COSSACK LABS

Secure Software Development Training

Breaking is easy. Building is hard.
Learn to get things done securely.

Secure engineering is not fair — an attacker has to make just a few correct guesses, while a developer has to take care of numerous challenges from the very beginning.

Cybersecurity skills are crucial for mitigating business risks and meeting the requirements of security compliances when building modern applications. The most cost-efficient way to secure the software is to make security an integral part of the ongoing development process. Security bugs caught early on in the Secure Software Development Lifecycle are easy and cheap to fix.

Unfortunately, simply being good at software development does not equal having good security skills — those are scarce and hard to attain. It takes more than reading a few manuals to master them. Learning and adopting fundamental security practices and goal-specific techniques allows turning security into an integral component of any software product or application. Our software development trainings provide the best industry experience in secure development practices in a form-factor adapted for regular developers.

What do you get from our training?

The program is based on various practical SSDLC methodologies (MS SDL, OWASP S-SDLC), our own thorough experience in implementing security tools and protecting products in finance, healthcare, critical infrastructures, and governmental systems on traditional and modern web/mobile stacks. Our customers are software development companies that create applications with a large user base for the EU/US market.

How long does it take to go Pro?

There are 2 training level options available: **Basic** and **Pro**:

- In the **Basic** training, the topics are covered in short 2-4 hour modules. The basic training is a good fit for gaining a general understanding of the security issues and identifying the problem areas that need to be addressed on a deeper level.
- The **Pro** version is targeted towards the professionals with some prior understanding of the covered topics and with a wish to deepen and broaden their security skills. The pro training dedicates 4-8 hours per module and involves practical exercises.

Website: www.cossacklabs.com
Inquiries: **training@cossacklabs.com**

Cossack Labs Limited, 10-16 Tiller Road,
Docklands, London E14 8PX

What to expect from training?

Most trainings start with **Intro** module to introduce development team to the basics of risk management, secure software development lifecycle, security controls, and typical security components of a software system. After that, **Speciality** modules are available, suited to different technological stacks and needs.

Each module is based on lectures and Q&A sessions and contains module-specific theory and practical parts (workshops or case studies). Special slots are allocated for giving detailed answers to the questions that emerge during training and to the discussions of particular individual scenarios.

During the training, we teach the proper way to address the OWASP Top 10 critical security risks for the selected stack, provide a set of typical security design patterns, methodologies, tools, and libraries. Our aim is to teach the security mindset first, cover the processes next, and recommend the exact tools and libraries in the end.

As a result, your team achieves security-oriented mindset and acquires decision-making skills, masters practical techniques of secure development, and ultimately learns building more secure applications. For companies, this will improve their value propositions and customer satisfaction through the improved security of their products.

How does it work?

- **We start with a call** to better understand the specifics of your work, your issues, the areas of knowledge you'd like to cover, and the technological stack your team is using.
- **We adapt materials** appropriate for your team's experience, stack, and specific tasks at hand.
- **The training takes place**, covering the selected module(s).
- During the training, **we additionally supply you with literature, sets of useful links, provide feedback and support**, and answer your questions.

Why Cossack Labs?

We have the skills, knowledge, and experience in developing the most intricate secure software — at Cossack Labs we build security components for other developers. Our team consists of academic cryptographers, experienced software engineers, and security engineers. We combine data security expertise with the experience in engineering domains where data security and encryption is a necessary risk mitigation measure. Our engineers have experience in teaching students and training development teams.

Website: www.cossacklabs.com
Inquiries: **training@cossacklabs.com**

Cossack Labs Limited, 10-16 Tiller Road,
Docklands, London E14 8PX

COSSACK LABS

Module curriculum and contents

Introduction to application security and secure development

Aimed at the general audience, adapted to workshop's themes and goals.
Lectures and Q&A sessions.

