Playbook

Beyond OSCP+: A Playbook for Pentesting Company Growth

OffSec
The Path to a Secure Future™

Executive Summary

Getting your team to OSCP+ is a big milestone. But it's not the finish line.

For growing pentesting companies, it's just the starting point.

This whitepaper is a playbook for what comes next. Whether you're trying to scale your team without sacrificing quality, deepen your service offerings, or retain the talent you've worked hard to develop, the answer isn't hiring unicorns. It's building a system and a culture that develops serious skills.

That's where OffSec comes in.

In this Playbook, you'll learn how pentesting firms are using OffSec's training ecosystem: from foundational certifications like OSCP+ to advanced specializations in web application testing, red teaming, and exploit development, to level up their people, strengthen client delivery, and grow without breaking what makes them great.

The results speak for themselves:

- Teams that adopted a strong adversary mindset after OffSec training jumped from 19% to 57%
- Time to productivity dropped by 15% for newly hired consultants
- 38% of teams now onboard junior hires in under four weeks
- Firms saw faster threat identification and better performance in red team exercises
- Senior staff stayed longer when challenged with real labs, Cyber Ranges, and leadership pathways

This guide walks through how to take your team beyond the baseline, with:

- A practical 6 – 12 month roadmap for developing client-ready talent
- A mapped path to service expansion using OffSec's certifications (OSWA, OSWE, OSEP, OSED)
- Strategies to retain top talent and reduce delivery risk as you scale
- A training matrix you can adapt to your firm's growth model

If you've built your team on OSCP+, you're already ahead of most. Now it's time to go further.

Table of Contents

1 Why OSCP+ is more than a certification

2 Building talent you can bill

3 Reducing risk while you scale

4 Beyond OSCP+: Specializing for service expansion

5 Certify to differentiate

6 Retain the talent you trained

7 Your playbook in action

Why OSCP+ is more than a certification

There are a lot of certifications out there. Some are decent, some are fluff, and some will promise to make someone "job-ready" after a couple of hours of videos and a few multiple-choice questions.

OSCP+ isn't in that category. If you're looking for that, stop reading here.

For pentesting companies that care about real capability, not just resumes, OSCP+ stands apart. It's not harder just for the sake of being hard. It's designed to replicate the work your consultants are actually expected to do in the field. There's no safety net, no answer bank, no partial credit for almost getting there. It's a 24-hour hands-on exam where the candidate is dropped into a live network and has to investigate, exploit, pivot, and document real vulnerabilities.

And when we say "live," we mean it. These aren't click-through labs or templated challenges. The environments reflect the kinds of systems your clients actually run: layered, unpredictable, and full of opportunity if you know how to dig.

That's the point.

OSCP+ isn't just a technical test. It's a mindset builder. It forces people to slow down, question assumptions, try new angles, and keep going when things break. It rewards curiosity and creative thinking. It demands persistence. In short, it instills what we call the **adversary mindset**: the ability to approach problems like a real attacker would.

> "OffSec doesn't just teach you how to hack into something. They actually teach you their methodology and then force you to define your own. The methodology teaches skills like critical thinking, and no other cybersecurity training platform does that."
>
> **-Sam Cosentino, Cisco Systems**

We've seen the impact of that shift firsthand. In a recent survey, teams that adopted a strong attacker mindset after going through OffSec training increased from **19% to 57%**. That wasn't just about confidence. It showed up in performance: better lateral thinking, sharper decision-making, and stronger results in both red team assessments and live client exercises.

The mindset is part of the training. It's also part of the culture. OffSec's **Try Harder** motto isn't a slogan; it's the expectation. It means going beyond the first tool output. It means solving the hard parts when others would stop. It means digging for the vulnerability no one else saw because you were willing to look longer and think harder.

That's what OSCP+ builds.

And when your team is built on that kind of foundation, everything gets better. Clients might not ask for certs up front, but they notice when reports are clear, thoughtful, and tailored, not just copy-pasted. They notice when consultants show up prepared, adapt on the fly, and explain technical findings in business-relevant terms. They notice when you help them improve, not just tick the box.

The structure of OSCP+ ensures that.

