Tools for Training White Hat Hackers

Rômulo Silva Pinheiro

Coordenador P&D

romulo.pinheiro@rnp.br

The **Internet2 Technology Exchange (TechEX)**

- The **Internet2 Technology Exchange (TechEX)** is a premier technical event aimed at the global research and education (R&E) community. The **2024 edition took place from December 9 to 13 in Boston, Massachusetts**, bringing together experts, engineers, IT leaders, and security professionals from academic institutions, national research networks, and industry partners.

Agenda

- Hacker do Bem Program Goals
- R&D Program Lifecycle
- R&D Working Groups
- Next steps and Final Remarks

Understanding the Brazilian Context

- 11 million young people aged 15 to 29 in Brazil were neither studying or working (IBGE)
- Brazil faces a gap of 300 thousand cybersecurity specialists (ISC2)
- Higher education courses often fail to align with the demands of cybersecurity companies
- The growing number of security and privacy incidents highlights the significant risks

Our motivation is to offer free learning opportunities for young students, enabling them to become skilled cybersecurity professionals!

About the *Hackers do Bem* Program

Implemented under Softex's National Priority Innovation Program, the initiative is executed by the RNP and Senai São Paulo, with support from ICT Law resources (**5,6 million USD – 3 years**).

This program aims at cybersecurity and privacy skilled human resource development through

(i) training actions using intensive experimentation environments, cybersecurity simulators, and technological residencies

(ii) RD&I actions and

(iii) Establishment of a National Cybersecurity Hub

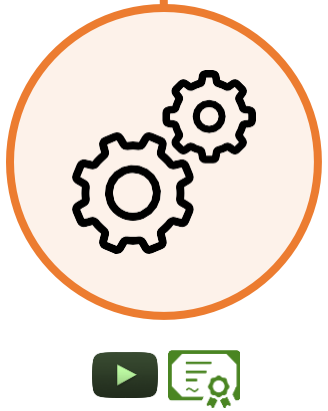
Defined Goals

- **Management and Governance of the Program (advisory board)**
- **Development of training infrastructure (Gamified Virtual Learning Environment)**
- **Development of cybersecurity skills content (leveling, basic, fundamental, specialized)**
- **Foster the cybersecurity innovation ecosystem (R&D projects, hackathons, CTFs, cybergames)**
- **Establishment of a National Cybersecurity Hub**
  - *It is a space for connection and synergies among actors in the cybersecurity ecosystem.*

Training program and key results

2 years

30,000	30,000	3,000	2,000	216
Leveling	Basic	Fundamental	Specialized	technological residency



asynchronous classes

Training program

Specialized

GRC - Governance, Risk, and Compliance

BlueTeam

RedTeam

Incident Response and Forensics

DevOps/ DevSecOps

Program Milestones

March 2023 – Launch of the Program

July 2023 – First Open Call for R&D projects

August 2023 – 1st Workshop on Cybersecurity Training

December 2023 – Opening of Training Registrations

January 2024 – Launch of the Teaching Platform (Leveling Module) and start of R&D projects

March 2024 – 1st CTF

September, 2024 – First group of students concluded the specialized certification

