DevSecOps approach

Timspark, 2024

What is Timspark

A custom software development boutique with a special business model that ignites and fosters full-fledged development teams and inspires every engineer to deliver outstanding results.

Core Teams

Understanding of industry & business domain

High-quality teams with a proven expertise

Teams are highly motivated

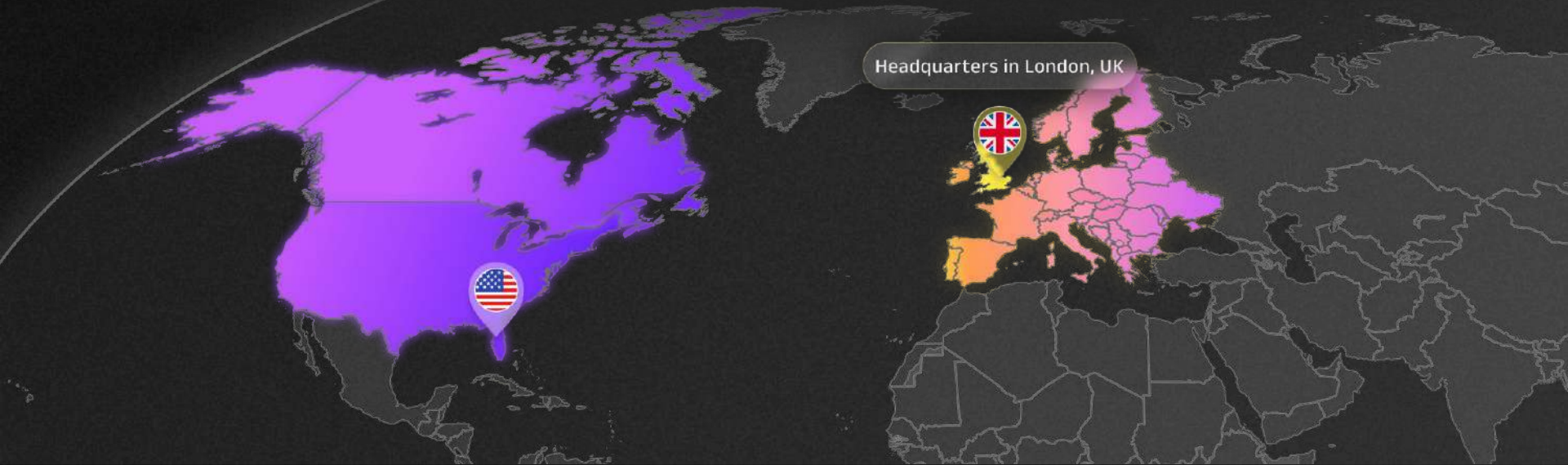
Accountability and ownership within the teams

Quick facts

30+
teams onboarded

1000+
vetted engineers involved

800+
projects accomplished



Key information

Certified development centers in

Poland, Lithuania, Georgia

Headquarters in

London, UK

Microsoft Partner

THE GLOBAL OUTSOURCING 100

CERTIFIED

ISO 9001 CERTIFIED

Forbes Technology Council

IAOP

Clutch

Inc. 5000

Global 200+ client base covering following industries:

Finance | Banking | Healthcare | eCommerce | Education | Logistics | Transportation | Manufacturing

timspark

How you can work with us

We are flexible. At Timspark, we offer different engagement models, from full-fledged teams to staff augmentation, to help you achieve your current business needs.

Core Teams

Pre-built development teams with deep expertise

Dedicated teams

Development units built specifically for your project

Team augmentation

Skilled engineers to enhance your in-house team

Technology stack

BACK-END

- JAVA
- RUBY
- SOLIDITY
- PYTHON
- C/C++
- UNITY
- .NET/C#
- RUST
- UNREAL ENGINE
- NODE.JS
- COBOL
- ELIXIR
- PHP
- GO
- SCALA

