

# The Vulnerability Multiverse

Only Proactive Training Can Keep It Together

With code evolving at the speed of light, securing software can feel like navigating a multiverse of possible failures. One path leads to secure releases, another to breach headlines.

Just-in-time (JIT) security training triggered by the discovery of a vulnerability, seems like a quick fix but often leads to more chaos than clarity.

## Just-In-Time (JIT) Training - Reacting After Damage Is Done

- ⚠️ Triggered after vulnerabilities are discovered
- ⚠️ Pulls developers out of workflow
- ⚠️ Addresses symptoms—not root causes
- ⚠️ Feels punitive and disconnected

## The High Cost of Waiting: NIST Defect Data

SECURITY BUGS COST MORE THE LATER YOU FIND THEM



Reactive training isn't cheap—it's a multiverse cleanup mission.

## How Proactive Training Holds the Timeline Together

In a secure development multiverse, proactive training keeps things from unraveling, equipping developers and engineers with the context and tools they need **before** the first line of code is written.

### Role-Specific Insight

- Tailored content results in actionable learning
- Everyone sees their version of the universe

### Aligned to Major Reality Shifts (Cloud, PCI)

- Cloud migration, platform upgrades
- AI adoption & API modernization
- PCI & compliance mandates

### Culture of Ownership

- No more punitive training
- Security becomes a team responsibility

### Builds Knowledge Early

- Security is embedded in the natural dev flow
- Fewer costly fixes later
- Faster releases, less rework

## Going Beyond the Code to Train the Whole SDLC

SECURITY IS A TEAM SPORT

Reactive Just-in-Time training focuses only on Dev errors, leaving gaps



Proactive training addresses systemic issues to create a shared security mindset

## CMD+CTRL: Your Anchor in the Vulnerability Multiverse

Proactive, Role-Based, SDLC-Aligned Security Training

### COMPREHENSIVE COVERAGE

- ✓ Modern languages & frameworks
- ✓ DevOps & CI/CD tooling
- ✓ Mobile, serverless, APIs, low-code
- ✓ GenAI & emerging risks
- ✓ Aligned to OWASP, ASVS, NIST

### ROLE-BASED LEARNING PATHS

- ✓ Front-end & back-end Devs
- ✓ QA & test engineers
- ✓ DevOps & SREs
- ✓ System architects

### IMMERSIVE CYBER RANGES

- ✓ Realistic web apps, services, cloud environments
- ✓ Offensive + defensive skill development
- ✓ Beginner → elite difficulty tracks

Keep security from fracturing with training that prevents vulnerabilities. **CMD+CTRL gives your teams the skills to keep your universe secure.**

EXPLORE OUR LEARNING JOURNEYS

### 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 [cmdntrlsecurity.com](https://cmdntrlsecurity.com) to learn how we can help you launch a best-in-class training program.

cmd+ctrl

