HackInSDN

Uma plataforma para capacitação e experimentação em cibersegurança

WTR BA

WTR PoP-BA, 2025-09-29

Trajetória até aqui…

2017: Proposta de ferramenta SDN-IPS (edital FIBRE uso de testbed para ensino)

2018: Salão de Ferramentas SBRC - Prêmio de melhor ferramenta

Artigo CSBC "Experiências com uso da ferramenta SDN-IPS no testbed FIBRE para práticas de ensino de redes e cibersegurança"

2020: Artigo SBIE "Uma Experiência de Avaliação Multidimensional de Cursos de Redes de Computadores em Ambientes de Testbeds" (RUBIK)

2023: Edital Hackers do Bem

2024: Início do projeto GT-HackInSDN

ibsec.com.br

Com salário de mais de R$ 30 mil, área de segurança da informação tem déficit de profissionais

07.05.2024 | #Carreiras em Cibersegurança — 1 minuto 53 segundos de leitura

Um levantamento do Google for Startups mostrou que o Brasil terá um déficit de 530 mil profissionais de tecnologia da informação (TI) da área até 2025, sendo a área de segurança de informação a que apresenta o maior déficit de talentos. O que é algo chocante visto que é uma área com bons salários com um plano de carreira bem diverso nas empresas.

Confira abaixo os profissionais de segurança da informação mais procurados e quais são seus salários *(via G1)*.

Salários de profissionais de cibersegurança

- **Analista de Segurança da Informação:** entre R$ 4 mil e R$ 8 mil
- **Pentester:** entre R$ 13.400 e R$ 18.400
- **Analista de DevSecOps:** entre R$ 14.650 e R$ 24.500
- **Analista de Governança, risco e compliance (GRC):** entre R$ 11.850 e R$ 18.150
- **Especialista de Governança, risco e compliance (GRC):** entre R$ 17.750 e R$ 22.600
- **Coordenador de cibersegurança:** entre R$ 17.350 e R$ 23.750
- **Gerente de cibersegurança:** entre R$ 23.100 e R$ 38.700

www.puc-campinas.edu.br/presidente-do-c

Home » Notícias » Presidente do Ciesp diz que o Brasil terá déficit de 140 mil profissionais de cibersegurança até 20

PRESIDENTE DO CIESP DIZ QUE O BRASIL TERÁ DÉFICIT DE 140 MIL PROFISSIONAIS DE CIBERSEGURANÇA ATÉ 2025

PUC-Campinas lançou Curso de Cibersegurança neste ano e oferece vagas no Vestibular de Inverno

A PUC-Campinas lançou em 2024 o seu Curso de Cibersegurança, o segundo em Graduação do Brasil, para atender a um crescente interesse por parte dos estudantes, de profissionais de TI e das empresas e órgãos governamentais em

veja.abril.com.br/coluna/radar-economico/cib

veja Negócios — Economia — ASSINE VEJA NEGÓCIOS

Cibersegurança movimenta R$ 17 bilhões no Brasil para mitigar ataques

Consultoria aponta crescimento do setor, que demanda gastos das empresas

Por Felipe Erlich SEGUIR
24 Maio 2025, 14h00

tecmundo.com.br

tecmundo — O que você procura?

TecFriday | Notícias | Últimas Notícias | Mais Lidas | Tutoriais | Colunas | Guia de Compras | Cupons | Anuncie

Home > Segurança

Brasil tem escassez de 750 mil profissionais de cibersegurança, diz estudo

09/07/2024 às 08:00 • 1 min de leitura

COMPARTILHE

Cenário atual

- Plataformas existentes: produção de conteúdo privado e não colaborativo, custo, escalabilidade vertical

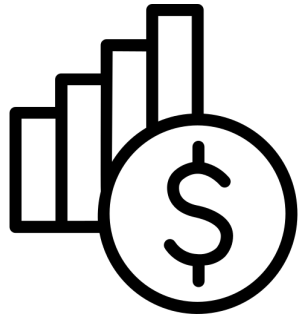
Difícil achar profissionais qualificados

Essa aula poderia ser mais prática! Mas qual laboratório vou usar?

Quero estudar cibersegurança, usando um ambiente realista e de larga escala!