FRONT-END

- REACT
- Next.js
- ANGULAR
- VUE.JS
- JAVASCRIPT
- TYPESCRIPT

MOBILE

- SWIFT
- KOTLIN
- FLUTTER
- REACT NATIVE
- XAMARIN, .NET MAUI

PLATFORMS

- AWS
- AZURE
- CGP
- SAP
- SALESFORCE

Industry competence

- eCommerce and retail
- Logistics, supply chain and transportation
- Architecture, construction and real estate
- Finance, banking and insurance
- Tourism and hospitality
- Energy, oil and gas
- Healthcare and life sciences
- Media and entertainment
- Public services and utilities
- Education
- Telecommunications
- Agriculture
- Manufacturing
- Business management
- Art and culture
- Automotive
- HR and recruiting
- Ecology

Application Testing Approach

Plan

The test plan development involves identifying the scenarios for where, how, and when testing will take place.

SECURITY ANALYSIS

SECURITY TEST PLAN

Code

We ensure secure API keys and passwords by addinglinters and Git controls.

LINTERS & UNIT TESTING

GIT & IDE CONTROLS

Build

Using Static Application Security Testing (SAST) tools during the build process to discover code problems before pushing it to the next stage.

CODE COVERAGE

SAST

Test

Enhancing the security of your application by utilizing Dynamic Application Security Testing (DAST) tools during runtime. These tools help identify potential vulnerabilities in areas such as user authentication and authorization, SQL injection, and API-related components.

INTEGRATION TESTING

DAST

Release

Utilizing security analysis tools to undertake rigorous penetration testing and vulnerability scanning before the release.

PENETRATION TESTING

ACCEPTANCE TESTING

Deploy

After conducting the aforementioned tests in the production environment, deploy a secure build to the production environment.

Cloud security audit vision

Planning and scope definition

This step involves defining the audit's objectives, scope, and approach.

Data collection

This step involves collecting data about the cloud environment. This data can be collected manually or through automated tools.

Analysis and reporting

This step involves analyzing the collected data and preparing a report that highlights risks and vulnerabilities.

Recommendations

This step involves providing recommendations on how to mitigate risks and vulnerabilities.

Remediation

The recommendations received in the previous step are used to fix the security loopholes in the cloud.

Web application security testing

Web Application Security Testing (WAST) is a comprehensive process employed to assess and validate the security of web applications. It involves conducting various testing techniques and methodologies to identify weaknesses and potential attack vectors within the application.

While it focuses mainly on the application layer, it aims to find vulnerabilities across the app and **all its functionalities.** Some features reviewed during WAST include server configuration, input and output handling, and authorization and authentication credentials.

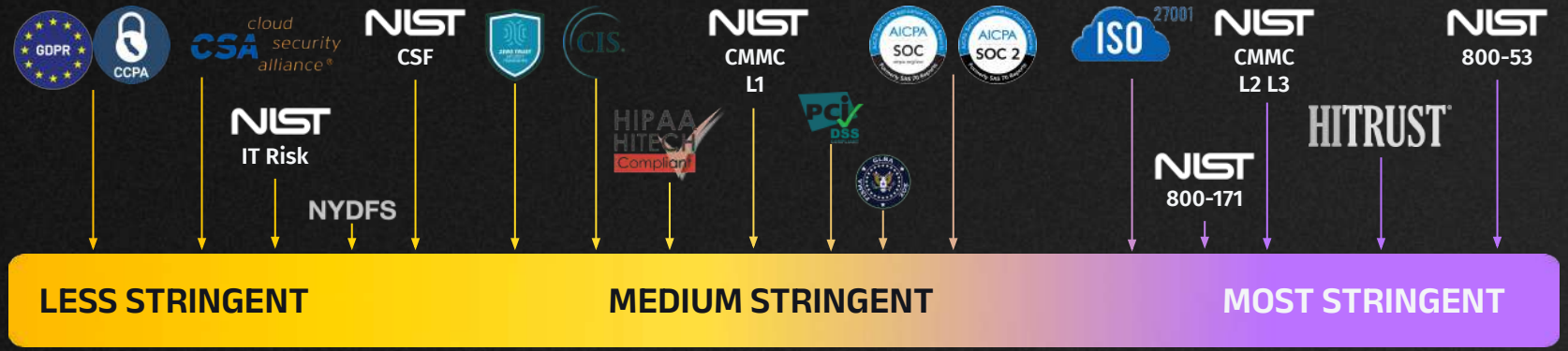
Web application security testing methodology

