 540 reflects an average level of cyber readiness.

You’ve established solid coverage across the MITRE ATT&CK framework, but there are noticeable knowledge gaps that could expose your defenses to exploitation. Strengthening these areas - and sharpening your team’s responsiveness to emerging threats will not only boost your score, but also build greater confidence in your staff’s ability to handle the unknown with precision and speed.

PROGRESS OVER TIME:



LAST 6 MONTHS:

+115

LAST 12 MONTHS:

+195

Benchmarking

- Introduction
- Your Industry
- Your Region



02

Benchmarking

In this section we'll split your organization's performance into two sub-sections. The first measures your performance against others in the financial services industry, and the second measures your performance against others in the US. This insight will provide clarity on the maturity of your overall security posture and culture.

Overall, we have found that financial services organizations in the US face intense regulatory scrutiny and are among the top targets for advanced cyber attacks. As a result of this, we assess the risk level for your sector and region as high.

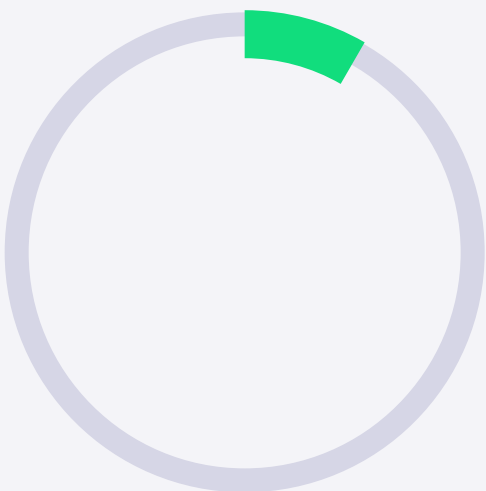
BENCHMARKING AGAINST YOUR INDUSTRY

↓ 4%

Your defensive team is 4% lower than average for coverage on MITRE ATT&CK defensive techniques

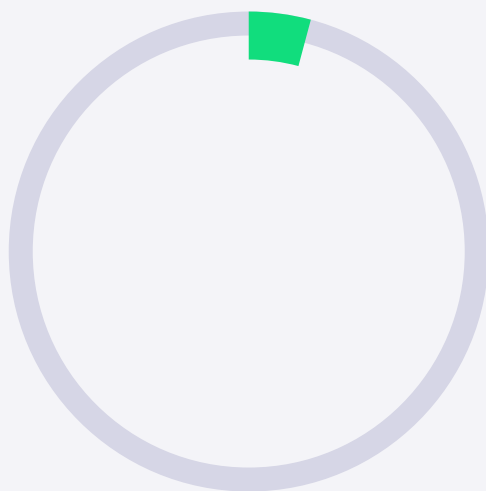
↓ 7%

Your offensive team is 7% lower than average for coverage on MITRE ATT&CK offensive techniques



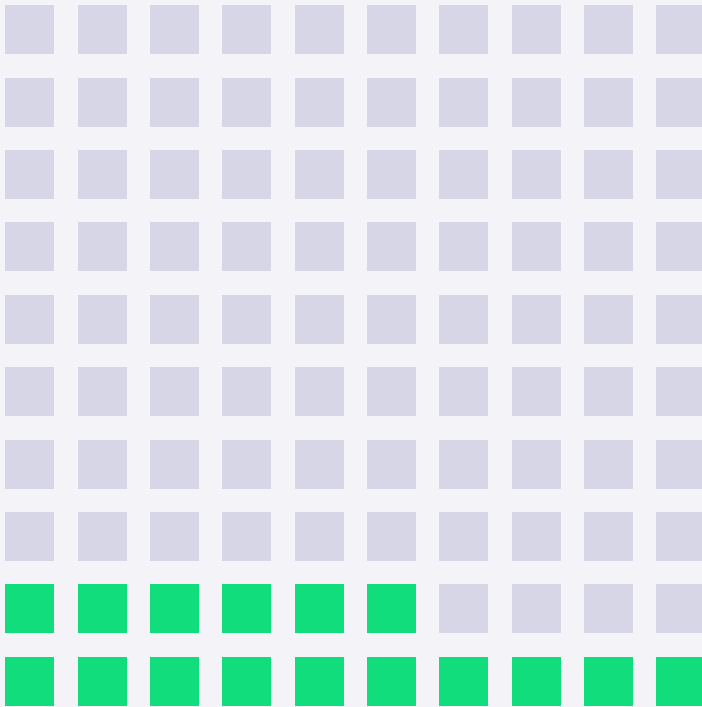
1.08 x

Developers have learned how to remediate 8% more vulnerabilities than others in your industry



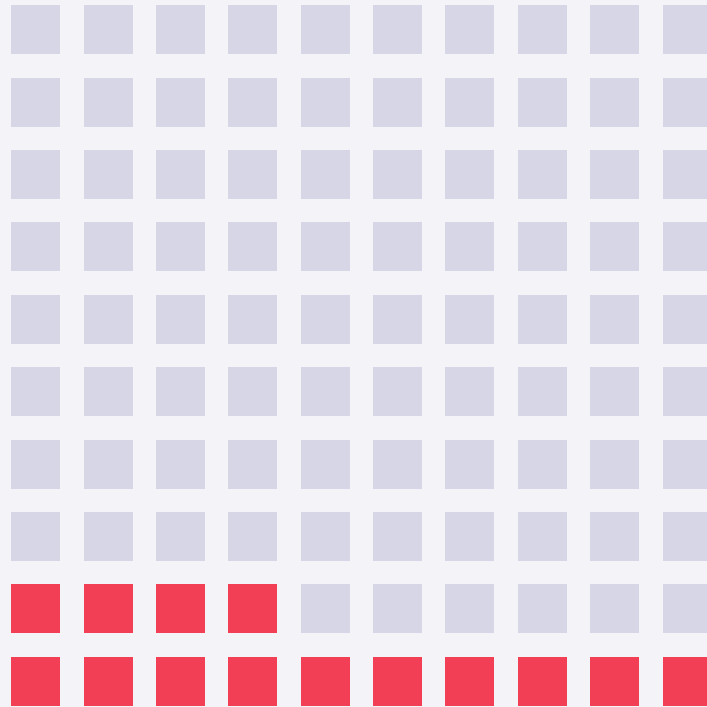
1.04 x

Your team is 4% faster at responding to emerging threats than the industry average



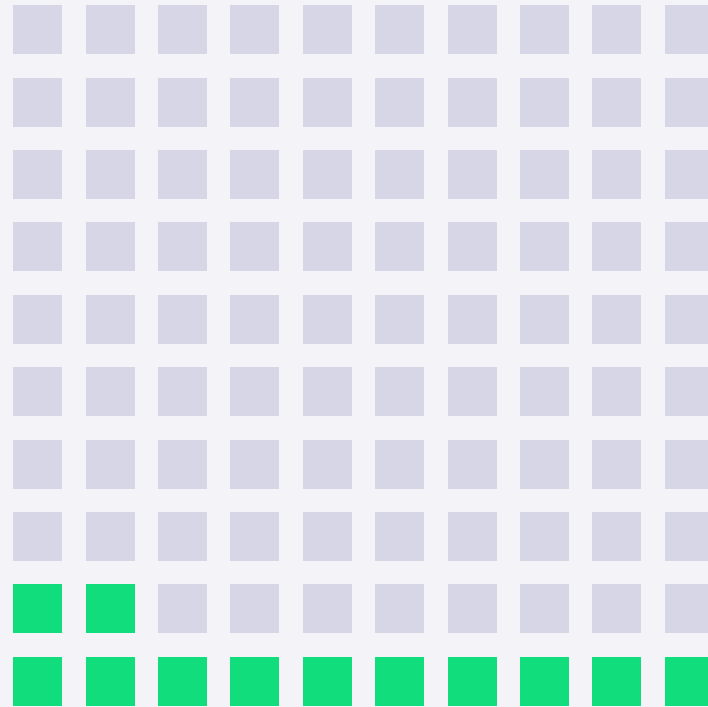
16%

Faster at completing assigned learning paths than the industry average



14%

Your workforce has completed 14% fewer scenarios than the regional average



12%

Your workforce has completed 12% more CVE-related labs on the latest threats targeting your industry

Lvl 7

Lvl 6

The average difficulty level of your users is Intermediate level 6, which is lower than the average Intermediate level 7 across your industry