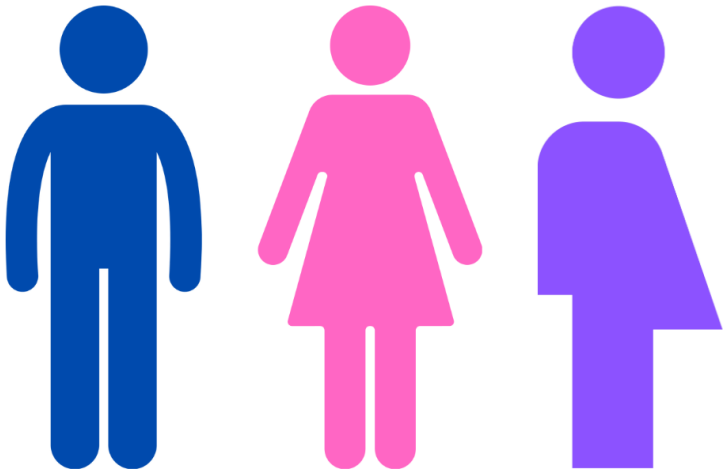
November 2024 – Demo day

HACKERS DO BEM_

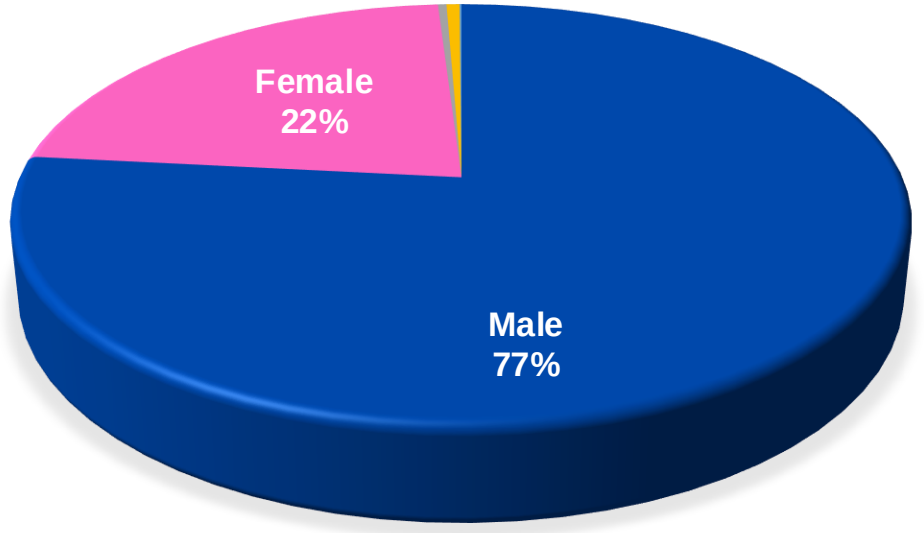
129,938 registered users

The registrations have been suspended since March 2024

Gender distribution of the registrations



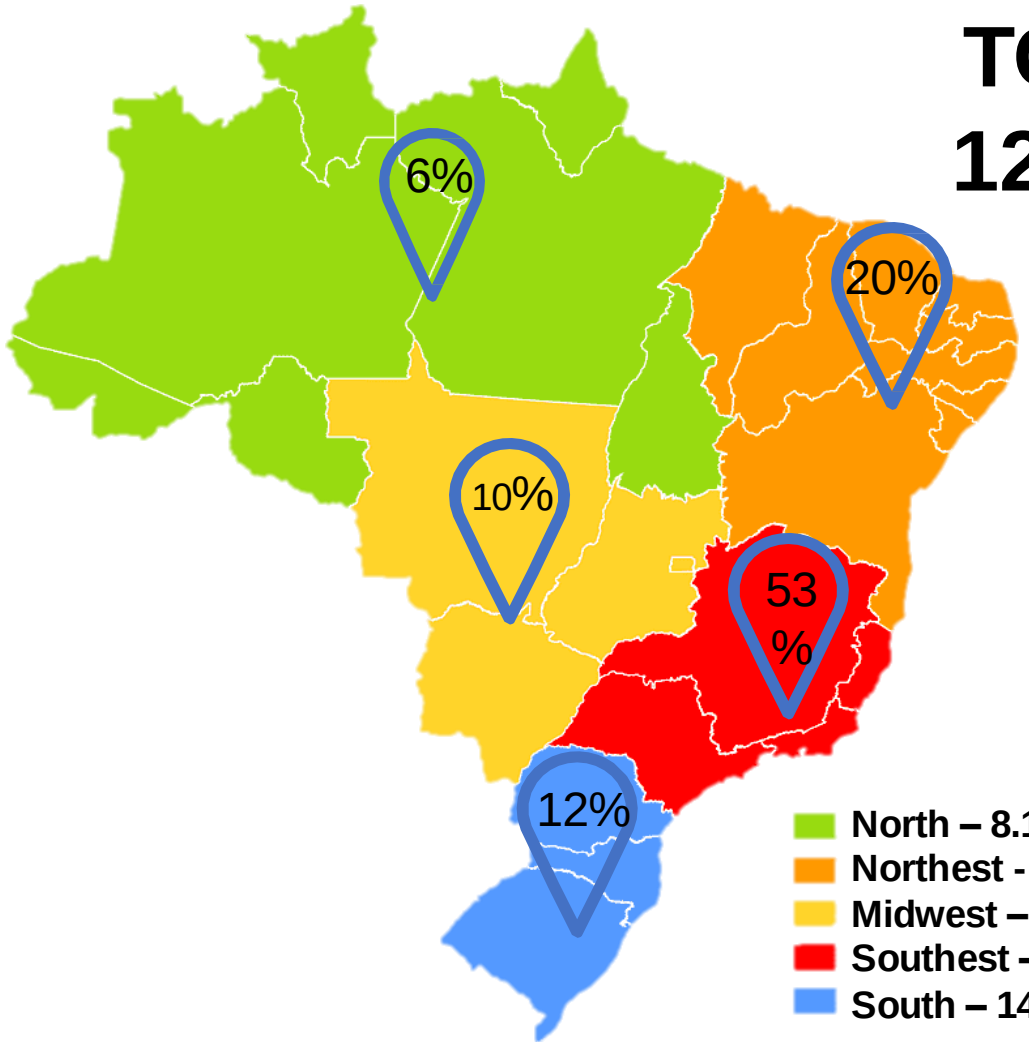
TOTAL
129.938



99,590 29,049 1,302

** Non-binary or others

Regional distribution of the registrations

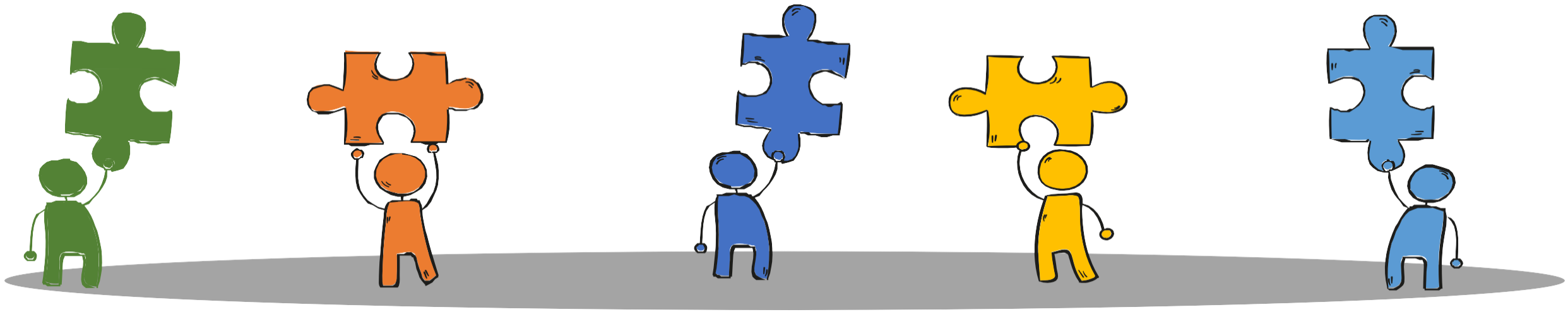


TOTAL
129.938

- North – 8.192
- Northest - 25.933
- Midwest – 12.378
- Southest – 67.893
- South – 14.882

Certification of the training

Specialized Training



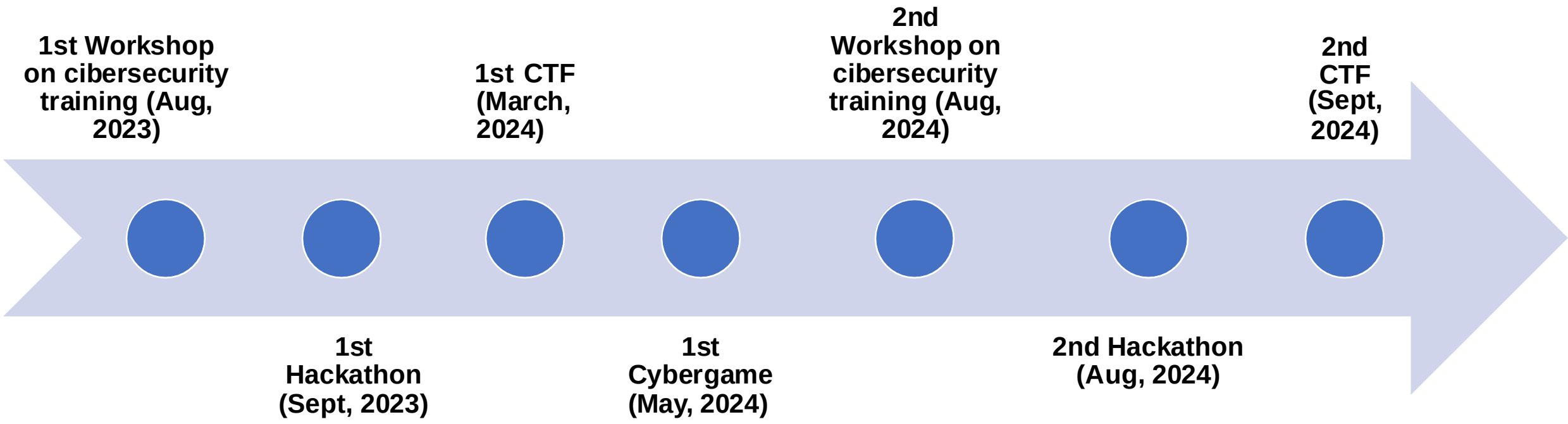
DevSecOps	Red Team	Blue Team	GRC	Forense
76	189	171	89	128