Information gathering | Planning analysis | Vulnerability detection | Penetration testing | Reporting

Web application security testing

In the face of ever-changing and evolving cyber threats, businesses remain vulnerable to attacks. It's not just about identifying vulnerabilities; it's crucial to **comprehend their potential impact and take appropriate mitigation steps.**

WAST encompasses more than just business protection; it also addresses **compliance requirements.** Regulations such as PCI-DSS, HIPAA, and SOC 2 necessitate safeguarding sensitive data and demonstrating sufficient security controls. Utilizing WAST as a guide ensures adherence to these regulatory mandates.



4 types of web application testing

01 SAST

SAST, or Static Application Security Testing, plays a crucial role **early in the development process, prior to application deployment.** By integrating it into the development process and automating it as part of the build process, security can be ingrained from the start.

SAST tools analyze the application's code and identify potential vulnerabilities **without the need for the application to be running.** They look for vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

02 DAST

DAST (Dynamic Application Security Testing) tools **simulate real-world attacks by sending requests to the application, analyzing the responses, and identifying potential vulnerabilities.** SAST is typically conducted during the testing phase of the SDLC to uncover any overlooked security flaws in the application.

DAST offers advantages in **identifying vulnerabilities that may not be found in the source code but are related to application configuration. Additionally, it can detect runtime-specific** vulnerabilities, including those arising from misconfigurations or server-related issues.

SAST

- White box tasting
- Requires source code
- Earlier detection
- Doesn’t find environment issues
- Supports all software

VS

DAST

- Black box testing
- Requires web application in staging or production
- Later detection
- Finds environment issues
- Predominantly web app testing

4 types of web application testing

03 PENETRATION TESTING

Penetration testing, performed by skilled ethical hackers, is a vital practice to ensure the application security.

Experts **simulate real-world attacks,** uncovering vulnerabilities that may go unnoticed through other methods. By understanding how attackers could exploit these vulnerabilities, organizations can effectively mitigate risks and enhance their overall security posture.

04 RASP

Runtime Application Self-Protection (RASP) **constantly monitors the runtime environment** of a web application to identify and prevent security threats.

RASP identifies vulnerabilities that may not be present in the source code but are present in how the application is configured and **only appear when the application runs.** This is the last line of defense that can help ensure the security of the web application.

Penetration testing

Information gathering and pentesting scoping

The process of collecting data about a target using various methods to obtain as much information as possible.

Vulnerability analysis

Vulnerability analysis tests web application weaknesses using tools and techniques to assess security risks.

Exploitation

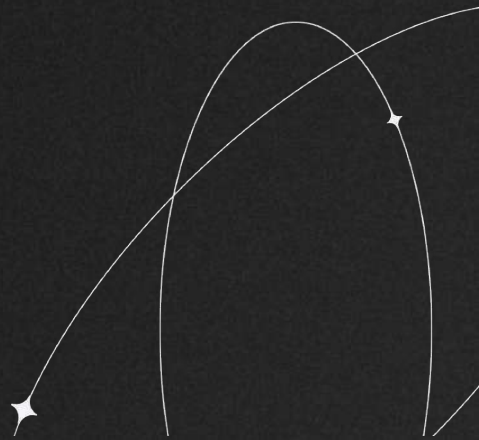
The team collects a range of exploits, including public and handcrafted ones, to leverage the identified vulnerabilities.

Reporting and remediation

The process involves documenting each vulnerability, its risk level, and providing instructions on how to address them.

Retesting

Retesting helps verify the effectiveness of the fixes. This phase often reveals any bypass or reoccurrence of the patched issues.



Penetration testing compliance

Innowise Group ensures **compliance with industry-specific standards** and regulations for penetration testing:

- **HIPAA** for healthcare institutions.
- **PCI-DSS** for companies processing payments.
- **RBI-ISMS** for banks and non-banking financial institutes.
- **SOC 2** for service organizations.
- **ISO 27001** for organizations seeking to establish a formalized approach to information security in business operations.

Penetration testing methodologies and standards ensure that a penetration test is authentic and covers all important aspects.

