Security by Design: Enabling R&D to Build Safer, Smarter Medical Devices

OVERVIEW

A leading global medical device manufacturer faced an urgent challenge: as its products became more software-driven and cloud-connected, the cybersecurity risks tied to patient safety, product integrity, and regulatory requirements grew exponentially.

Despite having focused cybersecurity personnel in some areas, the broader Product Development and R&D teams, those at the heart of product innovation, lacked structured, role-specific training. The organization needed a strategy to scale security fluency across diverse functions without compromising momentum while facing aggressive timelines, overburdened technical resources, and learners averse to conventional training.

To close these gaps and embed security into the product lifecycle, the company partnered with CMD+CTRL to build an immersive, flexible, and highly targeted cybersecurity training program aligned to the needs of engineers, testers, quality specialists, and innovation leaders.

THE CHALLENGE

Security by Design, Not by Exception

While Product Development and R&D teams played a vital role in delivering secure medical technologies, they lacked foundational knowledge in cybersecurity, secure-by-design practices, and evolving regulatory requirements. This skills gap was compounded by competing priorities—tight deadlines, complex innovation pipelines, and rigorous quality standards—leaving little capacity for traditional training.

Security education delivered through static processes and documentation was ineffective and perceived to be more disruptive than enabling. As a result, developers and other technical stakeholders struggled to find the materials relevant and failed to see how their roles were connected to product security.

Without an engaging, role-based training strategy, security responsibilities remained fragmented across teams, increasing the organization's risk exposure and limiting its preparedness for audits, regulatory compliance, and post-market vigilance.

Common challenges included:

- **Low engagement with conventional training** perceived as irrelevant or disruptive
- **Overburdened security personnel** without the bandwidth to upskill the broader organization
- **Minimal awareness of secure-by-design principles** across product lifecycle stages
- **Fragmented understanding** of emerging risk vectors and regulatory expectations
- **Increasing number of vulnerabilities** and poor application security performance

THE SOLUTION

A Scalable, Targeted Learning Strategy for the Connected Device Era

The organization partnered with CMD+CTRL to develop a scalable, precision-targeted learning program tailored to unique roles across engineering, quality and innovation functions. Recognizing the diverse technical fluency across these teams, CMD+CTRL helped architect tiered, role-specific learning paths, starting with foundational concepts and progressing to topics like secure development, threat modeling, and architecture-specific risk.

Rather than delivering generic content, CMD+CTRL worked closely with cross-functional stakeholders to map organizational pain points and align training with job-specific responsibilities and product risk profiles.

Key program components included:

- **Tailored learning journeys** for developers, testers, and quality professionals
- **Interactive labs and gamified simulations** to drive engagement and retention
- **Vulnerability-focused modules** deployed in response to real-world product issues
- **Incentive structures** to further boost completion rates

OUTCOMES & RESULTS

Measurable Impact, Industry Recognition

Achieving strong adoption across Product and R&D without mandatory enforcement, the program was showcased at an industry conference as an innovative model.

Key outcomes include:

- **Workforce upskilling** with over 40,000 courses completed across teams
- **High voluntary participation rates** driven by thoughtful incentives and relevant content
- **Strong security culture** established through positive learner feedback and engagement
- **Compliance requirements met**, with the program exceeding expectations

The program's success has sparked interest in future expansions, including streamlined integration with the company's LMS and deeper engagement with threat-based, on-demand training units.

CONCLUSION

This global medical device leader successfully shifted from reactive training to proactive, role-based upskilling, helping teams design and deliver secure products without slowing innovation. CMD+CTRL's tailored approach empowered Product and R&D professionals to take ownership of cybersecurity, advancing compliance, patient safety, and product resilience.

In an industry where every line of code can have real-world consequences, this training program is more than an initiative; it's a safeguard for the future of connected care.

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