653 students specialized in cybersecurity

100 students will begin their technological residency in **Abril 2025**

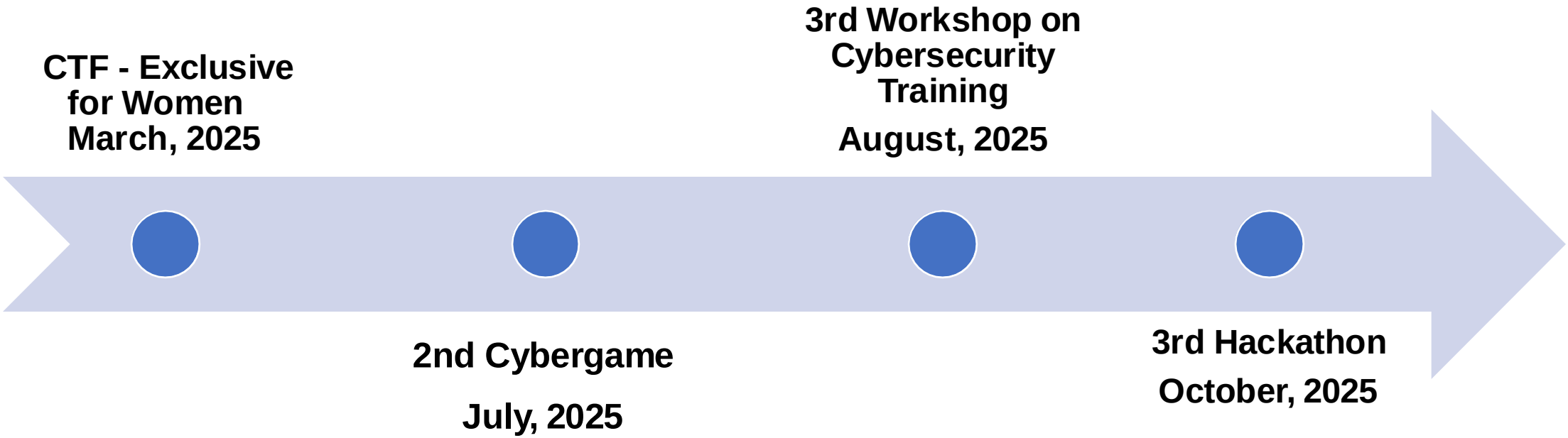
Organizing and hosting events to strengthen connections among cybersecurity ecosystem actors…

Events to strengthen connections




HACKERS
DO BEM

Event Planning for 2025



R&D Program Lifecycle

Objective of the R&D Program

To foster the development of innovative **educational tools**, such as simulators, games, digital platforms, and others, that contribute to practical and high-quality training in cybersecurity, especially for participants of the Hackers do Bem Program.

R&D Program Lifecycle

R&D Program

1st R&D Cycle

- 1 year (2024)
- 6 months - user evaluation (2025)
- **7 R&D projects**

2nd R&D Cycle

- 1 year – MVP (2025)
- 6 months - user evaluation (2026)
- **4 R&D projects**

1st Cycle

- Open call for R&D proposal (2023)
- Received 40 proposals.
- 7 working groups (WGs) focus on developing open-source solutions
- 43 scholarships - only 8 are females

Most tools are in Portuguese.

HACKERS DO BEM_

WG-EXSS

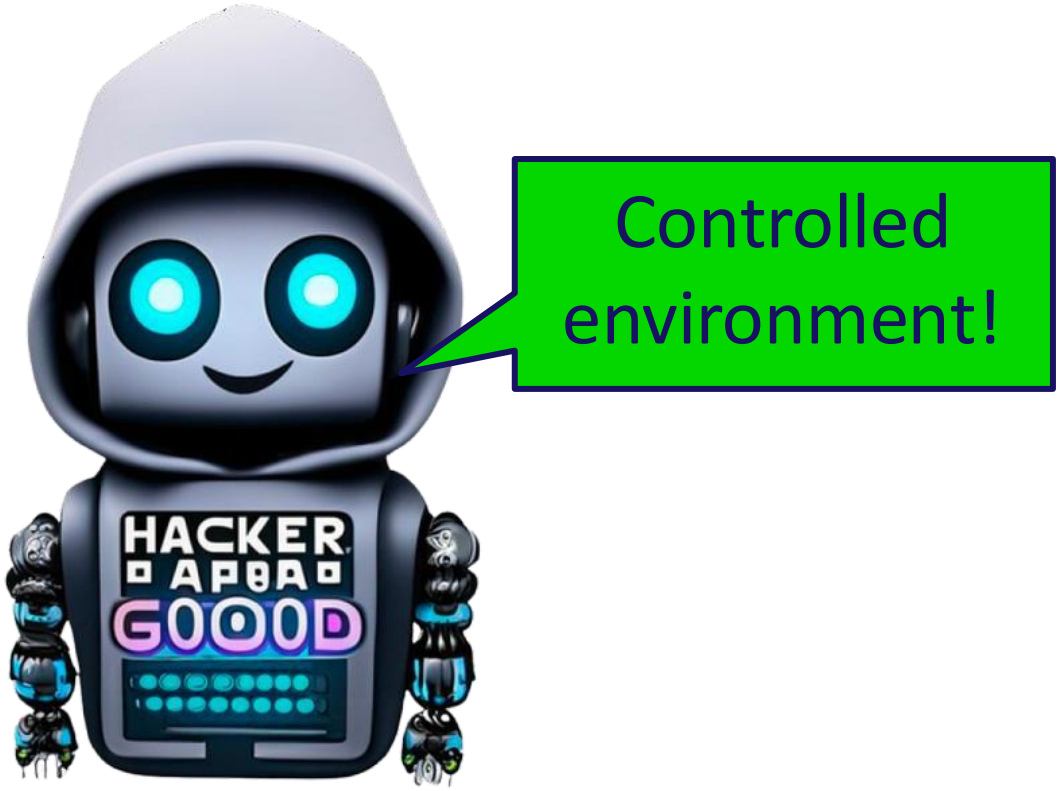
Prof. Igor Moraes (UFF)

https://gtexss.uff.br/

Controlled environment!