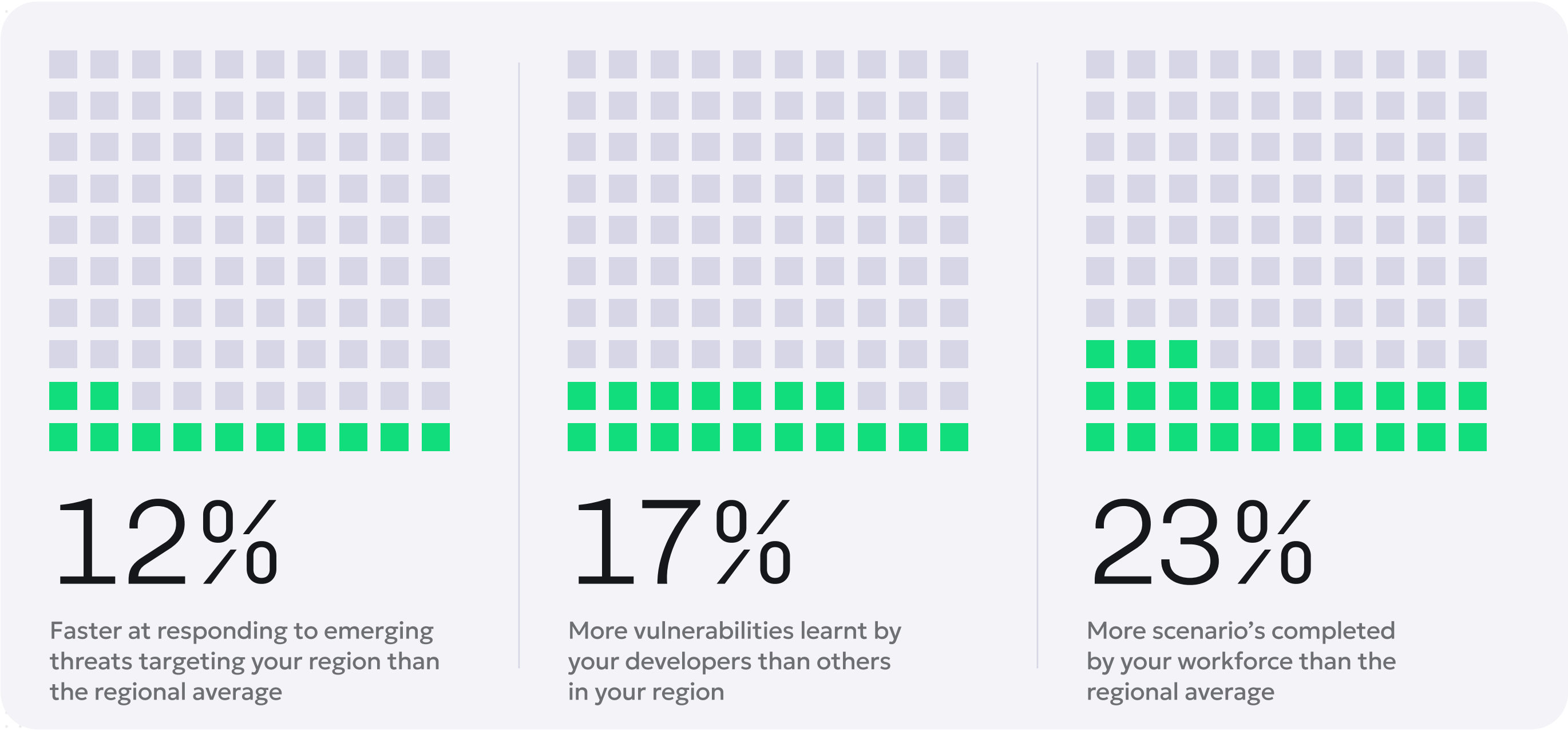
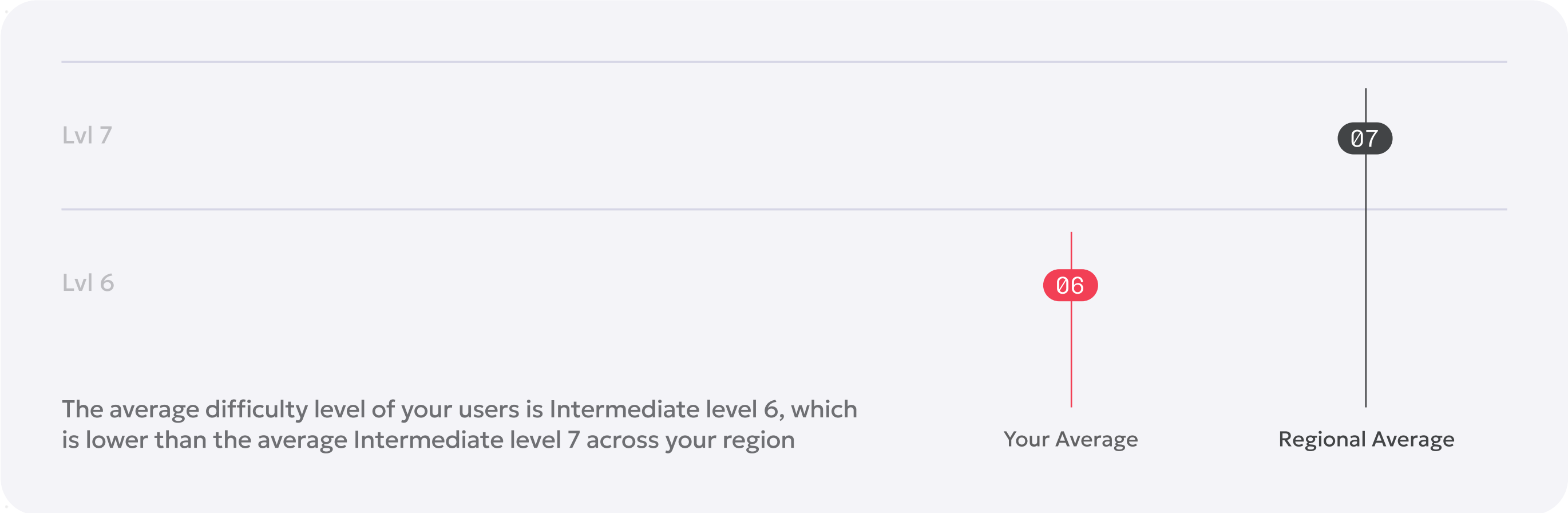
06

Your Average

07

Industry Average

BENCHMARKING AGAINST YOUR REGION



Executive Summary

Benchmarking

Threat Response

- Introduction
- Metrics
- Recommendations

Technical Skills

Compliance

Secure Code

C7 Insights

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

03

Threat Response

Cyber Threat Intelligence (CTI) Labs deliver real-world threat simulations within 24 hours of CVEs, emerging threats, or threat actor activity being reported. These dynamic labs replicate cutting-edge attack techniques used against companies just like yours - keeping your team on the front lines of cybersecurity.

This section reveals how well your team can detect and escalate the latest threats. We track two key metrics: Mean Time to Detect (MTTD) and Mean Time to Escalate (MTTE) - so you can measure your team's readiness directly against real-world threats.

CTI LAB COMPLETION

026 / 100

↗ 45%

The overall performance score of 26/100 highlights a significant opportunity for improvement, primarily driven by low user engagement with the CTI Labs. These labs are created to test your teams against threats happening in real-time.

A low completion rate and slow response time can raise potential questions about how responsive your teams are to new threats. The key challenge is to translate high potential into broad, timely participation.

❗ LOW

6

Users completed 5 out of 23 CTI Labs within a week of publication

↘ 3%

✅ HIGH

99%

Above industry benchmark

↗ 38%

🕒 MEDIUM

20d

Average completion time

↗ 38%

MEAN TIME TO DETECT:

100 MIN

↗ 21%

MEAN TIME TO ESCALATE:

50 MIN

↗ 18%

YOUR MEAN TIME TO DETECT AND MEAN TIME TO ESCALATE ARE CURRENTLY AT AN AVERAGE LEVEL

This means your team is identifying and escalating threats at a standard pace—but in today’s fast-moving threat landscape, average isn’t enough. The longer it takes to detect and escalate, the greater the window for attackers to exploit vulnerabilities.

As threats continue to evolve in speed and complexity, even minutes can be the difference between a contained incident and a major breach. Accelerating your response times will significantly enhance your overall resilience and readiness.

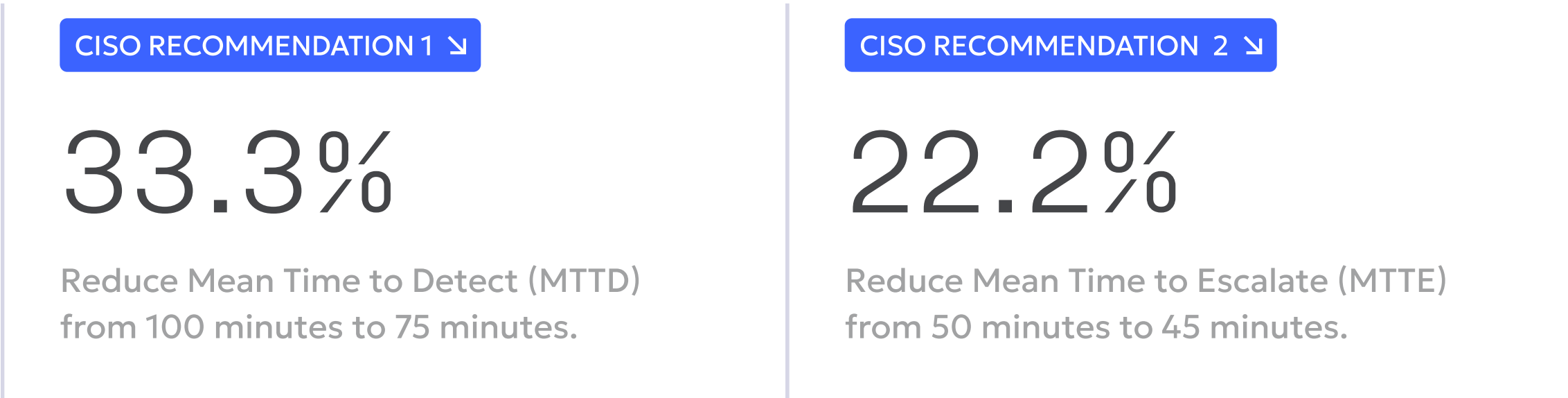


THREAT RESPONSE: RECOMMENDATIONS

CISO RECOMMENDATION

Based on your recent threat response performance, we’ve divided our recommendations into two sections: one tailored for the CISO, and the others for the broader team.

To materially reduce your cyber risk exposure, we recommend a targeted initiative to accelerate your threat response capabilities. The success of this initiative will be measured by achieving the following critical performance improvements:



Achieving these targets represents a 25% improvement in detection speed and a 10% improvement in escalation time. This will demonstrably shrink the window of opportunity for attackers, reducing the potential for a minor incident to evolve into a major breach and enhancing our overall operational resilience.

TEAM RECOMMENDATIONS

① TEAM RECOMMENDATION 1

Assign CTI Labs

Assign CTI Labs as soon as they’re released to your users. This will elevate your Resilience Score and reinforce confidence in your team’s ability to tackle the latest threats with speed and precision.

① TEAM RECOMMENDATION 2

Identify Internal Champions

Identify the users who are excelling in the labs and position them as internal champions. Peer-to-peer encouragement can be a powerful motivator to drive broader engagement and showcase the value of the training programme.

① TEAM RECOMMENDATION 3

Complete Upskill Labs

Each CTI Lab is paired with targeted upskilling labs - completing these is essential to strengthening your coverage of the MITRE ATT&CK framework and closing any knowledge gaps around threat actor tactics.

