Illumio – Global Leader in Zero Trust Segmentation

cmd+ctrl

Illumio's strategic security solutions reduce the risk of lateral attacks in organizations through visibility and micro-segmentation for endpoints, data centers, and clouds. The company has long incorporated security best practices into their software development lifecycle (SDLC), but they wanted to ensure that their team's security skills kept on pace with the company's ambitious product roadmap that protects a portfolio of the world's top organizations.

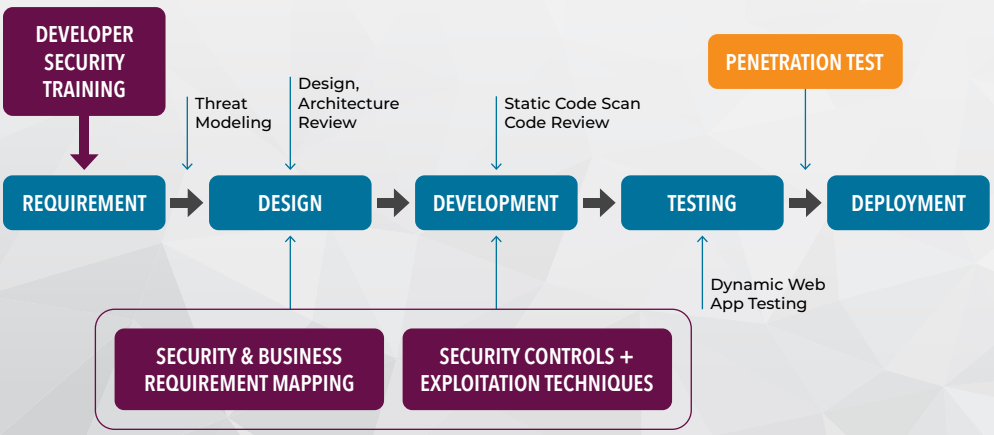
illumio

THE CHALLENGE: THINK BEYOND DEFENSIVE CODING

Illumio's development teams followed the classic red team (attack) and blue team (defend) roles. They were using a secure coding training platform but struggled with user adoption. The training content wasn't engaging enough and didn't offer exercises for those who did more than "just code." As a result, the broader team lacked a resource to build security proficiency within engineering and operations. This was a critical gap to delivering more secure software.

THE OPPORTUNITY: PURPLE TEAMING

Realizing that not all security checks can be automated, Illumio's AppSec program champion knew that the best path forward was to infuse exploitation techniques throughout the complete software development and delivery lifecycle. A former mobile game developer, she understood the importance of adopting an attacker mindset and utilizing a purple team approach — mixing offensive (red) and defensive (blue) techniques. To reach their goal, hands-on training was needed not just for developers, but managers, architects, IT, DevOps, and QA. By understanding abuse and exploitation cases (typical red team exercises), teams could implement proper defenses while defining requirements, building architecture, and writing code.



In the context of software security, purple teaming shifts security activities left. For Illumio, this meant reducing their reliance on the AppSec team, expediting the delivery of new features and improving product resiliency.

THE SOLUTION: REAL WORLD, COLLABORATIVE HACKING

Recognizing that the CMD+CTRL platform was designed to train developers to think like hackers, and support a purple team approach, Illumio partnered with CMD+CTRL to run a "Hack-the-Bank" cyber range event for all teams simultaneously. Combining players from various roles and skillsets, allowed them to maximize information sharing as they learned attack techniques.

The cyber range event ran alongside learn labs focused on SQL Injection, Session Management, and Cryptography. Combining experiential learning with formal instruction helped team members translate knowledge into mastered skills.

THE RESULT: A BLUEPRINT FOR ELEVATING THE SECURE SDLC APPROACH

With the rise in continuous integration/continuous delivery (CI/CD), siloed blue and red teaming efforts can slow down overall feature release. Proactively teaching developers purple approaches minimizes security defects and rework. After just one training session, Illumio established a long-term blueprint for elevating their security training program and gained a new perspective on reducing software risk.

1. **Optimized Competency**
   Real-time scoring and detailed reports allow for benchmarking player performance to deliver valuable insights and develop focused training plans.

2. **Building a Security-Minded Culture**
   By training together, teams developed a shared vision that reinforced the company's commitment to security and helped identify security champions.

3. **Progressive Learning**
   With cyber ranges that offer increasing levels of difficulty, participants can test their skills with new challenges and expand their security expertise in engaging environments.

CHOOSING THE RIGHT HANDS-ON TRAINING PLATFORM

Prior to working with CMD+CTRL, Illumio developers had access to short "tournament" style training programs that focused on code-level exercises. The program was not tailored to Illumio-specific learning elements – participants had to make it work on their own without the assistance of subject matter experts or instructors.

The CMD+CTRL cyber ranges and learning modules provided a robust platform to elevate Illumio's application security program. By incorporating real-world hacking and exploitation techniques, members of technical and non-technical staff alike gained a solid understanding of attack scenarios and their impact.

Uplevel your software security with more secure, resilient code. Whether you are implementing a purple-team approach, empowering a security culture or meeting compliance mandates, our programs can help you transform your software security posture.

We work with you to find the right combination of solutions to meet your organizational needs and eliminate skills gaps, mitigate risk and achieve compliance. **Request a demo today!**

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 cmdnctrlsecurity.com to learn how we can help you launch a best-in-class training program.

cmd+ctrl