INTEGRAÇÃO MISP E HACKINSDN

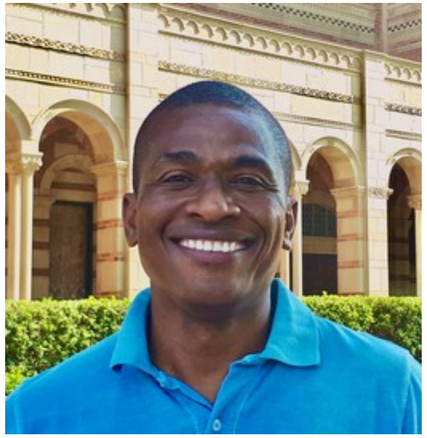
Italo Valcy (FIU)
Raquel Marques (PoP-BA/RNP)

AGENDA

EQUIPE DO HACKINSDN

Allan Freitas

Italo Valcy

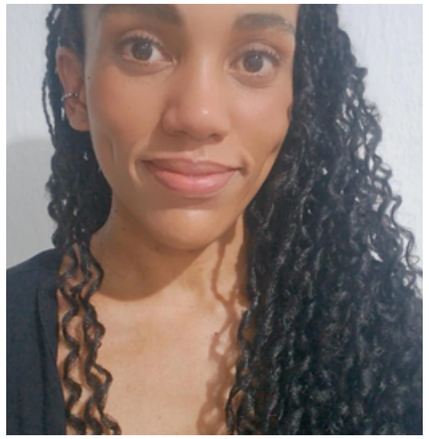


Leobino Sampaio

Gustavo Pinho

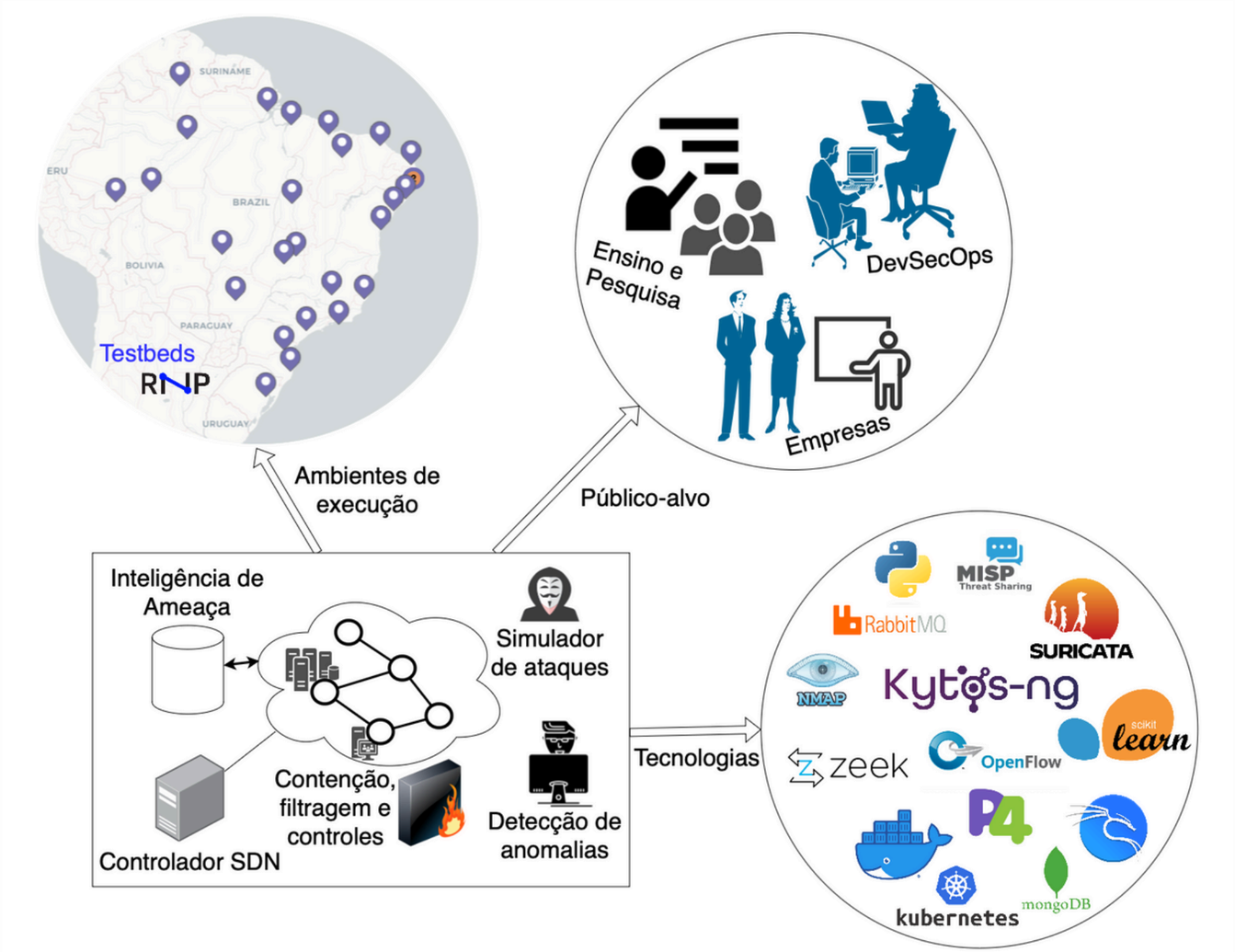
Henrique Queiroz

