cmd+ctrl

APPLICATION SECURITY AT SCALE: INSIGHTS FROM 1,000+ CYBER RANGE EVENTS

CONTENTS

INTRODUCTION

Software continues to expand as a primary attack surface, with 75% of security vulnerabilities originating in the codebase[1], resulting in mounting risk from breaches and malware attacks that can cost up to $9M on average in recovery, regulatory penalties, and reputational damage[2].

Most traditional training instills fundamental security concepts but doesn't replicate the pressure and complexity of real-world incidents the way immersive, hands-on training platforms can. Cyber ranges address this gap, providing realistic environments where developers, engineers, and security professionals can safely practice — defending against the same vulnerabilities, misconfigurations, and business logic flaws behind today's headline-grabbing breaches. Combining real-world simulations with active problem-solving, cyber ranges are designed to build practical skills, foster secure-by-design thinking, and deliver measurable improvements in organizational resilience.

While many cyber ranges focus on infrastructure defense and incident response, they don't address one of the largest and fastest-growing attack surfaces: the applications organizations build and deploy every day. CMD+CTRL stands apart as the only cyber range platform purpose-built for application security. By mirroring the flaws, misconfigurations, and errors that attackers exploit in real-world software, CMD+CTRL cyber ranges offer engaging, realistic scenarios that help development and engineering teams build secure applications from the start.

The value of cyber ranges extends beyond basic skill-building. They provide measurable insight into organizational readiness, highlight where vulnerabilities may persist across teams, and foster the secure-by-design culture and community needed to support innovation at scale. This study distills the findings from over 1,000 cyber range events, offering data-driven perspectives on how simulation-based training strengthens technical capabilities, reduces risk, helps benchmark performance, and maximizes the return on training investments.

[1] Synopsys 2020 Open Source Security and Risk Analysis (OSSRA)

[2] IBM 2024 Cost of a Data Breach Report

SUMMARY AND KEY FINDINGS

TRANSFORMING SECURITY THEORY INTO MEASURABLE BUSINESS VALUE

Cyber ranges transform security training by immersing teams in realistic, application-focused scenarios that build lasting skills. This study analyzes data from 1,173 application security events, tens of thousands of learners, and more than 600,000 completed challenges. The findings demonstrate that simulation-based, guided training not only strengthens security posture and reduces vulnerabilities, but the blended, hands-on approach consistently delivers measurable, scalable outcomes across all experience levels.

INSIGHTS:

Hands-on learning drives measurable growth:
On average, repeat cyber range participants showed a +3,317 point improvement (+126%) and solved 14 more challenges (+98%) than first-time players, confirming consistent skill development through repeated exposure.

Developers lead in participation, but defenders outperform:
70% of learners came from software development roles, reinforcing the need for secure coding training. However, red teamers and defenders consistently ranked among top performers, highlighting the value of advanced, role-specific content.

Scenarios highlight strengths and critical deficiencies:
Challenges focused on OWASP Top 10 vulnerabilities like Broken Access Control, XSS, and Injection—ensuring practical, real-world relevance and exposing the need for ongoing training and reinforcement of conceptual learning

Junior talent learns fastest:
Participants with 0–3 years of experience averaged 1,029 points per event, outpacing more experienced peers in learning velocity and skill adoption.

Moderate-difficulty drives momentum:
Most effective learning occurs in intermediate-level challenges, validating the importance of rich, scenario-based content that balances accessibility and technical depth.

Range usage reveals opportunity:
44% of events featured a basic level web application range, serving as an effective foundation for hands-on training—but repeat and experienced learners benefitted from access to advanced service and cloud ranges to prevent stagnation.

Integrated training drives stronger results:
Courses, journeys, assessments, and cyber ranges each offer unique benefits—but combining them as part of a cohesive program drives optimum engagement and accelerates outcomes.

METHODOLOGY

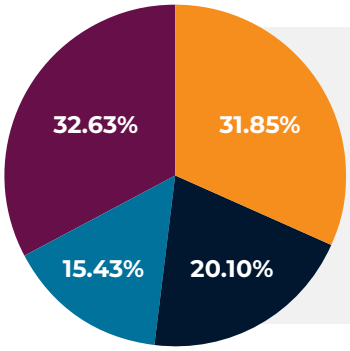
PARTICIPATION SNAPSHOT AND PERFORMANCE

For this study we examined the results from over 1,100 CMD+CTRL cyber range events from 2019 to 2025 representing over 600,000 total completed challenges.