If a candidate can't explain what they did, why it mattered, and how to fix it, they don't pass. That kind of discipline carries straight into client work, and it shows up in your delivery quality.

We've talked to firms that now require OSCP+ before a consultant ever sees a client-facing project. You're not guessing whether a junior hire can hold their own, as you already know they can. They've been through the fire and come out with the skills that matter.

So no, OSCP+ isn't just another cert. It's a filter, a growth path, and a signal to your clients, your team, and your competitors that you don't cut corners. You build talent with depth.

And that's where the real ROI begins.

What Makes OSCP+ Different?

Real-World Simulation

- Simulated environments mimic actual networks
- Multiple machines, pivot points, and defense layers
- No walkthroughs

Built for the Adversary Mindset

- Challenges learners to think like real attackers, not checklist testers
- Encourages persistence, creativity, and critical thinking under pressure
- Pushes beyond tool output to foster deeper decision-making

Professional Reporting

- Deliverables include a full, client-style report
- Emphasis on clarity, remediation guidance
- Reinforces real consulting deliverable standards

24-Hour Time-Boxed Challenge

- One shot, uninterrupted
- High-pressure environment mimics live engagements
- Tests time management, prioritization, and grit

Building talent you can bill

Almost every pentesting firm eventually runs into the same problem: the pipeline fills up, the projects stack up, and suddenly you don't have enough people to deliver the work. So you start looking, ideally for someone who's already certified, has real-world experience, knows the stack your clients use, can write a tight report, and somehow isn't already juggling offers from four other firms.

That person exists. But hiring them at scale? That's not a real strategy.

Even when you find them, they're expensive, and they know it. Which is why the firms that are growing sustainably aren't chasing unicorns: they're building their own bench.

The model's simple. Hire for potential, not polish. Bring in smart, curious people who are hungry to learn, and give them the kind of training that turns ambition into real-world skill. We've seen firms do this with huge success, taking new hires from first-day onboarding to client-ready in a matter of weeks, not months.

In fact, teams using OffSec to develop talent report cutting **time to productivity by 15%**, and **38% of them now onboard new hires in under four weeks.** That's not just efficient, that's a competitive advantage.

So what does that path look like?

It usually starts with **SEC-100**, OffSec's beginner-level course that lays the groundwork. It's designed for people who might understand IT or security basics but haven't put their hands on a live target before. It introduces the mindset, the terminology, and the way real attackers think and move. It's where you figure out who's really ready to do the work.

From there, most learners move into **OSCP+**. This is where the real transformation happens. Now they're in the lab building skills that translate directly to client engagements: enumeration, exploitation, lateral movement, and reporting.

By the time they pass, they're not just trained, they're tested. And for most firms, that's more than enough to start putting them on infrastructure or standard web assessments.

But if you want to go further in prepping for red team work or more complex environments, this is where **Cyber Ranges** come in. These aren't tutorials. They're simulated enterprise networks with real defenses, live detection, and layered architecture. Learners have to navigate pivot points, evade detection, and maintain access under pressure. It's messy. It's unpredictable. It's exactly what they'll face in real engagements.

The OffSec Enterprise Cyber Range (ECR)

Offensive Cyber Range (OCR)

Defensive Cyber Range (DCR)

