cais Inteligência em Cibersegurança

RNP

Como um time de segurança ofensiva pode auxiliar a sua organização

Leonardo Dias

$cat bio.txt

Leonardo Dias

Analista do Red Team do CAIS/RNP

- Graduado em Gestão da TI
- Especialização em Defesa Cibernética
- Na RNP desde 2017
- Desde de 2019 na área de segurança da informação
- Certificações: LPIC-1/ Comptia Linux + / Pentest +

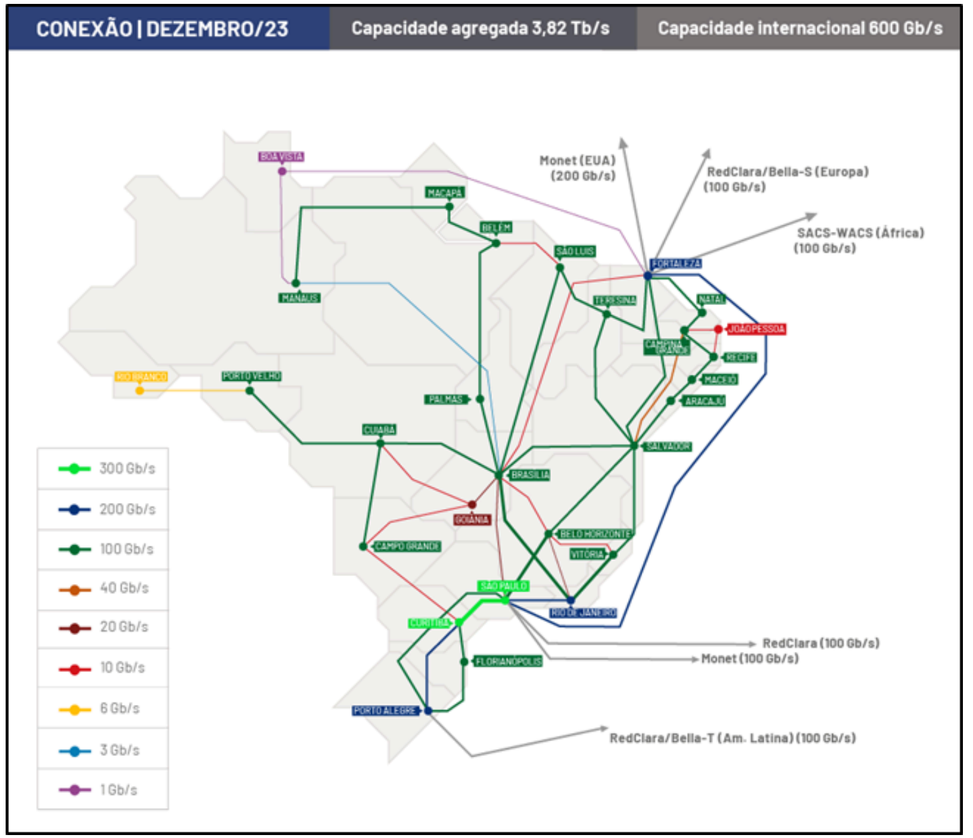
RNP - Rede Nacional de Ensino e Pesquisa

- Internet de alta capacidade, serviços personalizados e promoção de projetos de inovação.

- Beneficiamos 4 milhões de alunos, professores e pesquisadores brasileiros.

- Pioneiros, ao trazer a internet para o Brasil e a primeira rede de fibra ótica na América Latina em 2005.

- Apoiamos com tecnologia e serviços mais de 1500 universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.