Mayara Rodrigues



Raquel Marques

Talita Rocha



GT HACKINSDN

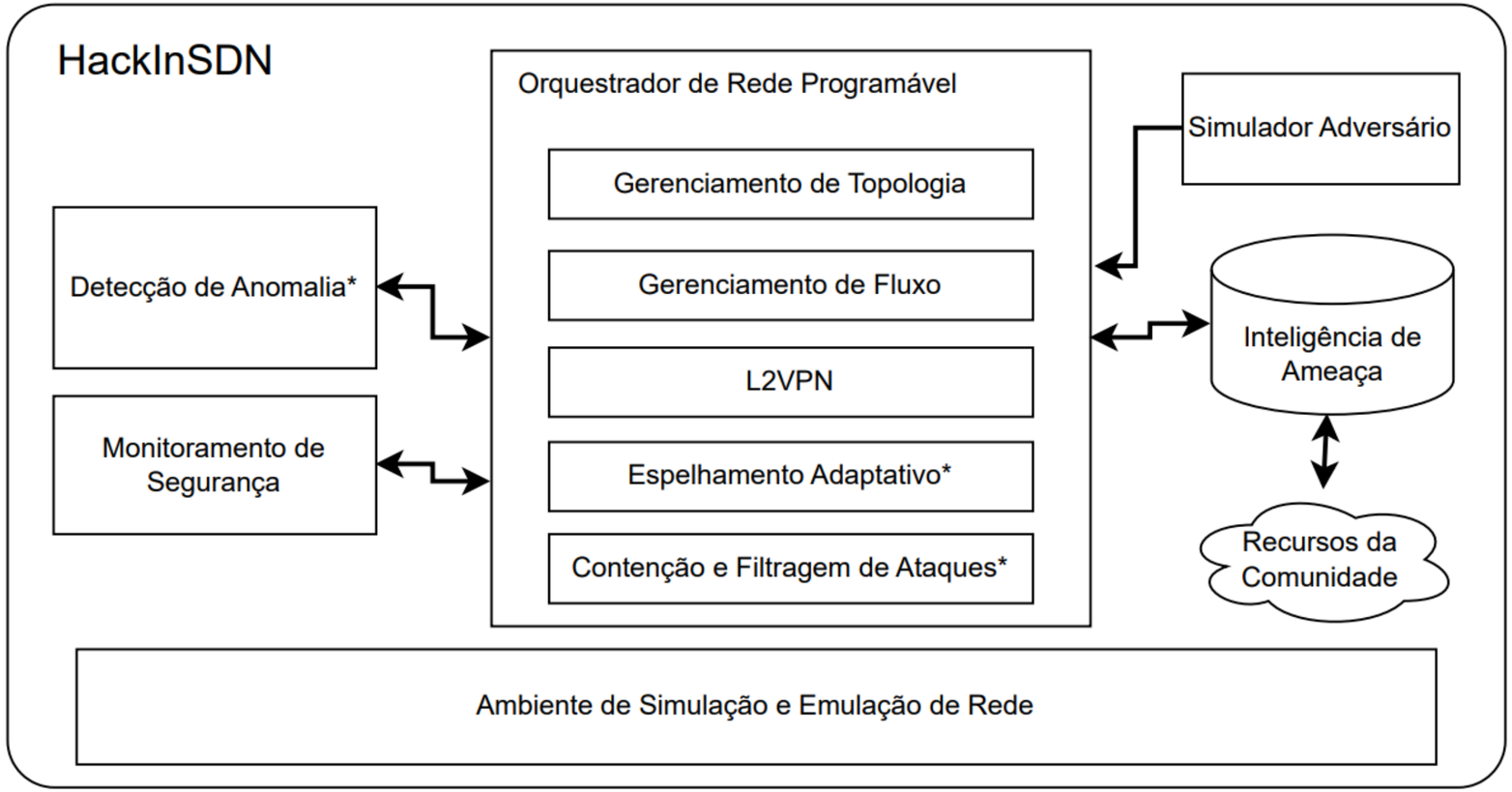
O HackInSDN - Infraestrutura programável em testbed para ensino de redes e segurança. O projeto foi contemplado na **Chamada Hackers do Bem**, chamada pública para Pesquisa e Desenvolvimento realizada em 2023.

