

Visão Executiva CISO

The Goat Blog

PERÍODO ANALISADO

20/10/2026 a 22/10/2026

Gerado em 22/10/2026 00:04 UTC

Este relatório apresenta uma visão executiva dos principais sinais de risco cibernético observados no período selecionado. A análise consolida notícias e fontes de Cyber Intelligence armazenadas localmente, priorizando eventos com evidências de exploração, criticidade, vulnerabilidades, ransomware, vazamentos e atividade de ameaças.

1. EXECUTIVE CYBER RISK SNAPSHOT

Indicadores consolidados do período selecionado

267

Notícias analisadas

2

Eventos de alta relevância

16

Indicadores críticos

0

Exploração ativa/conhecida

7

Ransomware

32

Data breach/vazamento

11

Threat actors/APT

2. RISCOS PRIORITÁRIOS DO PERÍODO

1. [65/100] Critical PHP Vulnerability (CVE-2026-109618, CVE-2026-109619) [info on yellow], (Wed, Oct 21st)

Fonte: SANS Internet Storm Center | 2026-10-21 | CVE

Evidências: CVSS crítico, criticidade alta, exploit, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

2. [63/100] FBI says SafePay ransomware gang ‘among most active’ with more than 600 victims since 2024

Fonte: The Record | 2026-10-20 | Ransomware

Evidências: criticidade alta, ransomware, exploit, phishing

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

3. [47/100] Threat Brief: Active Exploitation of PAN-OS CVE-2026-0257 (Updated October 20)

Fonte: Palo Alto Unit 42 | 2026-10-20 | Ransomware

Evidências: ransomware, exploit, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

2. RISCOS PRIORITÁRIOS DO PERÍODO — CONTINUAÇÃO

4. [45/100] iPhone 18 base aparece pela 1ª vez, mas só deve chegar em 2027

Fonte: Canaltech | 2026-10-20 | Threat Actor

Evidências: vazamento, threat actor/APT, threat actor

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

5. [32/100] PHP2Shell: duas falhas no motor do PHP, 70% da web, e a receita para hoje

Fonte: CyberS3c Portugal | 2026-10-21 | CVE

Evidências: CVSS crítico, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

6. [30/100] Fone barato chiando ou abafado? Truque no YouTube Music salva o som sem você gastar nada

Fonte: Canaltech | 2026-10-21 | Threat Actor

Evidências: threat actor/APT, threat actor

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

7. [30/100] Duolingo fora do ar? App apresenta falhas e usuários temem perder ofensiva

Fonte: Canaltech | 2026-10-21 | Threat Actor

Evidências: threat actor/APT, threat actor

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

8. [30/100] Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618, CVE-2026-109619

Fonte: Palo Alto Unit 42 | 2026-10-21 | CVE

Evidências: criticidade alta, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

2. RISCOS PRIORITÁRIOS DO PERÍODO — CONTINUAÇÃO

9. [30/100] O seu site corre em PHP? As duas falhas que levaram governos a desligar servidores

Fonte: Ciberseguranca.PT | 2026-10-21 | CVE

Evidências: criticidade alta, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

10. [30/100] PHP: falhas críticas CVE-2026-109618 e 109619 forçam patch - iMasters

Fonte: GN Vulnerabilidades CVE | 2026-10-21 | CVE

Evidências: criticidade alta, CVE

Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.

[Link Artigo](#)

3. PANORAMA E CONCENTRAÇÃO DOS SINAIS

Distribuição por categoria

- General Cybersecurity: 221
- CVE: 12
- Threat Actor: 10
- Cloud Security: 8
- Ransomware: 7
- Malware: 6
- Data Breach: 2
- Vulnerability: 1

Fontes com maior volume no período

- Olhar Digital: 58
- Canaltech: 44
- Tecnoblog: 33
- GN Vazamento de Dados: 23
- GN Cibersegurança Brasil: 14
- Ciberseguranca.PT: 13
- GN Segurança da Informação: 13
- The Record: 11

4. LEITURA EXECUTIVA

Os indicadores acima representam sinais externos observados nas fontes monitoradas. Pontuações mais altas indicam maior concentração de evidências textuais associadas a exploração, criticidade e impacto potencial; não representam, isoladamente, risco confirmado para a organização.

5. CONCLUSÃO E RECOMENDAÇÕES

No período foram analisadas 267 notícias, com 2 evento(s) de alta relevância. Os principais sinais observados incluem 7 ocorrência(s) relacionada(s) a ransomware, 32 ocorrência(s) de vazamento/data breach. A recomendação é confrontar estes sinais externos com ativos, tecnologias, exposição, vulnerabilidades e controles da organização antes da tomada de decisão.

6. METODOLOGIA E GOVERNANÇA

Relatório determinístico gerado localmente a partir do banco Cyber News Intelligence. Nenhum conteúdo é enviado a serviços de IA. O score considera evidências textuais como exploração ativa, CISA KEV, zero-day, CVE, criticidade, ransomware, vazamento, threat actors, supply chain, exploit, malware, phishing, identidade e cloud. Os resultados devem ser validados contra o contexto tecnológico e de negócio da organização.