

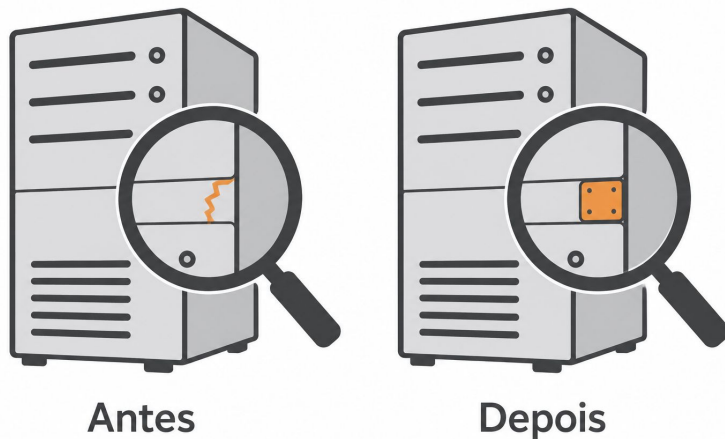


HACKINSDN
ENSINO DE REDES E SEGURANÇA

Gêmeos digitais para práticas de cibersegurança: casos de uso HackInSDN

Italo Valcy <idasilva@fiu.edu>
2026-09-28

Problema: Verificação da correção de uma vulnerabilidade

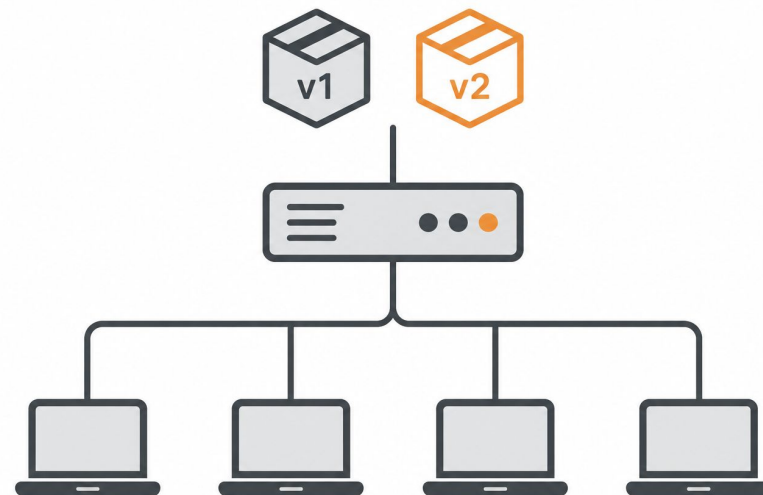


Uma vulnerabilidade afeta um serviço em produção. A equipe aplica uma correção.

- Como reproduzir as condições em que a vulnerabilidade ocorre?
- Que teste demonstra que a correção funciona?
- Como verificar se o serviço continua funcionando como esperado?

Evidência esperada: comparação do comportamento antes e depois da correção.

Problema: Testes de uma nova versão do sistema



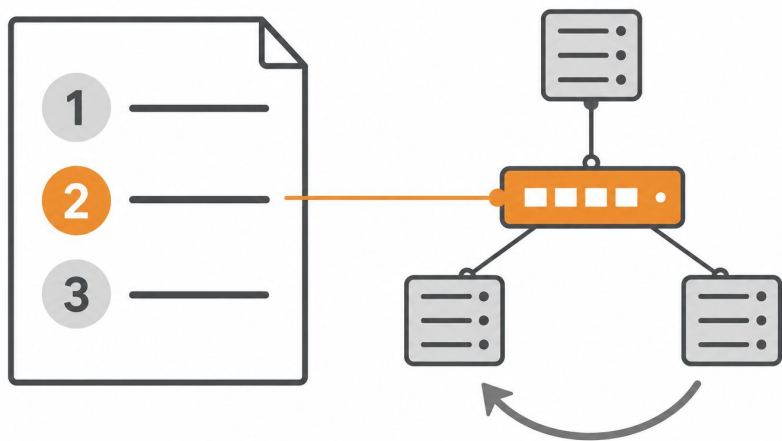
Uma nova versão do software de controle ou orquestração precisa entrar em operação.

- Os fluxos de operação existentes continuam funcionando?
- Como a versão se comporta diante de falhas e mudanças de topologia?
- É possível retornar à versão anterior se algo der errado?

Evidência esperada: comparação entre versões em um cenário representativo da rede.

Problema: Validação de um procedimento de mudança

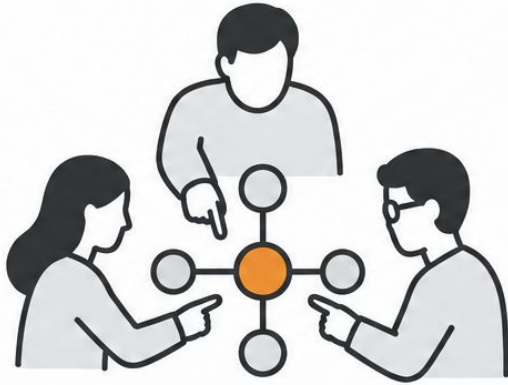
Uma solicitação de mudança chega para revisão técnica.



- Os pré-requisitos e a sequência de execução estão corretos?
- Quais serviços e dependências podem ser afetados?
- Os testes de aceitação e o procedimento de reversão funcionam?