Goal

- Develop an educational emulator for **Cross-Site Scripting (XSS)** attacks
  - Gamified features
- Three key learning pillars
  - Exploitation
  - Identification
  - Mitigation



Iniciante

HACKERS DO BEM

- Página Inicial
- Introdução
- XSS Refletido
- XSS Armazenado
- XSS DOM

Box Anti Hacker

R$ 50.00

Saiba mais

Cofre de Senhas

R$ 30.00

Saiba mais

Firewall

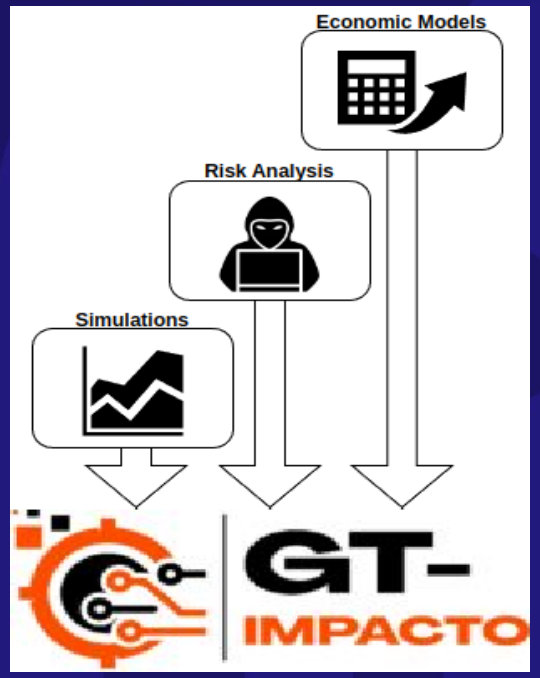
R$ 40.00

Saiba mais

WG-IMPACTO

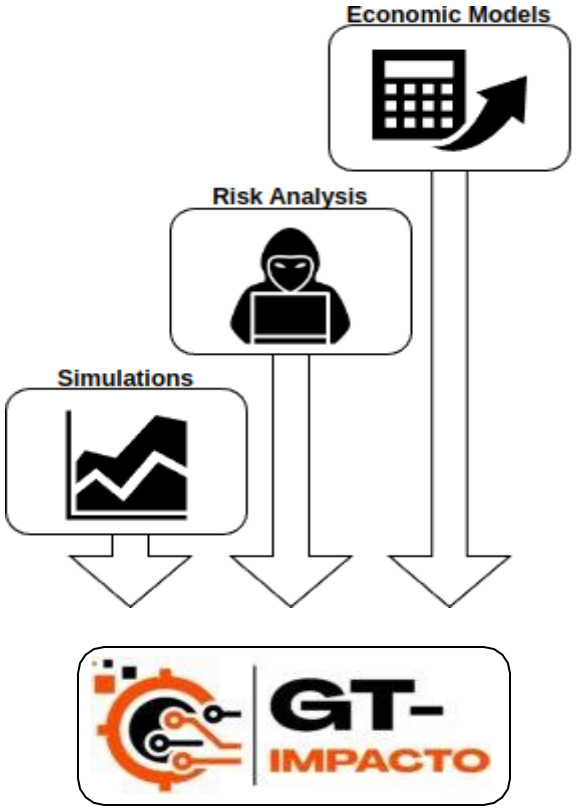
Prof. Jeferson Nobre (UFRGS)

https://www.inf.ufrgs.br/gt-impacto/



Goal

- Train security professionals on the technical and **economic aspects** of cybersecurity
- Effective financial planning is crucial for cybersecurity strategies, avoiding wasting resources
- Gap of training tools that address the economic perspective



GT-IMPACTO

GT Impacto

MENU

- Início
- Perfil de Empresa
- Regional Retail Gr...
  - Perfil de Empresa
  - Análise de Risco
  - Gestão Econômica
  - Editar Empresa
- Fonte de Dados

Dashboard Econômica de Regional Retail Group

Perfil de Empresa | Análise de Risco | Gestão Econômica | Editar | Cópia

Simulações de Gordon-Loeb - Server - $150000,00

Impactos

Status	Tipo	Possível dano	Probabilidade	Perda estimada	Invest. atual	Invest. ótimo	Invest. aceitável	Ajuste	Lucro
-	Malware	$88.1K	10,28%	$9.1K	-	$849.43	$526.41 - $1.4K	-	-
-	Phishing	$75.0K	10,14%	$7.6K	-	$717.73	$445.59 - $1.1K	-	-
-	DDoS	$99.4K	10,57%	$10.5K	-	$971.99	$600.16 - $1.6K	-	-
●	Geral	$97.4K	27,90%	$27.2K	$8.0K	$1.6K	$845.81 - $2.9K	$-6.4K	$5.1K

Server - Gráfico do EBIS para ataque selecionado

Geral - Eficiência aceitável: 97,5% - Alpha: 0,001

Atualizar Gráfico

HACKERS DO BEM_

WG-HIKARI

Prof. Lourenço Pereira (ITA)

https://hikari-edu.github.io/

Overview

HACKERS DO BEM

- Focusing on Threat Hunting
- Multi-staged: Logs and difficulty increase dynamically in runtime (timely or event-oriented)
- CTF-like: Engages with the language of the community – for fun and profit
- Challenges
  - Network Scanning, Web Exploits, EDR Analysis, Ransomware Behavior, etc.

Goal

HACKERS DO BEM_

- Empower students with the knowledge and skills needed for effective defense
- HIKARI – **Platform for blue-team training**
  - Platform flexible to adapt to different business needs.
  - Realistic environment for SIEM threat-hunting
- Target: students who aim to enhance their defensive capabilities

Bem-vindo ao HIKARI - Hunting

https://52e3-161-24-23-100.ngrok-free.app

Feedback sobre o HIKARI | Usuários | Painel de controle | Desafios | Painel do administrador | Notificações | Perfil | Configurações

Bem-vindo ao **HIKARI** - Hunting Integrado e Kompetição em Resposta a Incidentes!

