

# HOW TO MEET ENTERPRISE SECURITY REQUIREMENTS TO UNBLOCK DEALS



## LOCATION

New York

## INDUSTRY

Software  
Development

## EMPLOYEES

50-100

## CUSTOMERS

Dolby  
Cannondale  
Unicon

SkillCycle is an AI-powered talent development platform. As they prepared to sell into enterprise markets, they recognized that stronger security expectations could stall deals if issues surfaced too late. They engaged Software Secured to perform a SOC 2-aligned penetration test to proactively uncover and remediate security gaps before customer scrutiny.

## Enterprise Buyers Raised the Bar

As enterprise prospects entered the pipeline, security expectations rose quickly. Penetration testing, compliance evidence, and detailed questionnaires became requirements to move deals forward. As a fully remote company, SkillCycle also faced increased scrutiny around endpoint protection and physical security. SOC 2 emerged as a hard requirement, and without a recent application penetration test, customer data could not be onboarded to the platform.

The team wanted to take a proactive approach to discovering critical issues. Previous network-only testing yielded minimal findings and failed to satisfy enterprise buyers focused on cloud- and application-layer risks. The team knew there were gaps that they could not see.

SkillCycle partnered with Software Secured to deliver secure code training, helping their engineering team understand how attackers think and how vulnerabilities are introduced in real-world code. This combination allowed SkillCycle to meet enterprise security requirements with confidence while embedding security into its development lifecycle and strengthening the team's long-term capabilities.

## How SkillCycle Validated Application Security

SkillCycle engaged Software Secured for a SOC 2-aligned application penetration test paired with secure code training. The goal was to validate security for enterprise buyers and upskill the team for the long term.

Software Secured delivered a penetration test focused on real risk. Testing covered web applications, APIs, authentication, authorization, and OWASP Top 10 vulnerabilities. Findings were vetted, and false positives were eliminated. Results reflected real attacker behavior.

# HOW TO MEET ENTERPRISE SECURITY REQUIREMENTS TO UNBLOCK DEALS

The engagement was designed for flexibility. Endpoints could be swapped to control scope and cost. Heavy scanning was coordinated to avoid production impact. A staging environment was used where possible. Three authentication roles were defined to maximize coverage while keeping the test efficient.

Communication stayed tight throughout testing. Slack channels enabled blockers to be resolved quickly and for critical issues to be escalated immediately. Remediation support became the differentiator. Software Secured walked the team through the findings, using screenshots and straightforward steps. Engineers learned how vulnerabilities were introduced and how attackers exploit them. Three rounds of retesting ensured fixes held. Questions were answered without ambiguity.

Secure code training reinforced these lessons, and the team gained a practical understanding of how attackers think. Remediation best practices became part of everyday development decisions.

## From Annual Pentest to Embedded Security Practice

The results surprised the team in the best way. The penetration test confirmed that SkillCycle's security foundation was solid. There were no "horrifying critical" findings. Enterprise customers requesting penetration test evidence were satisfied with the report. Security questionnaires became easier to complete. Answers were validated, and the process reduced internal burden.

Manual penetration testing combined with remediation guidance strengthened enterprise sales conversations. Client-ready language helped SkillCycle explain controls around SQL injection, access control, and data protection with credibility. Most importantly, the team up-skilled. Security was no longer a once-a-year event. It became a shared responsibility embedded in the development process.

## Security as a Competitive Advantage

SkillCycle now meets enterprise security expectations with proof. Validated testing against OWASP Top 10 improved external perception. Penetration testing supports active deals and accelerates the sales cycle. SOC 2 progress is back on track and aligned with growth goals.

Security has become a competitive advantage.

SkillCycle now demonstrates validated application security, answers enterprise security questionnaires with clarity, and embeds security knowledge directly into its development lifecycle. The result is stronger trust with enterprise buyers and a more resilient security posture that scales with growth.