Desafios no uso de laboratórios físicos

- **Custos** elevados (CAPEX e OPEX)
  - Aquisição de hardware, instalação, manutenção, energia elétrica, refrigeração e atualização de equipamentos.
- Baixa **escalabilidade**; Baixa garantia de **reprodutibilidade**
  - ~ 50 alunos por turma
- Restrições de uso fora do horário normal e dificuldades de **acesso remoto**;
- Necessidade de **customização** (dinâmica) para cada aula;
- Tópicos que exigem **infraestruturas reais** de cibersegurança;
- Restrição para a realização de **atividades em rede**;
- **Ociosidade**.



Instalação (50u)
R$ 360.000,00

Manutenção (5y)
R$ 240.000,00

R$ 600.000,00

http://bit.ly/44SQhBV

HackInSDN

Um ambiente que oferece **laboratórios virtuais em escala**, recursos avançados de experimentação e modelo de criação de conteúdo baseado em economia compartilhada, destinado a apoiar e fortalecer a capacitação em cibersegurança.

Diferenciais do HackInSDN e parceiros chaves

Escalabilidade, serviço em nuvem (**LabaaS**)

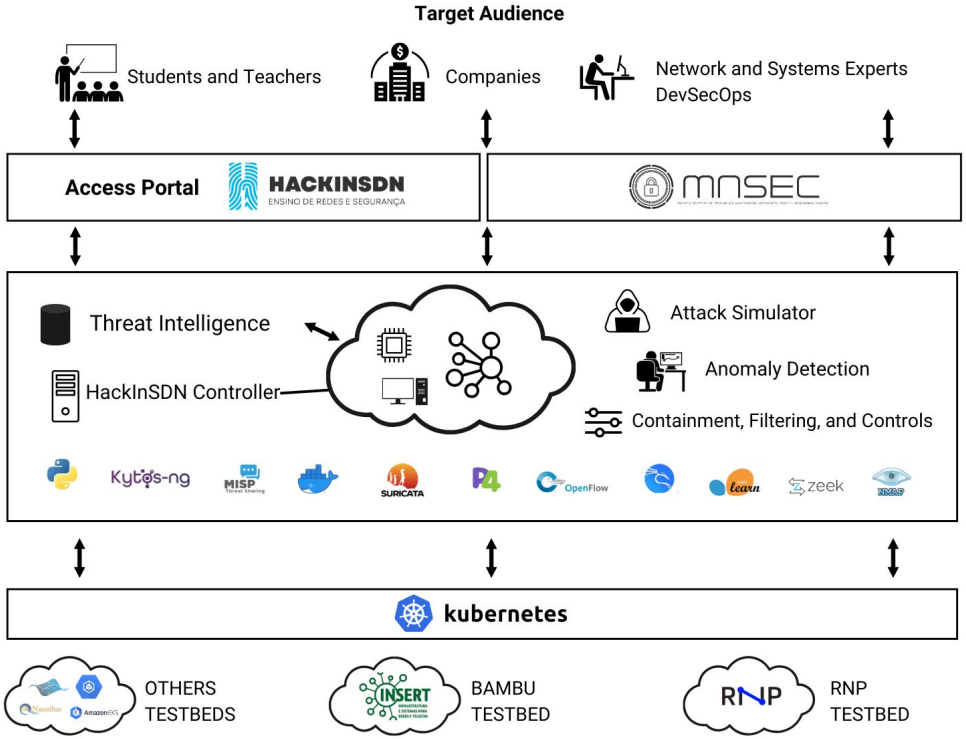
Produção de conteúdo baseado em **Economia compartilhada**

Treinamentos hands-on, **cenários reais**, ferramentas e práticas de **mercado**

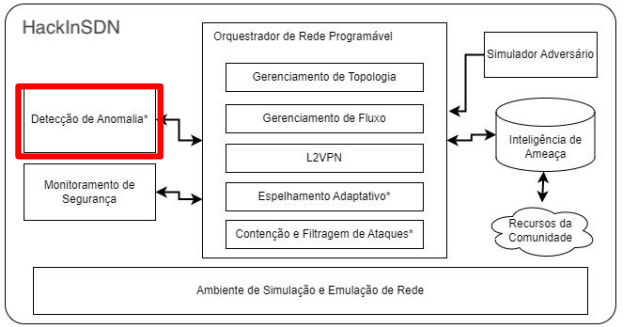
Trilhas de formação customizadas para o perfil do usuário e **certificações**

Uso de IA e sistema de recomendação do perfil de e-learning, skills e **recrutamento**

