USO PUBLICO

Cyber News Intelligence

Visão Executiva CISO

The Goat Blog

PERÍODO ANALISADO

17/11/2026 a 22/11/2026

Gerado em 22/11/2026 00:00 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.

Relatório executivo determinístico · Processamento local · Sem envio de conteúdo para IA

1. EXECUTIVE CYBER RISK SNAPSHOT

Indicadores consolidados do período selecionado

732
Notícias analisadas

4
Eventos de alta relevância

41
Indicadores críticos

1
Exploração ativa/conhecida

15
Ransomware

68
Data breach/vazamento

35
Threat actors/APT

2. RISCOS PRIORITÁRIOS DO PERÍODO

1. [100/100] ARMORY CASTLE Exploits vSphere

Fonte: Google Threat Intelligence | 2026-11-19 | Malware
Evidências: zero-day, criticidade alta, threat actor/APT, threat actor, exploit, CVE, malware, identidade, cloud
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

2. [88/100] COLD RELIC: A Case Study in Impersonation and Compromise

Fonte: Google Threat Intelligence | 2026-11-17 | Malware
Evidências: criticidade alta, threat actor/APT, threat actor, malware, phishing, identidade, cloud
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

3. [79/100] Armory Castle Attack

Fonte: FortiGuard Labs | 2026-11-21 | Malware
Evidências: zero-day, threat actor, exploit, CVE, malware
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

2. RISCOS PRIORITÁRIOS DO PERÍODO — CONTINUAÇÃO

4. [60/100] Apache corrige falha crítica no Roller sob exploração ativa

Fonte: CISO Advisor | 2026-11-18 | CVE
Evidências: exploração ativa, criticidade alta, CVE
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

5. [50/100] CVE-2026-90817 - Vanderbilt University Research Electronic Data Capture (REDCap) Code Injection Vulnerability

Fonte: CISA | 2026-11-18 | CVE
Evidências: threat actor/APT, exploit, CVE, cloud
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

6. [45/100] Java4Shell

Fonte: FortiGuard Labs | 2026-11-18 | CVE
Evidências: criticidade alta, exploit, CVE
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

7. [45/100] Hacker que invadiu Rockstar usando um Fire Stick e vazou GTA 6 se declara culpado

Fonte: Canaltech | 2026-11-17 | Threat Actor
Evidências: vazamento, threat actor/APT, threat actor
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

8. [40/100] Amazon says Chinese hackers used Cairn AI tool to discover apparent zero-day during attack on university

Fonte: The Record | 2026-11-20 | General Cybersecurity
Evidências: zero-day, threat actor
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

2. RISCOS PRIORITÁRIOS DO PERÍODO — CONTINUAÇÃO

9. [38/100] 8 melhores adaptações de games lançadas em 2026

Fonte: Canaltech | 2026-11-21 | Threat Actor
Evidências: threat actor/APT, threat actor, cloud
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

10. [38/100] Falha crítica no VMware vCenter: CVSS 9.8 - SempreUpdate

Fonte: GN Vulnerabilidades CVE | 2026-11-19 | General Cybersecurity
Evidências: CVSS crítico, criticidade alta
Ação CISO: validar exposição, aplicabilidade, controles e necessidade de resposta.
Link Artigo

3. PANORAMA E CONCENTRAÇÃO DOS SINAIS

Distribuição por categoria

- General Cybersecurity: 604
- CVE: 34
- Malware: 33
- Threat Actor: 30
- Ransomware: 15
- Cloud Security: 11
- Data Breach: 3
- Vulnerability: 2

Fontes com maior volume no período

- Olhar Digital: 151
- Canaltech: 110
- Tecnoblog: 71
- GN Vazamento de Dados: 55
- GN Cibersegurança Brasil: 53
- Cibersegurança.PT: 40
- GN Vulnerabilidades CVE: 37
- GN Segurança da Informação: 32

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 732 notícias, com 4 evento(s) de alta relevância. Os principais sinais observados incluem 1 sinal(is) de exploração ativa/conhecida, 15 ocorrência(s) relacionada(s) a ransomware, 68 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.