HACKERS DO BEM · RNP · INSERT · UFBA · INSTITUTO FEDERAL Bahia · FIU FLORIDA INTERNATIONAL UNIVERSITY

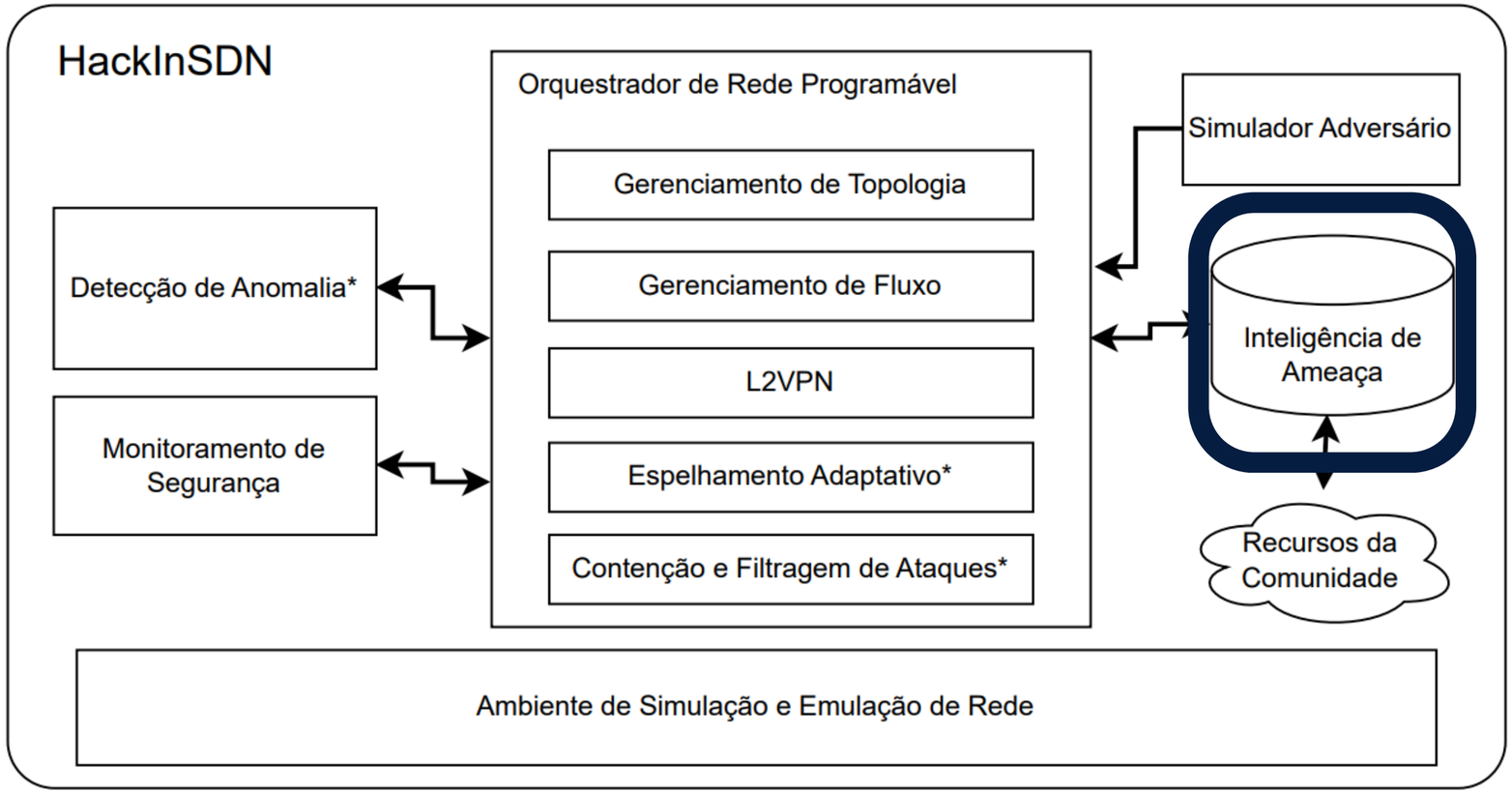
TLP:CLEAR

ARQUITETURA

- Flexível: baixo acoplamento dos módulos.
- Incremental: incorpora novos módulos sob demanda.
- Portável: amplo conjunto de usuários.
- Uso do HackInSDN para ensino de Segurança com SDN: Mais de 14 casos de uso mapeados



PAPEL DO MISP NA ARQUITETURA



- MISP vai armazenar informações de IoC identificadas pelos outros módulo.
- Compartilhamento de CTI para contenção antecipada.
- Aprimoramento dos outros módulos.
- Taxonomia de ataques, atributos, níveis de confiabilidade e confidencialidade dos dados

TLP:CLEAR

INTEGRAÇÃO COM O MISP

Dados inseridos no MISP

Os dados são coletados pelo módulo de monitoramento de segurança, além de outras fontes como: CERT.Bahia, CAUMA, OpenPhish, Serpro e Honeypot da AmLight/FIU.

Dados Exportados do MISP

Os IPs comprometidos são identificados nos feeds públicos (ex: CIRCL), e de comunidades conectadas (ex: Instância do CERT.Bahia e outras instâncias do HackInSDN), são usados para aprimorar os testes executados nos módulos da arquitetura.

Modelagem dos Dados

Os dados inseridos na instância do HackInSDN são classificados conforme o tipo de ameaça a que estão relacionados.