Executive Summary

Benchmarking

Threat Response

Technical Skills

- Introduction
- MITRE ATT&CK Coverage
- Upskilling Engagement
- Performance Analysis
- Recommendations

Compliance

Secure Code

C7 Insights

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

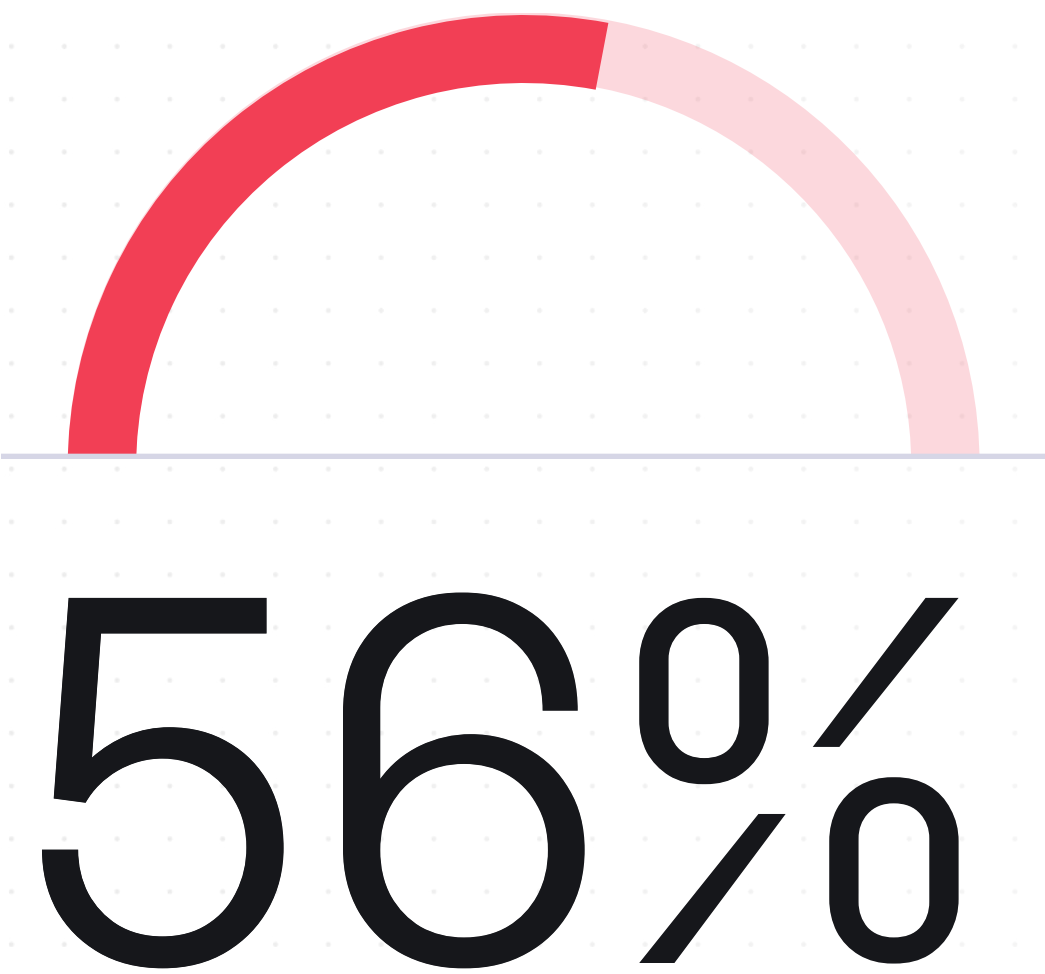
04

Technical Skills

Technical skills are essential to defend your organization against both internal and external cyber threats. To stay resilient, your workforce must continuously sharpen their capabilities to keep pace with the evolving threat landscape.

This section uses measurable evidence to prove your teams effectiveness in both offensive and defensive cybersecurity. It highlights current strengths, uncovers skill gaps, and provides actionable recommendations to help close those gaps and strengthen your overall security posture.

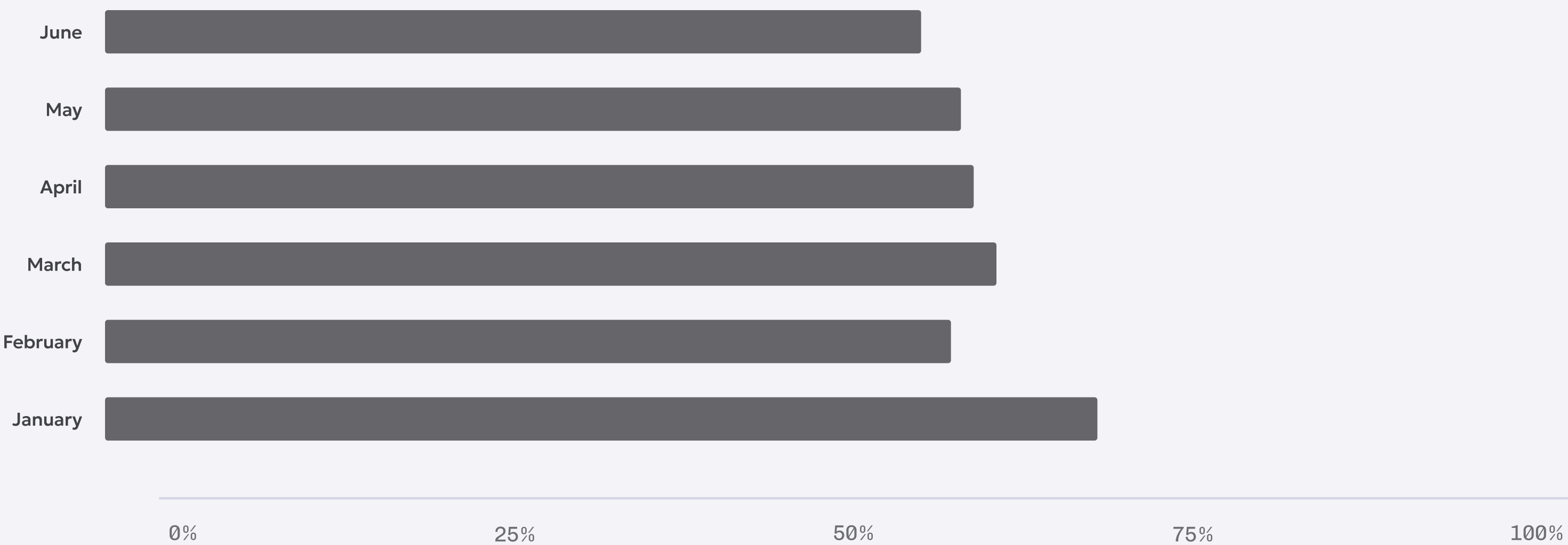
MITRE ATT&CK TOTAL
COVERAGE



↙ 5%

Your team covers 56% of key techniques. While 104 techniques have depth (5+ users each), there remains a significant opportunity to broaden your defensive capabilities against a wider range of threats.

SCORE OVER TIME



✓ HIGH

104

↗ 22%

Techniques have been completed by 5 or more people

✓ HIGH

10%

↗ 6%

Above industry benchmark

⌚ MEDIUM

50

↗ 10%

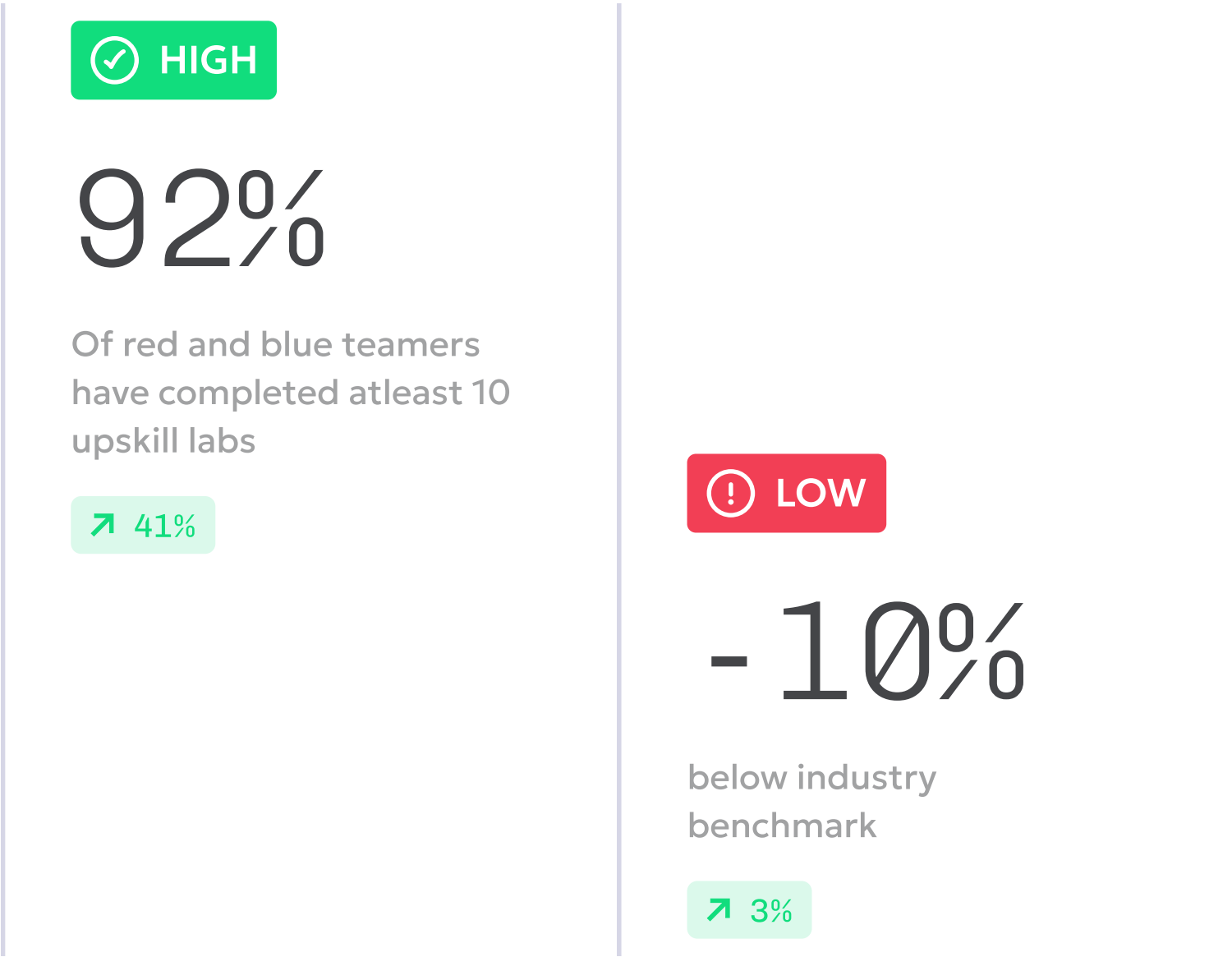
Out of the 137 techniques are covered by your organization

UPSKILLING ENGAGEMENT

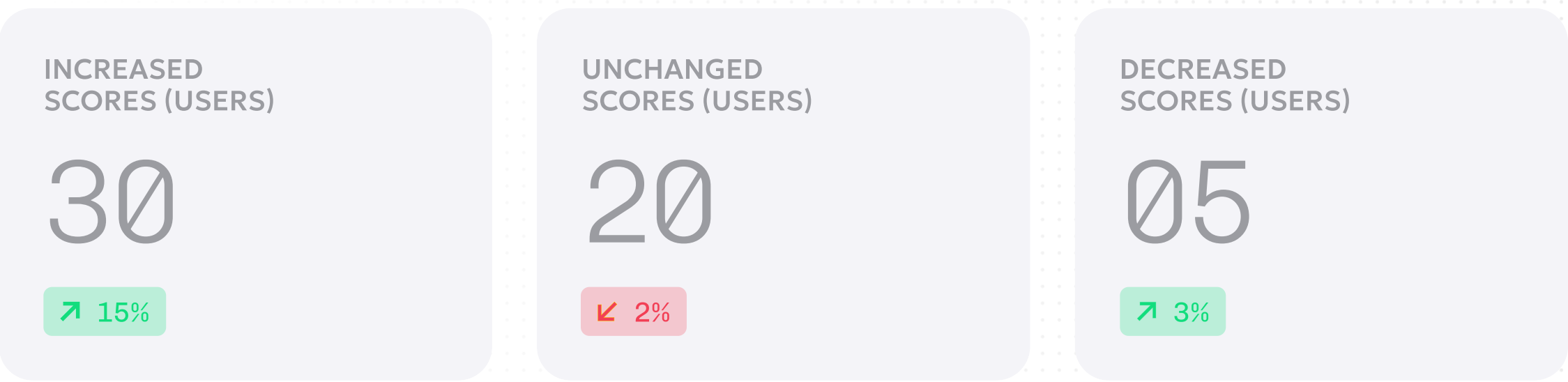


Your overall performance score of 68/100 indicates a strong foundation with several key successes, particularly in program adoption and skill development.