HackInSDN - Arquitetura



Detecção de Anomalia

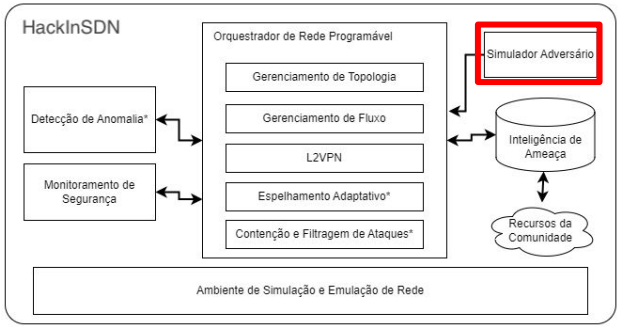


Extração de características de interesse e aplicação de algoritmos de Aprendizagem de Máquina para geração de alertas de novidade

- Recursos avançados de segurança

Tipos de entradas: telemetria do plano de dados, telemetria do plano de controle, estatísticas da rede

Simulador adversário



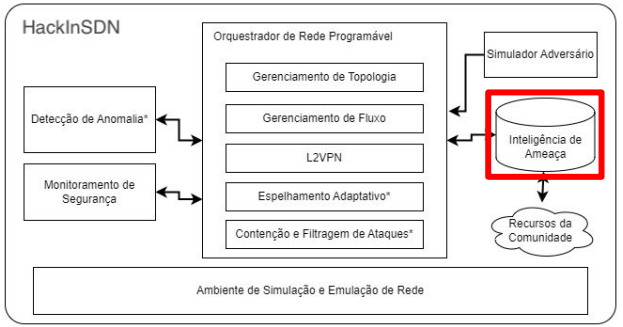
Gerador de tráfego especializado em cibersegurança com operação *stateless* e *stateful*

- realismo de cenários

Agrega diversas ferramentas de segurança ofensiva

Simulação de tráfego benigno baseado em modelos IMIX / EMIX, volume de tráfego, datasets customizados (DNS, HTTP/S, BGP, etc)

Inteligência de ameaça



Base de Inteligência de Ameaça usada na contenção de ataques e compartilhamento de informações de segurança

- Bloqueio pró-ativo
- Análise malware
- Processamento de consultas DNS

Além dos feeds tradicionais, incluímos URLs maliciosas, exemplares de malwares, dados de honeypots