Events were primarily instructor-led remote events, with approximately 20% held in-person, typically onsite at corporate offices. Software security experts were on hand for each event to guide participants through an average of 50 challenges ranging from beginner to advanced. Challenges are primarily mapped to OWASP Top 10 and MITRE ATT&CK frameworks.

Participants were comprised of technical and software development teams from mid-sized enterprise to Global 100 companies, and included security professionals from across the technology, manufacturing, healthcare and entertainment industries.

Participants primarily had software development backgrounds (70.41%) with remaining players representing vulnerability assessment (6.46%), systems architecture (4.15%), and cyber defense analysis (4.07%) roles. Other technology-adjacent roles made up the remaining percentage but each individually represents less than 3%.



EXPERIENCE LEVELS: A DIVERSE AUDIENCE

Participant experience levels were distributed across different career stages:

- Early-career professionals (0–3 years)
- Mid-career (7–10 years)
- Emerging practitioners (4–6 years)
- Seasoned veterans (10+ years)

In total, participants solved 861 distinct application-layer security challenges across a wide range of real-world scenarios. The breadth of content and depth of participation provided a robust dataset capturing both the technical capabilities and learning behaviors of today's workforce.

Cyber ranges referenced in this study include:

RANGE	LEVEL	DESCRIPTION
SHADOW BANK	Basic	Banking portal application range
SHRED	Basic	Retail e-commerce platform service range
ACCOUNTALL	Intermediate	HR management platform application range
SHADOW HEALTH	Intermediate	Medical information management portal application range
GOLD STANDARD	Advanced	Advanced banking website application range
MAIL JAY	Elite	Marketing Automation platform complex hybrid cloud range

PERFORMANCE SUMMARIES

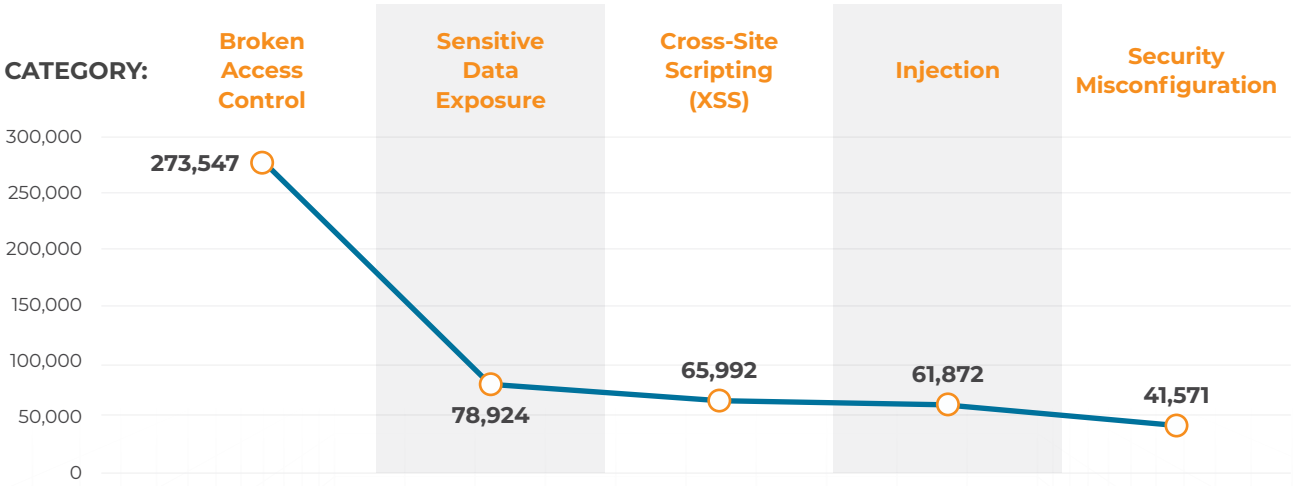
WHAT 600,000+ SOLVED CHALLENGES REVEAL ABOUT APPSEC READINESS

While participation data tells us who is engaging, performance data reveals how effectively participants are learning. With more than 614,000 challenges completed, clear trends emerge: learners excel when working through structured, moderately difficult tasks grounded in real-world application flaws. At the same time the data highlights friction points where learners struggled and missed opportunities for progression. This chapter examines performance patterns and their implications for training optimization.