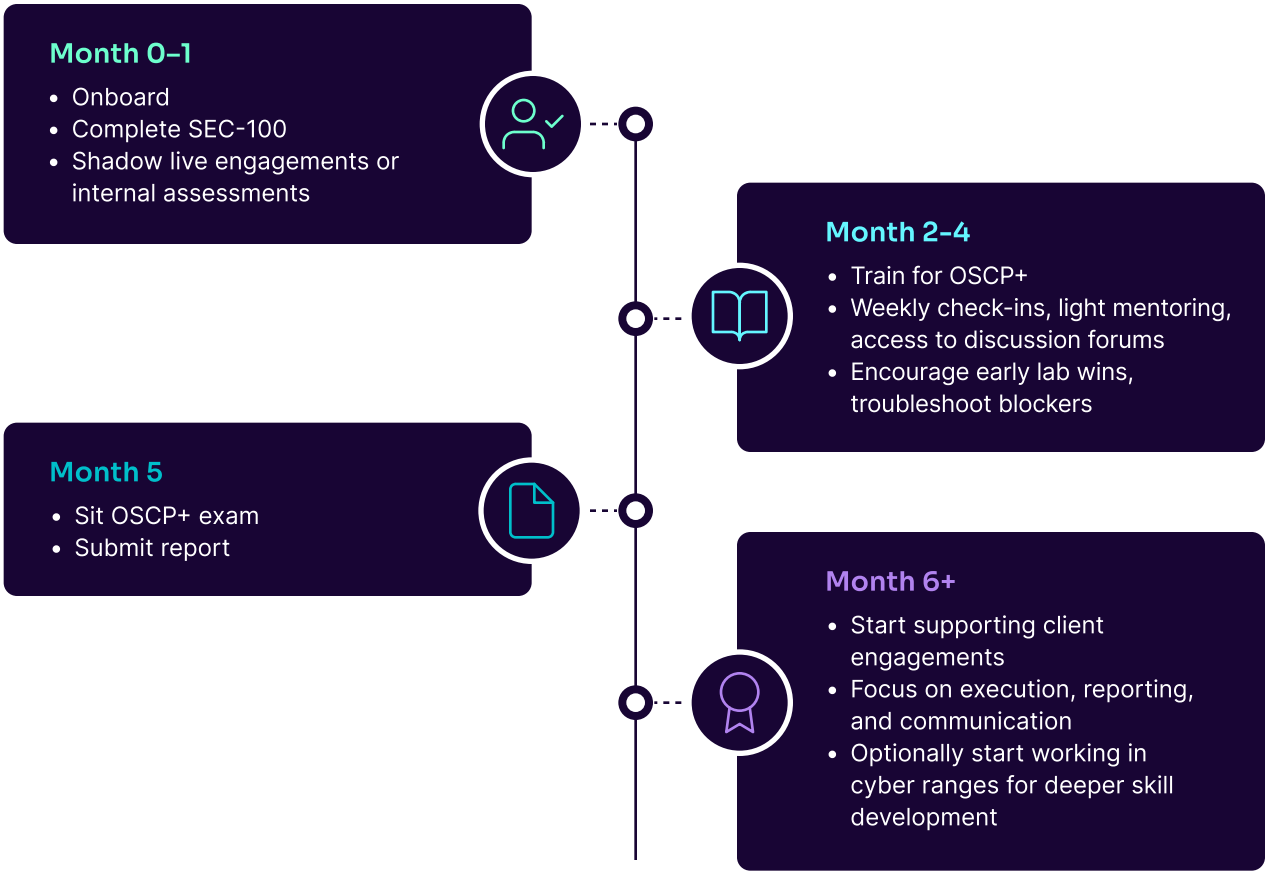
Versus Environment

And here's where it pays off: firms that invest in this kind of training see **faster threat identification from newly trained staff.** It's not just about getting someone through the door; it's about giving them the instincts and muscle memory to act fast when something doesn't look right.

You're not just training a junior hire. You're building someone who can handle themselves under pressure, think like an adversary, and deliver clean, actionable results when it counts.

That's how you scale: not with unicorns, but with people you've built, tested, and trusted.

Here's a rough timeline we've seen work:



This kind of progression keeps things simple. You don't need to guess if someone is ready since you've seen them build, break, and report on systems in controlled conditions. And they've built the muscle memory to do it again in the field.

More importantly, it gives your new hires a sense of direction. They know what's expected. They know what success looks like. And they know you're investing in them, not just as a resource, but as a future lead, mentor, or specialist.

You don't need a room full of unicorns. You just need a clear path and the right training partner.

We're here for that.

Reducing risk while you scale

It's a good problem to have: more clients than capacity. But if you scale too fast without the right foundation, things crack. And when those cracks show up in a pentest report or an engagement call, it's your reputation that takes the hit.

This is where quality starts to matter more than speed.

Most firms know how to scale the sales pipeline. Fewer have figured out how to scale delivery without sacrificing consistency. That's where structured, proven training makes the difference.

When you bring someone through OffSec training, you're not just teaching them how to find bugs. You're teaching them how to think, how to document, and how to approach problems like an actual consultant. The process becomes muscle memory: scope the environment, map the attack surface, test hypotheses, document along the way, and communicate clearly.