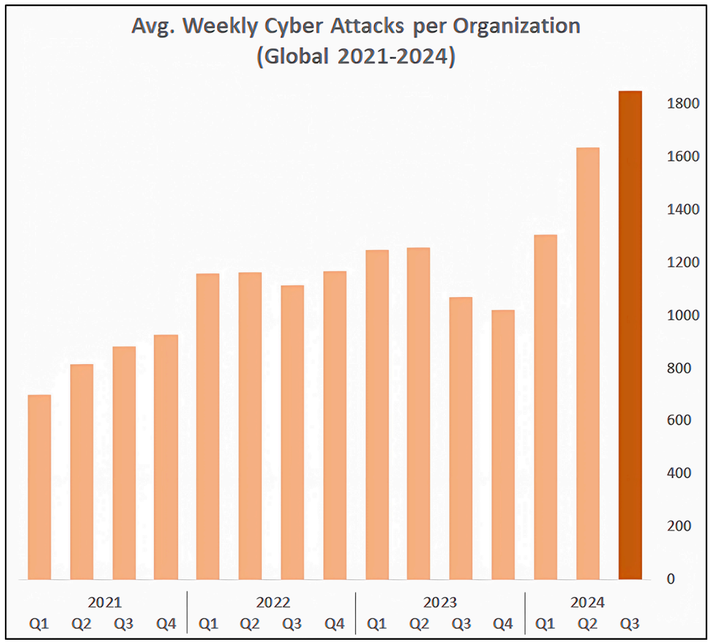
CAIS – Inteligência em Cibersegurança

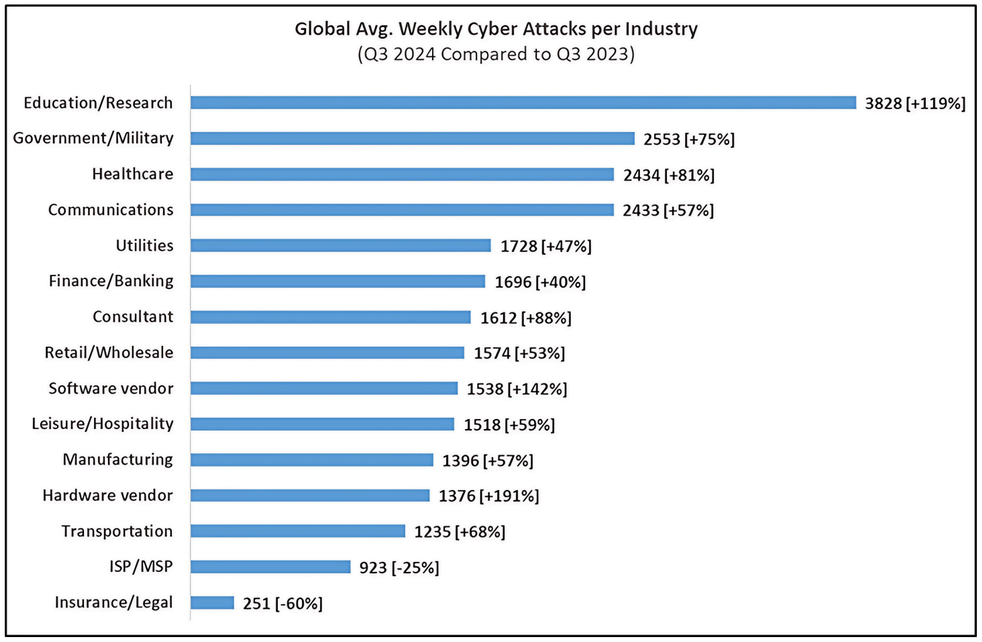
Cenário Atual

Ataques cibernéticos disparam no Brasil e no mundo no terceiro trimestre de 2024

Aumento recorde de ataques teve índice de 95% no Brasil e de 75% globalmente

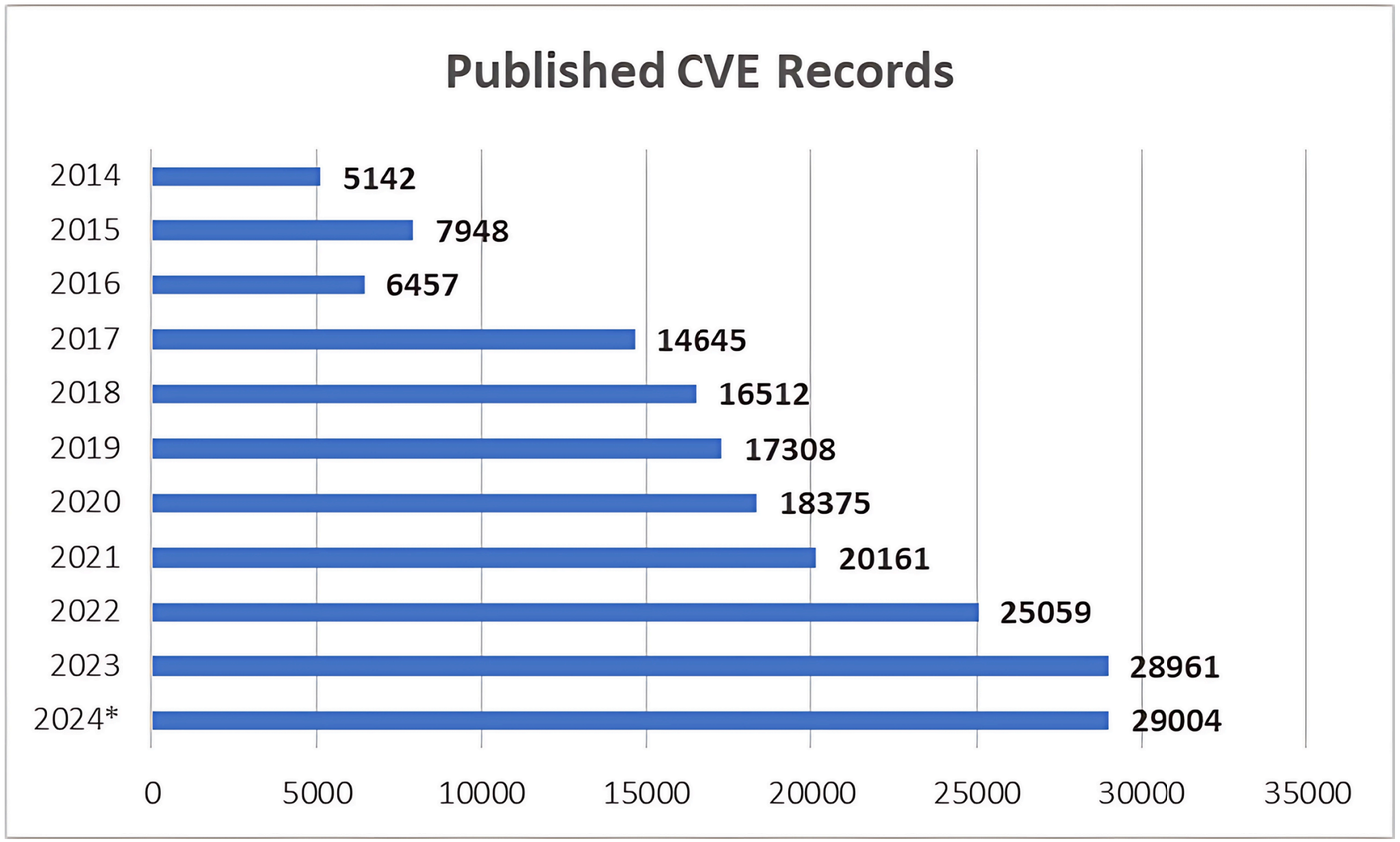
Outubro 25, 2024 Por: DatacenterDynamics Have your say





Fonte: https://www.datacenterdynamics.com/br/not%C3%ADcias/ataques-ciberneticos-disparam-no-brasil-e-no-mundo-no-terceiro-trimestre-de-2024/

Cenário Atual



Fonte: https://www.cve.org/About/Metrics

O que é Segurança Ofensiva?

Segurança ofensiva, ou "OffSec", refere-se a uma variedade de estratégias de segurança proativas que usam as mesmas táticas que os agentes maliciosos usam em ataques do mundo real para fortalecer a segurança da rede em vez de prejudicá-la. Entre os métodos de segurança ofensivos comuns estão: formação de red team, testes de intrusão e avaliação de vulnerabilidade.

Fonte: https://www.ibm.com/br-pt/topics/offensive-security

Principais atividades

Realização de testes de intrusão

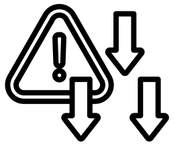
Análise de vulnerabilidades

Desenvolvimento de relatórios detalhados

Recomendação de medidas de mitigação

Como uma Equipe de Segurança Ofensiva pode ajudar?

Identificação proativa de vulnerabilidades.



Redução do risco de incidentes cibernéticos.

Melhoria da postura de segurança da organização.

Aumento da confiança dos clientes e parceiros.

Conformidade com Regulamentações e Padrões de Segurança

Números que falam por si só

- 56 análises
- + 2400 horas
- + 130 vulnerabilidades identificadas
  - + 20 vulnerbilidades críticas e alta
- CVEs
  - CVE-2024-3867
  - CVE-2024-48746

Conclusão

- **Redução de Riscos: Fortaleça defesas e cultive uma cultura de segurança.**
- **Segurança Proativa: Transforme ameaças em oportunidades.**
- **Proteção de Ativos: Valorize e proteja o que é mais importante.**
- **Retorno Garantido: Economize evitando incidentes e danos à reputação.**

“Não espere ser atacado para investir em segurança”

OBRIGADO(A)!

leonardo.silva@rnp.br

Linked in

cais RNP MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO