2025 WTR WORKSHOP TECNOLOGIAS DE REDE PoPRS

Como um time de segurança ofensiva pode auxiliar a sua organização

Rildo Souza

Coordenador de Segurança

RNP

CAIS – Inteligência em Cibersegurança

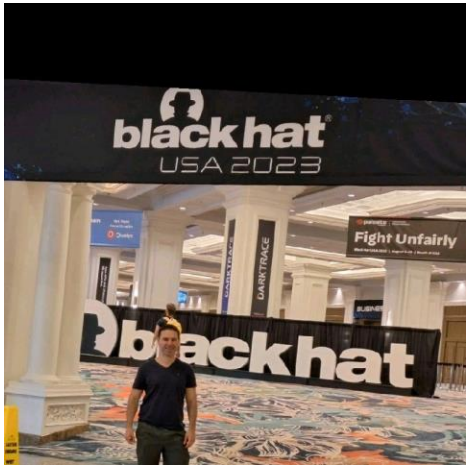
2025 WTR WORKSHOP TECNOLOGIAS DE REDE PoPRS

cais

- Pentest/Análise de Vulnerabilidades
- Incidentes de Segurança
- Desenvolvimento de CSIRTs
- SOC
- Conscientização de Segurança
- Governança, Risco e Compliance

RNP

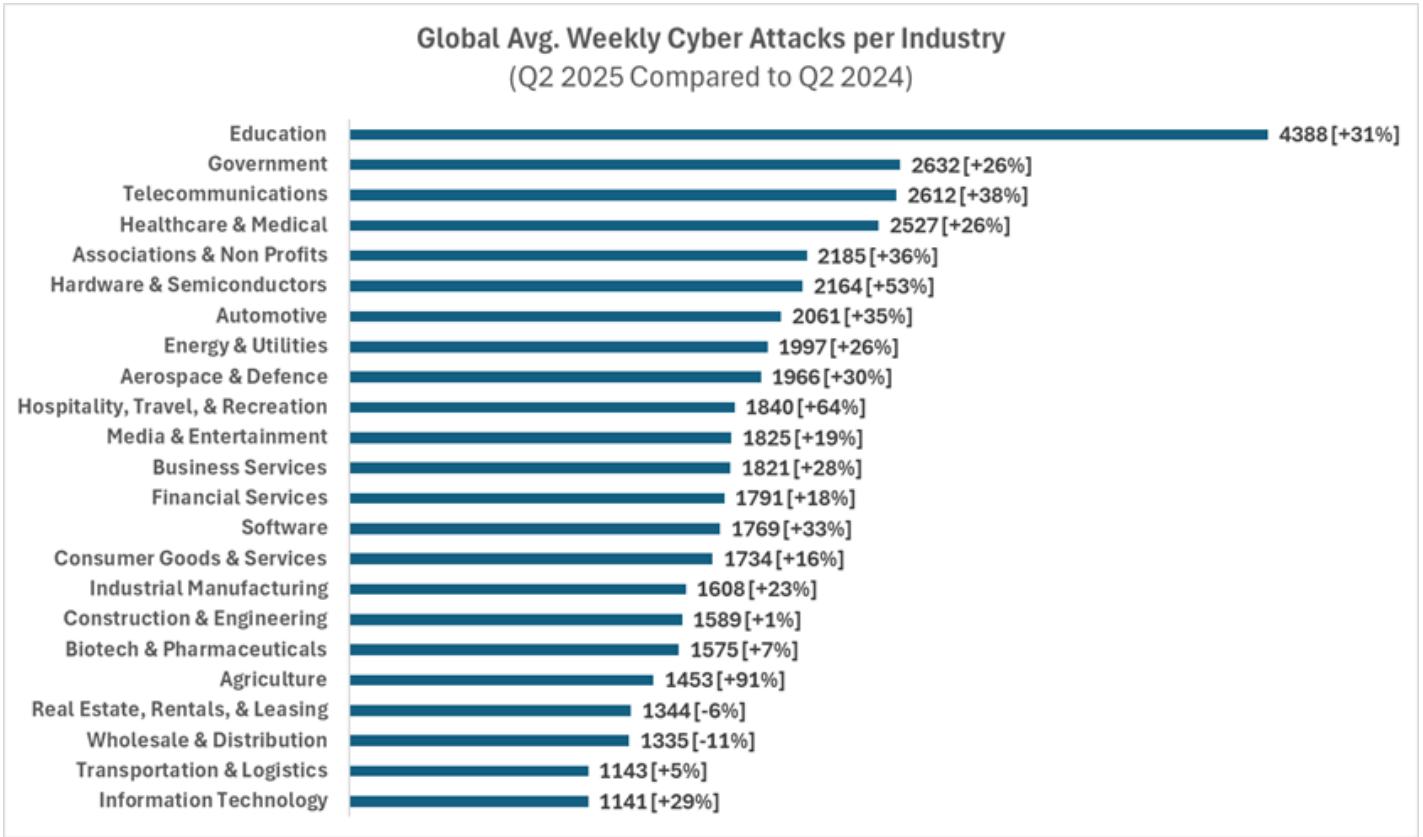
Quem sou



- Rildo Souza
- Pai da Mariana
- Coordenador do Red e Blue Team
- Algumas especializações e certificações
- Na área de segurança da informação formalmente desde 2009
- Mestre em Ciência da Computação

Introdução

Qual setor é o maior alvo de ciberataques no mundo ?



Fonte: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

Contexto

Ataques cibernéticos a universidades e instituições científicas crescem no país (4 notícias)

Publicado em 16 de junho de 2025

Essa notícia também repercutiu nos veículos:

APUFSC | Diário Tancredense | AnchisesBr

Entre 2023 e 2024, os ataques a universidades brasileiras cresceram 56%, ameaçando pesquisas e serviços essenciais.

Página inicial > Distrito Federal

Distrito Federal

UnB sofre ataque hacker e sistemas da universidade ficam fora do ar

O ataque ocorreu na manhã desta quarta-feira (9/4). Os sistemas já foram reestabelecidos e a UnB apura as circunstâncias da invasão

Samara Schwingel
09/04/2025 17:28, atualizado 09/04/2025 17:41

METRÓPOLES