Evidência esperada: ensaio da mudança para apoiar o revisor técnico da GMUD

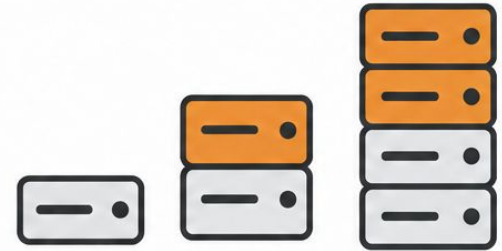
Motivação e missão



Colaboração

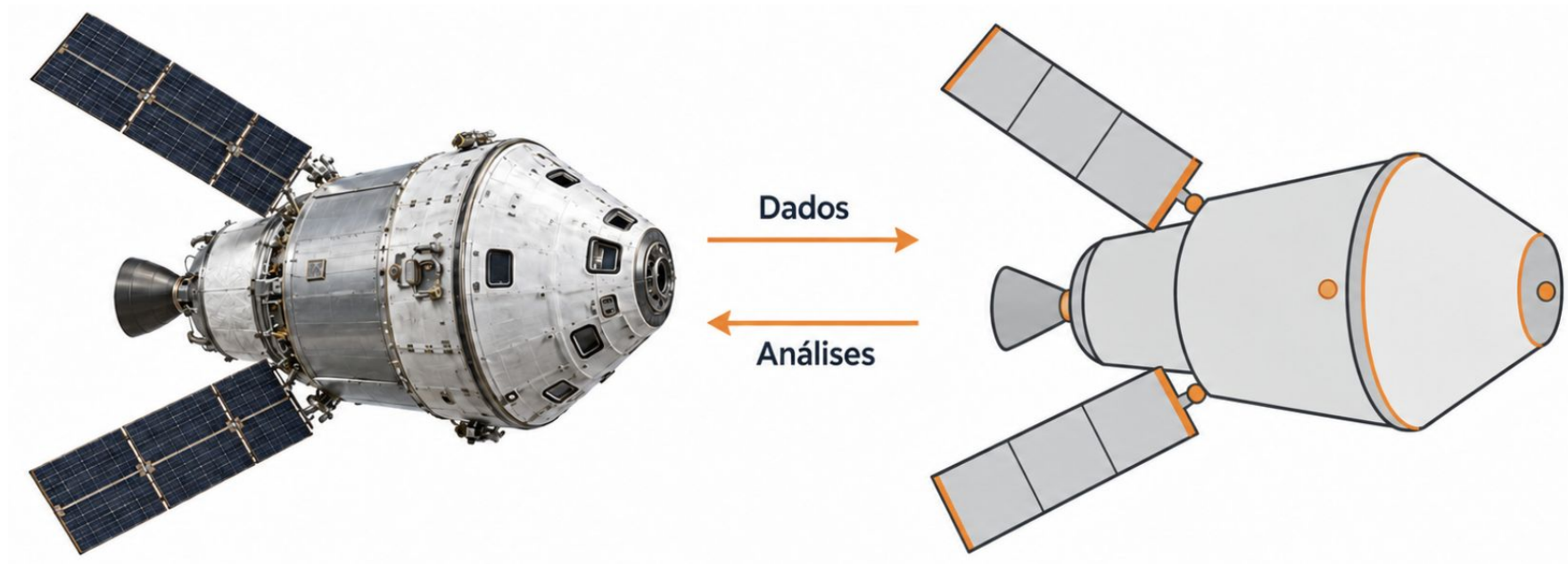


Replicabilidade



Escalabilidade

Gêmeos Digitais



Termo cunhado por John Vickers (2010) / NASA, conceito introduzido por Michael Grieves em 2002

Uso de gêmeos digitais nas práticas de cibersegurança



Para cada experimento, precisamos definir:

- Qual ambiente real serve de referência
- Quais topologias, configurações e comportamentos serão representados
- Quais correspondentes de software dos componentes do seu ambiente

O teste oferece evidências sobre aquilo que consequimos representar

Alternativas para montar o ambiente

Computador próprio

- Capacidade (memória e processamento) e segurança/disponibilidade

Laboratório dedicado, físico ou virtual

- Aquisição e capacidade, instalação de software, manutenção e acesso compartilhado

Infraestrutura de nuvem

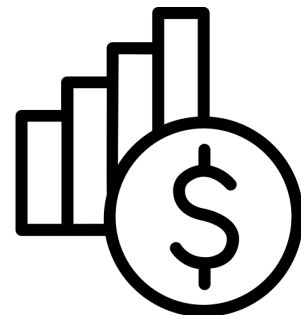
- Provisionamento, integração, controle de custos e operação

Soluções de Cyber Range comerciais

- Adequação dos exercícios e liberdade para modificar topologias e ferramentas

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**.



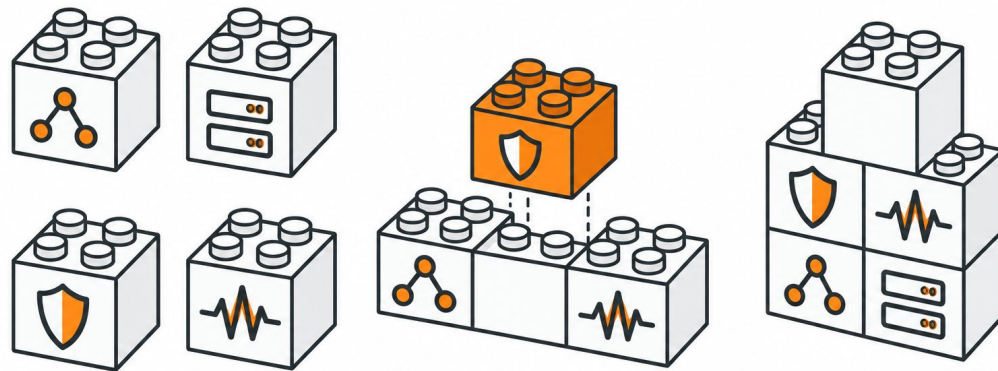
Instalação (50u)
R\$ 360.000,00

Manutenção (5y)
R\$ 240.000,00

R\$ 600.000,00

<http://bit.ly/44SQhBV>

Infraestruturas de Testbed



Infraestruturas de experimentação como base para montar o ambiente desejado

Idéia: combinar topologias, serviços, ferramentas de segurança e fontes de tráfego conforme o objetivo do teste.

- Laboratório Nacional Multiusuário da RNP [1]
- FABRIC [2] e NRP [3]
- Infraestrutura própria com Kubernetes (cloud ou *on-premise*)

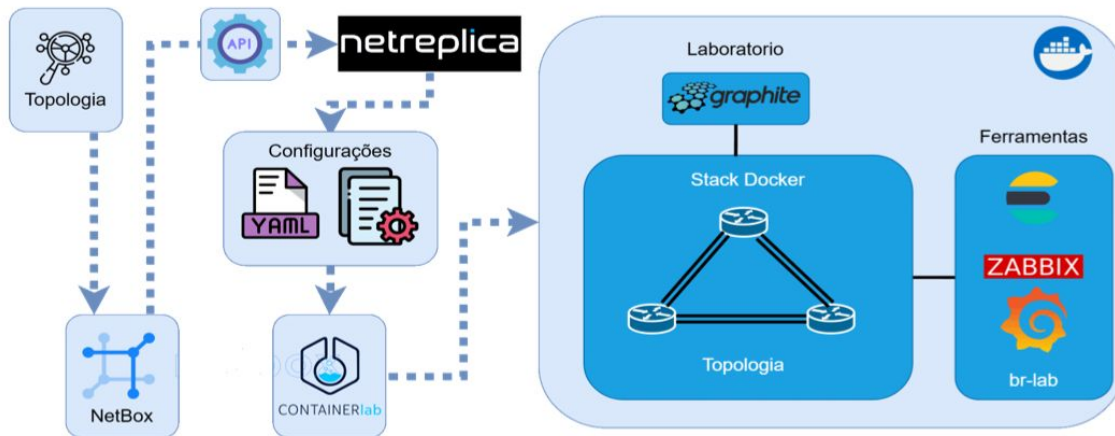
A infraestrutura fornece recursos. O cenário define como esses recursos se combinam para responder à pergunta do experimento.

Projeto Redes Abertas RNP

27^o
Workshop
RNP

LabRedes - Gêmeo Digital das Redes da RNP

Arquitetura



Netbox: Source of Truth

Containerlab: Laboratórios Virtuais de Rede

Netreplica: Automação e Integração entre Netbox/Containerlab

Projeto Redes Abertas RNP

27^o
Workshop
RNP

LabRedes - Gêmeo Digital das Redes da RNP

ContainerLab - Plataformas Suportadas

NOKIA - Srl - vr-sros	JUNIPER NETWORKS - vjunos - crpd - vr-vmx - vr-vqfx	ARISTA - ceos - vr-ceos	cisco - vr-n9kv - vr-csr - vr-xrv9k - xrd	ixia keysight_ixia-c
SONiC - Sonic-vs - frr	cvx	paloalto NETWORKS vr-pan	DELL vr-ftsov	MikroTik vr-ros
HUAWEI VRP	Extreme networks Virtual EXOS	ipinfusion ipinfus...	CHECK POINT checkpoint_cloudgard	

Legenda: Gratuito Gratuito com conta disponível com contrato



E pode melhorar?