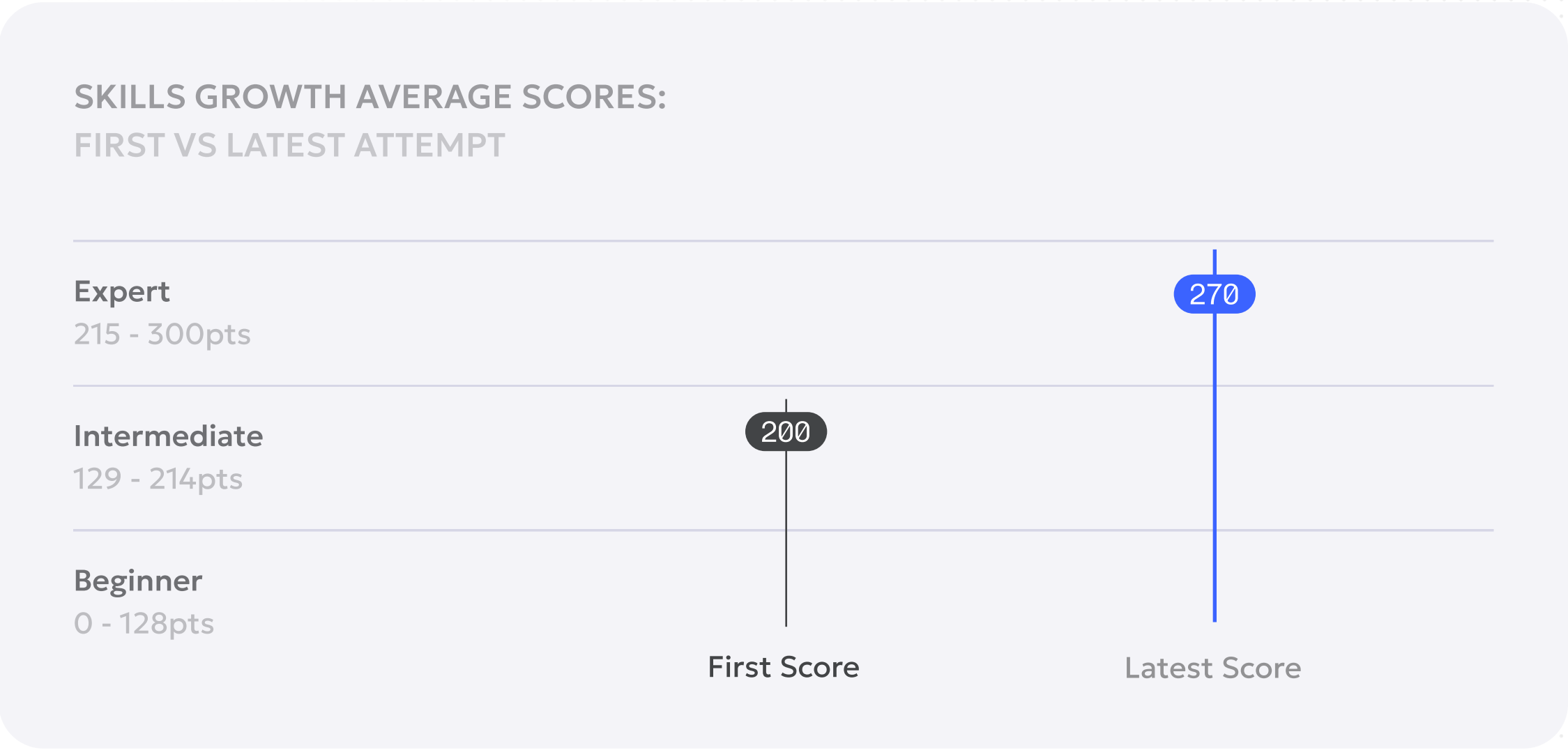
Nearly your entire team has engaged with the upskill labs, and users demonstrate significant improvement between their first and latest attempts.



SKILLS GROWTH

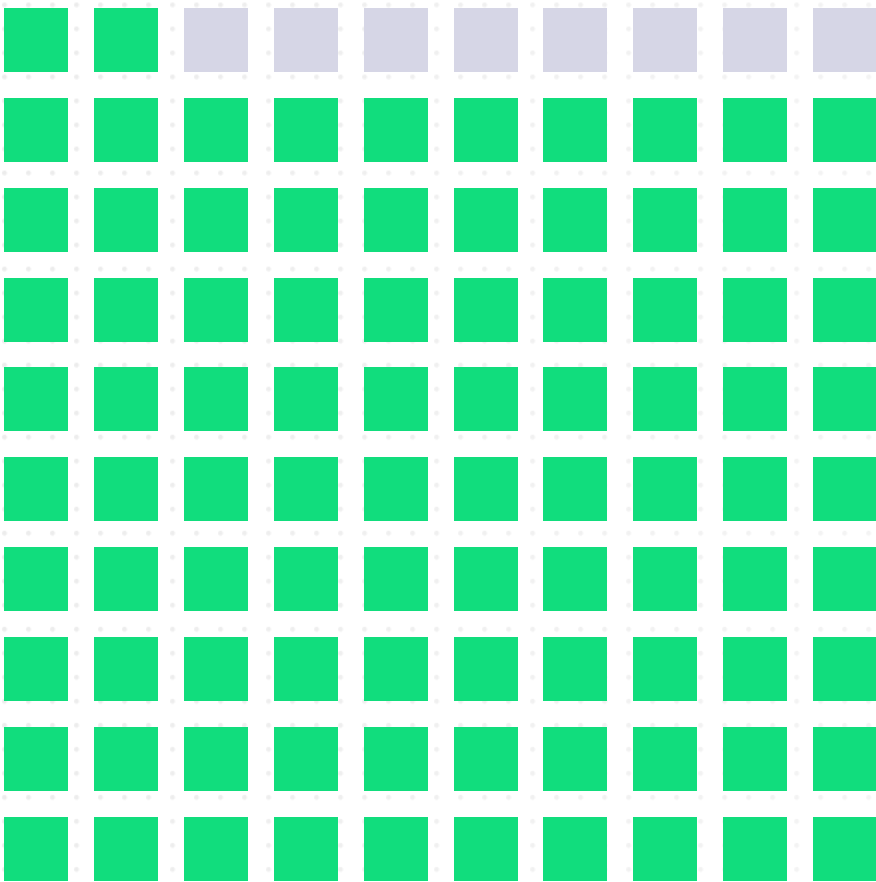


The increased, unchanged, and decreased scores show how many users' scores differed or didn't change from the previous time they were assessed. You can track this metric to ensure you're seeing your technical staff get better over time. This will ultimately lead to an increase in your resilience score.



TECHNICAL SKILLS: PERFORMANCE ANALYSIS

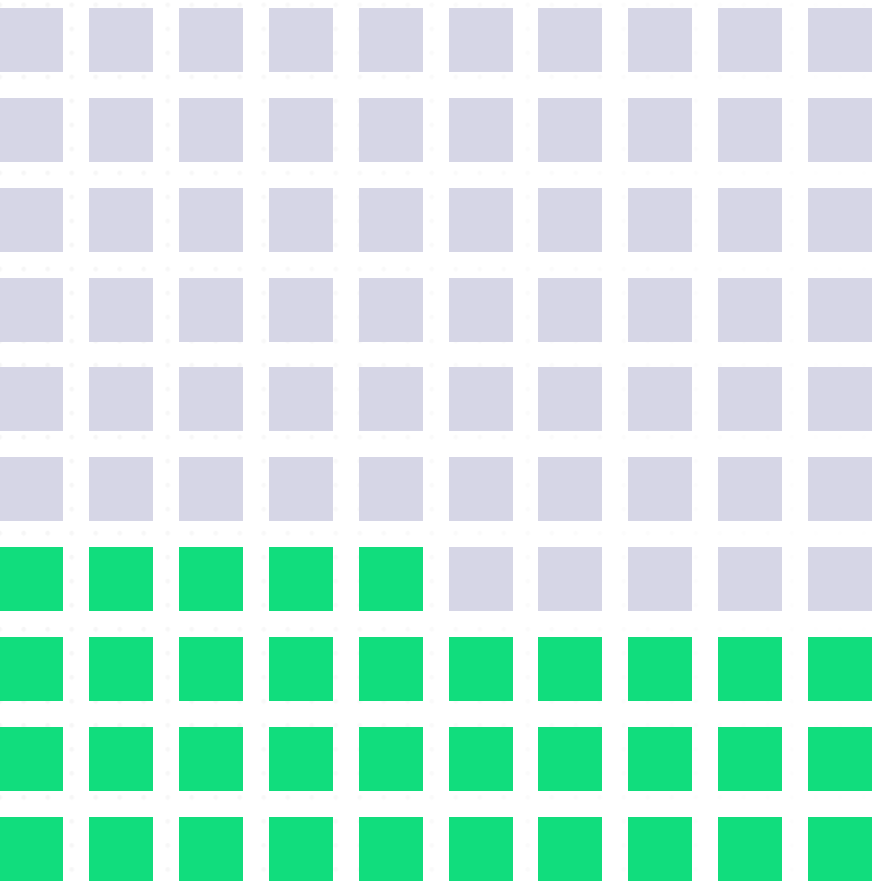
EXCELLENT
COMPLETION RATE:



92% ↗ 41%

Of red and blue team members (344 of 373) have completed at least 10 Upskill Labs - demonstrating an exceptionally high completion rate, and team-wide buy-in.

