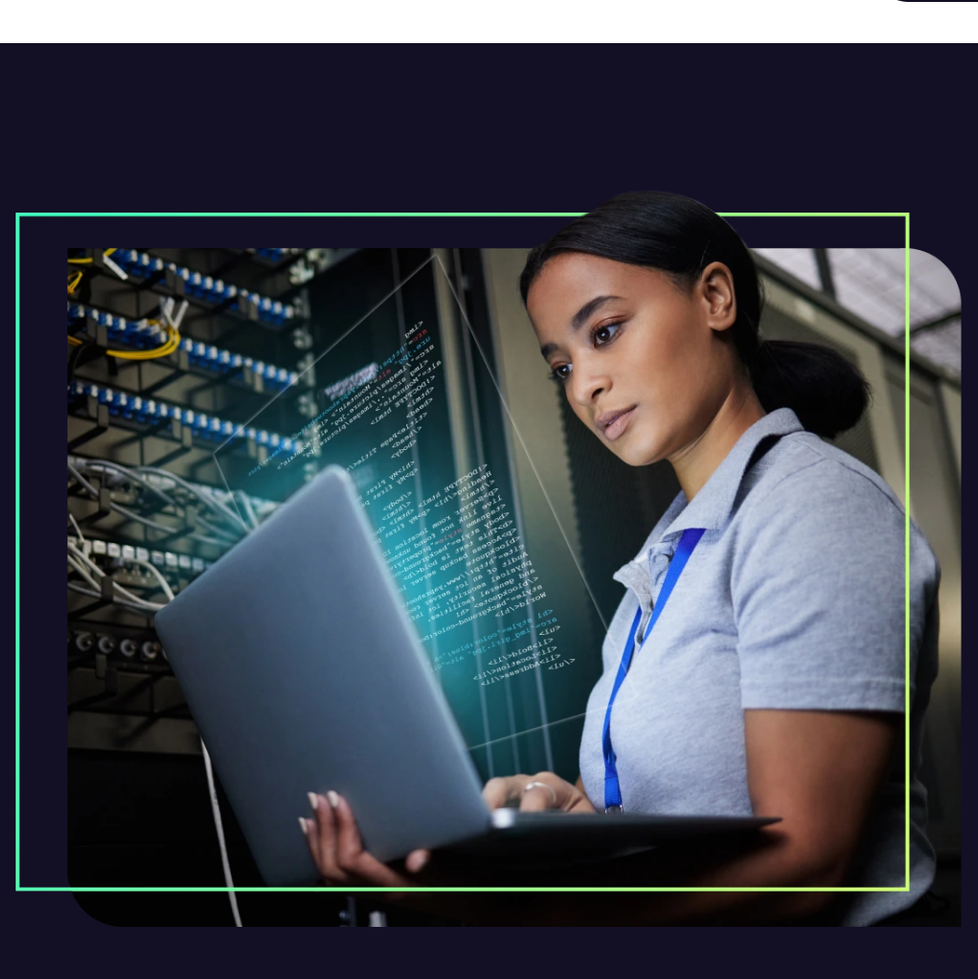
Pluralsight Secure Ready

Your people are your best security asset

With Secure Ready, you get an end-to-end security program built for modern enterprises.

Request a demo



WELLS FARGO · amazon · Microsoft · cisco · MERCK · Southwest

Security exposure threats are escalating faster than security teams can hire

$10M per breach

US breach costs have skyrocketed to an unprecedented $10.22 million per event.[1]

60% involved humans

60% of cybersecurity breaches involved a human element—not simply software flaws.[2]