HackInSDN - software tupiniquim

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

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

Produção de conteúdo baseado
em **Economia compartilhada**

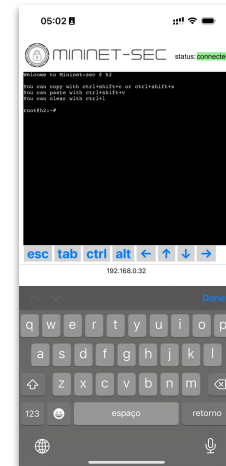
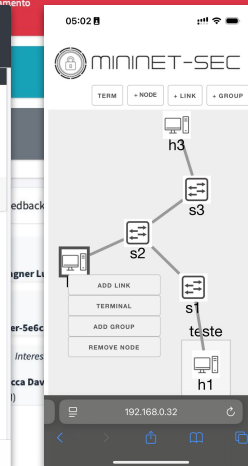
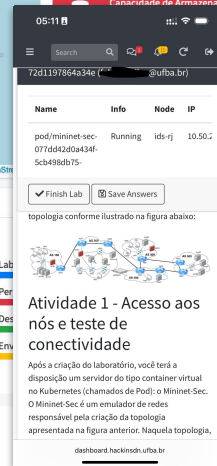
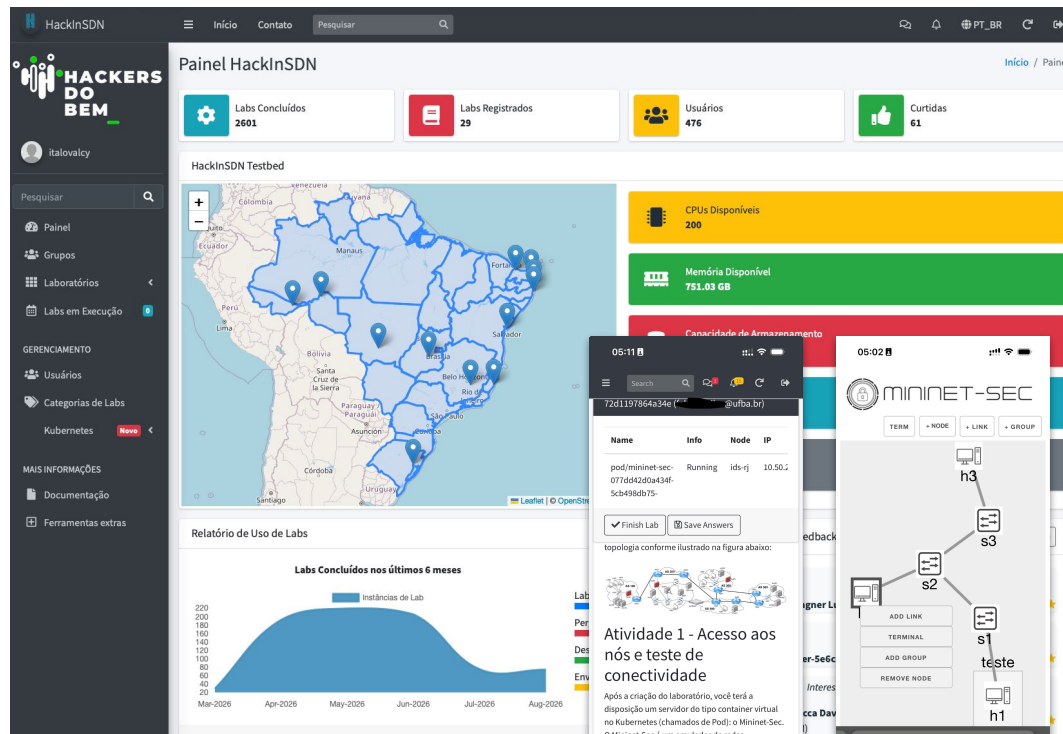
Trilhas de formação customizadas para
o perfil do usuário e **certificações**

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

Integração com LMS (Moodle) via LTI,
Telemetria de Aprendizagem (analytics)



Serviço em nuvem, autenticação federada e fácil acesso



HackInSDN

Projeto opensource, ativamente mantido, testado em cenários diversos e com uma comunidade em pleno crescimento

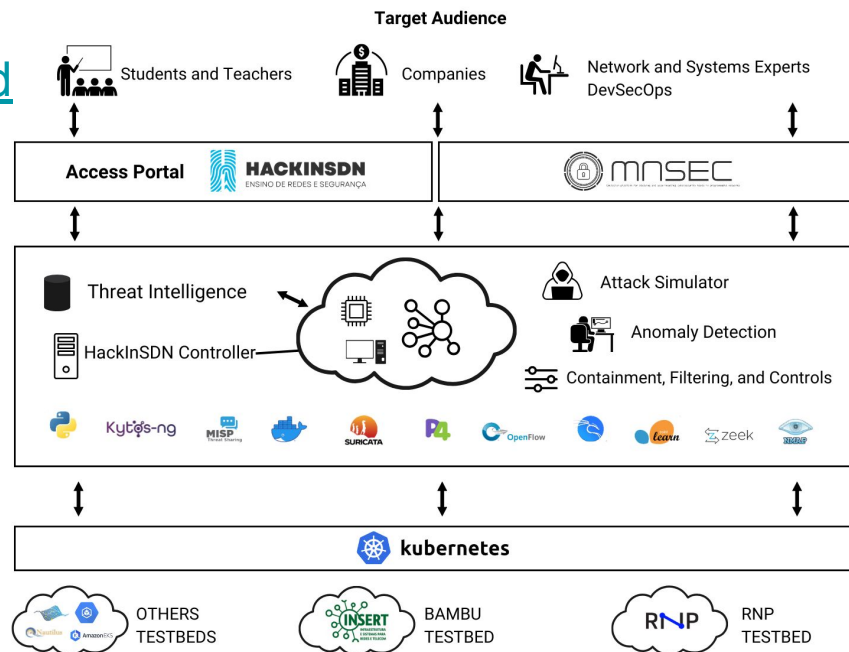
- <https://github.com/hackinsdn/dashboard>
- <https://hackinsdn.ufba.br/>

Ambientes disponíveis:

- Testbed RNP

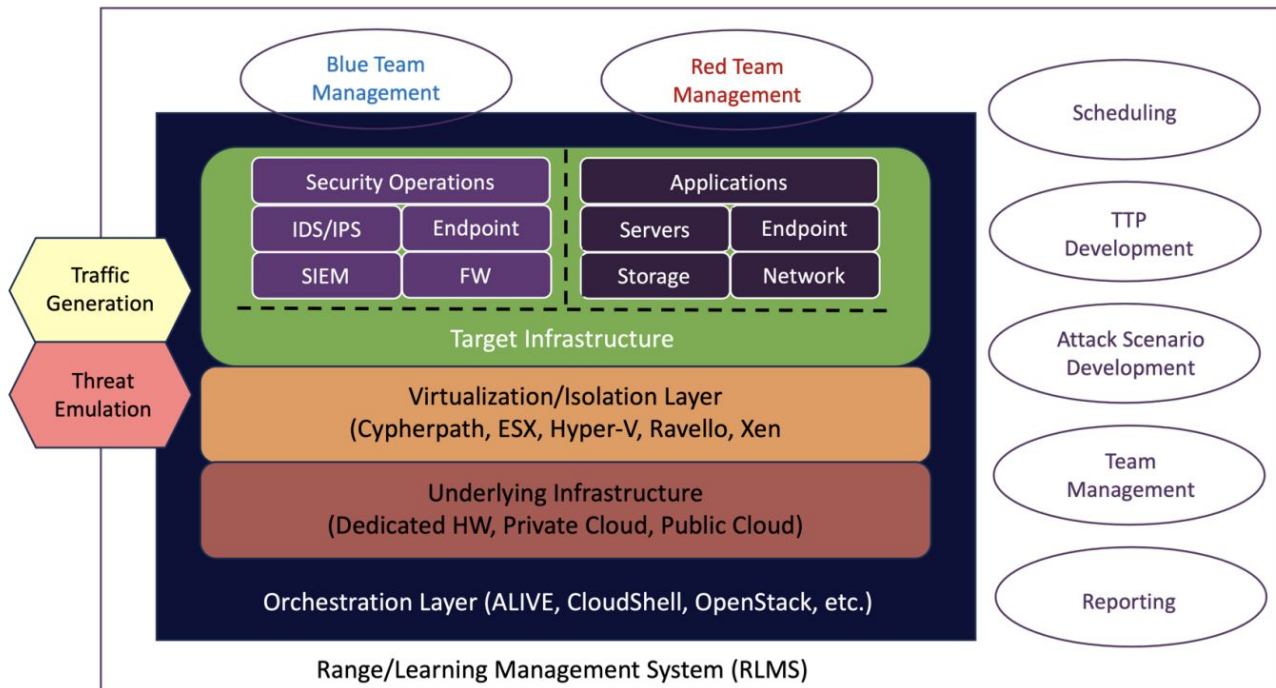
<https://dashboard.hackinsdn.ufba.br>

- BAMBU



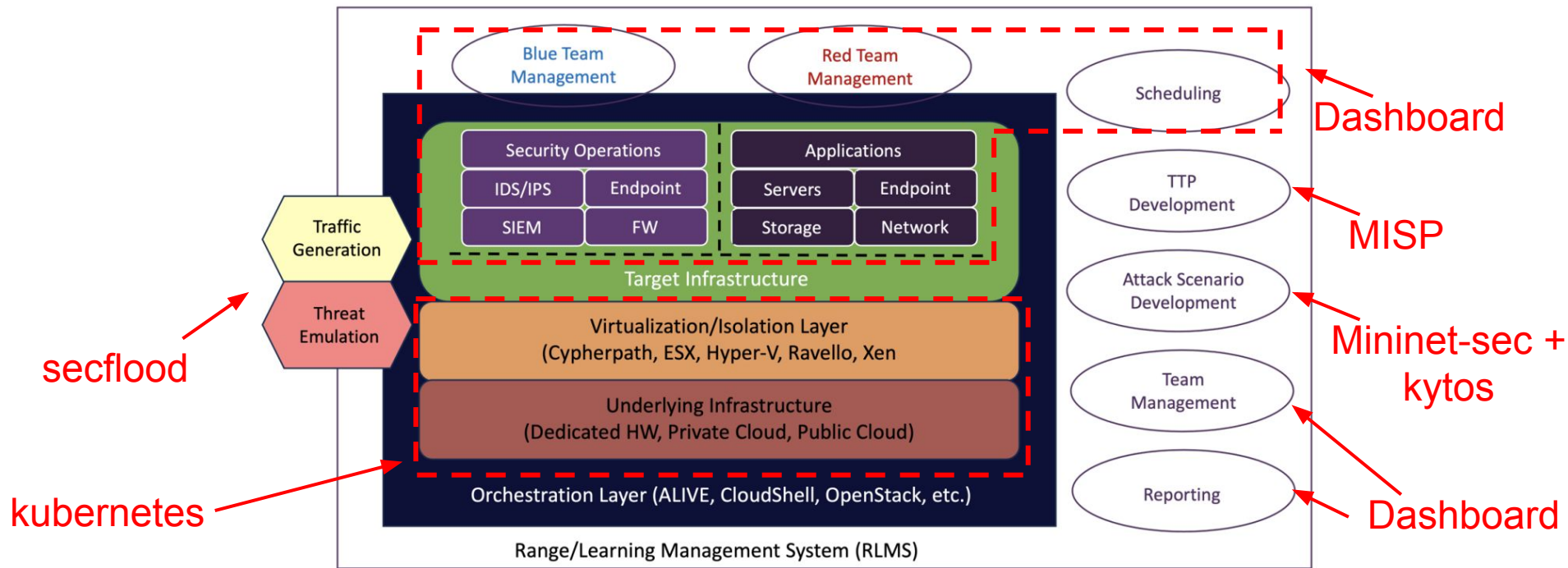
Gêmeos Digitais no HackInSDN

NISP publicou um guia de cyber ranges que trata justamente da relação entre infraestrutura, escalabilidade, custo e fidelidade



Gêmeos Digitais no HackInSDN

NISP publicou um guia de cyber ranges que trata justamente da relação entre infraestrutura, escalabilidade, custo e fidelidade



Caso de uso 1: validação de vulnerabilidade

Caso de uso 1: validação de vulnerabilidade

```
italo@megalossauro ~> git clone https://github.com/hackinsdn/labs hackinsdn-labs
Cloning into 'hackinsdn-labs'...
remote: Enumerating objects: 1331, done.
remote: Counting objects: 100% (298/298), done.
```

Caso de uso 1: validação de vulnerabilidade

```
italo@megalossauro ~> git clone https://github.com/hackinsdn/labs hackinsdn-labs
Cloning into 'hackinsdn-labs'...
remote: Enumerating objects: 1331, done.
remote: Counting objects: 100% (298/298), done.
```



Good morning, Italo Valcy

Você pode por favor criar um manifesto do HackInSDN para um lab pra eu validar a vulnerabilidade CVE-2026-60137 com base nos exemplos disponíveis em `/Users/italo/hackinsdn-labs ?`

+



Project or folder ▾ Output ▾

Opus 5.5 Medium Manual

Caso de uso 1: validação de vulnerabilidade

HackinSDN manifesto para CVE-2026-60137

List files in hackinsdn-labs directory >

Essa pasta está no seu computador, não no ambiente de nuvem onde eu trabalho. Vou pedir acesso à pasta no seu Mac para poder ver os exemplos.

Read 8 files, requested access to a folder on your computer, and 2 more steps >

Entendi bem o formato. O padrão (labs 02/03/05/06) é: um `ConfigMap` com a topologia mininet-sec (hosts, switches, links), um `Deployment` do mininet-sec com os placeholders `${pod_hash}` / `${allowed_nodes}`, e um `Service` NodePort.

O detalhe que me falta é a CVE em si. CVE-2026-87902 é posterior ao meu conhecimento (jan/2026), então preciso descobrir qual software/versão ela afeta para montar a topologia (imagem vulnerável, portas, atacante). Vou pesquisar.

Read 2 pages, searched the web >

Já tenho o que preciso sobre a CVE. Resumo: CVE-2026-87902 é um path traversal / LFI não autenticado no **WordPress Core (4.7.0 a 7.1.1, corrigido no 7.1.2)** que leva a RCE condicional, explorado via parâmetro `pagename` com traversal codificado (`%252f...`) combinado com um `page_id` válido, quando o tema tem um diretório `page=*`, o PHP está com `register_argc_argv` habilitado e existe um `pearcmd.php` acessível.

O padrão dos seus labs (como o lab02-sqli) é um pod atacante `secflood` + o alvo vulnerável, tudo dentro do mininet-sec. Antes de escrever o manifesto, só preciso confirmar um ponto que muda bastante o YAML — qual imagem do alvo WordPress usar:

Qual imagem de container devo usar para o alvo WordPress vulnerável no manifesto?

WordPress oficial + MariaDB separado

Qual host atacante incluir na topologia?

Host Linux simples (kali/attacker)

Manifesto do HackinSDN foi estruturado e documentado. >

Perfeito: WordPress oficial + MariaDB separado, com um host atacante Linux simples. Vou escrever o manifesto seguindo o padrão do lab02 (ConfigMap com a topologia + Deployment + Service) e gravá-lo numa nova pasta de lab no seu repositório.

Created a file, used Computer, and 2 more steps >

Pronto. Criei o manifesto em `hackinsdn-labs/lab07-wordpress-cve-2026-87902/manifest.yaml`, seguindo o mesmo formato do lab02-sqli (ConfigMap com a topologia mininet-sec + Deployment + Service, com os placeholders `${pod_hash}`, `${allowed_nodes}` e `${allowed_nodes_str}`).

A topologia tem três hosts num switch `s1`:

- **atacante** (192.168.0.10) — host Linux simples, de onde você dispara o payload com `curl/muclei`
- **wordpress** (192.168.0.20, k8spod, publish: 8080:80) — o alvo vulnerável, com as variáveis de conexão ao banco
- **mariaadb** (192.168.0.30, k8spod) — banco do WordPress

HackinSDN manifesto para CVE-2026-60137

por favor, pode procurar por uma imagem do wordpress que já esteja vulnerável no docker hub?