- Instituto de Pesquisas Energéticas e Nucleares (IPEN) teve um prejuízo de R$ 2,5 milhões com ransomware

Fonte: https://namidia.fapesp.br/ataques-ciberneticos-a-universidades-e-instituicoes-cientificas-crescem-no-pais/617379

Fonte: https://www.metropoles.com/distrito-federal/unb-sofre-ataque-hacker-e-sistemas-da-universidade-ficam-fora-do-ar

Problema atual

Por que proteger universidades é tão desafiador ?

- Proteger esses ambientes é particularmente desafiador devido à sua base de usuários diversificada (estudantes, professores e funcionários administrativos) que podem operar dentro das instalações da instituição ou remotamente;
- Em geral, as organizações dependem de fundos públicos e operam com orçamentos limitados;
- O uso de dispositivos pessoais é frequentemente incentivado;
- Hospedam grandes quantidades de dados pessoais e de pesquisa;
- Alvos altamente lucrativos para ameaças cibernéticas.

Como o CAIS pode te ajudar ?

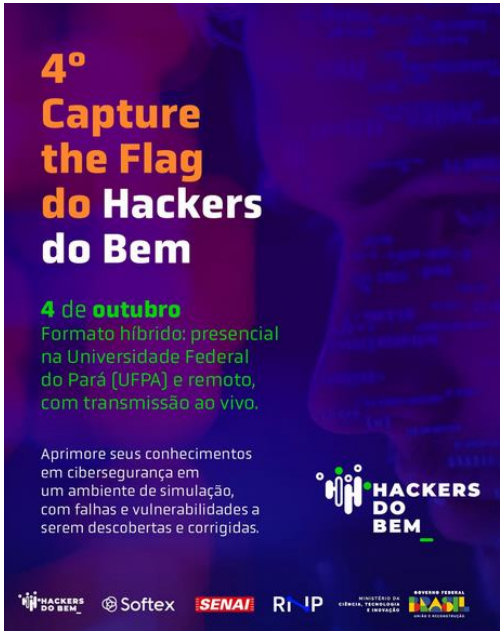
- Grupo de pessoas autorizadas e organizadas para emular os recursos de ataque ou exploração de um adversário em potencial contra a segurança da informação de uma organização [1].
- Equipe de segurança que ajuda a reconhecer e informar como corrigir as falhas de segurança identificadas durante um Pentest [2].
- Criado em 2022 oficialmente na RNP
- Profissionais qualificados e certificados

cais red team

[1] - https://csrc.nist.gov/glossary/term/red_team

[2] - Adaptado de: https://www.imperva.com/blog/what-are-red-team-exercises-and-why-are-they-important/