WHERE LEARNERS EXCELLED

TOP FIVE CHALLENGE CATEGORIES BY SOLVE COUNT

Out of all challenges completed, five OWASP-aligned top-level categories were among the most frequently solved:

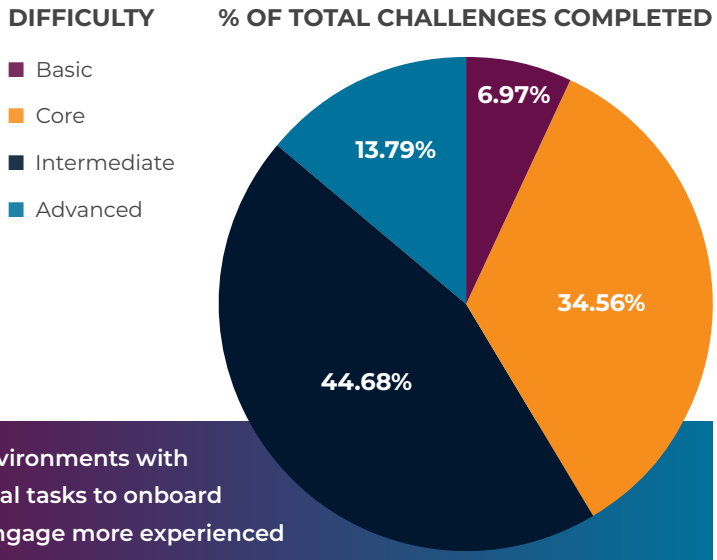


The significant focus on Broken Access Control indicates a strong alignment with real-world security concerns and regulatory pressure while the remaining categories correspond to common application-layer vulnerabilities, reinforcing the practical nature of hands-on cyber range learning.

Takeaway: Learners naturally gravitate toward challenges that reflect real-world environments, making these categories essential pillars of any training curriculum.

CHALLENGES SOLVED BY DIFFICULTY LEVEL

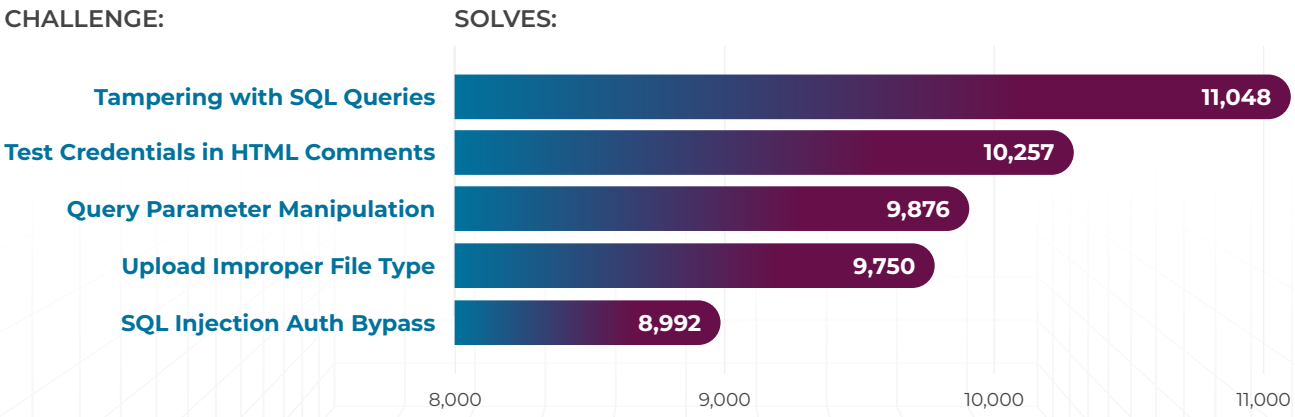
With nearly 45% of all solved challenges concentrated in intermediate-difficulty content, this tier serves as the training "sweet spot", with basic and core challenges a close second. Intermediate tasks are challenging enough to stretch skills, but accessible enough to drive consistent completion.



Recommendation: Provide a mix of environments with challenges across all levels: foundational tasks to onboard new learners, advanced scenarios to engage more experienced participants, and—most importantly—intermediate challenges, where the majority of players build and expand their skills.

HIGH-ENGAGEMENT HIGHLIGHTS: MOST SOLVED CHALLENGES

The most-frequently solved individual challenges are all tactile, relatable, and quick to test. They mimic mistakes seen in real-world codebases—making them ideal for both developers and security analysts. Their popularity reinforces the value of concise challenge setups with tangible outcomes.