Explore desafios baseados em cenários realistas e desenvolva suas habilidades em análise e resposta a incidentes cibernéticos.

Iniciar Desafios | Ver Ranking | Feedback

Desenvolvido por Equipe HIKARI

Desenvolvido por CTFd

Discover - Elastic

https://35c4-161-24-23-100.ngrok-free.app/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),ti

Elastic | Search Elastic

Discover | New | Open | Share | Inspect

Search | KQL | Refresh

+ Add filter

68,892 hits

_source

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 42888 Fortinet Protocol (custom): 6 Destination Port: 443 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic" Destination IP: 10.1.105.18 Low Level Category: Firewall Deny @timestamp: Nov 21, 2024 @ 17:56:25.200 Start Time: Nov 12, 2024, 12:21:45 PM Fortinet Subtype (custom): "forward" Source Asset Name: kali Duration_Seconds (custom): 6 Service Name (custom): HTTPS MasterSrcMAC (custom): "00:15:5d:24:11:02" Fortinet Level (custom): "notice" Application Category (custom): unscanned message: {"Event Name": "Firewall Deny", "Start Time": "Nov 12, 2024, 12:21:45 PM", "Low Level Category":

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 34664 Fortinet Protocol (custom): 6 Destination Port: 443 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic" Destination IP: 10.1.105.7 Low Level Category: Firewall Deny @timestamp: Nov 21, 2024 @ 17:56:25.538 Start Time: Nov 12, 2024, 12:19:47 PM Fortinet Subtype (custom): "forward" Source Asset Name: kali Duration_Seconds (custom): 6 Service Name (custom): HTTPS MasterSrcMAC (custom): "00:15:5d:24:11:02" Fortinet Level (custom): "notice" Application Category (custom): unscanned message: {"Event Name": "Firewall Deny", "Start Time": "Nov 12, 2024, 12:19:47 PM", "Low Level Category":

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 52104 Fortinet Protocol (custom): 6 Destination Port: 443 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic" Destination IP: 10.1.105.1 Low Level Category: Firewall Deny @timestamp: Nov 21, 2024 @ 17:56:25.569 Start Time: Nov 12, 2024, 12:19:47 PM Fortinet Subtype (custom): "forward" Source Asset Name: kali Duration_Seconds (custom): 6 Service Name (custom): HTTPS MasterSrcMAC (custom): "00:15:5d:24:11:02" Fortinet Level (custom): "notice" Application Category (custom): unscanned message: {"Event Name": "Firewall Deny", "Start Time": "Nov 12, 2024, 12:19:47 PM", "Low Level Category":

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 48358 Fortinet Protocol (custom): 6 Destination Port: 443 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic" Destination IP: 10.1.105.4 Low Level Category: Firewall Deny @timestamp: Nov 21, 2024 @ 17:56:25.569 Start Time: Nov 12, 2024, 12:19:47 PM Fortinet Subtype (custom): "forward" Source Asset Name: kali Duration_Seconds (custom): 6 Service Name (custom): HTTPS MasterSrcMAC (custom): "00:15:5d:24:11:02" Fortinet Level (custom): "notice" Application Category (custom): unscanned message: {"Event Name": "Firewall Deny", "Start Time": "Nov 12, 2024, 12:19:47 PM", "Low Level Category":

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 57044 Fortinet Protocol (custom): 6 Destination Port: 443 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic" Destination IP: 10.1.105.0 Low Level Category: Firewall Deny @timestamp: Nov 21, 2024 @ 17:56:25.569 Start Time: Nov 12, 2024, 12:19:47 PM Fortinet Subtype (custom): "forward" Source Asset Name: kali Duration_Seconds (custom): 6 Service Name (custom): HTTPS MasterSrcMAC (custom): "00:15:5d:24:11:02" Fortinet Level (custom): "notice" Application Category (custom): unscanned message: {"Event Name": "Firewall Deny", "Start Time": "Nov 12, 2024, 12:19:47 PM", "Low Level Category":

Action (custom): deny Username: N/A Source IP: 10.6.36.27 Fortinet Vdom (custom): "root" Event Name: Firewall Deny Destination Country (custom): Reserved Source Port: 53664 Fortinet Protocol (custom): 6 Destination Port: 80 DevType (custom): Router @version: 1 pipeline: competition1 Fortinet Type (custom): "traffic"