#1 skill

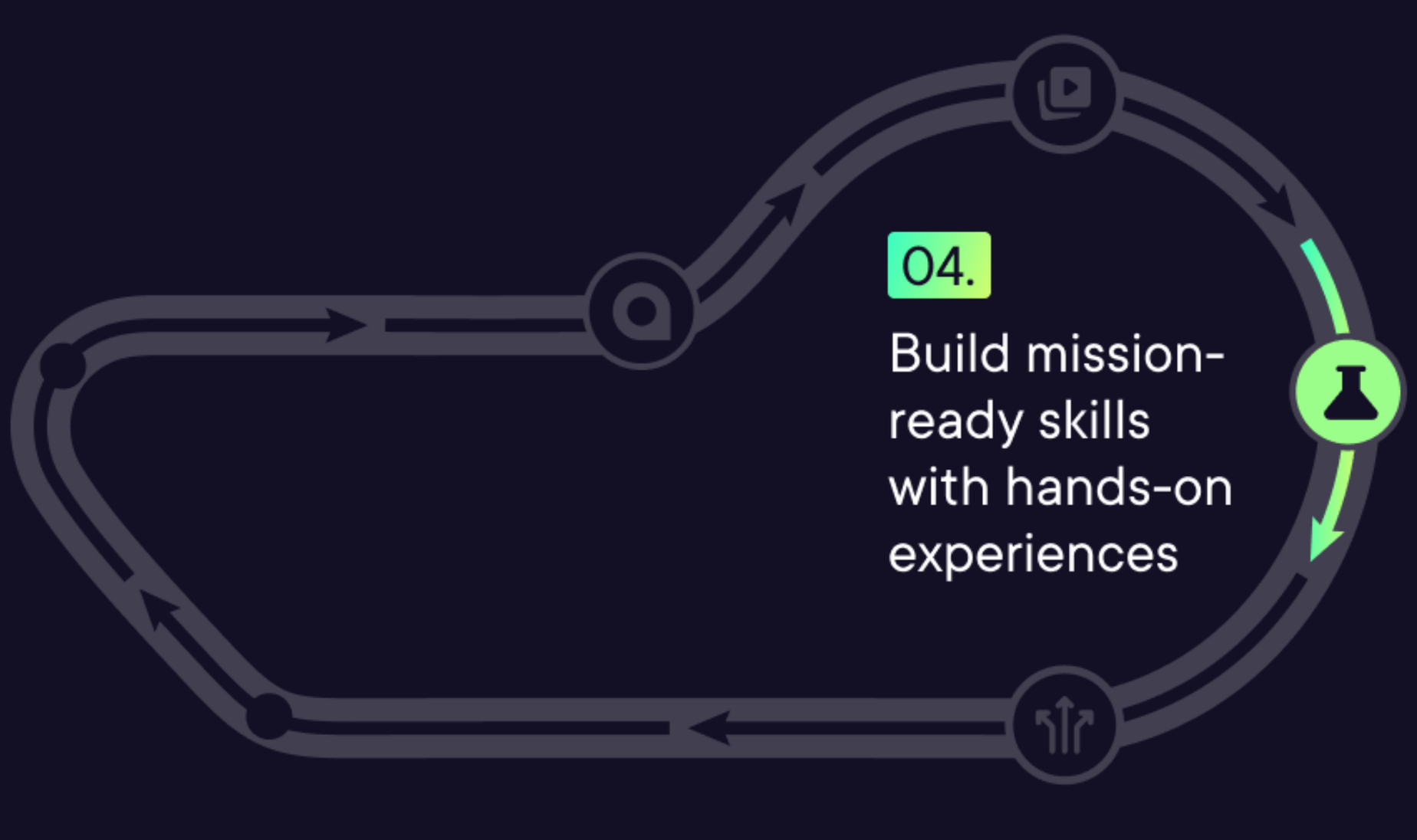
Application security was the most important skill cited by software engineering leaders.[3]

Build security readiness and operational skills with one unified and affordable platform

- Strengthen your security posture
- Grow expert talent from within
- Reduce cyber insurance premiums
- Eliminate redundant costs

Book a demo

Secure Ready prepares your workforce to detect, defend, and respond to real-world threats



01. Annual security readiness review

Assess readiness. Prioritize operational skills.

Secure Ready uses a structured, three-stage approach:

Stage 1

We'll meet with your security leaders to identify key priorities.

Stage 2

We launch a confidential, role-based self-assessment with both leaders and individual contributors to evaluate framework-based readiness, skill development goals, and organizational alignment.

Stage 3

You receive a detailed report outlining strengths, gaps, and misalignment. These results will inform program customization for the following 12 months.

02. Align roles and inventory skills

Structure teams to defend against emerging risks

Following your annual security readiness review, we'll align key skill capabilities from Pluralsight's built-in security role paths to your team's org chart so team members can focus on the skills that matter most to them.

Supported frameworks include:

1. NIST NICE Workforce Framework
2. DoD Cyber Workforce Framework (DCWF)

Practitioner skills inventory

Use targeted Skill IQ assessments to gauge practitioner capability, identify critical gaps, and guide role-specific learning.

03. Upskill efficiently with multimodal learning

On-demand security skill paths

Advance your team with 100+ specialized paths aligned to key security skills—like security event triage, pen testing, and incident response—delivered through:

Rapid-response courses

Expert-guided courses designed to address the specific emerging threats targeting your industry and tech stack.

CVE emulation and detection series

Within 48 hours of a major CVE disclosure, we release training and hands-on labs that replicate the exploit. Teams gain experience detecting and mitigating threats before they impact your environment.