Some of these include:

- **OSSTMM**
- **OWASP**
- **NIST**
- **PTES**
- **ISSAF**

Penetration testing compliance

Cloud Security Posture Management

CSPM-tools help mitigate risks and compliance violations by identifying and remediating misconfigurations across cloud environments. These tools include Chef Compliance, OpenSCAP, Prowler, CloudBots (CheckPoint), tfsec (aquasecurity).

Continuous Compliance Monitoring

Compliance monitoring tools, such as ELK, Nagios, and Prometheus, are employed to guarantee ongoing compliance with regulations throughout the software development process.

Dashboards and reports

Dashboards and reports provide real-time visibility into compliance status, issues, and trends. Tools like Grafana and Kibana offer the capability to create customized dashboards and reports, providing accessible insights to relevant stakeholders.

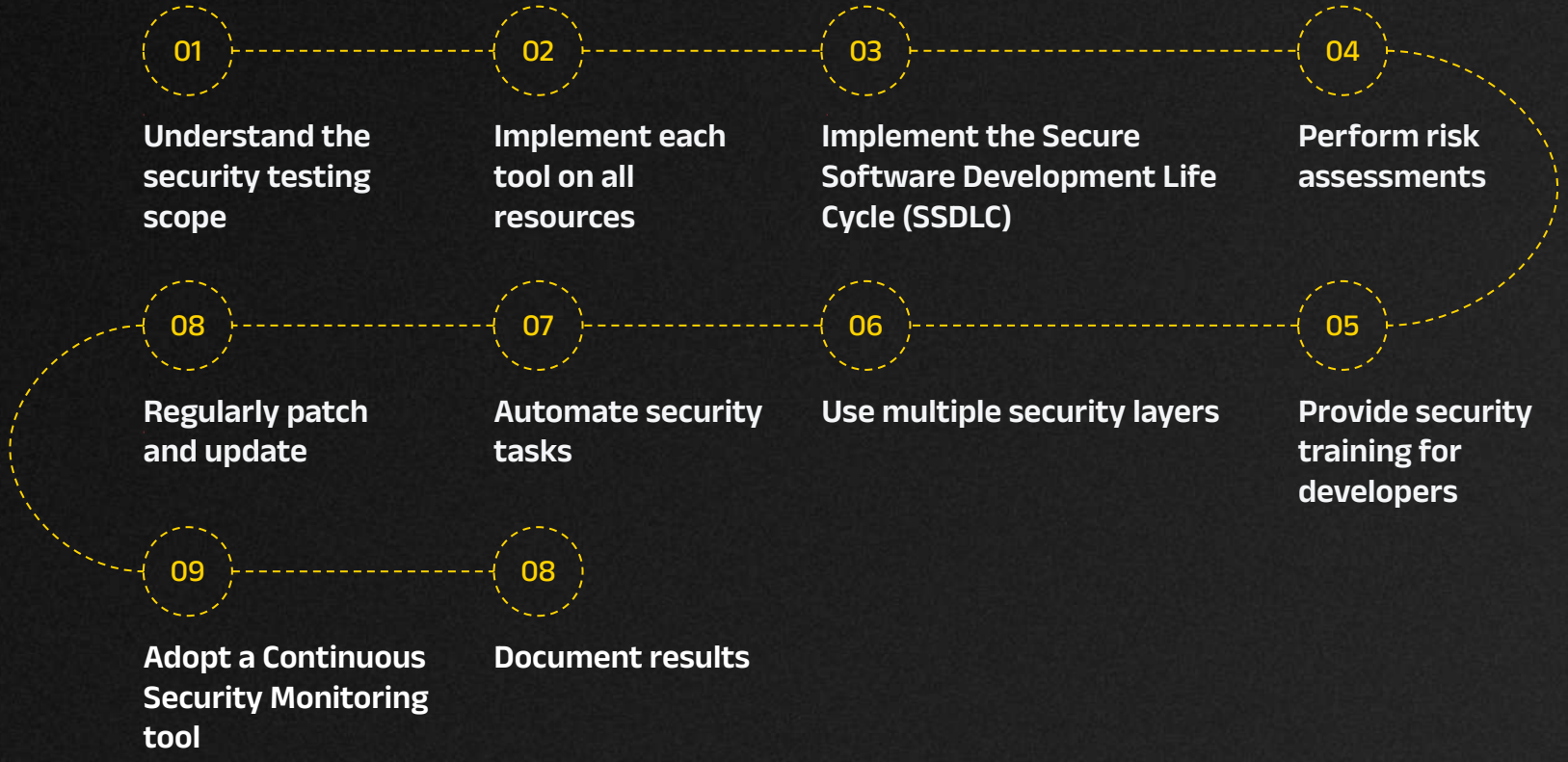
Compliance controls

To ensure compliance with specific regulatory requirements, the software development process incorporates a robust framework of pre-approved controls and processes. Tools like Terraform and Ansible enable the implementation of these controls.

Compliance audits

Regular audits are essential for ongoing adherence to relevant regulations. Tools such as Lynis, Wazuh, Checkov, OpenSCAP, and CIS-CAT are commonly utilized to conduct these audits and provide organizations with comprehensive insights into their compliance status.

10 essential WAST-steps we follow



Continuous security

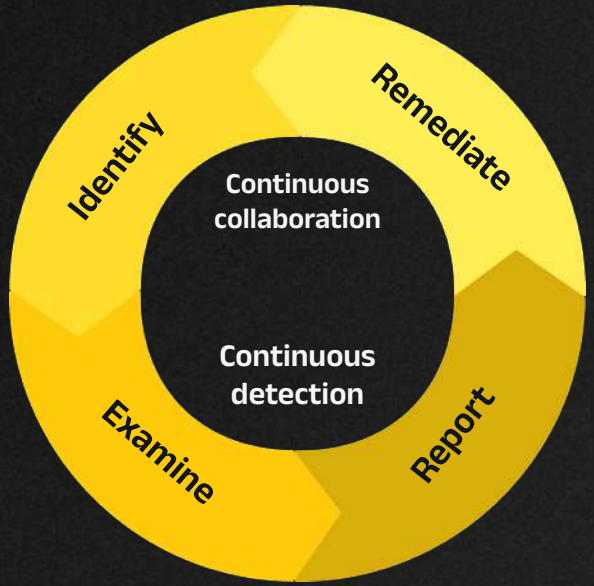
Our approach embraces continuous security as a fundamental component, encompassing ongoing measures to safeguard critical assets and data. It involves a systematic process of identifying, examining, reporting, and promptly remediating any security vulnerabilities while maintaining continuous collaboration.

Identify

- In-scope systems
