SealSec
COMMON SENSE SECURITY

info@sealsec.nl
www.sealsec.nl

Customer-Ready Security for Dutch SaaS

A focused security sprint for SaaS teams facing customer security questionnaires, procurement delays, ISO evidence work, or customer-data concerns. Delivered by a senior security engineer, directly with your product and engineering team.

SealSec turns findings and uncertainty into owned fixes, customer-ready evidence, and a practical remediation plan. After the sprint, you know what matters, who owns it, what to fix first, what evidence you can show customers, and what can safely wait.

Where SealSec Helps

- A prospect or customer sent a security questionnaire.
- A deal is slowing down because of security or ISO evidence.
- Pentest findings end up in PDF reports instead of becoming owned engineering work.
- Your product depends on many third-party components, but you cannot clearly explain or reduce supply-chain risk.
- You are not fully confident about tenant isolation, authorization, or high-impact flows.
- Your team ships quickly, uses AI-assisted development, and needs security review that can keep up.
- You need practical security work without hiring a full-time security person.

What SealSec Delivers

- A focused security baseline for the systems and data that matter most.
- High-risk product and access-control review, including tenant boundaries, roles, APIs, admin, and support paths.
- Pentest, scanner, SBOM, SAST, and supply-chain findings turned into real priorities.
- Owned remediation issues in your existing engineering workflow.
- Customer-ready evidence for procurement, security reviews, and ISO-related work.
- A practical 30/60/90-day plan for what to fix next.

From Inventory and Findings to Fixes and Evidence

INVENTORY
Map the systems, customer data, suppliers, components, owners, and exposed services that matter.

TEST
Review and test product flows, APIs, authentication, authorization, tenant boundaries, and admin paths.

TRIAGE
Turn scanner output, supply-chain findings, and pentest results into real priorities.

ASSIGN
Route security findings to owners with clear remediation paths and workflow labels.

REMEDIATE
Support practical mitigations that fit the product and engineering reality.

VERIFY
Retest or verify fixes so findings do not remain static report items.

MONITOR
Keep relevant logs, alerts, and exposure changes visible for investigation.

EVIDENCE
Keep customer-ready proof for security reviews, procurement, and ISO-related work.

SealSec

OFFER STRUCTURE

info@sealsec.nl
www.sealsec.nl

Common Sprint Shapes

Customer-ready baseline | **Pentest + remediation sprint** | **Supply-chain / SAST triage** | **Security logging foundation**

Procurement security support | **ISO evidence support** | **High-risk feature review** | **Tenant-boundary review**

Book a free fit call. In 30 minutes, we identify the security pressure, the likely sprint shape, and whether SealSec is a fit.

Core Package: First Security Readiness Sprint

Fixed-scope sprints usually land between EUR 6,000-18,000 depending on scope, urgency, and depth.

Scope and price depend on product complexity, number of systems, urgency, and the mix of testing, evidence work, and remediation support. The sprint establishes a usable baseline and turns the first round of security signals into owned engineering work.

INVENTORY / SBOM

Map systems, repositories, suppliers, data flows, exposed services, and software components.

TARGETED PENTEST

Test high-risk product flows, APIs, authentication, roles, tenant boundaries, admin, and support paths.

SUPPLY CHAIN

Review dependency, container, secret, and vulnerability signals and identify real supply-chain risk.

SAST / SDLC

Configure or review code scanning, secure development workflow, labels, ownership, and evidence paths.

FIRST TRIAGE

Reduce noise, remove duplicates, validate impact, prioritize findings, and agree owner actions.

REMEDIATION

Give practical mitigation guidance, create owned tickets, and define verification or retest steps.

Security logging, external exposure, privileged access, backup, incident-readiness, vulnerability disclosure, or monitoring work can be included when it affects customer-data readiness.

Sprint Deliverables

A security baseline your engineering team can use

- System, component, supplier, and customer-data inventory.
- SBOM and scanner coverage notes, including blind spots.
- Pentest findings and scanner results triaged into priorities.
- Finding workflow with owners, priorities, remediation status, and reusable evidence.
- Remediation guidance for findings that matter.
- Security logging or monitoring improvement plan where included.
- Security blockers and 30/60/90-day remediation plan.

Optional Monthly Retainer

From around EUR 2,500/month, usually starting with a 3-month engagement

Use the sprint deliverables as the operating model for ongoing security work.

- Review new scanner, SBOM, supply-chain, and SAST findings.
- Triage noise, duplicates, severity, exploitability, and ownership.
- Support remediation and mitigation decisions with developers.
- Verify fixes or retest high-risk findings.
- Targeted testing for risky changes and new product flows.
- Keep customer, ISO-related, or procurement evidence current.