WG-HackInSDN

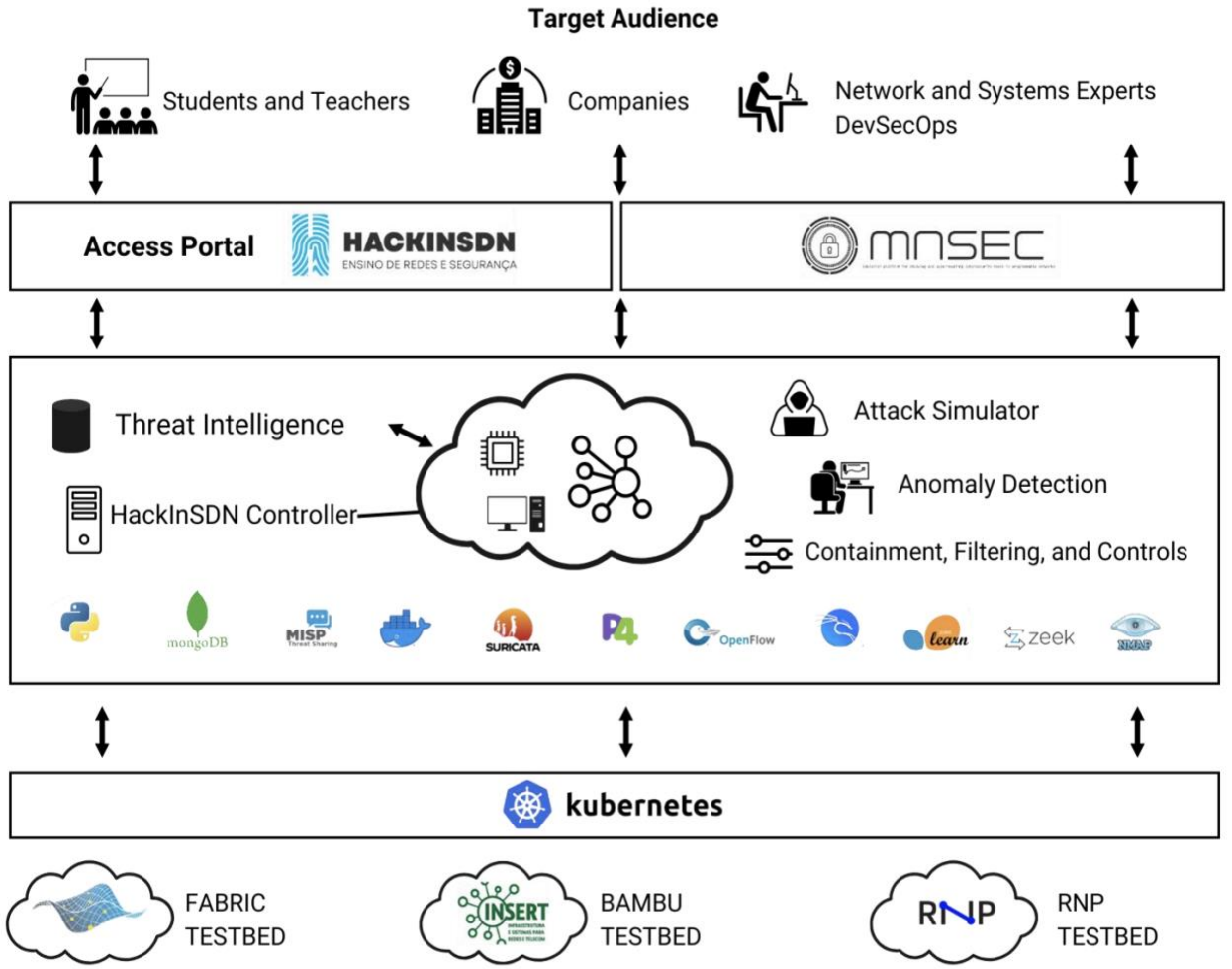
Cybersecurity Laboratory as a Service (LABaaS)

Prof. Leobino Sampaio (UFBA)

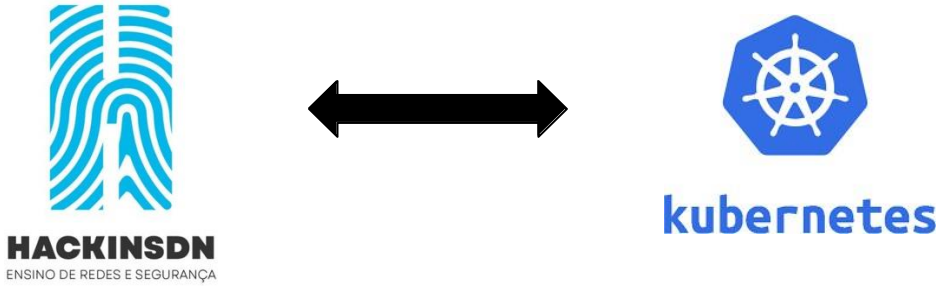
https://hackinsdn.ufba.br/docs/Index/index.html

Overview

- A set of tools that offer a comprehensive environment for training in advanced security topics through network programmability (RNP testbed)
- Loosely coupled architecture
- **Dashboard** for better user experience (UX)
- **MininetSec**: IDs, Firewalls, attack tools and threat intelligent databases.

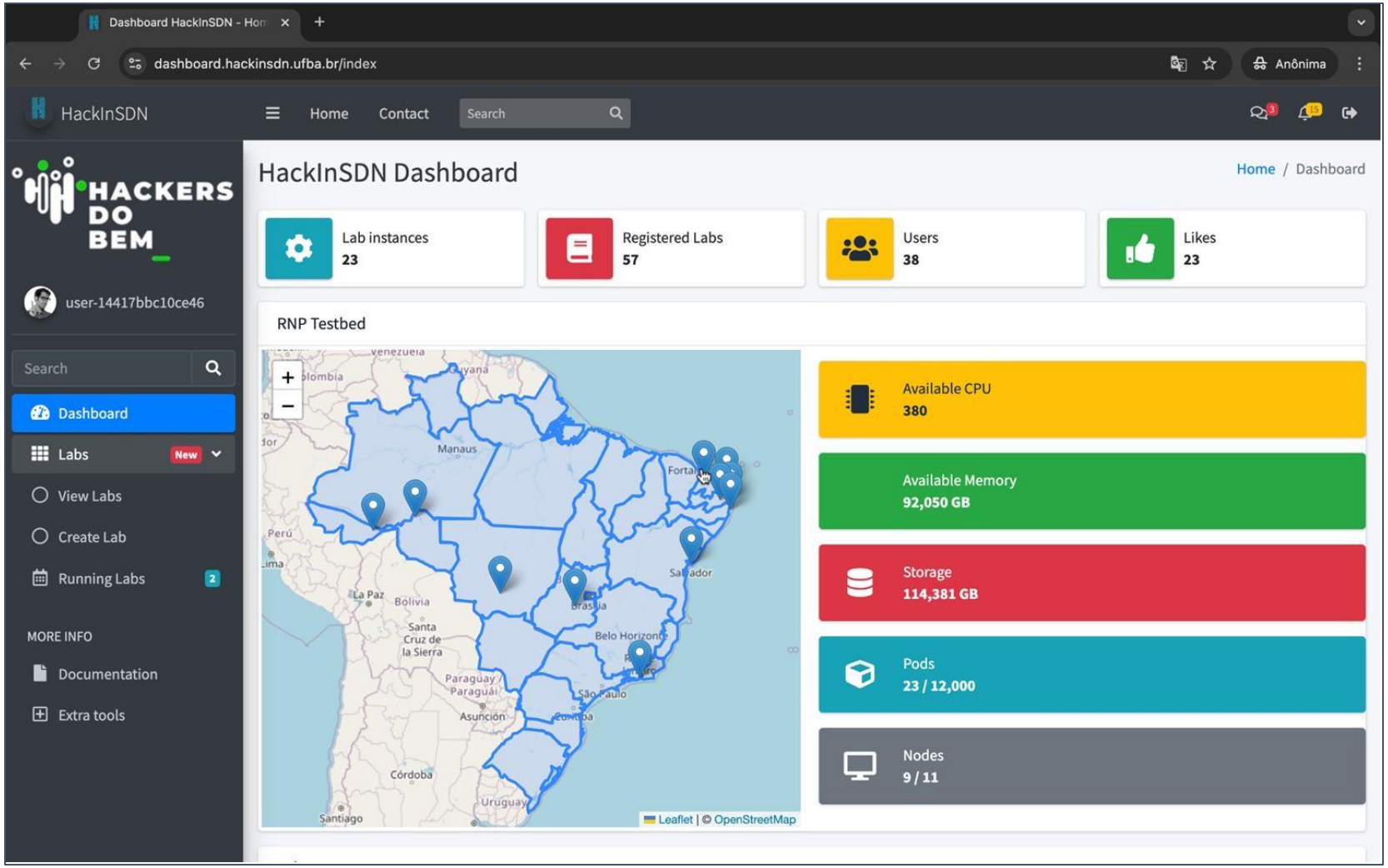


Goal



- An environment that provides real and distributed computational resources and services to support cybersecurity training (in Kubernetes-based clouds)