- Testing windows
- Additional attack surface
- Changer to systems

Examine

- Infrastructure
- Applications
- Authenticated systems
- Assess for vulnerability
- Remove false-positives
- Exploitability of issues
- Impact of exploitation



Remediate

- Prioritise remediation by impact
- Ongoing technical advice
- Reconfigure insecure systems
- Reduce vulnerability time to live
- Reduce risk of breach

Report

- Instant notifications for critical findings
- Scope alerts for discovered assets
- Remediation instructions
- Monthly security digest

Types of security assessments

Risk assessment

Architecture & design review

Penetration testing

Physical penetration testing

Code review

Vulnerability scanning

Wireless assessment

Web application assessment

Security Services

- Security automation and orchestration.
- Continuous vulnerability scanning and assessment.
- Security testing integration. Integration of security tools into the CI/CD pipeline.
- Secure infrastructure provision and configuration management.
- Security incident response and management. Continuous security assessment and reporting.
- Security training and awareness programs for developers.
- Security audit support and compliance management. Security policy and governance support.
- Secure deployment and release management. Secure secrets management and encryption.
- Integration of security controls in cloud environments. Secure containerization and orchestration.
- Secure code review and static analysis (SAST). Infrastructure and application security architecture review.

Keen to explore this further?

Let’s discuss your requirements and come up with a tailored solution!

At Timspark, we intend to bring value and competitive advantage to our clients. Our dedicated teams can help you achieve your goals and add value to your offerings.

REACH OUT

Samuel Krendel
Head of Partnerships

samuel.krendel@timspark.com