The problem with many certifications is that they separate knowledge from application. You can pass the test, but still not know how to run a real assessment. OSCP+ doesn't allow that. If you can't stay organized, document findings as you go, and explain what you did and why, you don't pass. That's exactly the kind of discipline that makes engagements go smoother and gives clients confidence.

Firms with OSCP+ certified consultants tend to see less rework. Fewer findings get missed. The level of handholding from senior staff drops because everyone's operating from the same baseline. You're not babysitting junior consultants. You're reviewing solid work and making it better, not fixing the foundation.

There's another layer here, too: retention.

Junior staff who are given a clear path to mastery and challenged in meaningful ways tend to stick around. They're more invested, more confident, and more likely to grow into senior roles that drive your business forward. Firms that create internal training matrices tied to OffSec's curriculum often find it easier to retain staff, promote from within, and reduce the constant churn that comes with relying too much on external hiring.

Here's a simplified example of a training matrix you can use to guide skill development and service assignments:

Role	Required Training	Project Type	Supervisor Involvement
Associate Pentester	SEC-100 + OSCP+	Internal testing, tooling reviews	High
Pentester	OSCP+	External infrastructure, basic web app testing	Moderate
Senior Pentester	OSCP+ + Cyber Ranges	Full-scope assessments, evasions	Low
Red Team Operator	OSCP+ + OSEP	Assumed breach, red team simulations	Peer-reviewed only

Beyond OSCP+: Specializing for service expansion

Getting your team to OSCP+ is a huge milestone. It gives you a solid, dependable foundation: people who can handle infrastructure assessments, dig deep on findings, and communicate clearly with clients. But for many firms, that's just the beginning.

As clients start asking for more targeted testing, more evasive, more application-specific, and more stealthy, your team needs to branch out. That means specialization. And the good news is: you don't have to go hunting for third-party trainers or cobble together custom learning paths from scattered content.

OffSec already has the tools.

Whether you're looking to grow your web application testing capabilities, level up into adversary simulation and red teaming, or dive into exploit development, there's a clear path forward, and it all stays within the OffSec ecosystem. That consistency makes it easier to train, easier to track, and easier to talk about when you're sitting across from a client explaining why your team is the right choice.

Let's break it down:

1. Web application pentesting

If you're expanding your services to include more in-depth web app testing, especially around logic flaws, advanced authentication, or chained exploits, you'll want your team on:

- **OSWA (The OffSec Web Assessor)**
  Covers essential techniques for identifying and exploiting XSS, SQL Injection, SSRF, and more, preparing learners for professional web application assessments.
- **OSWE (The OffSec Web Expert)**
  Much more advanced: advanced web application attacks and exploits, including advanced SSRF, persistent XSS, and blind SQLi to .NET deserialization, source code analysis, session hijacking, fuzzing, and authentication bypass.

2. Red teaming and adversary simulation

When clients want to go beyond point-in-time testing and simulate real-world attackers, red teaming comes into play. This is where your team needs to understand not just how to exploit, but how to move quietly, persist, and evade detection.

- **Cyber Ranges**
  Realistic environments that include active defenses, layered networks, and pivot opportunities.
- **OSEP (The OffSec Experienced Pentester)**
  Building on the skills gained through OSCP+. A must-have for operators doing assumed breach or full-scope red team work.

3. Exploit development

This is niche, but powerful. If you offer highly specialized assessments, test hardened targets, or want to do offensive research or vulnerability discovery, exploit dev is where the elite play.

- **OSED (The OffSec Exploit Developer)**
  Advanced exploit development techniques, including reverse engineering, writing shellcode, and bypassing modern mitigations. Not for beginners: this is for senior consultants or researchers looking to break into advanced territory.

Putting It all together

Here's a sample chart you can customize for your firm's internal planning or client marketing:

Service Offering	Recommended Training	Notes
Infra/App Pentesting	OSCP+	Baseline for most assessments
Web App Assessments	OSWA → OSWE	OSWA for coverage, OSWE for depth
Red Team Operations	OSEP, Cyber Ranges	Practical stealth and evasion skills
Exploit Development	OSED	Advanced specialization, high value

Training your team beyond OSCP+ isn't about padding resumes. It's about staying competitive. The market is maturing, clients are getting smarter, and expectations are rising. Being able to say, "Yes, we can test that, and we've got the right people for it," is a powerful position to be in.