Vou procurar no Docker Hub por imagens de WordPress já preparadas como vulneráveis.

Read 3 pages, searched the web >

A imagem oficial `wordpress` mantém 68 páginas de tags, incluindo versões antigas com variantes Apache. Deixa eu confirmar tags reais dentro do range vulnerável (4.7.0-7.1.1) via API do Docker Hub.

Read 2 pages, ran a command >

Confirmado. Resumo da busca:

Não existe imagem pública dedicada à CVE-2026-87902 — a CVE é de setembro/2026, recente demais, e as imagens "vulnerable-wordpress" de terceiros no Docker Hub são para outras falhas (ex: `rkw6467/vulnerable-wordpress-image` é do plugin *Photo Gallery*, CVE-2019-8943; `securecodebox/old-wordpress` e `vulhub/wordpress-4.6-rce` miram outras CVEs antigas). Nenhuma traz as pré-condições específicas desta CVE.

Mas como a CVE-2026-87902 é no **WordPress Core** (não num plugin), a rota mais confiável é usar a **imagem oficial** `wordpress` com uma tag de versão dentro do range vulnerável (4.7.0-7.1.1). Confirmer que essas tags antigas existem de verdade, por exemplo:

- `wordpress:5.9-php7.4-apache` (bem dentro do range; PHP 7.4)
- `wordpress:5.9-php8.1-apache`
- `wordpress:6.5.5-php8.2-apache`

Vou atualizar o manifesto para usar `wordpress:5.9-php7.4-apache`, que é uma versão comprovadamente no range e com o PHP mais fácil de ajustar as pré-condições (`register_argc_argv`, `PEAR`).

Edited a file, read a file, saved files to your computer >

Atualizei o manifesto no seu repositório (`lab07-wordpress-cve-2026-87902/manifest.yaml`).

Conclusão da busca: **não há imagem pública já preparada para a CVE-2026-87902** — é recente demais (set/2026), e as imagens "vulnerable-wordpress" que existem no Docker Hub são para outras falhas (plugins/versões antigas). Como esta CVE é no **WordPress Core**, o caminho confiável é a **imagem oficial** numa versão dentro do range 4.7.0-7.1.1. Troquei a tag para `wordpress:5.9-php7.4-apache`, que confirmei existir no Docker Hub e está bem dentro do range.

Fica uma ressalva importante: a versão vulnerável garante o **LFI/path traversal**, mas a **RCE completa** ainda depende das três pré-condições (tema com diretório `page=*`, `register_argc_argv` ligado e `pearcmd.php` presente). O `postStart` no manifesto cobre isso de forma best-effort, mas se você quiser um lab 100% reproduzível, o ideal é um `Dockerfile` derivando de `wordpress:5.9-php7.4-apache` com as condições embutidas — posso montar esse Dockerfile se quiser.

Tempo total:
6min



Change topology layout:

Show interface names

☐ enabled

☒ disabled

Change node data:

Node Data JSON: Edge Data JSON:

Dashboard

Users

Users (24) | Administrator (24)

Bulk actions: [v] Apply Change role to...: [v] Change

24 items 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

☐	Username	Name	Email	Role	Points
☐	administrator2	—	administrator2@wp2bhai.in	Administrator	0
☐	awright	—	awright27604@170.38.8.74	Administrator	3
☐	awright27604	—	awright27604@170.38.8.74	Administrator	0
☐	cachepopad588	—	cachepopad588@gmail.com	Administrator	0
☐	hellan	—	hrellap@gmail.com	Administrator	0
☐	mail	—	javascrpt@ets.facebook.com	Administrator	0
☐	Nh_53684747u95	—	Nh_53684747u95@wp2bhai.in	Administrator	0
☐	Nh_536848584284	—	Nh_536848584284@wp2bhai.in	Administrator	0
☐	site_admin	—	site_admin@wp2bhai.in	Administrator	0
☐	wp2_02491675502b	—	wp2_02491675502b@wp2bhai.local	Administrator	0
☐	wp2_3275c5d8f9	—	wp2_3275c5d8f9@wp2bhai.local	Administrator	0
☐	wp2_73a48c883d77	—	wp2_73a48c883d77@wp2bhai.local	Administrator	0
☐	wp2_service_424290	—	wp2_service_424290@wp2bhai.local	Administrator	0
☐	wp2_2446cd0962b4	—	wp2_2446cd0962b4@wp2bhai.in	Administrator	0
☐	wp2_098408c63a7	—	wp2_098408c63a7@wp2bhai.in	Administrator	0
☐	wp2_279a0977284	—	wp2_279a0977284@wp2bhai.in	Administrator	0
☐	wp2_36c6d75dc04	—	wp2_36c6d75dc04@wp2bhai.in	Administrator	0

```

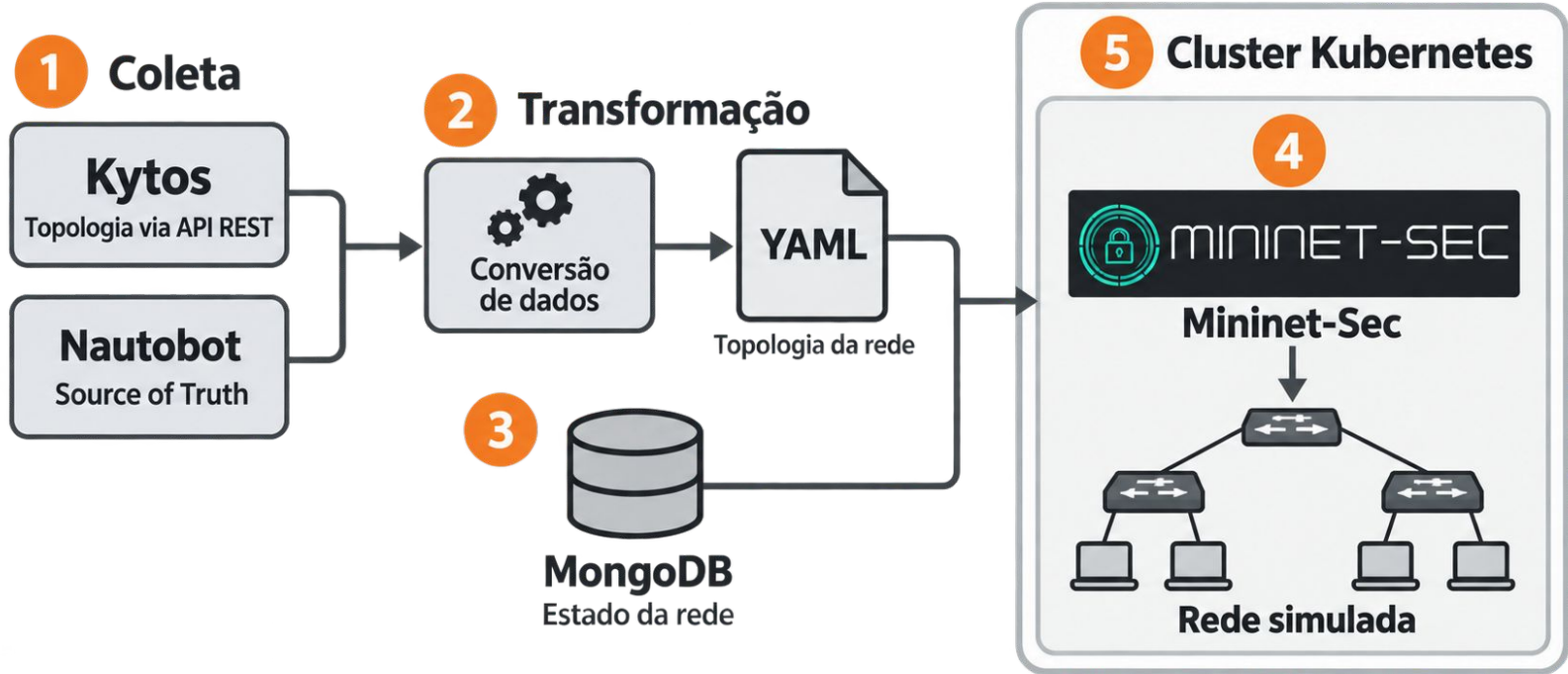
--
\ \      / /  _ _ \ / _ _ |
\ \ / \ / / | _ _ | ( _ _ _ _ _ _ _ _ _ _ ®
\ \ / \ / / | _ _ _ \ _ _ \ / _ _ | / _ _ | ' _ \
\ \ / \ / / | _ _ _ _ _ | ( _ _ | ( _ | | | | |
\ \ / \ / / | _ _ _ _ _ | _ _ _ \ _ _ | _ _ | | _ |
\ \ / \ / / | _ _ _ _ _ | _ _ _ \ _ _ | _ _ | | _ |

WordPress Security Scanner
Version 4.1.0
An Automattic endeavor
https://automattic.com

-----

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[i] Updating the Database ...
[i] Update completed.
```