TLP:CLEAR

INTEGRAÇÃO COM O MISP

Monitoramento de Segurança

Contenção e Filtragem de Ataques

Simulador Adversário

Connected communities

Forma de Distribuição

CERT.Bahia
CaUMa
OpenPhish
Serpro
Honeypot da AmLight/FIU

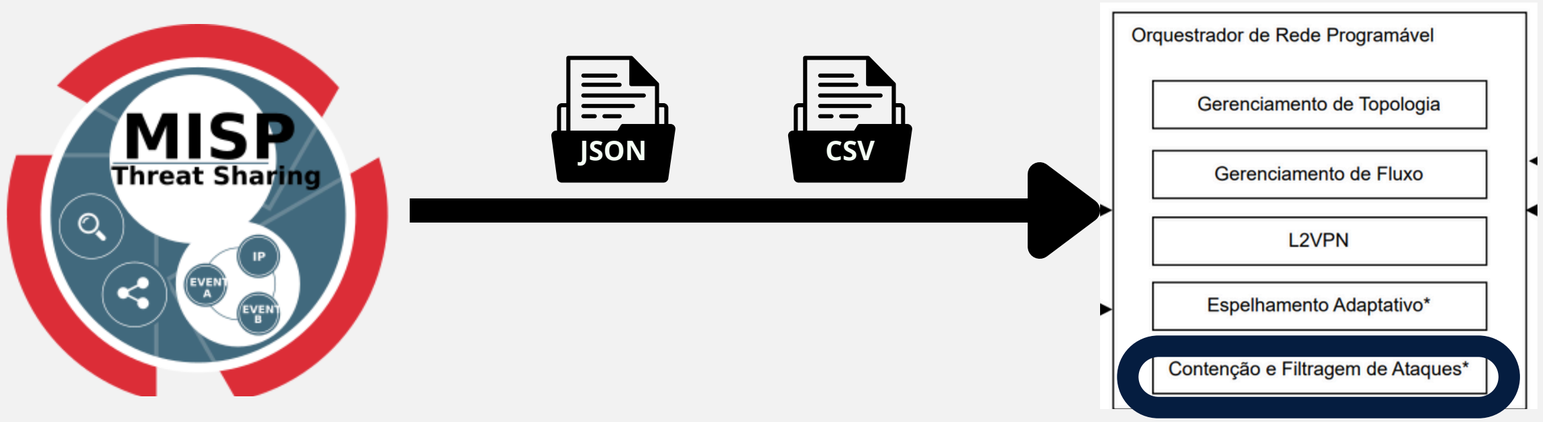
Fonte Externa dos Dados

PyMISP
csv export
json export
suricata export
json import
csv import

TLP:CLEAR

INTEGRAÇÃO COM O MISP

- **Integração com o módulo de contenção e filtragem de ataques:**




```
(teste) root@Kytos-NG:/home/kytos/contention# curl -H 'Content-type: application/json' -X POST
http://[redacted]/api/talitarp/contention/v1/contention -d '{"switch": "00:00:00:00:00:00:0
0:01", "interface": 1, "match": {"vlan": 100, "ipv4_src": "1[redacted]"}}'
"result: Contentation created successfully ID 1030a355e6c344"(teste) root@Kytos-NG:/home/kytos/
contention#
```

TLP:CLEAR

INTEGRAÇÃO COM O MISP

- **Integração com o módulo de monitoramento de segurança:**

```
pe:trojan-activity; sid:11098434; rev:1; priority:2; reference:url,https://localhost/events/view/1737;)
alert ip 4[redacted]1 any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: 4[redacted]";   class
type:trojan-activity; sid:11098444; rev:1; priority:2; reference:url,https://localhost/events/view/1737;)
alert ip [redacted]3 any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]";   cla
sstype:trojan-activity; sid:11098454; rev:1; priority:2; reference:url,https://localhost/events/view/1737;
)
alert ip [redacted] any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]";   cla
sstype:trojan-activity; sid:11098464; rev:1; priority:2; reference:url,https://localhost/events/view/1737;
)
alert ip [redacted] any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]";   c
lasstype:trojan-activity; sid:11098474; rev:1; priority:2; reference:url,https://localhost/events/view/173
7;)
alert ip [redacted]any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]";   class
type:trojan-activity; sid:11098484; rev:1; priority:2; reference:url,https://localhost/events/view/1737;)
alert ip [redacted] any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]';   class