And when those people are trained and certified through OffSec, the conversation gets a whole lot easier.

Certify to differentiate

Most clients can't evaluate technical depth, not really. They don't know the difference between someone who runs Burp Suite and someone who writes custom deserialization exploits. What they do understand is trust. They look for signs of professionalism, consistency, and credibility.

Certifications play a big part in that.

It's not just about having letters after your name. It's about showing that your team has been through something rigorous and proven they can perform. That's especially true with OffSec certifications because they're earned, not handed out. When a client sees OSCP+, OSWE, or OSEP on a consultant's profile, it tells them a few things right away: this person didn't just study; they executed. That's a strong signal.

And for pentesting firms, it's a clear differentiator.

In RFPs, during procurement reviews, and even informal selection processes, the presence of OffSec-certified consultants can tip the scale. Clients want to know that the people assessing their environments have real-world skills. If they see a team stacked with OSCP+ and OSWE certs, and if your competitors can't show the same, it becomes a clear edge.

The trick is knowing how to highlight that.

Here are a few simple ways we've seen firms put OffSec certifications to work:

1. Include certification badges in staff bios

In your proposals, pitches, and website, don't just list roles. List credentials. Make it easy for clients to see the caliber of your team. A staff bio that says:

> **"Jane Doe – OffSec Certified Professional (OSCP+)"**
> "Over 200 successful engagements, specializing in post-exploitation and lateral movement in enterprise networks."

...is going to hit harder than "Jane Doe – Senior Pentester."

2. Create a training transparency statement

This is especially effective in proposals or security questionnaires. Include a short section that explains how your team is trained and how often certifications are renewed. Something like:

> "All technical consultants complete OffSec's hands-on certification programs, including OSCP+ as a baseline. Advanced operators hold OSEP and OSWE certifications, with access to OffSec's live Cyber Ranges for ongoing development."

It doesn't need to be long, it just needs to show you're investing in the right things.

3. Build case studies around capability

When presenting a project win or a client success, tie outcomes back to training investment:

> "Our consultant, certified through OffSec's OSWE program, identified a critical business logic flaw that had previously passed multiple automated scans."

It's not about bragging, it's about showing how skill translates to client value.

4. Make it part of your brand

Certifications don't just build trust with clients, they also tell prospective hires and partners that you care about quality. You're not cutting corners. You're building a team that earns its credibility.

Display your team's collective certifications on your website, on pitch decks, and on social. Post when team members pass their exams. Celebrate wins. It's good marketing, but it's also good culture.

> **Sample language for an RFP Response:**
>
> "Each consultant assigned to this engagement holds, at minimum, an OSCP+ certification. OffSec certifications are known for their hands-on, real-world testing standards. In addition, our team includes consultants with advanced certifications such as OSWE and OSEP, ensuring deep capability in both web application testing and red team operations."

Certifying your team does more than validate skills: it builds a reputation. And in a crowded market, reputation is everything.

When your clients see OffSec next to your consultants' names, they know they're in good hands.

Retain the talent you trained

Getting someone up to speed is only half the battle. The real challenge? Keeping them.

Top pentesters don't stick around for long if they feel like they're stagnating. If every day starts to feel like another cookie-cutter engagement, or if there's no clear path to grow, they'll start looking elsewhere. And when they go, you don't just lose a person. You lose experience, client trust, team momentum, and all the time you invested in getting them trained.

The firms that retain talent the longest are the ones that don't let learning stop once the first cert is earned. They build in room for curiosity, deeper challenges, and internal leadership.

One way to keep that spark alive is through **OffSec Enterprise Cyber Ranges (ECR)**. These aren't lightweight practice environments. They're complex, high-stakes simulations built to stretch even experienced consultants. You're dealing with monitored networks, live defenses, and realistic adversary scenarios. There's no checklist and no one right way through. It's a space where your senior consultants can explore, experiment, and push themselves in ways that keep the work interesting.