Recommendation: Use these challenges to seed structured learning paths, groupings of related tasks that progress from simple discovery to full exploit. Incentivize replays through achievement tracking or time-based scoring.

EXPOSING SKILL GAPS

Despite the high overall volume of challenges solved, a surprising number of Basic and Core challenges remained largely untouched. Some key overlooked categories include Top 10 OWASP vulnerabilities:

- Sensitive Data Exposure
- Broken Access Control
- Broken Authentication
- Obfuscated Files or Information

These gaps are notable because the topics are highly relevant and map to core OWASP risks, but may be more difficult for leaners to uncover in simulated scenarios.

Key Insight: Low solve rates don't always equal high difficulty. Even foundational ranges include underutilized content. The challenge is often structural, not conceptual — forcing learners to consider a variety of situations where the vulnerability might appear.

MISSED CHALLENGES BY DIFFICULTY LEVEL: WHERE PLAYERS STRUGGLED

A breakdown of commonly missed challenge types by difficulty levels reveals more than just what's hard, it highlights where learners require stronger scaffolding and reinforcement.

DIFFICULTY	MOST MISSED CHALLENGE TYPES
Basic	Sensitive Data Exposure
Core	Broken Authentication, Obfuscation
Intermediate	Clickjacking, Phishing, Injection
Advanced	Persistent XSS, RCE, Reverse Engineering

Recommendation: Select ranges that provide structured hints, guided walkthroughs and contextual learning, particularly for commonly missed challenges, especially those at the core and intermediate levels. Reinforce concepts with refresher training to position learners for success.

PERFORMANCE BENCHMARKS

Cyber range data from tens of thousands of participants demonstrates a wide performance spectrum:

CHALLENGES SOLVED PER CYBER RANGE

26.4	17	1	225	9	35
Average	Median	Minimum	Maximum	25th Percentile	75th Percentile

These benchmarks tell us a few important things:

- Most participants solve between 9 and 35 challenges per event with a group of high-performing power users solving all challenges.
- The median score of 17 suggests that even single-day events can deliver measurable value with the well-structured challenge design and pacing.
- Top performers completed over 200 challenges, reinforcing the need for depth and variety of content to engage advanced users.

Recommendation: Select environments which track individual performance—providing a guide for recommending progressive difficulty levels based on prior performance and encouraging stretch goals to sustain engagement.

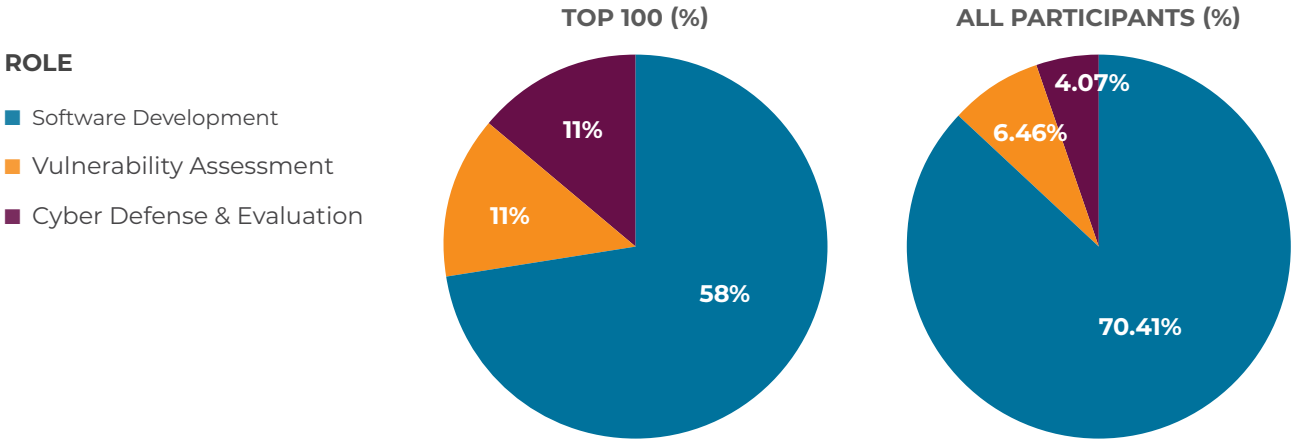
KEY TRENDS

As cyber range participation scales, so does the opportunity to fine-tune security training for maximum effectiveness. This chapter highlights the key trends revealed by performance, range utilization, and knowledge retention metrics, offering concrete guidance on the best ways to engage, challenge, and upskill today's security workforce.

