



# Security Simplified.

[seisollc.com](https://seisollc.com)

(412) 206-6591

[sales@seisollc.com](mailto:sales@seisollc.com)

## Production Application Security Management

### vProdSec Services

Virtual application security expertise—built for scale. Get deep software security and pentesting capabilities without the cost of full-time hires. Accelerate development with confidence.

Strengthen cybersecurity with senior expertise in cloud security assessments, software development security program builds, web application penetration testing, and guardrail automation. vProdSec delivers technical security advisory and appsec program build services using scalable, agile development best practices.

Acting as an extension of your team, our devsecops, appsec, and red/blue engineers work closely with your team to identify configuration issues, design and optimize robust security pipelines, and implement guardrails that best fit your specific situation.



### What You Get:

#### Cloud & Application Security Expertise

Gain flexible access to senior security experts with deep cloud security, DevOps, software development, defensive, offensive, and app security knowledge to streamline compliance, optimize toolsets, and enhance adoption.

#### Assessment & Real-World Planning

Cloud security assessments, secure code reviews, web application pentesting, and technical workshops outline a threat modeled approach that is achievable and cost-effective.

#### Technical Compliance Navigation

As security frameworks, regulations, and certifications demand technical control alignment, our security experts translate the requirements into actionable implementation and risk mitigation strategies.

### Product & Platform Security That Scales



**Risk Based Assessments:** Identify configuration, security design, and operational gaps in the software development lifecycle quickly and efficiently.



**Compliance Integration:** Map technical finding to compliance outcomes, operating alongside GRC teams..



**Quality & Automation:** Streamline secure coding best practices using cloud-native automation and enhance code quality at the same time.



**Supply-Chain Risk Management:** Implement built-in risk visibility, finding and mitigating vulnerabilities throughout the development pipeline.



**Security Assurance and Advantage:**

Demonstrate effective controls, enhance security capabilities, and build awareness with minimal disruption.

#### Direct Integration With Development Teams

Our security experts work with your application development and DevOps teams to implement security best practices into the development process, ensuring faster time-to-market without compromising security.

#### Reputation Protection

By securing your product and platform using the vProdSec model, we help safeguard your company's reputation, protecting you from data breaches, compliance violations, and legal issues.

#### Expert Knowledge Transfer

During any engagement, your teams will have the ability to ask questions, gain insights, and learn directly from industry experts that empowers your team to own and scale security confidently.



# Security Simplified.

[seisollc.com](https://seisollc.com)

(412) 206-6591

[sales@seisollc.com](mailto:sales@seisollc.com)

## vProdSec Services

Designed for teams building cloud-native and custom applications, our virtual product security service integrates secure coding practices, product risk assessments, cloud configuration hardening, and web app pentesting directly into your development workflows. We start with a focused assessment to uncover gaps in architecture, code, SSDLC program maturity, and cloud posture, then provide ongoing technical guidance to remediate vulnerabilities, optimize DevSecOps pipelines, and elevate your product's security maturity.

Whether you're launching a new platform or scaling an existing one, vProdSec helps you build resilient, secure software—faster.



## Our Process:

### Conduct Platform & Product Risk Assessment

Our structured approach applies industry best practices to classify system components across architectural and data protection layers, enabling focused assessment based on the software's current stage of development.

### Integrate With Compliance & Plan for Remediation

Technical controls are aligned with application and cloud security frameworks such as OWASP SAMM and CSA Cloud Controls. Implementation plans emphasize automation, transparency, and operational oversight—accelerating security performance without slowing delivery.

### Deploy Remediation Plans & Monitor Effectiveness

Execute targeted initiatives to close application security gaps through secure coding training, enhanced software testing capabilities, and dashboards that track compliance and highlight areas for improvement.

#### Stage 0

Determine Baseline Maturity Level & Future State Goals

#### Stage 1

Assess Threats, Vulnerabilities, Risks, and Areas of Concern

#### Stage 2

Establish AppSec Program, Embed Security into SSDLC, & Develop CI/CD Automation

#### Stage 3

Bridge Compliance, InfoSec, DevOps with Production Deployment Cycle

#### Stage 4

Implement Continuous Improvement, Training, Monitoring, and Reporting Processes

## OUR APPROACH

# vProdSec Objectives

### Security Simplified.

Our approach to product & platform security is driven by a desire to simplify and reconnect development teams to information security best practice. We target security objectives one-by-one, bringing together a cohesive application security management program using an iterative, agile approach.