Caso de uso 2: teste de uma nova versão



Caso de uso 2: teste de uma nova versão

HackInSDN

**HACKERS
DO
BEM**

 italovalcy



 Painel

 Grupos

 Laboratórios ▾

☐ Ver Labs

☐ Criar Lab

☐ Respostas dos Labs

☐ Gabarito

☐ Labs Concluídos

Run LabHome / Labs / Run Lab

Lab -- AmLight + Kytos Prod Digital Twin

Overall information

User label

italo@amlight.net

Lab category

Lab execution

Lab Duration/Expiration

4 hours ▾

Custom variables

Variable name	Value

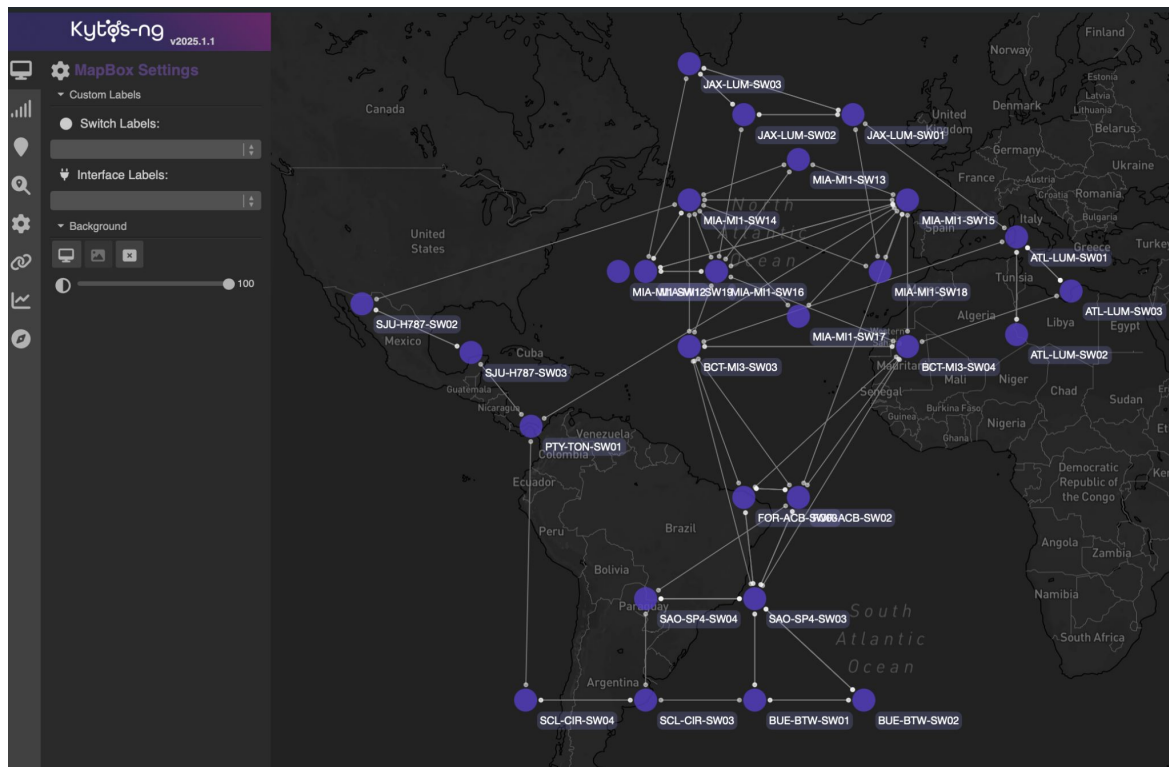
+ Add more answers

Save answer sheet

Run



Caso de uso 2: teste de uma nova versão



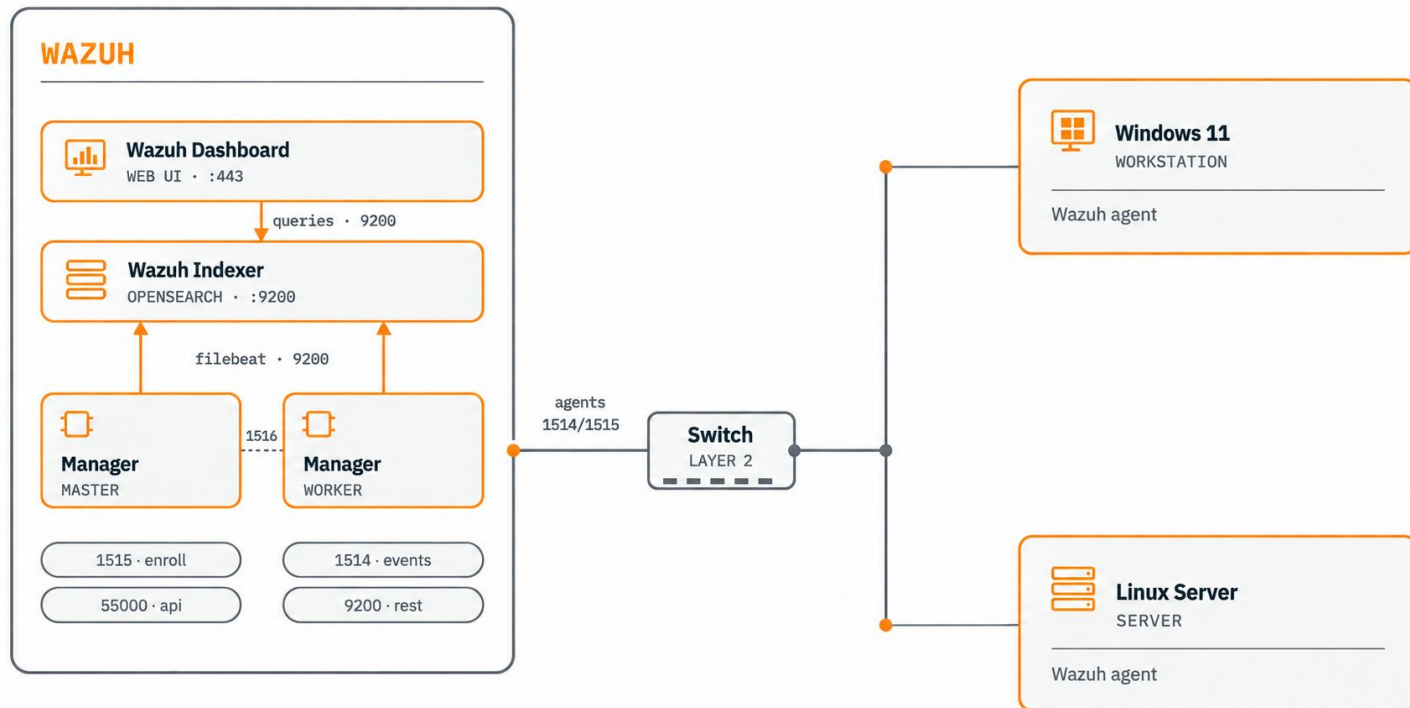
Caso de uso 3: PoC de soluções de segurança

