SealSec
COMMON SENSE SECURITY

info@sealsec.nl
www.sealsec.nl

Security Sprint voor Nederlandse SaaS

Een gerichte security sprint voor SaaS-teams die securityvragen van klanten krijgen, vertraging oplopen in procurement, ISO-bewijsvoering nodig hebben of klantdata verantwoord willen verwerken. Uitgevoerd door een senior security engineer, direct met uw product- en engineeringteam.

SealSec zet bevindingen en onzekerheid om in toegewezen verbeterpunten, bruikbare bewijsvoering en een praktisch plan voor opvolging. Na de sprint weet u wat ertoe doet, wie eigenaar is, wat eerst moet worden aangepakt, welke bewijsvoering u kunt delen met klanten en wat verantwoord kan wachten.

Waar SealSec helpt

- Een prospect of klant stuurt een securityvragenlijst.
- Een deal loopt vertraging op door security- of ISO-bewijsvoering.
- Pentestbevindingen blijven hangen in PDF-rapporten in plaats van toegewezen engineeringwerk te worden.
- Uw product gebruikt veel externe componenten, maar supply-chainrisico is nog niet helder.
- U bent niet volledig zeker over tenant isolation, autorisatie of high-impact productflows.
- Uw team levert snel, gebruikt AI-assisted development en heeft security review nodig die kan meekomen.
- U heeft praktisch securitywerk nodig zonder direct een fulltime securityrol aan te nemen.

Wat SealSec oplevert

- Een gerichte security baseline voor de systemen en data die het belangrijkst zijn.
- Review van high-risk productflows en access control, waaronder tenant boundaries, rollen, API's, admin- en supportpaden.
- Pentest-, scanner-, SBOM-, SAST- en supply-chainbevindingen vertaald naar echte prioriteiten.
- Toegewezen verbeterpunten in uw bestaande engineeringworkflow.
- Bruikbare bewijsvoering voor procurement, security reviews en ISO-gerelateerd werk.
- Een praktisch 30/60/90-dagenplan voor wat daarna moet worden aangepakt.

Van inventarisatie en bevindingen naar fixes en bewijsvoering

INVENTARISATIE
Breng relevante systemen, klantdata, leveranciers, componenten, eigenaren en exposed services in kaart.

TESTEN
Review en test productflows, API's, authenticatie, autorisatie, tenant boundaries en adminpaden.

TRIAGE
Zet scanneroutput, supply-chainbevindingen en pentestresultaten om in echte prioriteiten.

TOEWIJZEN
Routeer securitybevindingen naar eigenaren met duidelijke opvolging en workflowlabels.

VERBETEREN
Ondersteun praktische maatregelen die passen bij het product en de engineeringrealiteit.

VERIFIËREN
Hertest of verifieer fixes zodat bevindingen geen statische rapportitems blijven.

MONITOREN
Maak relevante logs, alerts en exposure-wijzigingen zichtbaar voor onderzoek.

BEWIJSVOERING
Bewaar bruikbare bewijsvoering voor security reviews, procurement en ISO-gerelateerd werk.

SealSec

OPBOUW VAN HET AANBOD

info@sealsec.nl
www.sealsec.nl

Veelvoorkomende sprintvormen

Baseline voor klantvragen | **Pentest + remediation sprint** | **Supply-chain / SAST-triage** | **Basis voor securitylogging**

Ondersteuning bij ISO-bewijsvoering | **Review van high-risk features** | **Tenant-boundary review**

Plan een gratis verkenningsgesprek. In 30 minuten brengen we de securitydruk, de logische sprintvorm en de fit met SealSec in kaart.

Kernpakket: Eerste Security Readiness Sprint

Fixed-scope sprints liggen meestal tussen EUR 6.000 en 18.000, afhankelijk van scope, urgentie en diepgang.

Scope en prijs hangen af van productcomplexiteit, aantal systemen, urgentie en de mix van testing, bewijsvoering en opvolgingssupport. De sprint legt een bruikbare baseline en zet de eerste ronde securitysignalen om in toegewezen engineeringwerk.

INVENTARISATIE / SBOM

Breng systemen, repositories, leveranciers, dataflows, exposed services en softwarecomponenten in kaart.

GERICHTE PENTEST

Test high-risk productflows, API's, authenticatie, rollen, tenant boundaries, admin- en supportpaden.

SUPPLY CHAIN

Review dependency-, container-, secret- en vulnerabilitysignalen en identificeer echt supply-chainrisico.

SAST / SDLC

Configureer of review code scanning, secure-developmentworkflow, labels, eigenaarschap en bewijsvoering.

EERSTE TRIAGE

Verminder ruis, verwijder duplicaten, valideer impact, prioriteer bevindingen en spreek eigenaaracties af.

OPVOLGING

Geef praktische verbeteradviezen, maak toegewezen tickets en definieer verificatie- of herteststappen.

Securitylogging, external exposure, privileged access, back-ups, incident-readiness, vulnerability disclosure of monitoring kunnen worden meegenomen wanneer dit raakt aan readiness voor klantdata.

Sprint Deliverables

Security baseline die uw team direct kan gebruiken

- Inventarisatie van systemen, componenten, leveranciers en klantdata.
- SBOM- en scannercoveragenotities, inclusief blind spots.
- Pentestbevindingen en scannerresultaten getriageerd naar prioriteiten.
- Findingworkflow met eigenaren, prioriteiten, opvolgingsstatus en herbruikbare bewijsvoering.
- Praktische verbeteradviezen voor bevindingen die ertoe doen.
- Verbeterplan voor securitylogging of monitoring waar dit is meegenomen.
- Securityblockers en een 30/60/90-dagenplan voor opvolging.

Optionele maandelijkse retainer

Vanaf ongeveer EUR 2.500 per maand, meestal vanaf een traject van 3 maanden

Gebruik de sprint deliverables als operating model voor doorlopend securitywerk.

- Review nieuwe scanner-, SBOM-, supply-chain- en SAST-bevindingen.
- Triage op ruis, duplicaten, severity, exploitability en eigenaarschap.
- Ondersteun remediation- en mitigatiebeslissingen met ontwikkelaars.
- Verifieer fixes of hertest high-risk bevindingen.
- Gerichte tests voor risicovolle wijzigingen en nieuwe productflows.
- Houd bewijsvoering voor klanten, ISO-gerelateerd werk of procurement actueel.