BEGINNERS OUTSHINE SEASONED PROS

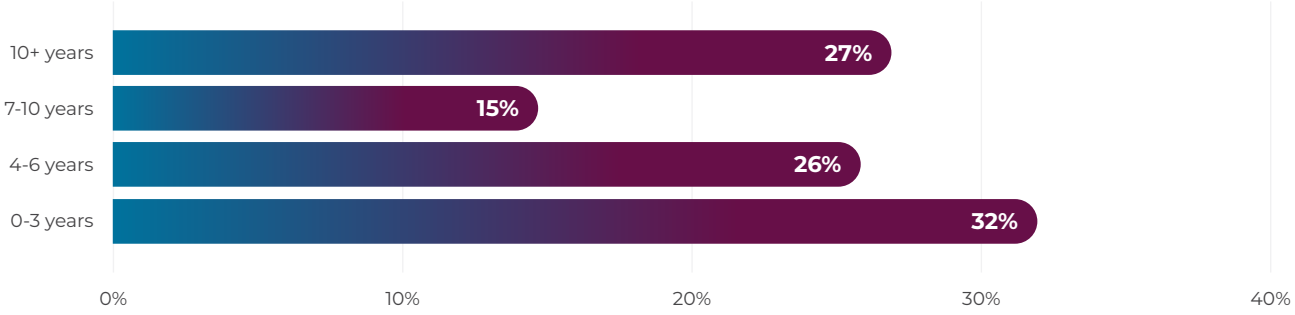
Analyzing the top 100 scorers across all events reveals compelling shifts in how we think about talent.

HIGH PERFORMERS BY ROLE



While developers make up the majority of participants overall, red teamers and defenders are disproportionately represented among the highest performers. This suggests that hands-on security experience provides a distinct advantage in recognizing vulnerabilities, understanding exploit chains, and solving complex challenges. The findings highlight the importance of cross-disciplinary training—bridging development and security expertise—to build resilient, high-performing teams.

HIGH-PERFORMERS BY EXPERIENCE LEVEL



This distribution confirms that strong performance isn't limited to seasoned professionals. Early-career participants frequently demonstrate high aptitude and growth potential—particularly when curiosity and motivation are high.

Addressing the needs of cybersecurity professionals of varying skill levels creates a unique challenge, and opportunity, for training architects. Beginners require more structured guidance and onboarding support, while experienced professionals expect depth, nuance, and variation in the challenges

Key Takeaways: Developers and early-career professionals generally dominate cyber range participation. The most effective cyber range programs balance introductory content with progressive complexity to serve the full spectrum of experience levels.

Recommendation: Invest in beginner-focused onboarding flows—such as guided tutorials, just-in-time hints, and low-friction registration. Simultaneously, unlock advanced tracks that challenge senior team members and incentivize repeat play. Some clients include a "step-up" option to keep more advanced learners engaged.

CYBER RANGES BY LEVEL OF DIFFICULTY:

The basic level ranges are utilized most frequently to drive broad participation across roles and experience levels. As engagement progresses there's a clear need for more advanced scenario-rich environments to challenge learners and support growth.

DIFFICULTY	# OF EVENTS	% OF TOTAL
Basic	725	61.8%
Intermediate	300	25.6%
Advanced	201	17.1%
Elite	51	4.4%

Key Takeaway: Foundational ranges drive broad participation, but advanced scenarios are essential to challenge and retain top performers.

Recommendation: Promote paths for learners to graduate to advanced content, for example:

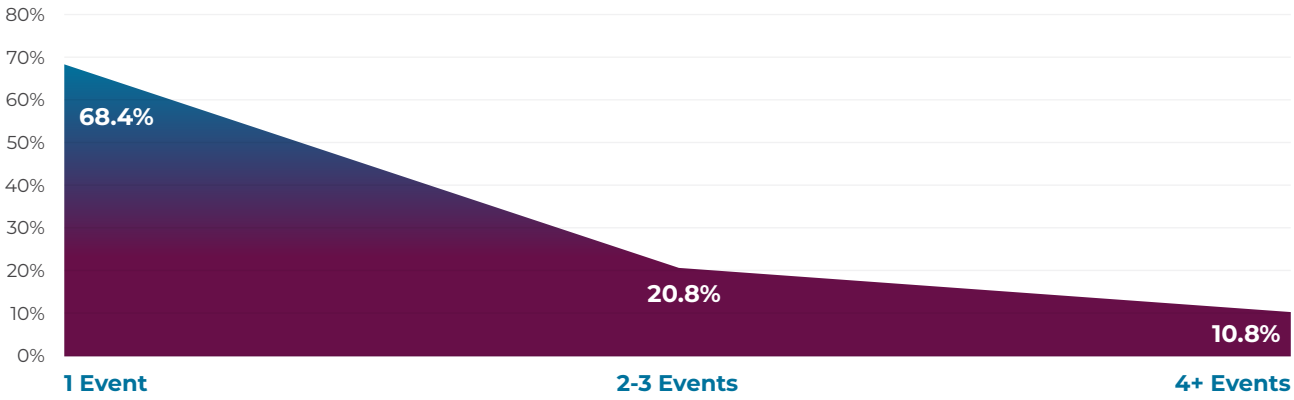
- Unlock higher-level ranges after completing milestone challenges.
- Recognize achievement and skill mastery with badges or certifications for elite-tier challenges.

KNOWLEDGE RETENTION AND LEARNER ENGAGEMENT

SUSTAINED, HANDS-ON PRACTICE DRIVES LASTING SKILL RETENTION

Repeat cyber range players represented 32% of the sample group, demonstrating the power of cyber ranges to engage learners and drive participation.

PERCENTAGE OF PARTICIPANTS BY NUMBER OF EVENTS



PERFORMANCE GAINS FOR REPEAT PLAYERS:

- **+3,317 points average gain** (126% median increase)
- **+14.1 challenges completed** (98% median increase)

CHALLENGE COMPLETION SPEED (TIME TO SOLVE 5 CHALLENGES):

- **Median:** 56 minutes
- **75th Percentile:** 1 hour, 48 minutes

Retention data shows that while most learners participate once, **repeat engagement delivers outsized impact**. Returning players improve their scores by 126% on average, complete nearly twice as many challenges, and demonstrate faster problem-solving over time. These findings underscore that sustained, accessible practice helps scale skill development and reinforce long-term knowledge retention across all experience levels

Key Takeaway: Ongoing access leads to measurable improvement—repeat participants learn more, solve more, and achieve significantly higher scores over time.

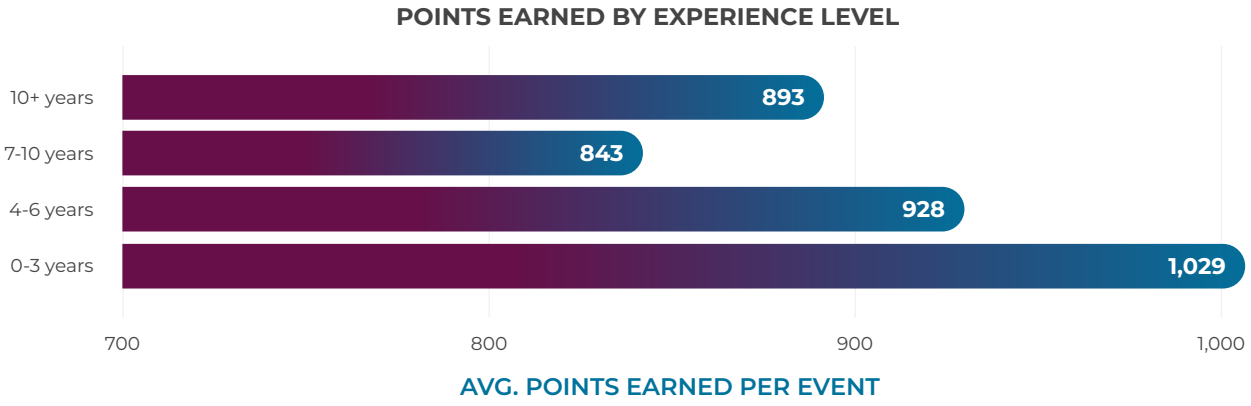
OPTIMIZING LEARNING VELOCITY

CLOSING THE APPSEC SKILLS GAP: HANDS-ON TRAINING ACCELERATES GROWTH AND REINFORCES PRACTICAL KNOWLEDGE

As cyber threats evolve, training methods must keep pace. Cyber ranges keep learning current by connecting theory to practice while accelerating the acquisition, retention, and application of critical security skills.