#### Maturity Assessment

Understand existing development practices, architecture, and security posture using OWASP SAMM, BSIMM, and DSOMM assessment criteria. Inventory the application, evaluate the tech stack, identify security tools, interview DevOps, Dev, Compliance, and Security Teams.



#### Embed Security Into SSDLC

Define SSDLC stages, map security controls to each phase, incorporate DevSecOps practice, and select or improve tools to integrate (SAST, DAST, IAST, SCA, Secrets Detection, SBOM, etc.)



#### Perform Risk Assessments

Conduct threat modeling of the app architecture, utilize SAST, DAST, SCA, and IaC scanning to categorize high impact vulnerabilities, inventory secrets, conduct pentesting, and review supply chain risks.



#### Code Review Process

Find and remediate insecure coding practices, implement security into CI/CD pipelines, create code review checklists, establish peer review process, flag insecure API's, mandate code review sign-off by security team.



#### Implement AppSec Program

Establish the long-term, sustainable AppSec strategy, appoint an AppSec lead, define AppSec roadmap, set metrics and KPI's, appoint security champions, define policies, standards, and SLAs, integrate tooling and alerts.



#### Secure Coding Training

Raise developer awareness and capabilities in writing secure code, conduct a baseline skills assessment, roll out training program, establish secure coding as part of new hire onboarding, track training metrics and completion rates.



#### Bridge Compliance, InfoSec, and DevOps

Align all stakeholders under a unified AppSec strategy, creating cross-functional appsec governance committees, defining shared goals, prioritize security tasks by risk, adopt tools that support collaboration, and hold regularly scheduled security reviews with all teams.



#### Measure & Communicate Progress

Track effectiveness and maintain stakeholder buy-in, create dashboards for vulnerabilities, training status, SLA compliance, and time to remediation, and report to executive leadership on AppSec KPI's regularly.

## Customer Results

Our customers eliminate complexity, accelerate compliance, and turn security into advantage. We help them achieve these objectives with a simplified approach tailored for small teams in highly regulated industries.

**100%** Certification Success

**95%** Customer Retention

Our unwavering commitment to customer satisfaction has enabled our customers to achieve their certifications without fail and turn security into advantage.



### **Achieved ISO 27001 and SOC 2 Audit Readiness Ahead of Expected Time.**

This med-tech SaaS provider achieved audit-readiness for ISO 27001 and SOC 2 in less than 9-months to close a massive new customer deal.

[Full case study](#)

*"Seiso guided us through dual audits with no nonconformities and we earned our ISO 27001 certification along with a SOC 2 attestation. This allowed us to close a significant deal with our biggest customer ever."*

— James Gianoutsos, Founder and CEO, Rimsys



**AI software web application pentesting** Using our offensive, defensive, and secure coding testing capabilities, we provided key insights that allowed this SaaS provider to enhance security within the application before it shipped to production.

*"We partnered with Seiso to strengthen both our web application and our development process through a secure code review and penetration test, all on a tight delivery timeline. Their team was flexible and adaptive. They adjusted their approach to fit our schedule while maintaining the quality we needed. The clear and efficient communication made collaboration easy. Most importantly, Seiso provided actionable insights that not only addressed immediate concerns but also set us up for continuous improvement of the security of our application and development practices over time."*

—Mike Pino, Managing Director, Problem Solutions



### **Cybersecurity Maturity for Business Growth**

Developed, implemented, and maintained an information security management system that has withstood the test of evolving healthcare SaaS application market requirements and compliance demand over time. [Full case study](#)

*"Seiso has been instrumental in transforming our cybersecurity posture, allowing us to confidently expand our services and meet rigorous industry standards. Their expertise and dedication have made them an invaluable partner in our growth journey. They are simply great to work with and I highly recommend them."*

— Brian Abercrombie, VP, IT and Information Security Officer, TeleTracking, Inc.