

example.com

DATA DA ANÁLISE 21/09/2026, 08:00	ÂMBITO Passiva e ativa (com verificação de portas) + OpenVAS	HOSTS VERIFICADOS 8	FONTES crt.sh, certspotter
--------------------------------------	---	------------------------	-------------------------------

PONTUAÇÃO DE EXPOSIÇÃO

36 / 100



Prioridade média de todos os achados, de 0 a 100.
Quanto mais baixa, melhor.

ACHADOS: 10

0 CRÍTICA	3 ALTA	3 MÉDIA	4 BAIXA
--------------	-----------	------------	------------

O essencial em resumo

Trate primeiro estes achados. Combinam uma gravidade elevada com a importância do sistema afetado.

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
61	ALTA	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ALTA	vpn.example.com RDP acessível a partir da internet (porta 3389) → Feche a porta na firewall ou restrinja-a a endereços IP conhecidos.
56	ALTA	shop.example.com Interface de administração acessível publicamente (phpMyAdmin) → Torne-a acessível apenas através de VPN ou de uma lista de IPs permitidos.
34	MÉDIA	dev.example.com Sistema de desenvolvimento ou de teste acessível publicamente → Proteja-o com início de sessão, VPN ou lista de IPs permitidos e desligue os sistemas que já não são necessários.
34	MÉDIA	mail.example.com O certificado TLS expira dentro de 9 dias → Renove o certificado e verifique se a renovação automática funciona.

Todos os achados por host

example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
24	BAIXA	A política DMARC é p=none, o correio falsificado não é rejeitado → Depois de analisar os relatórios, eleve a política para p=quarantine ou p=reject.

www.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
24	BAIXA	Versão de software visível no cabeçalho Server (Apache/2.4.49) → Desative a indicação da versão no servidor web (p. ex., server_tokens off, ServerTokens Prod).
20	BAIXA	Falta o cabeçalho Content-Security-Policy → Defina uma Content-Security-Policy que permita apenas as fontes necessárias.

shop.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
56	ALTA	Interface de administração acessível publicamente (phpMyAdmin) → Torne-a acessível apenas através de VPN ou de uma lista de IPs permitidos.
32	MÉDIA	Falta o cabeçalho Strict-Transport-Security → Defina Strict-Transport-Security: max-age=31536000; includeSubDomains.

mail.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
34	MÉDIA	O certificado TLS expira dentro de 9 dias → Renove o certificado e verifique se a renovação automática funciona.

vpn.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
61	ALTA	OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ALTA	RDP acessível a partir da internet (porta 3389) → Feche a porta na firewall ou restrinja-a a endereços IP conhecidos.

dev.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
34	MÉDIA	Sistema de desenvolvimento ou de teste acessível publicamente → Proteja-o com início de sessão, VPN ou lista de IPs permitidos e desligue os sistemas que já não são necessários.

portal.example.com

PRIOR.	GRAVIDADE	ACHADO E RECOMENDAÇÃO
17	BAIXA	Falta o cabeçalho X-Content-Type-Options → Defina X-Content-Type-Options: nosniff.

Sem achados

cdn.example.com

Método e limites

Os subdomínios provêm dos registos públicos de certificados (Certificate Transparency). Apenas foram verificados os hosts que resolvem por DNS.

Em cada host foram verificados o certificado TLS, o redirecionamento de HTTP para HTTPS, os cabeçalhos de segurança da página inicial e as interfaces de administração reconhecíveis; no domínio principal, também SPF e DMARC.

Uma análise passiva não verifica portas abertas nem ataca aplicações. Mostra o que é visível do exterior sem credenciais.

Este relatório é um retrato do momento indicado. A prioridade é uma avaliação e não substitui um teste de intrusão.

Além disso, foi realizada com OpenVAS (Greenbone) uma análise ativa de vulnerabilidades dos endereços públicos, com base na titularidade comprovada do domínio. Apenas foram incluídos achados com uma qualidade de deteção de pelo menos 70 por cento.

Próximos passos

Teremos todo o gosto em analisar o relatório consigo e mostrar como a veyrisk monitoriza continuamente a sua superfície de ataque, em vez de olhar apenas uma vez.

CONTACTO

neonotu GmbH
Edelsbergstraße 8, 80686 München
+49 89 2000 7975 0 · contact@veyrisk.com