



SAST

SCA · SBOM

DAST próprio

ASM · Nuvem

Governança

Limen

Segurança de aplicações do código à nuvem — numa só plataforma



O CENÁRIO

Por que os programas de AppSec travam

Fragmentação

4 a 6 ferramentas que não conversam, geram ruído e não dão rastreabilidade para auditoria.

Falso-positivo

Gate de SCA vira fila de chamado: CVE de SO sem análise, dependência não usada, sem VEX.

Sem DAST próprio

A maioria dos ASPM modernos só orchestra terceiros — não confirma exploração real.

Regulatório e dados

Ferramentas internacionais não endereçam PCI/BACEN/ANS/LGPD a fundo nem oferecem residência de dados local.

A Limen resolve os quatro numa plataforma só — em português e com opção on-premise.

Uma plataforma, do código à nuvem



Governança, conformidade e priorização transparente atravessam todas as etapas — com trilha de auditoria à prova de adulteração.



Detecção — do código ao runtime

SAST + IA

Análise estática por regras e camada com IA para falhas de lógica (IDOR, quebra de acesso).

SCA com reachability

Vulnerável e chamável no código (heurística + call-graph), priorizado por EPSS e CISA KEV.

DAST próprio

Nuclei + OWASP ZAP, confirmação ativa não-destrutiva, verificação de domínio, DAST de API.

Segredos & IaC

GitLeaks e Checkov, ativáveis por módulo.

Container

Scan de imagem (Trivy) e postura de registro.

Runtime (IAST)

Sinais de execução que confirmam exploração e elevam a prioridade.



Supply chain & SBOM

Firewall de supply chain

Denylist de malware OSS com gate de dependência no CI — prevenção, não só CVE.

SBOM CycloneDX/SPDX

Importa e converte os dois formatos (protobom); alimenta o inventário.

Vigilância contínua de CVE

Espelho OSV (~290 mil) casa CVE nova com o inventário e dispara comunicado automático.

VEX + org-wide

OpenVEX + veredito próprio suprimem falso-positivo por CVE no tenant inteiro.

Saúde de pacote + CBOM

Deprecated/licença/node-lock e inventário de cripto pós-quântico (HNDL, prontidão PQC).

Gate de BOM

cdx-validate (SCVS/EU CRA) + assinatura de procedência no pipeline.



DIFERENCIAL

Priorização: risk score transparente

A nota de risco de cada achado é composta de forma auditável — não é uma caixa-preta:

Severidade

EPSS

CISA KEV

Reachability

Exposição (ASM/nuvem)

Runtime

Criticidade do ativo

Pipeline de qualidade antes do placar: exclusões do ativo → supressões → VEX version-aware → correlação e deduplicação. Menos ruído, sem apagar histórico.



Governança & conformidade

Aceite de risco

Termo tokenizado, validade por severidade, alçada e reabertura automática no vencimento.

PCI • ASVS • SAMM

PCI-DSS com subrequisitos, ASVS oficial + benchmarks, maturidade SAMM.

Threat modeling as-code

STRIDE/LINDDUN com biblioteca, YAML e DFD visual.

Trilha de auditoria

Registro encadeado por hash — à prova de adulteração.

Higiene de ativos

Rotina proativa de consistência + taxa por squad + série histórica.

Playbooks com evidência

Processos padronizados com anexo obrigatório.



Operação & fluxo de trabalho

Gates de CI/CD

Gate de PR e de deploy com política por ambiente e token de CI.

Ticketing bidirecional

GitHub, GitLab, Azure Boards, Jira e ServiceNow.

Auto-Fix

Sugestão de correção e PR, com opção de LLM.

Tombamento em lote

Onboarding em massa + push para ASOC (Dependency-Track/webhook).

Analytics de revisão

Carga e reatribuição de code review, inclusive por eventos reais de PR.

Command center

Dashboards por sigla/squad/sistema e relatório de programa.

Diferenciais

1

DAST próprio nativo com confirmação ativa — a maioria só orquestra terceiros.

3

Governança e conformidade profundas (PCI/BACEN/ANS/LGPD).

5

Trilha de auditoria à prova de adulteração.

7

Plataforma única, em português, com presença local.

2

Risk score transparente e auditável, não uma nota opaca.

4

Threat modeling as-code com biblioteca e DFD.

6

CBOM / pós-quântico — diferencial de fronteira.

8

Self-hostável — residência de dados e opção on-premise.



IMPLANTAÇÃO

Do SaaS ao on-premise — seus dados, sua escolha

SaaS gerenciado

Operado pela Limen. Onboarding rápido, sem infraestrutura do cliente.

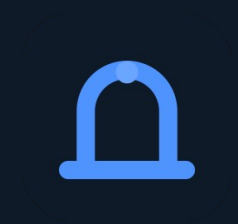
On-premise / nuvem privada

Self-hostável via Docker Compose. Residência de dados total — LGPD.

Híbrido

Núcleo gerenciado; scanners e conectores no ambiente do cliente.

Multi-tenant • RBAC • SSO • segredos cifrados em repouso • licenciamento por volume de ativos e módulos (ligáveis/desligáveis no Admin).



Vamos ver no seu código

Demonstração guiada · piloto com repositórios reais · proposta ajustada ao seu porte

Limen · Segurança de aplicações do código à nuvem — numa só plataforma