Certification-aligned paths

Rigorous prep for ISC2, CompTIA, AWS, Microsoft, and others that include expert-led coursework, hands-on labs, and included certification practice exams.

04. Build mission-ready skills with hands-on experiences

Go beyond simple scenario challenges

Secure Ready includes 350+ advanced labs that truly emulate enterprise-grade conditions:

End-to-end adversary simulation

Execute the full offensive workflow—from external mapping to Active Directory takeover—in environments designed to mirror the complexity and scope of modern cyberattacks.

Attack and defend in the same lab

Pivot immediately from "making the exploit work" to "proving you can catch it." Use forensic tools like Autopsy and Volatility to trace attacker activity and build the intuition needed for high-stakes threat response.

Real-world data analysis

Simulate the true friction of a breach using real SIEM telemetry (Splunk, ELK, Zeek). Learners practice correlating signals, filtering noise, and operating as part of an active SOC workflow.

05. Measure progress and optimize

See what your team can actually do

Track skill progression and validate hands-on readiness through:

Challenge labs

Shift from training to testing with unguided scenarios that force learners to solve problems with zero assistance, providing objective validation of independent execution.

Security sandboxes

Assess role-specific skills and cross-functional execution to generate the performance data CISOs need to measure organizational collective response.

06. Deliver security results that matter

Transform learning into collaborative capability

Address org-wide objectives with live workshops add-ons:

Intensive multi-day security workshops

Select from over 40 hands-on and collaborative workshops for your security team—like a four day digital forensics and incident response workshop, a three-day AI threat session, or smaller focused workshops on critical areas.

Security for engineering

When you need to extend and augment your security posture beyond your core practitioners, you can engage with Pluralsight instructors to teach courses on DevSecOps, language-specific secure coding, and security architecture.

Rapid certification prep

Secure Ready includes access to security prep coursework and practice exams across every major hyperscaler, plus access to top-tier certifications like CISSP, CompTia Security+, and SC-900. But when you want to get your entire team certified in record time, we can also host live certification training for 5 days of intensive learning.

Book a demo

What you get with Secure Ready

For CISOs and security leaders

For CISOs and security leaders

Security skill development isn't one-size-fits-all. We'll work with your team to map standard capability frameworks (such as NICE or DCWF) to your org chart, so we can ensure every team member is focused on what matters most to them—and so your org isn't leaving skill blind spots. Our team will review this annually as organizational needs evolve so you stay ahead of the curve.

Program governance and operationalization

Structured training programs make it easy to run a consistent cadence across onboarding, refreshers, and attestations without starting from scratch each cycle.

Skill measurement and benchmarking

Built-in skill assessments establish baselines, identify gaps, and demonstrate measurable improvement over time.

Annual security awareness enablement

Pluralsight's unique approach starts with an annual readiness assessment where leaders and security professionals both evaluate team strengths and opportunities across 16 key security capabilities. Our team will report back on potential areas to focus efforts, in addition to areas of misalignment between groups—which often highlight under-recognized risk.

For security teams

Role-tailored skill paths

Curated learning paths mapped to security work roles and industry frameworks (including DCWF and NIST) are designed to standardize training expectations across security, IT, and engineering.

Rapid-response CVE seminars

Get rapid insights on new, critical CVEs and expert analysis on emerging threats, breaches, and techniques shaping today's cybersecurity landscape.

Hands-on labs

350+ expert labs enable learners to apply skills in realistic environments, turning training into evidence of operational capability.

Instructor-led workshops

Expert-led sessions are designed around real threats, common attack paths, and your team's environment. Topics range from phishing and social engineering to incident response and adversary emulation.

Book a demo

Secure Ready FAQs

What security leaders are asking

- Who is Pluralsight Secure Ready designed for?
- How is this different from standard security learning platforms?
- How do we measure success for a program like this?
- How does the program account for teams that are at very different skill levels?
- How does this assist with compliance and audits?
- How does the program stay current as threats evolve?

Defend your org

Close skill gaps. Reduce risk. Measure team performance.

Talk with our team about your goals, and we'll show you exactly how to align learning to frameworks, threats, and outcomes that matter.

Book a demo to see Secure Ready in action

First name*

Last name*

Email address*

Company:*

Phone number*

Country:*
Select...

By clicking submit, you agree to our Privacy Policy and Terms of Use, and consent to receive marketing emails from Pluralsight.

Submit

[1] IBM Cost of a Data Breach Report 2025
[2] Verizon 2025 Data Breach Investigations Report
[3] Gartner 2025 Software Engineering Survey