type:trojan-activity; sid:11098494; rev:1; priority:2; reference:url,https://localhost/events/view/1737;)
alert ip 1[redacted] any -> $HOME_NET any (msg: "MISP e1737 [] Incoming From IP: [redacted]";   class
type:trojan-activity; sid:11098504; rev:1; priority:2; reference:url,https://localhost/events/view/1737;)
```

TLP:CLEAR

MODELAGEM DOS DADOS

Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
		1746	**Attack Pattern** Malicious Link - T1204.001 Phishing - T1566 Spearphishing Link - T1566.002 **attck4fraud** Fake Invoice Fraud Malware Phishing Scam Spear phishing	tlp:amber admiralty-scale:source-reliability="a" admiralty-scale:information-credibility="1" phishing:techniques="fake-website" malware_classification:malware-category="Virus" malware_classification:malware-category="Trojan" circl:incident-classification="phishing" circl:incident-classification="malware"	82	5	hackinsdn@ufba.br	2024-07-26	Urls Maliciosas-CAUMA	Organisation	

Scope toggle | Deleted | Decay score | Context | Related Tags | Filtering tool — Enter value to search

Date	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2024-07-26*	e60...b1b	Network activity	url	https://[redacted]			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	903...099	Network activity	url	http://[redacted]97d63681s			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	930...e60	Network activity	url	https://[redacted]n.php			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	98e...810	Network activity	url	https://dow[redacted]p			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	b3e...f4f	Network activity	url	http://2[redacted]/			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	18c...108	Network activity	url	https://log[redacted]/			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	23d...16d	Network activity	url	https://s[redacted]			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	31c...251	Network activity	url	http://c[redacted]n/			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		
2024-07-26*	3c7...d3f	Network activity	url	https://ar[redacted]			Feed Urls	✓	1718 1740 1741 1742 1743		✓	Inherit	(0/0/0)		