HackInSDN Dashboard



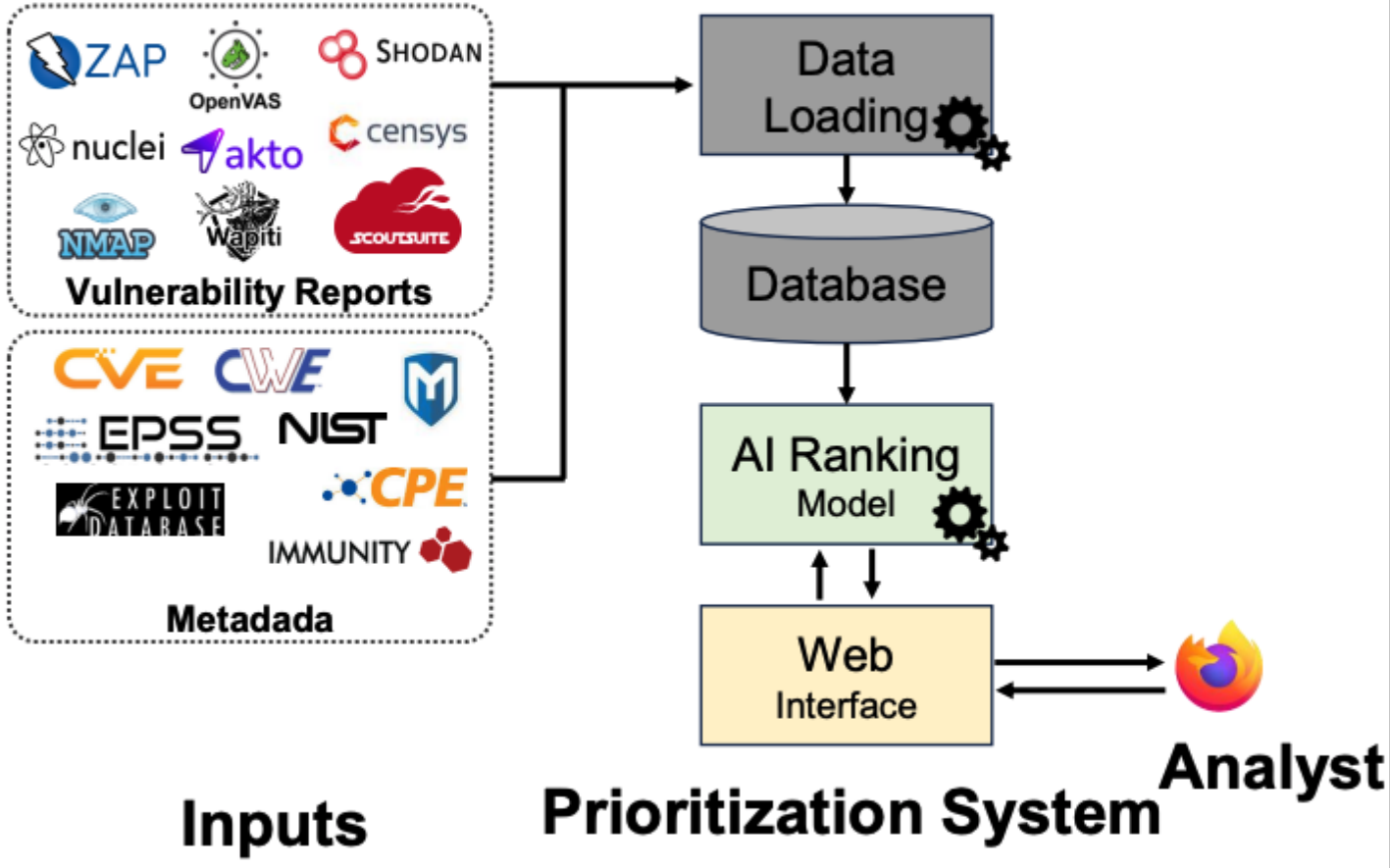
WG-CRIVO

Prof. Italo Cunha (UFMG)

https://gt-crivo.dcc.ufmg.br/

Overview

- Innovative approach for managing vulnerabilities
- Identify the most critical vulnerabilities using the AI ranking model
- Prioritize threats with the highest potential impact on the business.



Goals

- Develop a solution for **prioritizing security vulnerabilities** based on an organization's specific context and business needs.
- Create an AI-based solution that integrates technical and **strategic factors**.
- **Help security teams** in focusing efforts on the most critical and relevant risks.
- Align mitigation actions with organizational goals and **business impact**.

SAM/CRIVO Cybersecurity Dashboards

2024-06-26

cunha

Advanced Analysis (IP Data) | View 1 - EPSS summary | View 2 - by organizations/IP | View 3 - More details by CVE | View 4 - Maps | -

Shodan's banners about IPs with vulnerabilities in Brazil. Using this interface, users can filter banners by each column, ranking its vulnerabilities and clicking on IP column to check details.

SERVICE										VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 02:59:2										Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 05:29:3										Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 18:44:1										Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 23:04:2										Skip
HTTP/1.1 Server: Microsoft-IIS/7.5 Date: Wed, 26 Jun 2024 11:46:39 GMT	189.89.181.190	8140	Salvador	Wind ows	Its Telecomunicacoes	189-89-181- 190.STATIC.itsweb.com .br	itsweb.com.br	0.9754	3.9230	Skip

A vulnerability management system for

SHODAN

WG-Malware Datalab

Prof. Diego Kreutz (UNIPAMPA)

https://malwaredatalab.github.io

Goal

- Hands-on training in Generative AI to combat AI threats
- Promoting ethical “white hat” practices
- Generation of high-quality synthetic data
- Supports innovative solutions and training in Android malware detection

Empower White Hat Hackers with cutting-edge synthetic data technologies to tackle the critical challenge of securing Android users.

