

SOFTWARE & READINESS

Secure Software Development

Instead of leaving security to the end of the lifecycle, we help you build more secure and sustainable software by integrating it into every stage from design to release.

**6**

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

Fixing a vulnerability found in production costs far more than catching it at design.



Secure software development makes habits and automated checks that prevent weaknesses early part of your team's process.

// WHO IS IT FOR?

Who is this service for?



Companies and teams developing software products



Those who want to raise security maturity before release



Those who want to meet secure development controls under ISO 27001



Those who want to combine DevOps transformation with security

// SCOPE

What does it cover?



Secure SDLC design

We define the security gates and responsibilities that fit your development process.



Threat modelling

We reveal possible attack paths at design time and plan countermeasures early.



Secure coding standards

We prepare coding guidelines based on sources such as OWASP Top 10 and ASVS.



Code review

We find vulnerabilities in your code base through manual review and static analysis tools.



DevSecOps

We integrate security checks into the CI/CD pipeline, dependency and secret scanning.



Developer training

We deliver hands-on training matched to the languages and frameworks you use.



Think like an attacker, build like a defender.

// METHOD

How we work

1

Current-process assessment

We review your development process, tools and risks.

2

Target process and standards

We define the secure development lifecycle and standards that fit you.

3

Tools and automation

We integrate security controls into your existing CI/CD pipeline.

4

Pilot and training

We apply them in one project, train the team and improve with feedback.

5

Rollout and measurement

We extend to other projects and track progress with measurable indicators.

// DELIVERABLES

What do we deliver?

- ✓ Secure SDLC process document
- ✓ Threat models
- ✓ CI/CD security control pipeline

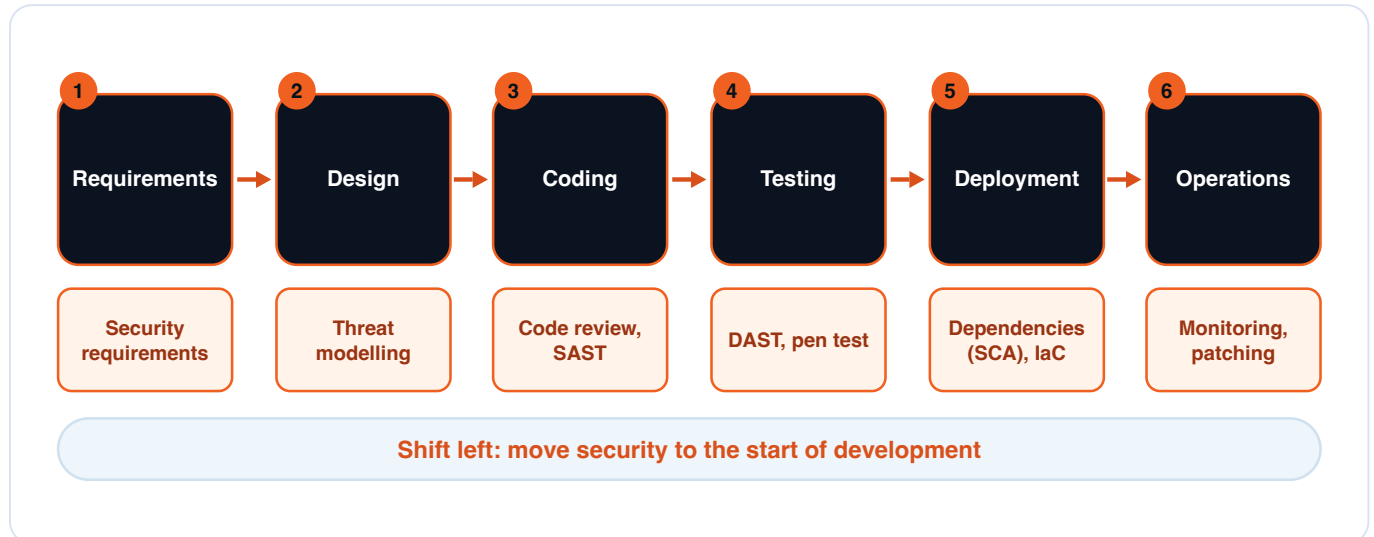
- ✓ Secure coding guideline
- ✓ Code review findings and remediation recommendations
- ✓ Training materials and measurement indicators

// VISUAL GUIDE

Service-specific visuals

Secure software development lifecycle

Security is a gate at every stage of development, not a step at the end.



Early gates

Decisions in requirements and design prevent many later flaws.