- Laboratório de Análise de vulnerabilidade com Wazuh e IA



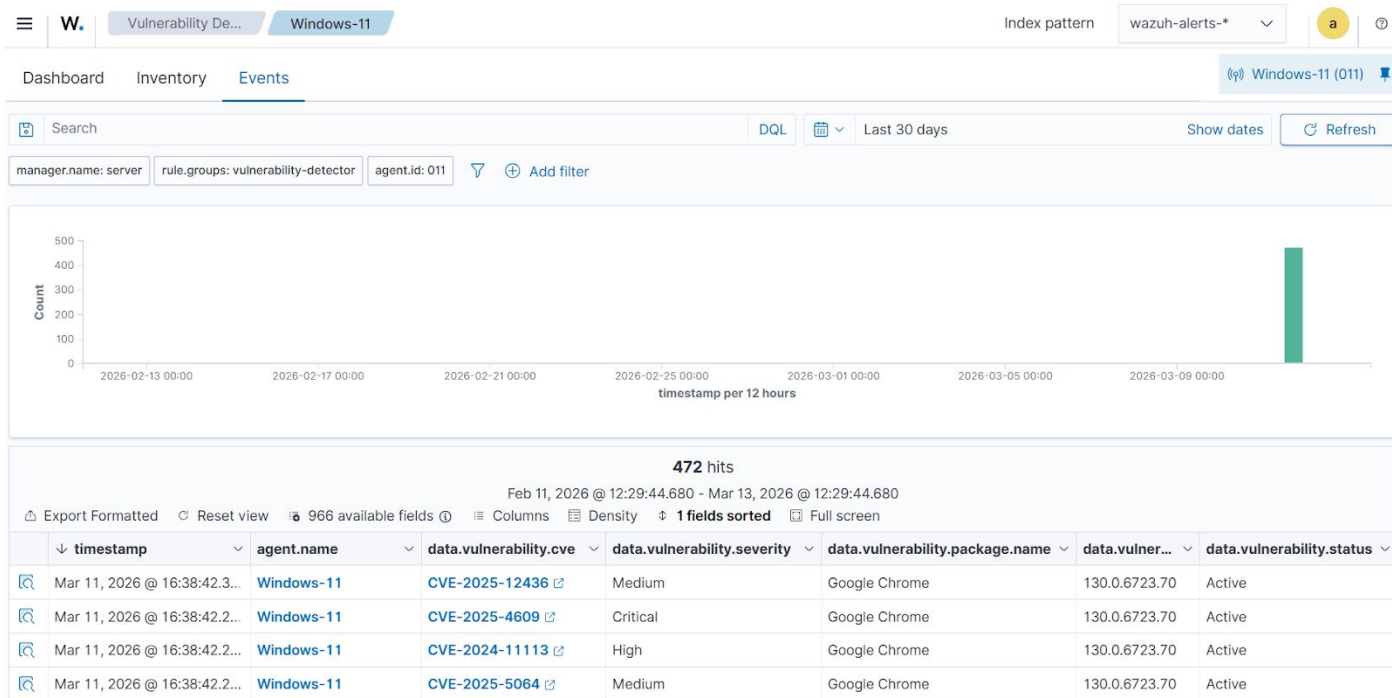
Caso de uso 3: PoC de soluções de segurança

- Passo 1: executar topologia no HackInSDN



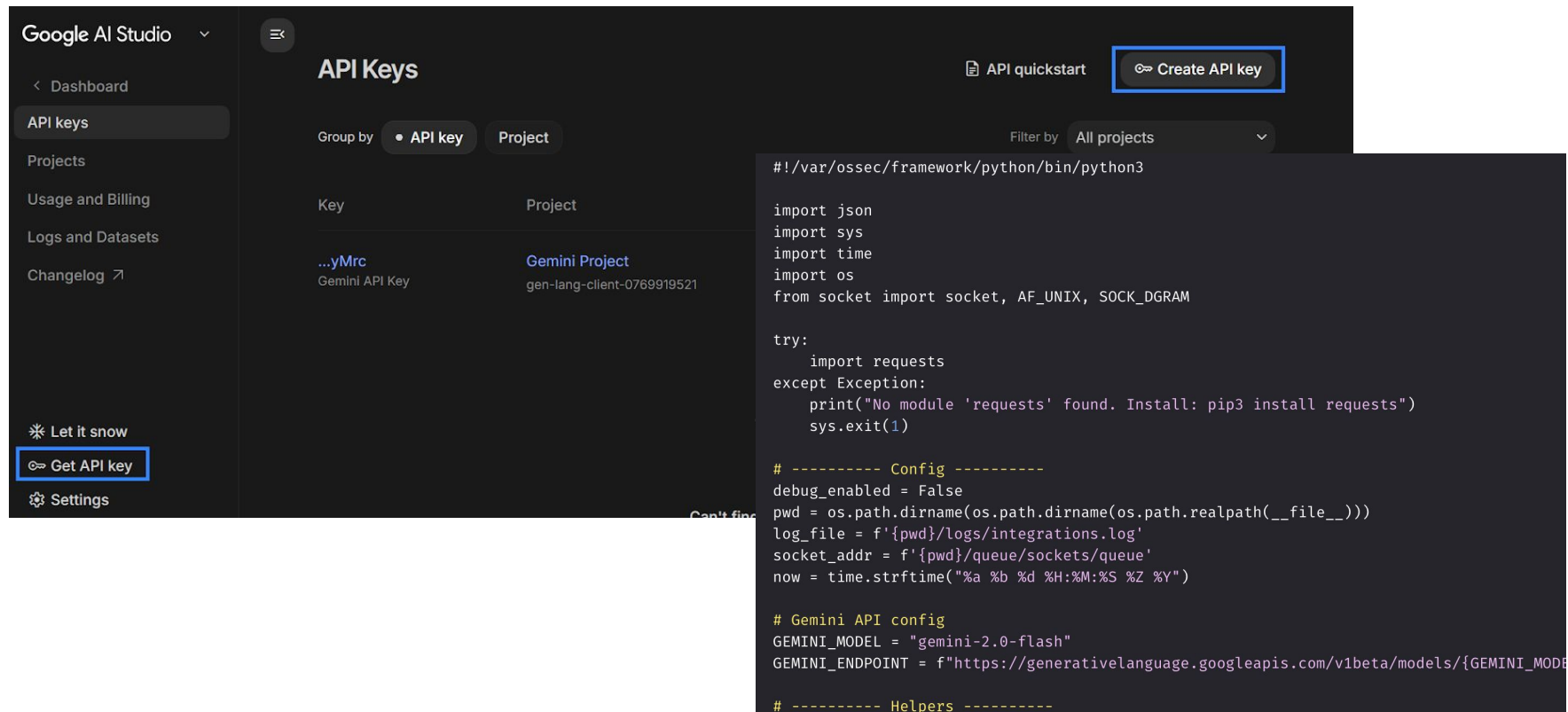
Caso de uso 3: PoC de soluções de segurança

- Passo 2: setup do wazuh e adicionar o Wazuh agent no host Windows-11



Caso de uso 3: PoC de soluções de segurança

- Passo 3: conta gratuita no Google Gemini e script de integração wazuh



The image shows the Google AI Studio interface for managing API keys. On the left, a sidebar contains navigation links: Dashboard, API keys (selected), Projects, Usage and Billing, Logs and Datasets, and Changelog. The main area is titled 'API Keys' and shows a table with columns 'Key' and 'Project'. A single key is listed: '...yMrc' (Gemini API Key) associated with the 'Gemini Project' (gen-lang-client-0769919521). A 'Create API key' button is highlighted in the top right. In the bottom left, a 'Get API key' button is also highlighted. Overlaid on the right is a Python script for Wazuh integration, which includes imports for json, sys, time, and os, and uses the Gemini API to fetch data.

