Arquitetura de Segurança

Arquitetura de Segurança

Campo	Valor
Distribuição	WCT Portuguese — OpenC5ISR
Produto	OpenC5ISR
Versão	0.15.1
Implantação	`openc5isr-pt.wallacecorptech.com`
Fonte	`/srv/wct/releases/OpenC5ISR-v0.15.0-20app-pt`
Evidência	Controles de referência e indicadores estáticos de segurança
Impressão digital da fonte	`e92dc1580aa26f7545815bcf40300b21bc5485b0a2ae46a715538a48365cc801`
Estado	Linha de base gerada — revisão humana obrigatória

> **Limite de verificação:** Esta página combina orientação de projeto da plataforma com evidências estáticas da distribuição. Ela não comprova que todas as interfaces detectadas estejam habilitadas, acessíveis, seguras ou operacionais no ambiente implantado.

Modelo de segurança

A segurança deve ser aplicada à identidade, conteúdo, interfaces, transporte, implantação e evidências — não apenas adicionada à interface do usuário. Cada módulo deve autenticar sujeitos, autorizar ações e dados, proteger transporte, minimizar segredos, emitir eventos de auditoria e preservar proveniência.

Indicadores observados

Indicador	Observado
Variáveis de ambiente designadas como segredo	ANTHROPIC_API_KEY, OPENAAR_SIGNING_KEY, OPENAI_API_KEY, OPENBUS_API_TOKEN, OPENCYBERSEC_AGENT_TOKEN, OPENCYBERSEC_OPERATOR_TOKEN, OPENCYBERSEC_READ_TOKEN, OPENKNOWLEDGE_EDITOR_TOKEN, OPENLLM_ANTHROPIC_API_KEY, OPENLLM_OPENAI_API_KEY, OPENLLM_OPENWEBUI_API_KEY, OPENLLM_OPERATOR_TOKEN, OPENPNT_AGENT_TOKEN, OPENPNT_TOKEN, OPENRF_AGENT_TOKEN, OPENRF_OPERATOR_TOKEN, OPENRF_READ_TOKEN, OPENSSA_SENSOR_TOKEN, OPENWEBUI_API_KEY, ROCKETCHAT_AUTH_TOKEN, ROCKETCHAT_OUTGOING_TOKEN, TOKEN
Contagem de termos de segurança	TLS: 1960, authorization/RBAC: 172, audit: 101, authentication: 64, CORS: 19
Nomes de arquivos potencialmente sensíveis	—

Controles necessários

Limite	Controle mínimo
Identidade usuário/API	Contas nomeadas ou identidades de serviço, privilégio mínimo, tokens revogáveis e MFA quando suportado.
Transporte	TLS para interfaces públicas e de gerenciamento; links autenticados/criptografados para barramentos operacionais conforme a ameaça.
Conteúdo	Rótulos de tratamento/liberação, política por função/atributo, autorização em nível de objeto e exportações protegidas.
Segredos	Nenhum segredo em código, documentação, URLs ou logs; usar ambientes/armazenamentos protegidos e rotação.
Auditoria/evidência	Registrar ator, ação, alvo, resultado, tempo da fonte e identificadores de correlação com retenção resistente a adulteração.
Cadeia de suprimentos	Dependências/imagens fixadas, revisão de vulnerabilidades, artefatos assinados e registros reproduzíveis de implantação.

Ações imediatas de revisão

- Rotacionar qualquer token ou senha exposto em chat, histórico do shell, logs ou documentação.
- Verificar que credenciais BookStack/API estejam somente na configuração protegida do gerador.
- Testar autorização de cada edição para que documentação e dados operacionais não cruzem limites não pretendidos.
- Documentar resposta a incidentes, confidencialidade de backup e autorização de restauração.

Notas do Mantenedor

Adicione aqui notas de implantação revisadas por pessoas, correções, decisões, capturas de tela e links. O conteúdo fora do bloco gerado é preservado nas próximas execuções.

Revision #1
Created 2026-08-28 15:06:17 UTC by Nexus Ops Administrator
Updated 2026-08-28 15:06:17 UTC by Nexus Ops Administrator