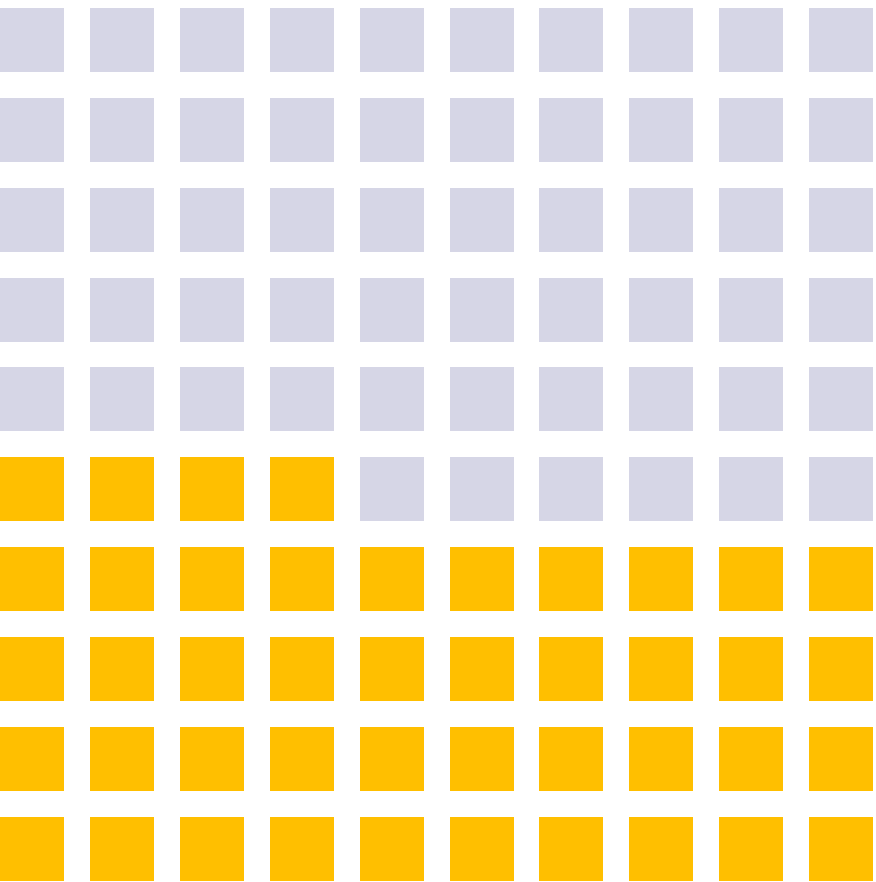
EXCELLENT
SKILLS GROWTH:



35% ↗ 18%

User scores increased by 35% from 200 (intermediate) on the first attempt to 270 (expert) on the latest attempt - proving clear evidence of effective learning and skill retention.

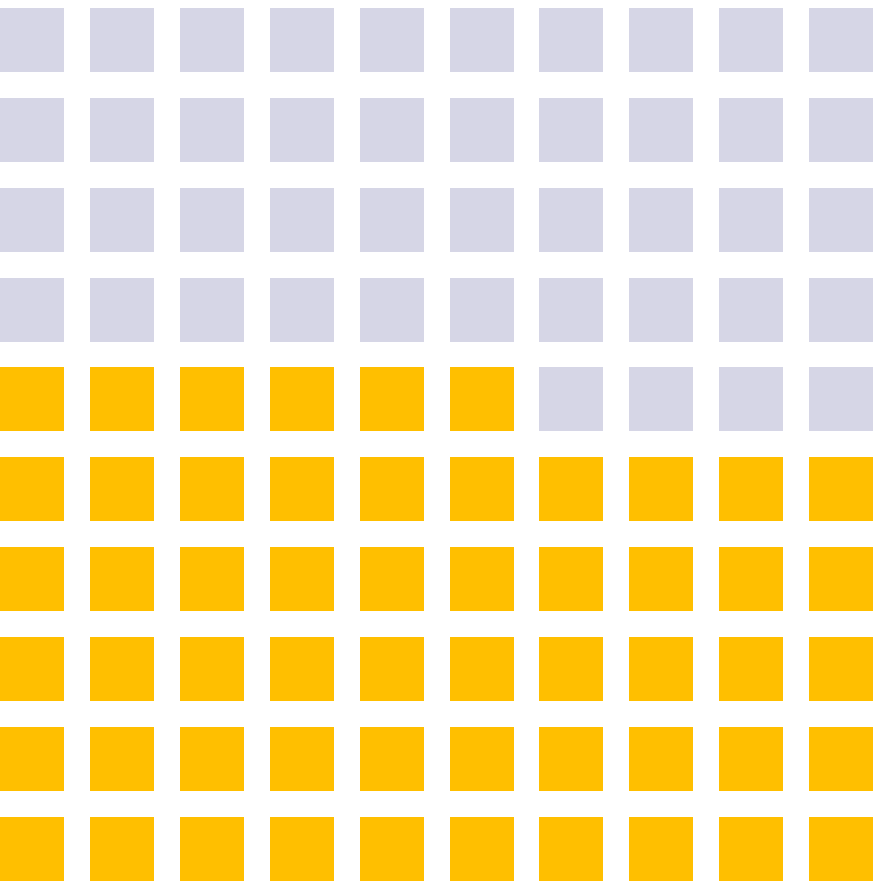
AVERAGE
ONGOING ENGAGEMENT:



44% ↗ 11%

Of users (165 of 373) have completed content in the past six months. Continue to drive engagement within your teams to keep skills sharp and up-to-date.

AVERAGE MITRE
ATT&CK® COVERAGE:



56% ↘ 5%

Your team covers 56% of key techniques (50 of 137). While 104 techniques have depth (5+ users each) there remains a significant opportunity to broaden your defensive capabilities against a wider range of threats.

THREAT RESPONSE: RECOMMENDATIONS

CISO RECOMMENDATION

Based on your recent secure code performance, we’ve divided our recommendations into two sections: one tailored for the CISO, and the others for the broader team.

To stay ahead of evolving threats, focus on boosting ongoing engagement and expanding MITRE ATT&CK coverage to close critical defensive gaps. Participation is strong, but continuous learning is the key to surpassing the industry benchmark.



TEAM RECOMMENDATIONS

① TEAM RECOMMENDATION 1

Launch Crisis Simulation Scenarios

Based on recent threats to help drive engagement with the Immersive One platform and help you understand your employees' responses to crises.

① TEAM RECOMMENDATION 3

Strategically Expand MITRE ATT&CK® Coverage

Analyse the 87 techniques not yet covered by your team. Prioritise them based on threat intelligence relevant to your industry and create a clear roadmap for the next two quarters.

Assign specific labs to teams or individuals to increase your coverage.

① TEAM RECOMMENDATION 2

Launch a Re-Engagement Campaign

To address the moderate ongoing engagement, create a campaign focused on continuous professional development. Use our Capture-the-Flag exercises to drive engagement.

① TEAM RECOMMENDATION 4

Target Stagnant Scores

Focus on the 25 users whose scores were unchanged or decreased during re-assessment. These individuals may be struggling with specific concepts.

Offer them lower technical labs or curated learning programs designed to help them overcome their learning plateaus and contribute to raising the team's average score.

Executive Summary

Benchmarking

Threat Response

Technical Skills

Compliance

- Introduction
- Performance Analysis
- Recommendations

Secure Code

C7 Insights

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

05

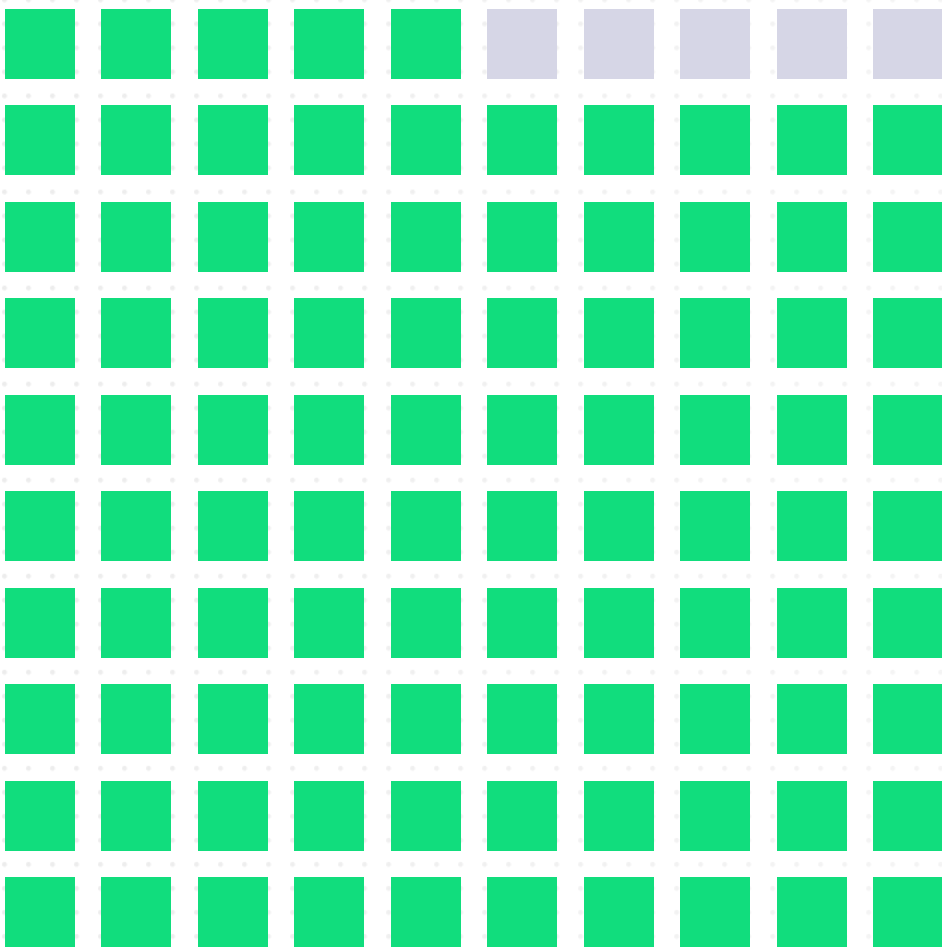
Compliance

In a highly regulated industry like financial services, proving cybersecurity readiness and regulatory compliance isn't optional - it's essential.

This section looks at your compliance performance within the platform, which also serves as an auditable record, which is invaluable for demonstrating compliance during a certification audit.