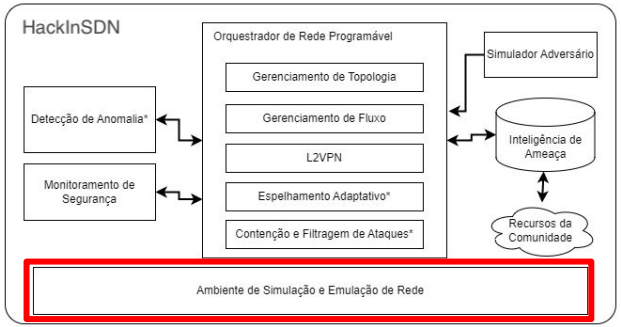
Gerenciamento de cenários

Gerenciamento da topologia

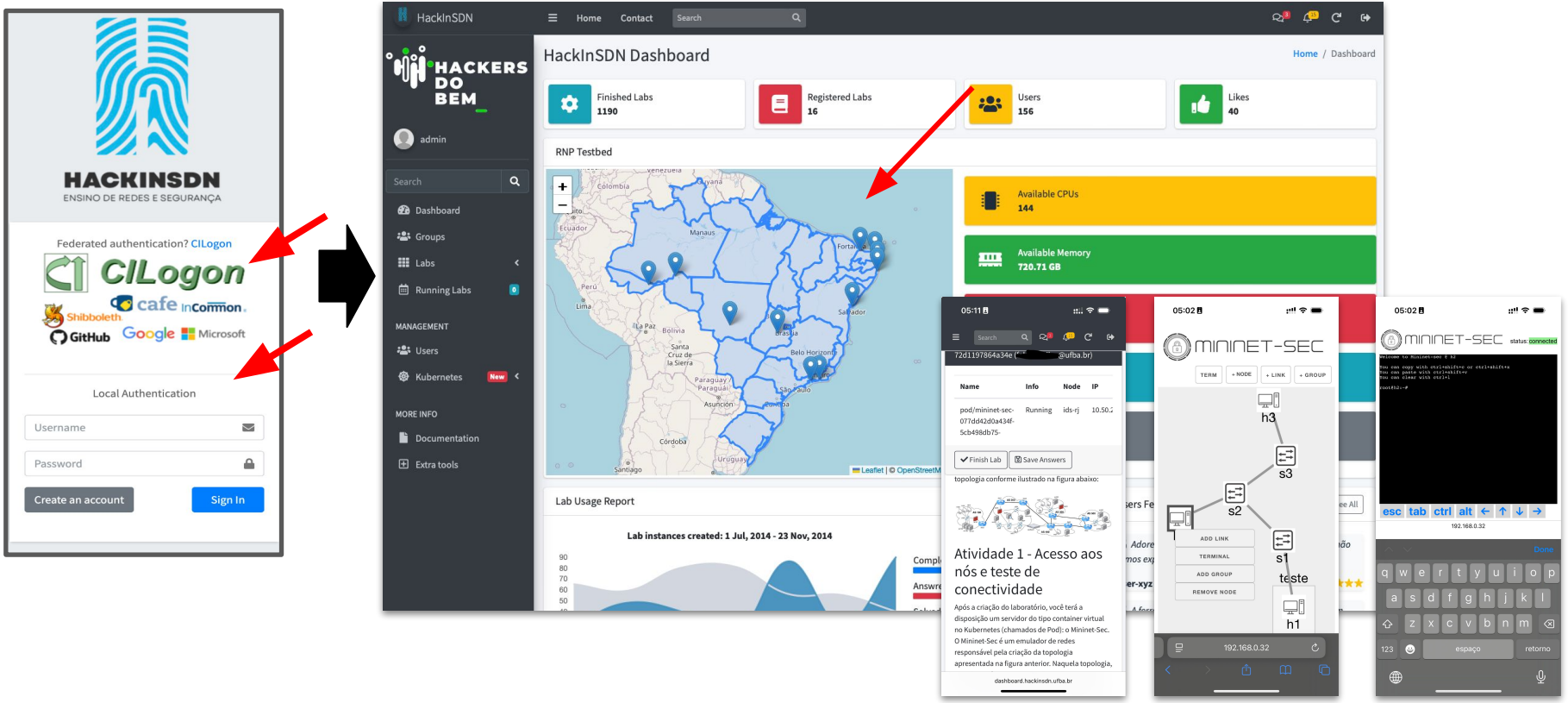
Biblioteca de nós

Gerenciamento de Aplicações

Interconexão de recursos



Serviço em nuvem, autenticação federada e facilidade de acesso



Exemplos de laboratórios disponíveis

Ataques básicos e defesas: scan de rede, brute-force e DoS
Orquestração, Execução, Detecção e Mitigação de DDoS
Injeção de SQL
Tunelamento DNS: impactos e contra-medidas
Análise de Malware
Exploração de binários
Roteamento Seguro na Internet
NDN: Redes de Dados Nomeados
Técnicas de Exfiltração de dados
...

Primeiros resultados

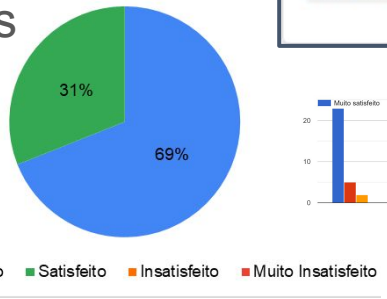
6 meses de operação piloto (sem divulgação)

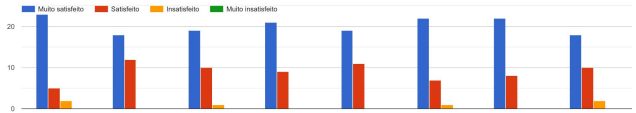
156 usuários cadastrados na base de dados

16 laboratórios, sobre diferentes tópicos de cibersegurança, foram criados

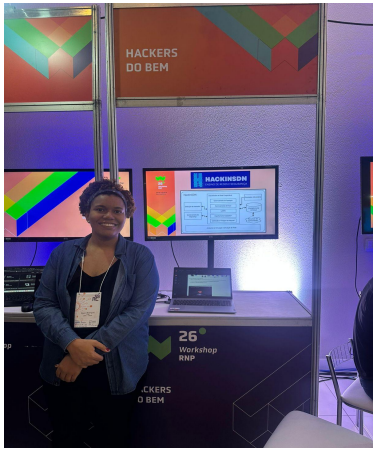
~ 1200 execuções

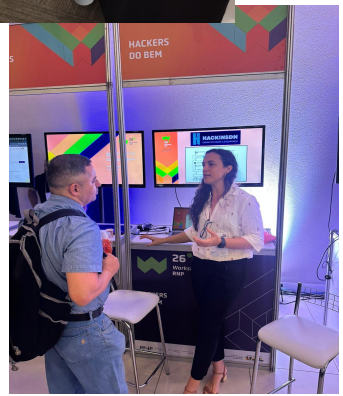
Alunos de graduação e pós-graduação da UFBA, IFBA, UFRGS e outras instituições de ensino no Brasil, Residentes do programa HdB, Donas Security