LEARNING VELOCITY: RISING TALENT SHOW RAPID GAINS

Not all learners advance at the same pace—and our data reveals a surprising trend: **junior professionals consistently** ramp up faster than their more experienced peers.



Professionals with 0–3 years of experience consistently demonstrated the highest learning velocity, earning more points per event than their more senior peers. This trend highlights the effectiveness of immersive, gamified training in accelerating skill development, enabling organizations to onboard and upskill new talent efficiently and effectively.

Key Takeaway: Early-career professionals are the most responsive to hands-on learning.

Recommendation: Investment in entry-level training pipelines, internship programs, and junior-level security roles, supported by structured cyber range access, yields the greatest training ROI.

REAL-WORLD RELEVANCE: BUILDING PRACTICAL SKILLS

A training program is only as effective as its relevance to real-world threats. The most commonly solved cyber range challenges provide strong validation that the format doesn't just build skill, it helps reinforce the right skills.

MOST FREQUENTLY SOLVED CHALLENGE CATEGORIES:

- Broken Access Control
- Cross-Site Scripting (XSS)
- Injection Attacks
- Sensitive Data Exposure

These categories map directly to the OWASP Top 10, a widely recognized standard of the most critical web application security risks which helps developers defend against many of the most common software vulnerabilities.

Key Takeaway: Cyber range challenges mirror real-world attack vectors, making training both practical and defensible.

Recommendation: Use cyber range outcomes to inform secure coding workshops, developer education, and red/blue team simulations. Build cross-functional programs around these common vulnerabilities to reinforce secure-by-design principles across disciplines.

THE ROI OF SECURITY EDUCATION

Cyber ranges do more than engage—they deliver measurable outcomes. The combined effect of real-world alignment, progressive complexity, and repeatable challenge structures creates a learning environment where value is realized immediately and deepens over time.

SECURITY TRAINING ROI HIGHLIGHTS:

- **One session** is enough to measure learning impact and identify skill gaps.
- **Repeat play** leads to major improvements in both speed and score.
- **Engagement is strong** across all experience levels, not just early-career.
- **Junior learners show accelerated growth**, making early investment more impactful.

Recommendation: Utilize cyber ranges as strategic levers for building and retaining top security talent.

- **Identify emerging champions** based on performance data.
- **Reinforce security mindsets** in non-traditional security roles (e.g. DevOps, product teams).
- **Track progress** and tailor learning paths with real-time feedback and adaptive content.

STRATEGIC RECOMMENDATIONS FOR TRAINING LEADERS

TURNING INSIGHTS INTO ACTION FOR SCALABLE, HIGH-IMPACT SECURITY EDUCATION

Cybersecurity training leaders face a dual mandate: build resilient, skilled teams while demonstrating the value of educational investments. An analysis of data from over 1,100 cyber range events and millions of course completions highlights where programs can drive the most value and how to scale impact to deliver measurable results over time.

1. ALIGN LEARNING TO ROLES

Insight: Learners are more motivated and engaged when training maps to daily responsibilities. Structured developer journeys show higher enrollment and completion rates over time compared to unstructured learning paths.

Action: Design curated journeys for key roles (e.g., Developer, Security Analyst, Architect) and tie completion to advancement or recognition. Refresh content regularly to maintain relevance.

2. REINFORCE LEARNING WITH SIMULATED ENVIRONMENTS

Insight: Cyber ranges accelerate learning by bridging theory and practice. Repeat players achieve 126% median performance gains and consistently solve significantly more challenges over time. Training with simulated environments can help uncover high performers across experience tiers

Action: Introduce ranges early, pair them with relevant courses to reinforce practical skills and provide ongoing access to track growth and identify rising talent across all seniority levels.

3. INVEST IN EARLY-CAREER DEVELOPMENT

Insight: Junior professionals with 0–3 years of experience demonstrate the fastest learning velocity, outperforming other cohorts.

Action: Offer blended training paths (courses + ranges + mentorship) for early-career individuals, track top performers for promotion, and provide advanced tracks to keep senior staff engaged.

4. TRACK LEARNING ROI THROUGH RANGE METRICS

Insight: Unlike traditional programs, ranges deliver rich, actionable data and real-time visibility into training outcomes: challenges solved, difficulty level, time-to-complete, peer benchmarking and progressive improvement

Action: Use these metrics as program KPIs and integrate them into quarterly reporting to justify program funding and expansion

5. OFFER JOURNEYS WITH BLENDED CONTENT

Insight: Stand-alone courses average 27% completion, while courses integrated with hands-on training and capstone activities show far higher engagement.