COMPLIANCE: PERFORMANCE ANALYSIS

EXCELLENT
COMPLETION RATE:

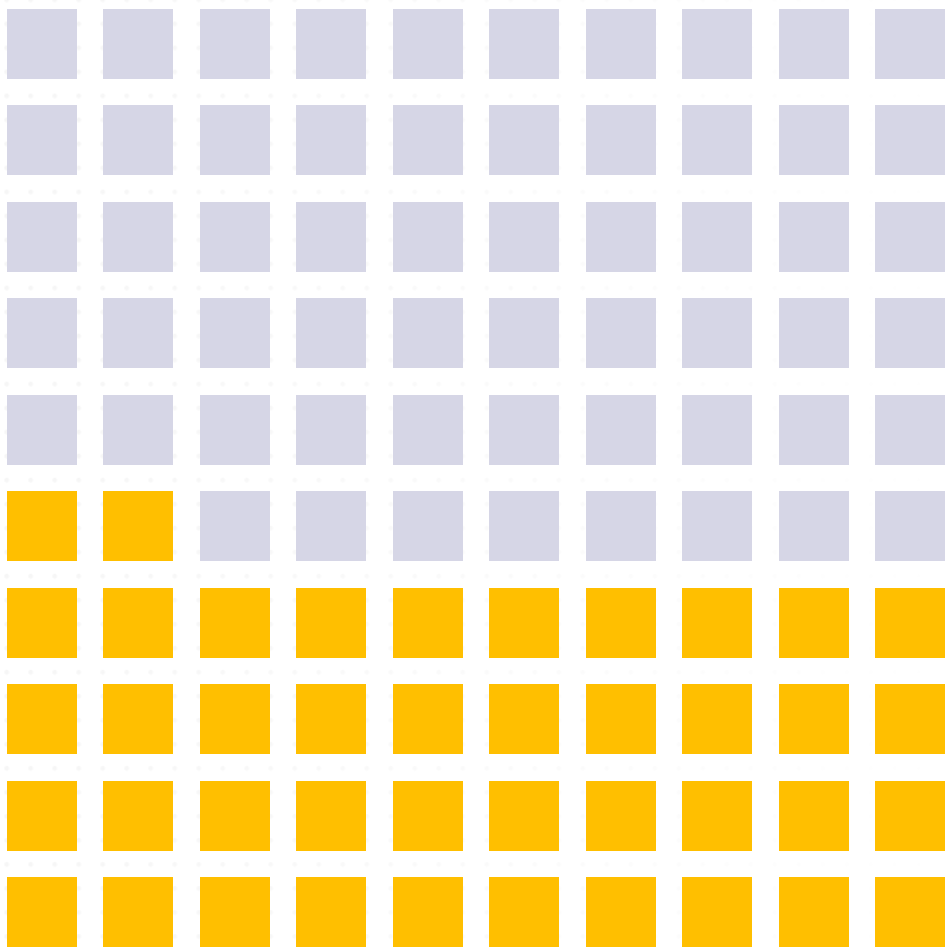


95%

↗ 56%

Of your developers have completed the full application security assignment.

AVERAGE SKILLS
GROWTH:

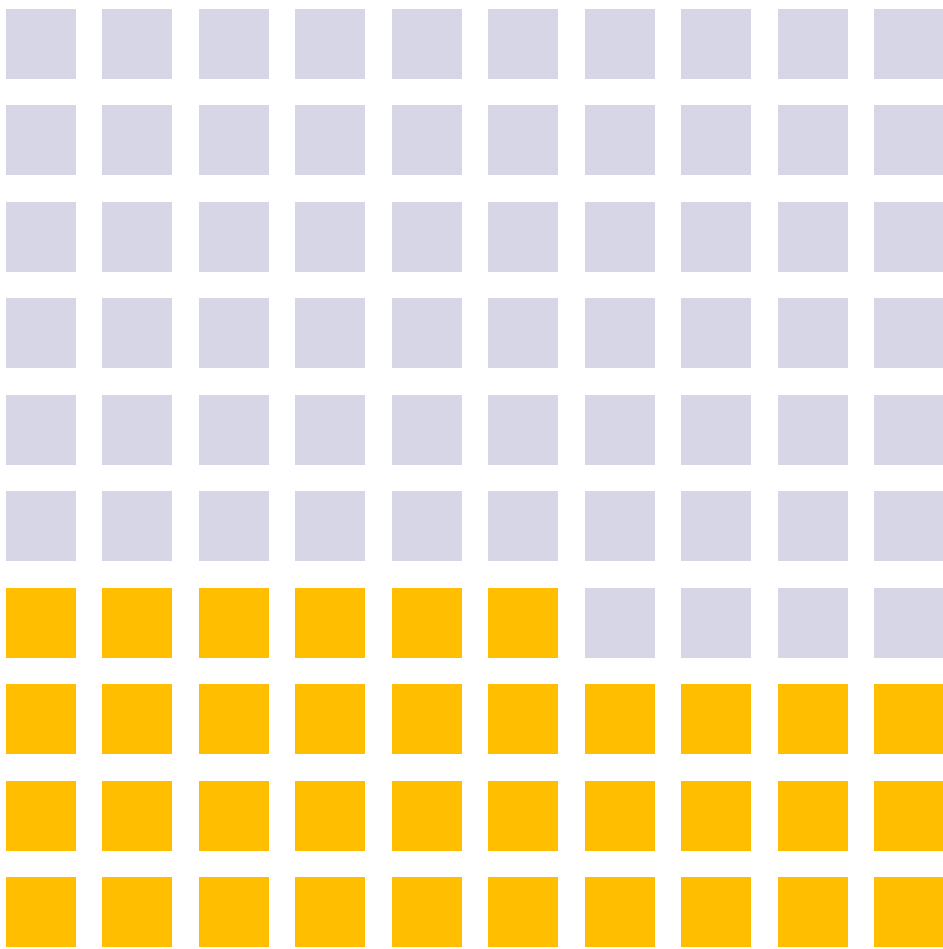


42%

↗ 7%

Of your cloud security engineers have completed the cloud configuration assignment.

AVERAGE
UPSKILLING:



36%

↗ 7%

Your team completed 36% of the defensive content on the platform, which shows continuous upskilling in this area

YOU ALSO COMPLETED:

- ✓ 10 Workforce micro-simulations across the general workforce to identify employee cohorts with poor cyber hygiene.
- ✓ 2 Cyber drills that exercised your SEC disclosure protocols.
- ✓ 1 End-to-end cyber drill completed that benchmarked the security operations team, and various mid-level teams in their readiness to respond to a ransomware attack.
- ✓ 1 Executive-level exercise completed on breaches related to customer data; 5 divisional and 3 functional leadership teams have also completed exercises measuring their response readiness to a customer data breach.

COMPLIANCE: RECOMMENDATIONS

CISO RECOMMENDATIONS

Rather than one-off exercises, you must establish a continuous, automated stream of auditable proof.

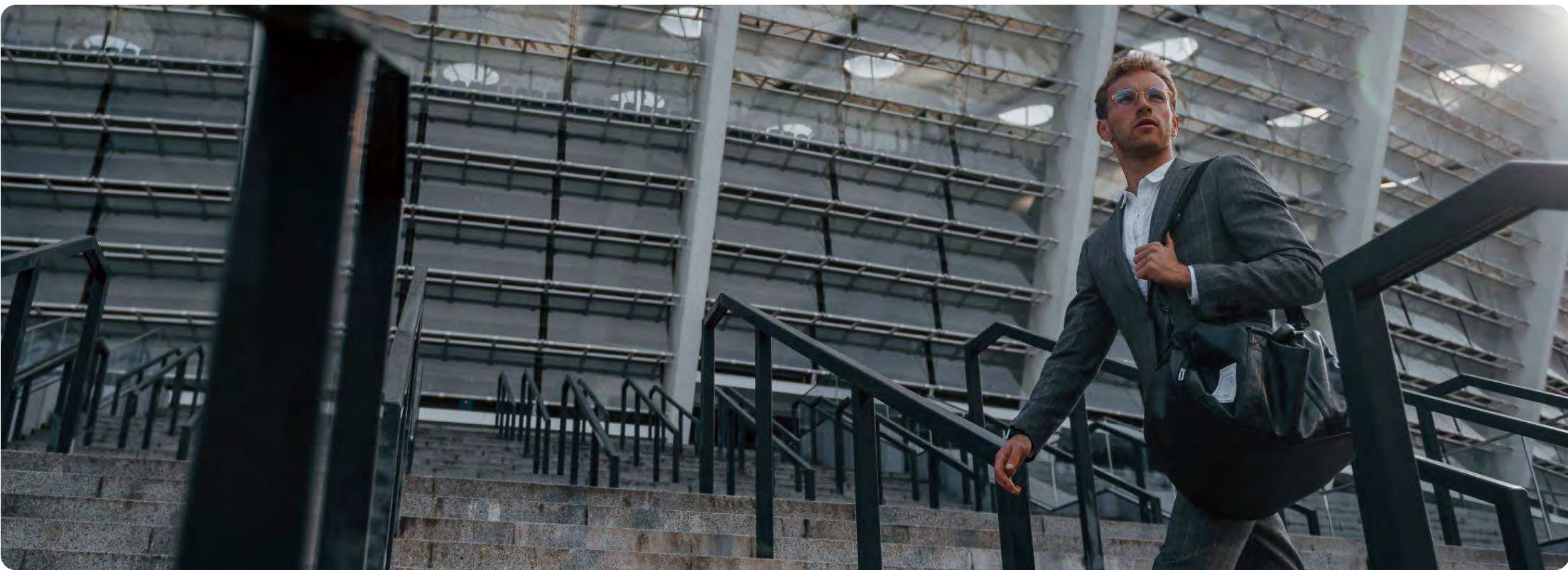
CISO RECOMMENDATION 1 ↘

Phishing awareness
(ISO 27001)

CISO RECOMMENDATION 2 ↘

Incident notification timelines
(OCC)

You should formalize a quarterly schedule of enterprise-wide simulations focused on critical regulatory requirements, such as phishing awareness (ISO 27001) and incident notification timelines (OCC). This embeds compliance validation into our operations and significantly reduces the burden of audit preparation



TEAM RECOMMENDATIONS

! TEAM RECOMMENDATION 1

Company Wide Workforce Scenarios

Launch two company-wide workforce scenarios about phishing before the end of the year to provide measurable evidence for ISO 27001 control A.6.3 (Information security awareness).

! TEAM RECOMMENDATION 2

Test 36-Hour Incident Notification Rule

Conduct quarterly crisis simulations that specifically test the 36-hour incident notification rule to demonstrate operational readiness to the OCC.