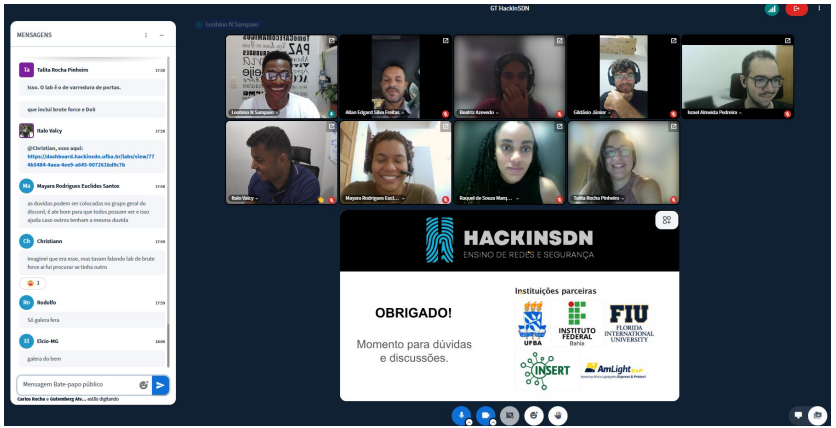




Primeiros resultados







Produções e reconhecimentos

- Artigo Completo no salão de ferramentas do SBSeg 2024;
- Apresentação no Palco INOVA do WRNP 2025;
- Artigo Completo na Trilha Principal do SBRC 2025: “HackInSDN: Uma Arquitetura Flexível, Incremental e Portável para Experimentação em Cibersegurança”;
- Artigo e demonstração no Salão de Ferramentas do SBRC 2025: “Dashboard HackInSDN: Plataforma Web para Experimentação em Redes e Cibersegurança através de Clusters Kubernetes”;
- Artigo no WTG do SBRC 2025: “Avaliação de estratégias para o aperfeiçoamento da detecção de anomalias no tráfego DNS” .
- Apresentação no Workshop do MISP / Encontro de CSIRTs do CERT.br
- Apresentação no HackBahia
- Apresentação no Tech Talks das Federais

Produções e reconhecimentos

- **Prêmio no Selo de Inovação SBC** (2o lugar) durante CSBC 2025: “*HackInSDN: Plataforma Inteligente de Laboratório como Serviço para experimentação em Cibersegurança*”;
- No SBRC 2025, o trabalho apresentado no WTG recebeu o prêmio de **melhor artigo;**
- No Salão de Ferramentas do SBRC 2025, o trabalho apresentado recebeu **menção honrosa**.

Iniciativas mais recentes

Parceria com RNP no projeto KubeRNP

- Integração com ContainerLabs
- Biblioteca para execução de experimentos e ciência de dados (ex: Jupyter notebooks)
- Piloto para replicar cenário da Remessa no HackInSDN

Adicionando suporte à LTI (Learning Tools Interoperability)

Melhorias técnicas:

- Controle de acesso baseado em IAP (Identity-aware proxy)
- Captura de visualização de pacotes na web (wireshark web)
- Integração com Apache Guacamole
- Expansão da biblioteca de nós e recursos de experimentação (ex: Tofino model)

Considerações finais

- Arquitetura HackInSDN favorece experimentação em cibersegurança e laboratórios virtuais
  - Conceito de Laboratório como Serviço
- Reprodutibilidade, Reuso e Compartilhamento de laboratórios
- Alta escalabilidade com integração aos ambientes experimentais existentes
- Transformação no processo de ensino e aprendizagem em cibersegurança
  - Mapeamento das demandas de mercado e skills dos alunos (sistema de recomendação)

Obrigado!

idasilva@fiu.edu
italovalcy@ufba.br

Agradecimentos

RNP HACKERS DO BEM fapesb