ECR often becomes a proving ground for next-level growth. We've seen firms use them as part of promotion pathways or as prerequisites for leading red team engagements. Consultants who thrive in those environments often come back energized, not just because they learned something new, but because they were reminded why they got into this field in the first place.

It also helps to make that learning visible. You can also create **Custom Learning Paths** tied to roles and career progression. Show junior staff what it takes to lead projects. Show mid-level consultants how to become technical mentors or red team operators. When people can see the next step, they're more likely to stick around to reach it.

You can also turn up the engagement in more creative ways. A few we've seen work well:

- **Mentorship programs** that pair newer consultants with experienced staff during their OSCP+ prep
- **Lab competitions or internal CTFs** using ECR to keep skills sharp
- **"Lab Fridays"** where staff can explore new techniques without client deadlines
- **Knowledge-sharing sessions** where someone who recently passed OSEP or OSWE walks through what they learned and how they approached the exam

These kinds of initiatives don't require a huge investment, but they send a clear message. You're not just using your team for billable hours. You're developing them. And that builds loyalty.

It's easy to think retention is all about perks or pay. But the best people tend to stay where they're challenged, supported, and given space to grow. OffSec gives you the tools to do that in a way that's hands-on, relevant, and tied directly to the work your firm does every day.

You trained them. Now give them a reason to keep building with you.

Your playbook in action

From building a rock-solid foundation with OSCP+, to developing specialized capabilities for web, red team, and exploit development, to keeping your best people engaged, this isn't theory. It's a playbook for building a high-performing pentest practice with long-term staying power.

So, where's your firm today? And where could it go?

Quick Check: Where you stand

Talent pipeline

- ☐ Do you have a repeatable way to train new hires to billable readiness within 3–6 months?
- ☐ Are you onboarding junior staff with SEC-100 and moving them toward OSCP+?

Baseline capability

- ☐ Are all client-facing consultants certified to a minimum of OSCP+?
- ☐ Can your team handle assessments without constant oversight or rework?

Specialization

- ☐ Do you offer deeper services backed by certs like OSWE, OSEP, or OSED?
- ☐ Can you confidently say you have the right person for each type of engagement?

Consistency and quality

- ☐ Are your consultants documenting clearly, communicating effectively, and aligned in methodology?
- ☐ Do you trust your team to deliver without needing to recheck every report?

Retention and growth

- ☐ Do your senior consultants have access to advanced labs and Cyber Ranges?
- ☐ Is there a learning culture that encourages mentorship, internal growth, and continuous challenge?

If you're seeing gaps in any of these, we can help.

OffSec's enterprise training solutions are built for teams that want to scale without compromise. At the heart of that offering is **Learn Enterprise**: a flexible, structured training platform designed to help firms onboard, upskill, and retain talent at every stage of their growth.

With Learn Enterprise, you get:

- **Access to OffSec's entire course catalog**, including foundational and advanced content
- **Team-level management tools**, so you can assign learning paths, create custom learning paths, track progress, and report on readiness
- **Hands-on labs and Cyber Ranges** that simulate the real-world complexity your team faces in the field
- **Certifications that matter**, like OSCP+, OSWE, and OSEP, backed by challenging, practical exams
- **Role-based learning journeys**, so every consultant is building the right skills for the services you offer

It's more than a subscription. It's a system for building consistency, depth, and performance into your delivery model and keeping your top people challenged along the way.

Let's talk about your team

Book a consultation with our team to explore how Learn Enterprise can support your firm's growth.

Book a consultation

Or browse our team training solutions to see what's possible when you invest in building talent, not just buying it.

Explore team solutions

About OffSec

OffSec is the leading provider of continuous professional and workforce development, training, and education for cybersecurity practitioners.

OffSec's distinct pedagogy and practical, hands-on learning help organizations fill the infosec talent gap by training their teams on today's most critical skills. With the OffSec Learning Library featuring 6,000 hours of content, 1,500 videos, 2,500 exercises, and 900 hands-on labs, OffSec demonstrates its commitment to empowering individuals and organizations to fight cyber threats with indispensable cybersecurity skills and resources. OffSec also funds and maintains Kali Linux, the leading operating system for penetration testing, ethical hacking, and network security assessments.

Learn more at offsec.com

OffSec™
The Path to a Secure Future™