Aprender

Pesquisar

Boas vindas

Abrir | Visão geral

Abrir | Avaliação Diagnóstica | Nota: 8

Módulo 1: Nivelamento

Abrir | Tutorial

Abrir | Vídeo aula

Abrir | Avaliação Formativa

Abrir | Avaliação Formativa

mdl.unihacker.club

Lab. de Ensino-Aprendizagem | Lab. de Experimentação | Ambiente

Malware DataLab | Aprender | Gerar Dados | Analisar Resultados | Explorar Ferramentas | Perfil | Sair

Dados

Subir | Pesquisar

Teste - Drebin

Reduzido | Teste | Balanceado

Id: 4768aeec-ea54-4f5f-b5cf-c1a7e3c1109f
Criado em: 2024-11-25T21:33:49.817Z
Atualizado em: 2024-11-25T21:35:57.586Z

Baixar dados originais | Gerar

Teste - Kronodroid

Reduzido | Teste | Balanceado

Id: bee18b3f-d8a6-4cd6-8bdc-e0e382633c1f
Criado em: 2024-11-25T21:31:14.793Z
Atualizado em: 2024-11-25T21:34:26.420Z

Baixar dados originais | Gerar

Teste - Adroit

Reduzido | Teste | Balanceado

Id: 1d151c15-9864-4109-9c26-a025a53e5deb
Criado em: 2024-11-25T19:30:56.508Z
Atualizado em: 2024-11-25T21:29:21.908Z

Android Permissions

HACKERS DO BEM

mdl.unihacker.club

Lab. de Ensino-Aprendizagem | Lab. de Experimentação | Ambiente

Malware DataLab | Aprender | Gerar Dados | Analisar Resultados | Explorar Ferramentas | Perfil | Sair

Teste - Adroit, sintetizado por MalSynGen

PARÂMETROS | CURVAS DE TREINAMENTO | MÉTRICAS DE SIMILARIDADE | MÉTRICAS DE APLICABILIDADE | MATRIZES DE CONFUSÃO

Interação entre Gerador e Discriminador em cGAN

As figuras ilustram a interação entre o gerador e o discriminador durante o aprendizado de uma cGAN. Essa interação pode ser descrita da seguinte forma:

Gerador:tem o objetivo de criar amostras que sejam capazes de enganar o discriminador.
Discriminador: busca melhorar continuamente sua capacidade de distinguir entre amostras reais e falsas.
Competição e Convergência: essa competição entre gerador e discriminador resulta em uma convergência, onde as amostras geradas tornam-se quase indistinguíveis dos dados reais.

A não convergência das redes GAN pode ser identificada monitorando as curvas de perda. Estas devem apresentar uma tendência de diminuição e estabilização ao longo do tempo para indicar sucesso no treinamento.

Para cada fold (dobra) de treinamento é apresentada uma figura.

Fold 1

WG-ETSC

Emulator for Cybersecurity Training

Prof. Edmar Gurjão (UFCG)

https://cyberedu.com.br/

Goals

- Develop a virtual learning environment integrated with physical components for analyzing and testing network security.
- Provide hands-on experience with vulnerability assessments, threat analysis, and risk mitigation tools.
- Support holistic learning of key cybersecurity concepts and practices

Tudo isso só é possível, pois nascemos na academia e desenvolvemos tecnologias inovadoras desde o princípio. Nossa plataforma de treinamento virtualizada permite aos nossos alunos realizarem ações de cibersegurança em um ambiente controlado e realístico.

Cursos disponíveis

BlueTeam (inglês/english)

Cybersecurity tools

RedTeam (inglês/english)

Forende Digital

Professor: Fernando Barros

Blue Team

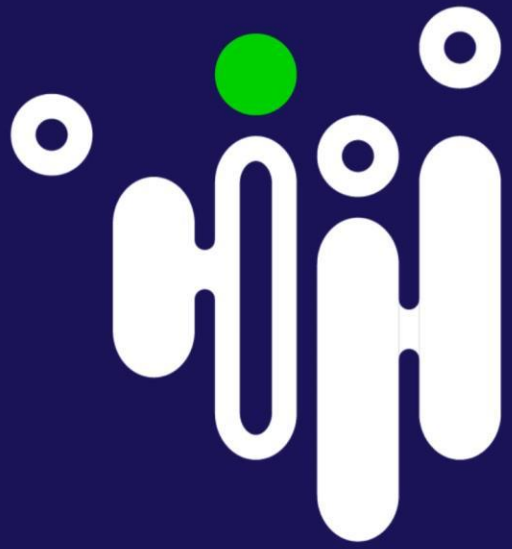
Red Team

Ferramentas para Cibersegurança

Red Team - Residência RNP

Ferramentas para Cibersegurança - Residência RNP

Blue Team - Residência RNP



HACKERS DO BEM

DEMO DAY

DEMO DAY November, 29 2024

HACKERS DO BEM_

NEXT STEPS

6 months for evaluation and improvements

- November: MVPs passed their tech maturity check and got a 6-month extension (recommendations)
- User evaluation (3 months)
- Implementation of the MVP 2.0 (3 months)
- Promote and release of the seven open-source tools

Four Projects Approved for Cycle 2

- ✓ **WG-LFI (Learn From Incidents): Teaching-Learning System, Gamification, and Classification Based on Incidents**

  Prof. Rodrigo Sanches Miani (UFU)

- ✓ **WG-CASTLE: Learning Environment for Cybersecurity Assessment, Simulation, and Training**

  Prof. André Ricardo Abed Grégio (UFPR)

- ✓ **WG-IR (We Got Hacked): Training Simulator for Incident Response Learning**

  Prof. Luciano Ignaczak (UNISINOS)

- ✓ **WG-ViTuRi: Intelligent Tutor Videobot**

  Prof. Danielle Rousy Dias Ricarte (UFPB)

Final remarks

The **demand for skilled cybersecurity professionals** is rapidly increasing. To meet this need, we must enhance our training programs with **innovative strategies**.

Final remarks

Active methodologies in education empower students to learn independently, applying concepts through **practical tools** that link learning to real-world problem-solving.


HACKERS
DO
BEM