- Understanding risk modelling, threats, trust.
- Secure software development lifecycle methodology (SSDLC).
- "Do's and don'ts" of secure development.
- Defining the risk scope and assets (sensitive data, trusted/untrusted perimeter).
- Components of a security system: data protection, component security, process security, infrastructure security.
- Core principles of security controls' design.
- Estimating, planning, and implementing security controls.

Speciality modules

Building secure architectures

Aimed at CTOs, architects, DevOps, security teams.

Basic:
Lectures and Q&A sessions.

- Secure architecture and planning.
- Data security architectures (centralised, end-to-end encrypted, distributed trust).
- Modelling, planning, assessing data flow and trust across all components.
- Architecture design patterns: DMZ, sandboxing, echelonisation / defence in depth, separation of duties, firewalling, jumpboxes.
- Attack surface management: access control, isolation, cryptography.
- Monitoring, logging, intrusion detection and prevention.

Pro:
Lectures, case-studies and Q&A sessions.

- Component security and trust: nodes, technical roles, people and processes.
- Microservice security.
- Problems with implementing quality attributes.
- Ensuring ongoing security.

Building secure web applications

Aimed at front-end and back-end web developers.

Basic:
Lectures and Q&A sessions.

- Trust model in a modern web application.
- Understanding the top vulnerabilities of frontend / backend, typical attacks.
- OWASP Top 10 web apps security risks.
- SSDLC during web apps development.
- Baseline: protecting sensitive data and components.
- Security controls: credential / key management, authentication, access control, encryption, session handling, JWT tokens, logging.
- Preventing vulnerabilities: input validation, working with dependencies, static analysis.
- Infrastructure security: transport, authentication, databases.

Pro:
Lectures, practical sessions and Q&A sessions.

- Designing secure APIs and microservices.
- Root causes for web attacks and mitigation strategies.
- Deep dive into application security.
- Deep dive into infrastructure security.
- Demo-cases of building secure data flow for typical web infrastructure.

COSSACK LABS

Building secure mobile apps (iOS/Android)

Aimed at mobile and backend developers.

Basic:
Lectures and Q&A sessions.

- Understanding platform-specific threats and risks.
- OWASP Top 10 mobile apps security risks.
- SSDLC during the development of mobile apps.
- Protecting user data in storage and in transit: data validation, encryption, access security, authentication patterns.
- In-depth into the key management.
- Transport security: TLS, other specialized cryptographic protocols.
- Infrastructure security: app secrets, external dependencies, code obfuscation.
- Various practical tips & tricks.

Pro:
Lectures, practical sessions and Q&A sessions.

- Building end-to-end encryption apps.
- Designing secure APIs.
- Demo-examples of building encrypted data flow for typical mobile application.

Security as a must-have attribute of your product

Aimed at project and product managers.

Lectures, case studies and Q&A sessions.

- Assessing security demands of projects.
- Understanding industry-specific security and compliance requirements.
- Understanding authentication and authorisation.
- Advantages of using cryptography to reduce time and cost of implementing security features.
- Mapping SSDLC to the real-world projects.
- Understanding risks, threats, and appropriate security measures for their mitigation.
- Planning and estimating security features, prioritization.
- Specificities of composing security roadmap.

Technical GDPR requirements for your product

Aimed at senior technical staff.

Lectures and Q&A sessions.

- GDPR: personal and personal sensitive data definitions.
- Understanding and mapping user rights to the technical properties of a system.
- Understanding data flow and designing security measures according to the lifecycle of sensitive data.
- Implementing principles: user consent, data protection, availability, access control and logging, firewalling, reacting to data breaches.
- Implementing real security instead of blindly following checklists.

Form factor and pricing

Training is group-based (up to 15 people). It takes from 3.5 to 7 hours per day in your office or in a dedicated convenient workshop/event space. It's also possible to conduct training online. Pricing depends on the number of participants and the selected modules.

Interested?

Please drop us an e-mail at training@cossacklabs.com

Website: www.cossacklabs.com
Inquiries: **training@cossacklabs.com**

Cossack Labs Limited, 10-16 Tiller Road,
Docklands, London E14 8PX