! TEAM RECOMMENDATION 3

Assign Threat Intel Labs

Assign the newly released threat intelligence labs to the security team to build the skills needed to satisfy the ISO 27001 control A.5.7

Executive Summary

Benchmarking

Threat Response

Technical Skills

Compliance

Secure Code

- Introduction
- OWASP Completion
- Coding Language
- Recommendations

C7 Insights

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

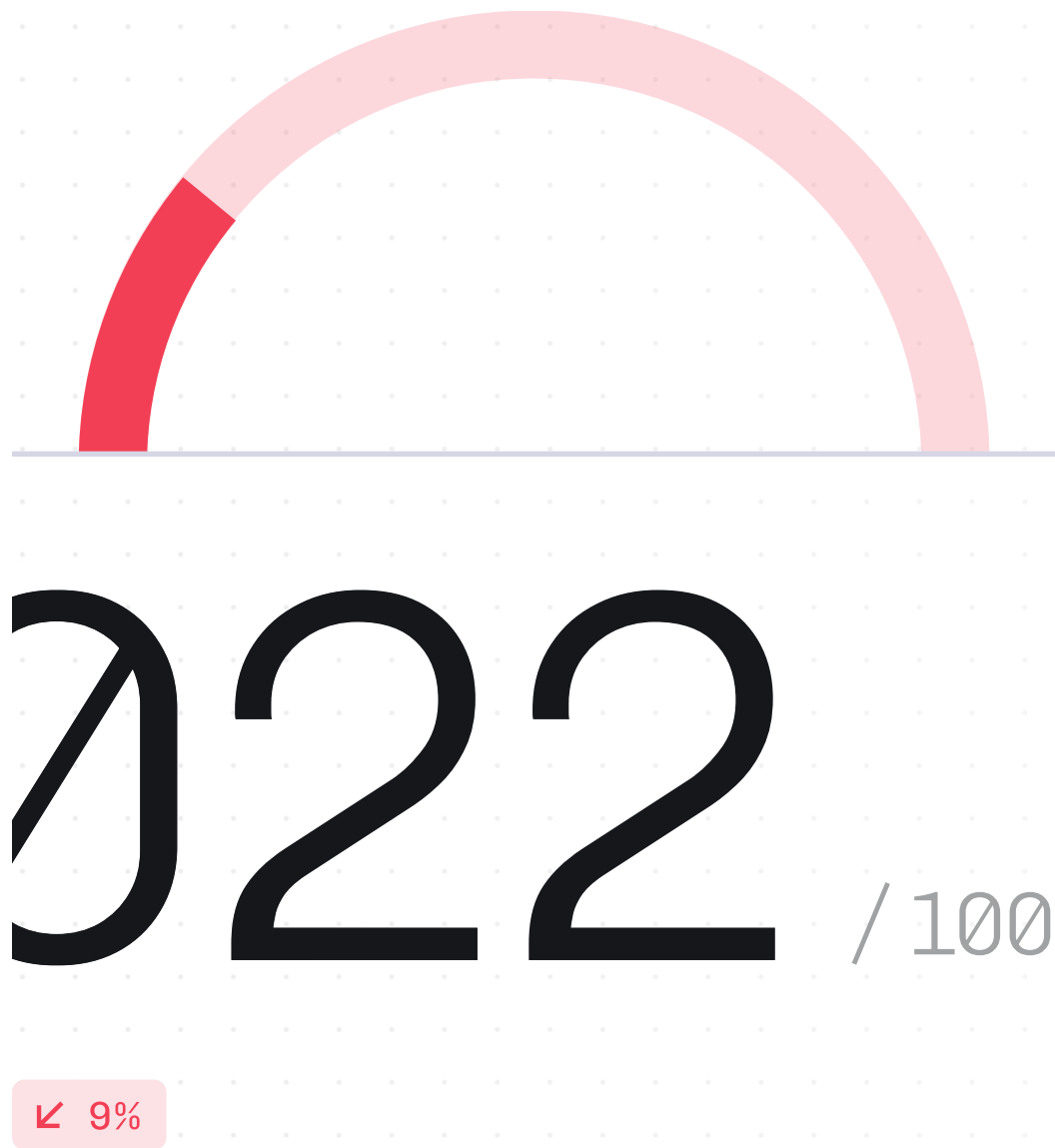
06

Secure Code

Implementing security throughout the entire application and software development lifecycle is essential in today’s threat landscape. Many vulnerabilities arise but from developers lacking awareness of the security implications of the code they write. Embedding security knowledge early and consistently helps reduce risk and build more resilient software from the ground up.

This section shows you gaps in the security knowledge of your developers against well-known and robust application security frameworks - giving you clarity on where you need to improve.

OWASP TOP 10 COMPLETION



Overall performance is low, primarily due to very poor engagement with the main, comprehensive training collection.

Your score of 22/100 and the extremely low completion rate, with only 8 of 67 developers (12%) finishing the content.

SCORE OVER TIME



! LOW

12%

Software developers have completed the whole collection

17%

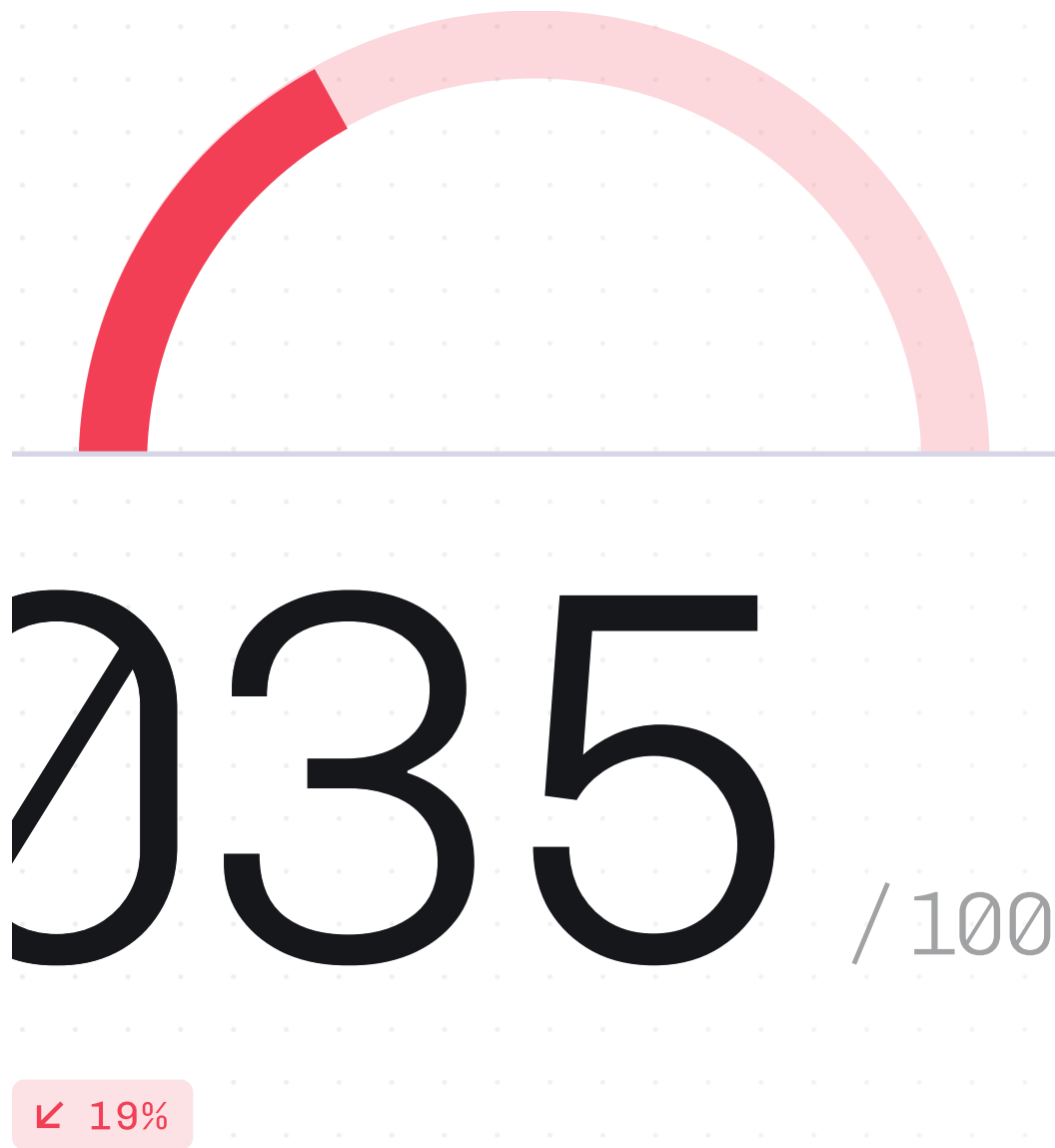
! LOW

-51%

Below industry benchmark

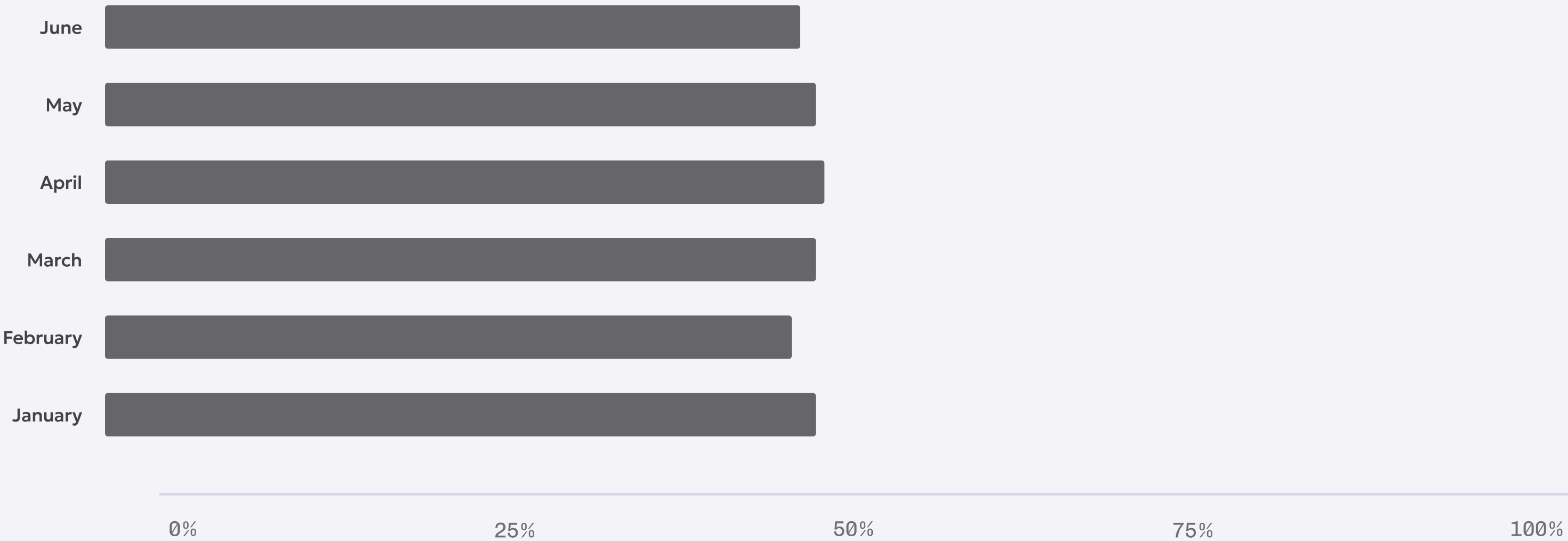
16%

CODING LANGUAGE



Developers are significantly more willing to engage with targeted, language-specific content. While still below the benchmark, the score of 35/100 is much better, and a majority of developers, 34 out of 67 (51%), have completed these modules.