Action: Offer a mix of content formats to sustain engagement, build pacing guides to keep learners on track, and offer hands-on capstone events to mark milestones and drive participation.

6. CREATE GRADUATION PATHS

Insight: Without structured paths for advancement learners can plateau. While foundational ranges provide an effective introduction to simulated learning environments, offering more complex service and cloud ranges are key to growth for advanced participants.

Action: Define clear progression paths (e.g., unlock advanced ranges as milestones are attained), award badges or certifications to acknowledge achievement and encourage advancement.

STRATEGIC TRAINING LEADER CHECKLIST

This checklist distills key recommendations from cyber range events, learner journeys, and performance data to help cybersecurity training leaders design high-impact, scalable education programs. Each item offers a practical step to drive engagement, accelerate skill development, and demonstrate measurable training ROI across experience levels.

Start with Role-Aligned Journeys	• Design curated learning journeys mapped to key stakeholder roles like Architect, Engineer, Developer • Promote journey completion as a milestone for advancement • Regularly refresh content to match the needs of each functional role
Use cyber ranges to Reinforce and Validate Learning	• Introduce cyber ranges early in the learning cycle • Provide repeat access to track skill progression • Pair courses and assessments with relevant range challenges
Complement Assessments with Demonstrated Mastery	• Supplement quizzes and exams with cyber ranges and retrospectives • Use knowledge checks to identify gaps and assign related challenges • Acknowledge hands-on performance, not just test scores
Focus on Early-Career Development	• Target junior hires with blended learning and mentorship • Use performance data to support promotions and upskilling • Offer advanced options to retain high performers
Track Learning ROI Through Range Metrics	• Monitor challenge completion, repeat performance, and improvement over time • Use range metrics as KPIs for program success • Share data with stakeholders to justify budget and program expansion
Offer Blended Paths to Completion	• Combine courses, ranges, and structured journeys to drive adoption and completion • Provide hands-on “capstone” range events to recognize milestones • Use pacing guides or reminders to sustain progress
Create Graduation Paths	• Promote progression from foundational to advanced ranges • Establish performance-based unlock criteria (e.g., 4,500 points or 20 challenges solved) • Offer badges or certifications tied to range advancement

CONCLUSION

Train for Impact, Prove Business Value

The data reveals more than learning trends—it highlights opportunities to accelerate risk reduction and maximize return on training investments. Developers, early-career professionals, and repeat participants form the foundation of today's security talent pipeline. With tailored learning experiences and the right challenge design, these groups can rapidly mature into capable defenders, directly strengthening organizational resilience.

Build Adaptive, Scalable Programs

Security training can no longer be built around static, one-size fits all courses. Effective training programs incorporate role-aligned content as part of progressive learning journeys to deliver an ecosystem that scales across the enterprise. Cyber ranges provide the hands-on layer essential for real skill development, while integrated data from learner performance delivers the visibility CISOs need to identify talent, track ROI, and justify continued investment.

Let Data Drive Strategy

Leverage performance metrics as strategic signals. The challenges learners solve (and the ones they miss) reveal where organizations should double down on strengths, refine content, or reinforce fundamentals. With a balanced curriculum that includes basic through advanced hands-on training environments, training leaders can ensure accessibility and drive long-term retention.

Train Smarter, Accelerate Security

Velocity matters. The faster teams acquire and apply skills, the faster the organization secures its code, infrastructure, and operations. Given the right pathways, early-career professionals can quickly become force multipliers, while high performers with access to increasingly complex environments and advanced challenges become critical anchors for resilient security teams.

Looking Ahead

As cyber ranges become a standard component of application security training, hands-on simulated environments are reshaping how organizations build resilient teams. Real-world scenarios reinforce secure practices, accelerate skill development, highlight emerging talent, and give leaders clear, actionable insights into training ROI—proving that strategic, immersive education has the potential to transform an organization's security posture.

ABOUT CMD+CTRL SECURITY

CMD+CTRL Security is a pioneer in software security training. For over two decades, organizations of all sizes, from mid-sized to Global 100 companies, have relied on our training solutions to transform their software security. Our role-based modules, skill labs, and hands-on cyber ranges are designed to build skills that stick. Visit **www.cmdnctrlsecurity.com** to learn how we can help you launch a best-in-class training program.

cmd+ctrl