ILLUMIO – GLOBAL LEADER IN ZERO TRUST SEGMENTATION

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.
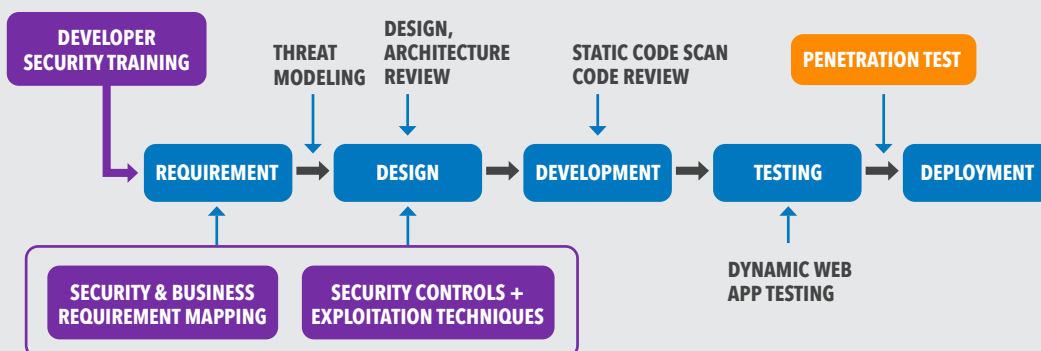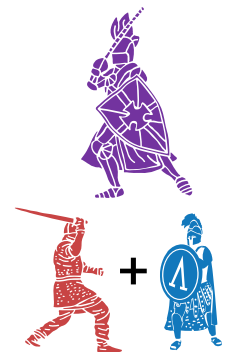
The Challenge: Think Beyond Defensive Coding

Illumio's development teams followed the classic Red Team (attack) and Blue Team (defend roles). They were previously using a secure coding training platform, but struggled with adoption - it wasn't engaging enough and didn't have 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, Trupti Shiralkar, knew that the best path forward was to infuse exploitation techniques throughout the complete software development and delivery lifecycle. As a former mobile game developer, she knows how critical an attacker mindset is and encouraged Illumio to adopt a purple team approach.

Purple Teaming is a mix of 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 (aka Red Team exercises), teams could implement proper defenses while defining requirements, building architecture, and writing code.

DEVELOPER SECURITY TRAINING

THREAT MODELING

DESIGN, ARCHITECTURE REVIEW

STATIC CODE SCAN CODE REVIEW

PENETRATION TEST

REQUIREMENT → DESIGN → DEVELOPMENT → TESTING → DEPLOYMENT

SECURITY & BUSINESS REQUIREMENT MAPPING

SECURITY CONTROLS + EXPLOITATION TECHNIQUES

DYNAMIC WEB APP TESTING

In the context of software security, purple teaming shifts security activities left. For Illumio, this would reduce their reliance on the AppSec team, expedite the delivery of new features, and improve product resiliency.

The Solution: Real World, Collaborative Hacking

After encountering the Security Innovation CMD+CTRL platform at an industry conference, Trupti instantly saw the power of a training program to groom developers to 'think like hackers' and instantiate her vision of a Purple Team. Illumio partnered with Security Innovation to run a cyber range event, "Hack the Bank", for all teams simultaneously. They opted for the team mode, combining players from various roles and skillsets, to maximize information sharing as they learned attack techniques.

The cyber range event ran alongside computer-based training (CBT) learning 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: Permanently Altered Secure SDLC Approaches

With the rise in continuous integration/continuous delivery, siloed Blue and Red Teaming efforts can slow down overall feature release. Proactively teaching developers Purple approaches will minimize security defects and the time spent fixing them. After just one training session, Illumio had a long-term blueprint for elevating their security training program, and entirely new perspectives on how to reduce software risk.

> *"From my experience, all software developers are now security engineers whether they know it, admit it or do it. Your code is now the security of the org you work for"*
>
> Jim Manico
> Founder, Manicode Security

1 Optimized Competency

Based on real-time performance assessments, training participants received detailed reports analyzing their strengths and learning opportunities. Illumio used these insights to target additional training with focused topics. Illumio also learned that its team possessed skills above the industry average - a valuable selling point for a cybersecurity company. Assumptions about skills and gaps were replaced with clear, actionable insights.

2 A Culture That Values AppSec

Having teams train together not only helped to decrease the strain introduced by cross-functional activities, but it created a shared vision and reinforced the company's commitment to security. It also gave Illumio new insights into their overall team strengths and revealed valuable opportunities for mentoring (aka "security champions").

3 Aspiring to New Heights of Excellence

Illumio plans to run future cyber range events at higher degrees of difficulty so that participants can reapply the skills they learned against new challenges and expand their security expertise. Illumio can now keep AppSec on pace with the company's ambitions.

Choosing the Right Hands-on Training Platform

Prior to working with Security Innovation, Illumio developers had access to training though a secure coding training company that ran "tournament" style programs. Lasting only 90 minutes, it was focused only on secure coding through code-level exercises and was relevant only for participants in development roles. The event was not tailored to Illumio-specific learning elements – participants had to make it work on their own without the assistance or instruction of subject matter experts.

Security Innovation's CMD+CTRL cyber range and CBT 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 good understanding of attack scenarios and their impact. The bar of product security awareness was raised, and participants are eagerly waiting for the next event.

If you want to create a culture of security-conscious team members who detect security defects faster and avoid common vulnerabilities during product development, explore Purple Team models. Train your entire organization on security through Security Innovation's CMD+CTRL training platform.

CMD+CTRL Training Platform – Build Skills that Stick!

Consider what Security Innovation offers above and beyond secure coding training, which addresses only a small fraction of the risk software introduces:

Fully supported
Live or remote expert proctors, learning labs, cheat sheets, and live chat support ensure desired outcomes can be attained.

Relatable
Cyber range events that reflect participants' skill level and real-world application environment makes events applicable to all companies and learners

Learn by Doing
Hands-on hacking and immersion keeps training exciting and engaging while still being informative. Players had so much fun they don't realize how much they're learning.

Baseline skills
Individual and group reporting provides a clear picture into competency and mechanism to track progress over time