Google AI Studio

< Dashboard

API keys

Projects

Usage and Billing

Logs and Datasets

Changelog ↗

✳ Let it snow

🔑 Get API key

⚙ Settings

API Keys

API quickstart

Create API key

Group by • API key Project

Filter by All projects

Key	Project
...yMrc Gemini API Key	Gemini Project gen-lang-client-0769919521

```
#!/var/ossec/framework/python/bin/python3

import json
import sys
import time
import os
from socket import socket, AF_UNIX, SOCK_DGRAM

try:
    import requests
except Exception:
    print("No module 'requests' found. Install: pip3 install requests")
    sys.exit(1)

# ----- Config -----
debug_enabled = False
pwd = os.path.dirname(os.path.dirname(os.path.realpath(__file__)))
log_file = f'{pwd}/logs/integrations.log'
socket_addr = f'{pwd}/queue/sockets/queue'
now = time.strftime("%a %b %d %H:%M:%S %Z %Y")

# Gemini API config
GEMINI_MODEL = "gemini-2.0-flash"
GEMINI_ENDPOINT = f"https://generativelanguage.googleapis.com/v1beta/models/{GEMINI_MODEL}"

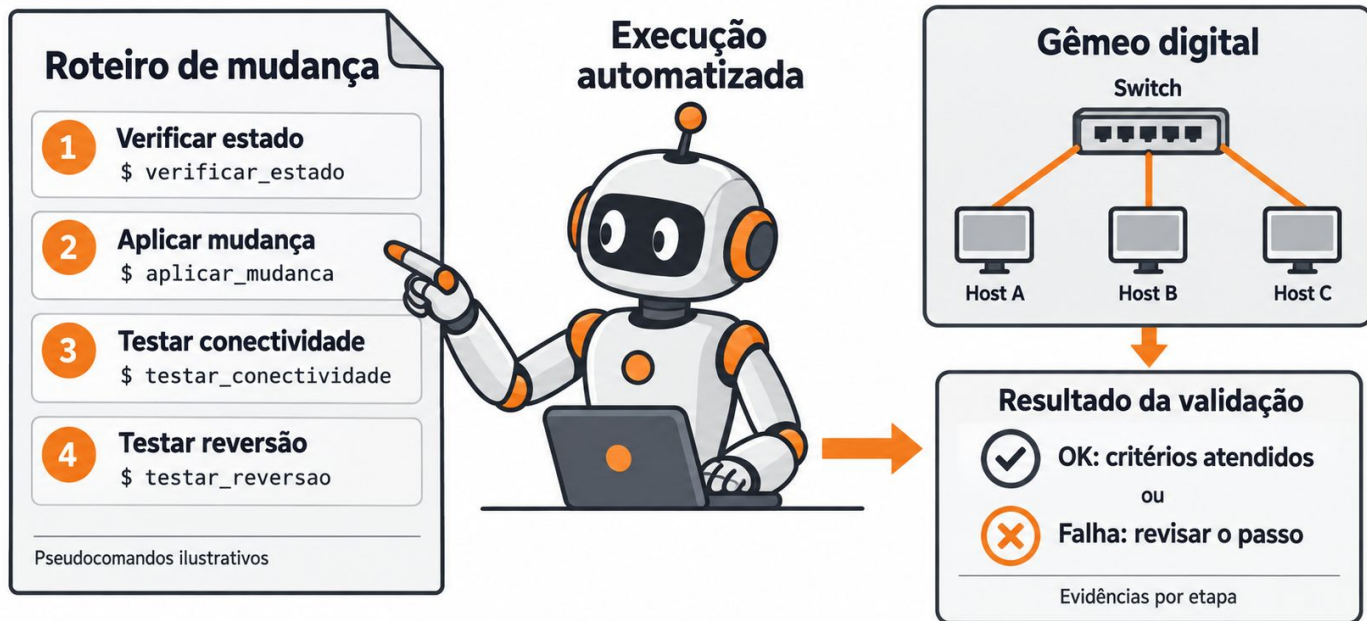
# ----- Helpers -----
```

Caso de uso 3: PoC de soluções de segurança

- Passo 4: checar os detalhes dos alertas

W.	Discover	wazuh-alerts-4.x-2026.03.17#LXT7-pwBXvIwIF2G-S-9	a	?
t	data.gemini.source.cve	CVE-2026-3926		
t	data.gemini.source.description	CVE-2026-3926 affects Google Chrome		
t	data.gemini.source.groups	vulnerability-detector		
t	data.gemini.source.level	10		
t	data.gemini.source.location	vulnerability-detector		
t	data.gemini.source.mitre	null		
t	data.gemini.source.reference	https://cti.wazuh.com/vulnerabilities/cves/CVE-2026-3926		
t	data.gemini.source.rule	23505		
t	data.gemini.source.severity	High		
t	data.gemini.source.timestamp	2026-03-17T08:44:48.949+0000		
t	data.gemini.source.vendor_reference	https://issues.chromium.org/issues/478659010, https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html		
t	data.gemini.summary	A CVE-2026-3926 é uma vulnerabilidade de alta gravidade no Google Chrome relacionada a uma leitura fora dos limites no mecanismo JavaScript V8. Um atacante remoto pode explorá-la por meio de uma página HTML maliciosa para potencialmente acessar informações sensíveis, modificar dados ou causar uma negação de serviço. A exploração não exige privilégios, mas requer interação do usuário, como visitar a página preparada. **Urgência da correção: Alta.** Devido à alta pontuação CVSS, ao vetor de ataque pela rede e ao potencial de alto impacto na confidencialidade, integridade e disponibilidade, a aplicação da correção deve ser priorizada. **Etapas de correção:** Atualize o Google Chrome para a versão 146.0.7680.71 ou posterior. Verifique se a versão atualizada está instalada após o processo de atualização.		
t	data.integration	custom-gemini		
t	decoder.name	json		
t	id	1773737340.5549882		

Caso de uso 4: Auxiliar de revisor de GMUD



- Robô revisor do passo-a-passo que lê o roteiro da mudança, executa os passos no gêmeo digital e dá um veredito se está okay ou não
- **Em desenvolvimento!**

Fidelidade dos experimentos

Gêmeos, *pero no mucho*

Fidelidade das réplicas é proporcional ao custo!

- É viável construir gêmeos digitais de recortes operacionais da organização, combinando **containers**, **máquinas virtuais** e **appliances virtuais**

Melhor feito que perfeito!



Considerações finais

Gêmeos digitais é não é uma tecnologia ou sistema que você implanta, mas um **conceito** que você adota gradualmente para **validação do ambiente**

Passo importante em direção a **automação** e **laço fechado de orquestração**

HackInSDN oferece mecanismos para facilitar a criação de réplicas do ambiente para testes, treinamento, experimentos

- Ambiente disponível via Lab Nacional Multi-usuário RNP
- Possibilidade de implantação local (on-premise)
- Facilidade de criação de cenários (muitos exemplos + GenAI-friendly)



Obrigado!

Italo Valcy <idasilva@fiu.edu>
 <italovalcy@ufba.br>
 <italo@pop-ba.rnp.br>
 <italovalcy@gmail.com>

Agradecimentos