SCORE OVER TIME



! LOW

51%

Software developers have completed some language specific content

26%

! LOW

-1%

Below industry benchmark

11%

SECURE CODE: RECOMMENDATIONS

CISO RECOMMENDATION

Based on your recent secure code performance, we’ve divided our recommendations into two sections: one tailored for the CISO, and the others for the broader team.

To improve the efficiency of the security training and reduce risk in your applications, you should sponsor ensuring that vulnerability training is completed before any developers can push their code to production.



TEAM RECOMMENDATION

① TEAM RECOMMENDATION 1

Prioritise Language Specific Training

Since developers are already engaging with content tailored to their specific programming languages, this is your area of greatest opportunity. Instead of assigning the generic collection, assign the Java security collection to your Java team, the Python collection to the Python team, and so on.

This immediately increases relevance and value to your development team. We find developers tend to want to be fast, so they can get on with their day jobs. Ensuring the language is specific to their skills will increase the chances of them completing the labs.

② TEAM RECOMMENDATION 2

Try the New Application Security Cyber Range

The application security cyber range gets developers involved in what a crisis scenario might look like. They have to triage bugs coming in from an exploit, fix them, and put code into production.

For an organization, this shows how quickly your staff can respond and fix new vulnerabilities, increasing the confidence in your developers to triage bugs quickly.

Executive Summary

Benchmarking

Threat Response

Technical Skills

Compliance

Secure Code

C7 Insights

- Introduction
- Current & Emerging Threats
- Scattered Spider
- Windows Exploits
- Recommendations

Targets for H2

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

07

C7 Insights

Container 7 is Immersive’s home for technical research, threat intelligence, and expert-led insight. It’s where our most experienced practitioners - leaders in offensive and defensive security, cloud, application security, and cyber threat intelligence - come together to share discoveries, publish responsible disclosures, and explore the latest adversary techniques.

In this section we’ll take a look at current and emerging threats that could directly impact your industry and region.

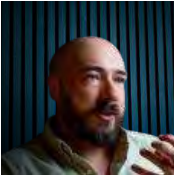
MEET THE C7 TEAM

- 

MAX VETTER
Immersive Vice President of Cyber
[in](#)
- 

KEV BREEN
Senior Director of Threat Research
[in](#)
- 

DAVE SPENCER
Director of Technical Product Management
[in](#)
- 

KEV MARRIOTT
Senior Manager of Cyber at Immersive
[in](#)
- 

MATT PARVEN
Principal Cyber Security Engineer
- 

CHRIS WOOD
Principal Cyber Security Engineer
[in](#)
- 

BEN MCCARTHY
Lead Cyber Security Engineer
[in](#)

CURRENT AND EMERGING THREATS

The threat landscape is ever-evolving. Throughout H1 2025 - we’re continuing to see an expansion of capabilities in the following areas that threat actors have access to:



ARTIFICIAL INTELLIGENCE:

Threat actors are using AI capabilities to deliver attacks faster. Each stage of the MITRE ATT&CK framework has seen expansion in capabilities because AI can help bridge these skills gaps in threat actors. This causes trouble with tracking threat actors and their tactics because we are seeing many of them expand their arsenal.



ACCESS BROKERS:

Threat actors have seen the success of famous breaches in the past quarter, where access to a business was bought on a brokerage on the dark web and used to successfully access a company. Couple that with the successes of actors like Scattered Spider, who have shown the industry that effective social engineering techniques can outperform highly technical, skilled hackers in many scenarios.



EXTORTION TACTIC CHANGES:

Threat actors, while still deploying traditional ransomware, have been seen to start to threaten companies to give their stolen data over to AI companies to train their data. This causes a huge number of issues because this data begins to be available to everyone using that AI.



CURRENT AND EMERGING THREATS - FINANCIAL SERVICES

Financial Services organizations are under increased pressure of a cyber attack. In May 2024, FS-ISAC raised it’s threat level in the US region because of successful breaches against many financial services organizations.

THREAT 1: SCATTERED SPIDER

Scattered Spider, also known as UNC3944, represents a significant threat due to its mastery of advanced social engineering and its crucial role within the cybercrime ecosystem. The group's success stems from a highly persistent, multi-channel approach that goes far beyond simple phishing emails. Their operators, often native English speakers, engage in sophisticated vishing (voice phishing) campaigns, directly calling IT help desks while impersonating employees to have their credentials and multi-factor authentication (MFA) devices reset.

They combine this with MFA fatigue tactics—spamming users with push notifications until they relent and approve access—and SIM swapping to bypass security controls. Once initial access is achieved, Scattered Spider excels at moving laterally through a network, escalating privileges, and exfiltrating sensitive data. Their primary function is often that of an initial access broker, establishing a deep and persistent foothold within a target's network before handing off that access to a ransomware affiliate, most notably the ALPHV/BlackCat group, for the final data encryption and extortion phase. This specialization has enabled them to execute devastating breaches across a wide range of critical sectors, including financial services, telecommunications, healthcare, and technology.

Your organization's breakdown of this is:





CURRENT AND EMERGING THREATS - FINANCIAL SERVICES

THREAT 2: WINDOWS EXPLOITS

These are vulnerabilities released on Patch Tuesday in the past quarter. Threat actors normally find and replicate exploits for Windows vulnerabilities rapidly, aiming to utilise the difficult patching process that organizations go through.

The monthly "Patch Tuesday" releases from the past quarter have become a predictable starting gun for a high-stakes race between cyber adversaries and enterprise defenders. Threat actors systematically reverse-engineer these security updates, analyzing the patched code to pinpoint the underlying flaw and rapidly develop a functional exploit. This allows them to weaponize the vulnerability, sometimes in a matter of hours, and launch attacks before organizations can complete their own internal processes. For many organizations, the patching process itself is a significant operational hurdle, fraught with challenges like ensuring business continuity, scheduling downtime for critical systems, and validating patch compatibility across a diverse IT environment. It is precisely this window of vulnerability that attackers exploit.

In response, Container 7 has released five new CVE labs focused on high-impact Windows vulnerabilities from this period. These labs are crucial because they simulate the exact exploits that have been actively used in the wild against prime targets like the financial services industry, allowing security teams to gain hands-on experience and build resilience against threats that have already proven effective.

Your organization's breakdown of this is:

01

Only 3 of the 5 CVE labs were completed in the two days of release.

02

The offensive lab was completed more than the defensive lab for each of these vulnerabilities.

CURRENT AND EMERGING THREATS: RECOMMENDATIONS

TEAM RECOMMENDATIONS

! TEAM RECOMMENDATION 1

Latest Windows Vulnerabilities

When new CTI labs are released, ensure there is a cadence of defensive and offensive members of your team completing labs on the latest Windows vulnerabilities like: CVE-2025-53770 (ToolShell SharePoint RCE): Defensive and CVE-2025-33073 (SMB Elevation of Privilege): Defensive

! TEAM RECOMMENDATION 3

Further Lab Suggestions

Assign the following labs to your defensive cyber teams: Scattered Spider and DragonForce: Campaign Analysis and Threat Actors: Scattered Spider

! TEAM RECOMMENDATION 2

Assign Scattered Spider Scenario

Assign the Social Engineering Techniques Scattered Spider workforce scenario to your workforce to ensure they understand these new types of social engineering techniques.

! TEAM RECOMMENDATION 4

Crisis Simulations

Assign more crisis simulations to your incident response team, running through the scenario Responding to a Scattered Spider Attack, this will help you understand how your organization would currently respond to Scattered Spider.



Executive Summary

Benchmarking

Threat Response

Technical Skills

Compliance

Secure Code

C7 Insights

Targets for H2

- Orchid Bank

Conclusion



Executive Readiness Pack

© Immersive -
All Rights Reserved

08

Targets for H2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.



01

Increase MITRE ATTACK
Coverage from 56% Total
Coverage to 62%

This will increase your resilience score and
score you much higher in the industry
benchmarking.



02

Increase the number of people
who have completed 100
techniques from 5 to 8

This will increase your resilience score while
also ensuring more of your staff are
equipped to deal with threat actors
tactics and techniques.



03

Complete one workforce exercise
covering at least 65% of your
non-cyber workforce.

Your workforce is one of your most
important assets, and with over 65% of
breaches starting with the human element
within an organization, they need to be
aware of techniques posed by groups like
Scattered Spider.



04

Increase your specific language
adoption of application security
labs from 34/67 to 45/67

Vulnerable code is one of the other largest
attack vectors after phishing. Completion
of application security labs ensures your
teams know how to implement robust
and secure code, leading to less security
bugs and less of an attack surface for
your organization.

Executive Summary

Benchmarking

Threat Response

Technical Skills

Compliance

Secure Code

C7 Insights

Targets for H2

Conclusion

- Summary



Executive Readiness Pack

© Immersive -
All Rights Reserved

79

Conclusion

Overall, your organization is demonstrating average progress across the Immersive One platform, with clear strengths in parts of your technical defence. However, gaps in areas such as application security, workforce scenarios, and crisis simulations are limiting your ability to consistently prove resilience against evolving threats - creating blind spots in your most critical defensive asset: your people.

This pack has been designed to do more than highlight performance - it enables you to prove where you stand today, benchmark against peers, and clearly identify where focused improvement will have the greatest impact.

Our cyber threat intelligence team has provided targeted recommendations and measurable goals to help you close these gaps, strengthen decision-making under pressure, and build confidence across your organization’s most critical risk areas. By acting on these insights, you will not only improve resilience in practice, but also strengthen how you report it - with clear, defensible evidence that demonstrates progress over time and against industry benchmarks.