Principais serviços do Red Team



Pentest

Teste de Intrusão que simula ataques cibernéticos reais contra um sistema, rede ou aplicação;

Analistas do Red Team do CAIS da RNP realizam testes manuais contra um sistema e/ou aplicação;

Facilitar a identificação de vulnerabilidades na organização e como corrigi-las;

Prevenir ataques contra a organização;

Reduzir riscos de ataques cibernéticos;

Permite testar os controles de segurança da organização.

Análise de Vulnerabilidades

Análise de vulnerabilidades utilizando ferramentas automatizadas;

Foco na identificação e listagem das vulnerabilidades;

Pode ser aplicada a uma ampla gama de sistemas e/ou aplicações em um curto período de tempo;

Análise manual do analista para evitar falsos positivos;

A profundidade de uma análise de vulnerabilidades é inferior a realização de um Pentest.

Análise de Arquitetura – Auditoria técnica para nuvens públicas

Governança de Identidade e Acesso: identificação de permissões excessivas, usuários inativos e papéis de risco.

Segurança da Infraestrutura de Rede: análise da exposição a internet e de regras de firewall (Security Groups, NACLs)

Proteção e Confidencialidade de Dados: verificação de dados em buckets, bancos de dados quanto a exposição pública e controle de acesso

Configuração Segura de Serviços (Hardening): auditoria das configurações de serviços (ex: EC2, Lambda, RDS) em busca de desvios das melhores práticas

Criação de CTFs

Desenvolvimento de competições práticas de cibersegurança sob medida

Simulações de cenários reais de ataque e defesa

Estrutura com narrativa imersivas e níveis de dificuldades progressivos

Fortalecimento da cultura de segurança

Desafios em diferentes áreas: segurança ofensiva, defensiva, criptografia, cloud, forense dentre outros

O que esses serviços entregam para a organização ?

Identificação proativa de vulnerabilidades

Redução do risco de incidents cibernéticos

Melhoria na posta de segurança da organização

Aumento da confiança dos clientes e parceiros

Conformidade com regulamentações e padrões de segurança como ISO e PPSI

Números do Red Team da RNP em 2025

+1800 Horas de pentest

+40 pentests realizados

+10 CVEs

+250 Vulnerabilidades identificadas

+50 Vulnerabilidades críticas e altas

1 Novo exploit

Conheça nossos cases

UPE

INSTITUTO FEDERAL
Sul de Minas Gerais

Colégio Pedro II

SGB
SERVIÇO GEOLÓGICO DO BRASIL

impa
Instituto de Matemática Pura e Aplicada

MINISTÉRIO DA DEFESA

CAPES

MINISTÉRIO DA EDUCAÇÃO
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

MINISTÉRIO DAS COMUNICAÇÕES
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Como contratar esses serviços ?

RNP+

Análise de Vulnerabilidades

MAIS análises, MAIS segurança.

Identifique as vulnerabilidades existentes nas plataformas de serviços ou ativos digitais de forma automatizada e personalizada para sua instituição.

SAIBA MAIS

RNP+

Pentest

MAIS segurança em suas plataformas.

Identifique vulnerabilidades em sistemas, aplicações e integrações, simulando ataques reais para avaliar riscos e apoiar na correção antes que sejam explorados por invasores.

SAIBA MAIS

Conclusão

Reduzir riscos não é apenas uma opção, é uma necessidade !

Nós não entregamos apenas relatórios, mas tranquilidade, proteção e confiança

Investir em segurança ofensiva é garantir economia, credibilidade e continuidade;

Vamos conversar sobre como adaptar nossas simulações e exercícios à realidade da sua organização e transformar ameaças em oportunidades de fortalecimento ?

Obrigado

rildo.souza@rnp.br

PATROCÍNIO

APOIO

REALIZAÇÃO