Automated checks

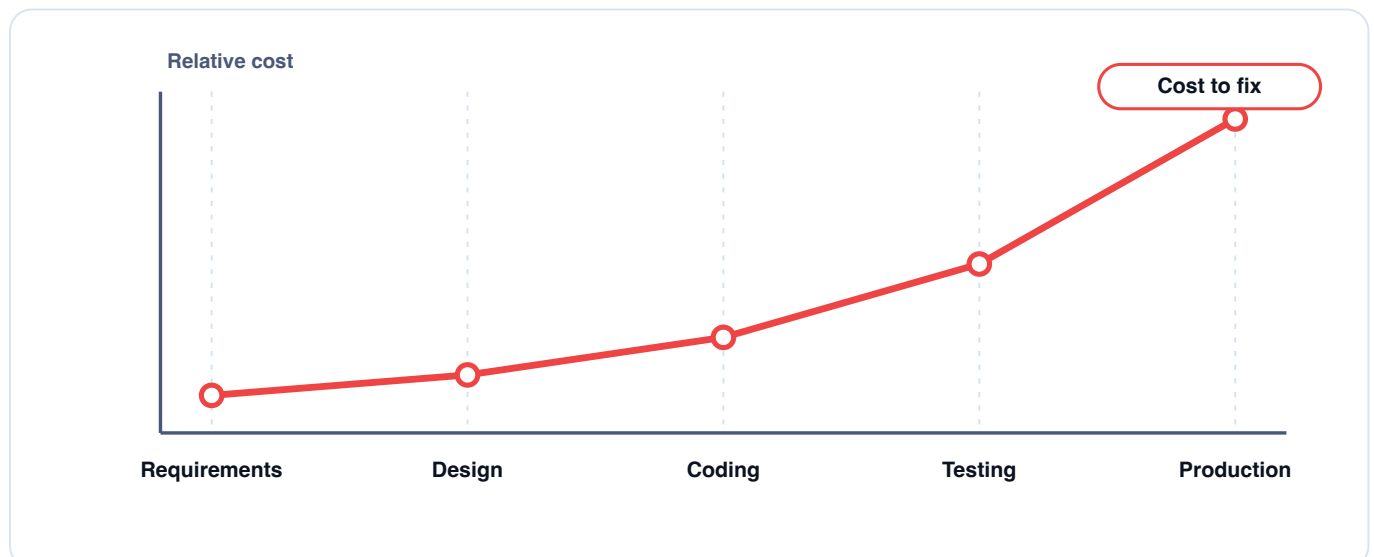
Tools such as SAST, DAST and SCA are built into the CI/CD pipeline.

Continues in operations

Monitoring and fast patching in production complete the lifecycle.

The cost of finding a flaw late

Schematic view: the cost of fixing a security flaw rises sharply as development progresses.



Cost rises

The same flaw costs many times more to fix in production than in design.

Test early

Moving security testing earlier lowers the total cost.

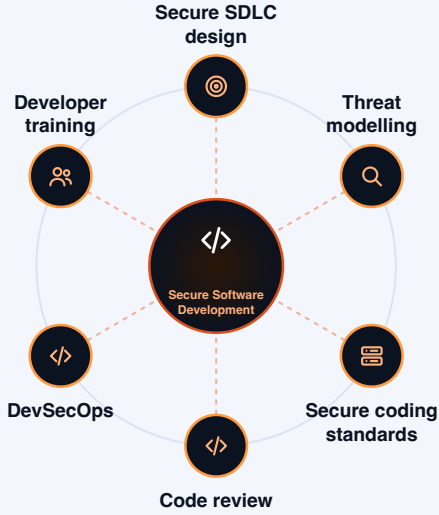
Developer training

Secure coding knowledge prevents flaws at the source.

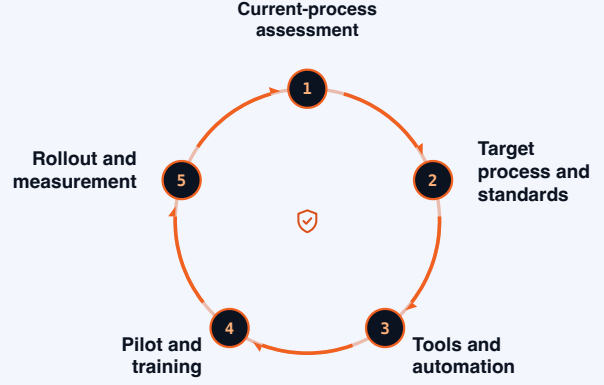
// AT A GLANCE

Service overview

SCOPE MAP



OUR DELIVERY LOOP



// UNDER ONE ROOF

Our other services

- | | | |
|---|---|--|
|  ISO 27001 Consulting |  ISO 22301 Consulting |  ISO 14298 Consulting |
|  KVKK Compliance Consulting |  Cyber Security Consulting |  Risk Management Consulting |
|  Penetration Testing |  Regular Vulnerability Scanning and Management |  DoS, DDoS Testing and Protection |
|  SOC / SIEM Implementation |  Endpoint Security Monitoring |  Information Security Awareness Program |
|  Incident Response Readiness | | |

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Scan the QR code for the service page and information form