TLP:CLEAR

MODELAGEM DOS DADOS

- **Classificação por meio das taxonomias:**

TLP	
TAG1	iep2-policy:tlp="red"
TAG2	iep2-policy:tlp="amber"
TAG3	iep2-policy:tlp="green"
TAG4	iep2-policy:tlp="white"

Admiralty Scale	
TAG1	admiralty-scale:source-reliability="a"
TAG2	admiralty-scale:source-reliability="b"
TAG3	admiralty-scale:source-reliability="c"
TAG4	admiralty-scale:information-credibility="1"
TAG5	admiralty-scale:information-credibility="2"
TAG6	admiralty-scale:information-credibility="3"

CERT-XLM	
TAG1	CERT-XLM:information-gathering="social-engineering"
TAG2	CERT-XLM:fraud="phishing"
TAG3	CERT-XLM:malicious-code="virus"
TAG4	CERT-XLM:malicious-code="trojan-malware"
TAG5	CERT-XLM:availability="dos"
TAG6	CERT-XLM:availability="ddos"

social-engineering-attack-vectors	
TAG1	social-engineering-attack-vectors:technical="spear-phishing"
TAG2	social-engineering-attack-vectors:technical="phishing-and-trojan-email"
TAG3	social-engineering-attack-vectors:technical="spam-email"
TAG4	social-engineering-attack-vectors:non-technical="hoaxing"
TAG5	social-engineering-attack-vectors:non-technical="pretexting-impersonation"

Phishing	
TAG1	phishing:techniques="fake-website"
TAG2	phishing:techniques="email-spoofing"

TLP:CLEAR

MODELAGEM DOS DADOS

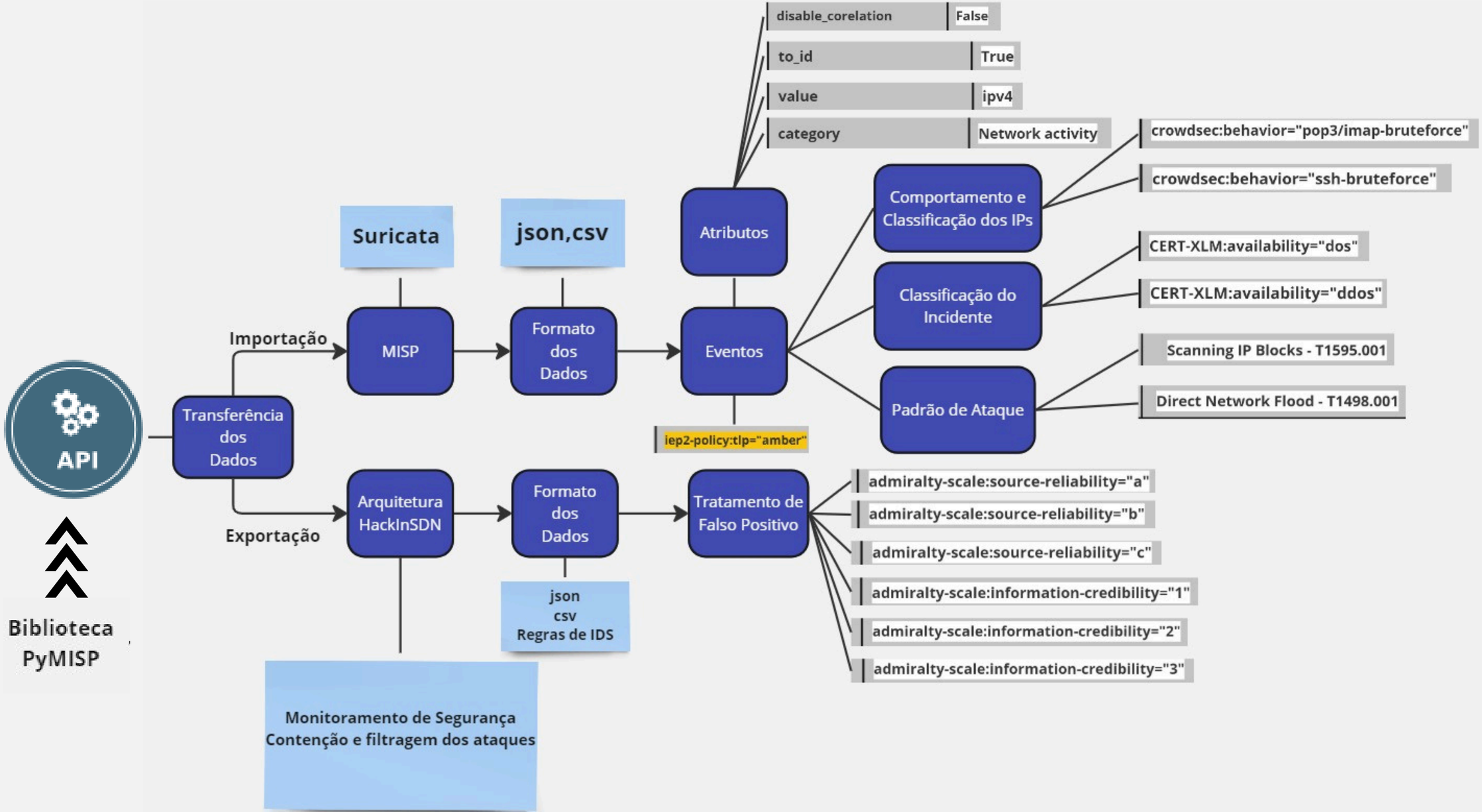
- **Classificação por meio do MISP Galaxy:**

Bhadra Framework	
1	DNS-based attacks
2	Port scanning or sweeping
3	Detect abnormal events

Attack Pattern	
1	Malicious Link - T1204.001
2	Phishing - T1566
3	Spearphishing Link - T1566.002
4	Spearphishing Attachment - T1193
5	Email Accounts - T1586.002
6	Malicious File - T1204.002
7	Scanning IP Blocks - T1595.001
8	Direct Network Flood - T1498.001

attck4fraud	
1	Phishing
2	Spear phishing
3	Malware
4	Fake Invoice Fraud
5	Scam

MODELAGEM DOS DADOS



TLP:CLEAR

CASOS DE USO

Detecção de Ataques

Detecção de scans, brute-force e negação de serviço simples (bloqueio [local e distribuído], compartilhamento de CTI, bloqueio preventivo via reputação CTI).

Orquestração, Execução e Mitigação de Ataques

Orquestração, Execução e Mitigação de ataques de negação de serviço distribuído (C&C channel via DGA, Zombie bots executando o ataque, impacto à aplicação, mitigação [quarentena, rate-limit], compartilhamento de CTI).

Práticas de Ensino

Laboratório de redteam/blueteam (CTF com pentest de uma aplicação; análise forense de incidente e lições aprendidas).

PRÁTICAS DE ENSINO

A partir da experiência obtida com a SDN-IPS , o projeto visa expandir a capacitação em temas de segurança cibernética em ambientes de testbeds.

Tópico - Fundamentos de Segurança

Taxonomias, níveis de confiabilidade e confidencialidade

Tópico - Gestão de Ameaças

Compartilhamento de informações de CTI para prevenção de ataques ou contenção antecipada

Tópico - Tratamento de Incidentes

Pesquisa em segurança usando IoC ou dados históricos de ataques

Próximos Passos

- OpenPhishing
(incluir capturas de tela e explorar a classificação dos atributos)
- Avaliação de escalalabilidade
- Execução de pilotos de treinamento

TLP:CLEAR

CONSIDERAÇÕES FINAIS

O HackInSDN é um projeto em andamento e esta apresentação buscou compartilhar resultados preliminares e obter feedback da comunidade. Boas perspectivas para inclusão do MISP na agenda de capacitação em cibersegurança no HackersDoBem, ESR/RNP e extensão UFBA.

AGRADECEMOS A ATENÇÃO DE TODOS(AS)!

julho de 2024

idasilva@fiu.edu

raquelsms@ufba.br

http://hackinsdn.ufba.br

PERGUNTAS