Arquitetura de Cibersegurança no Open Finance: O Poder da Análise com Grafos Integrados ao MISP

12º Fórum de CSIRTs | 5º Workshop MISP

Paulo Henrique Bezzani Salkys

Especialista em Segurança da Informação

ipt INSTITUTO DE PESQUISAS TECNOLÓGICAS

Paulo Henrique Bessani Salkys

Especialista em Segurança da Informação

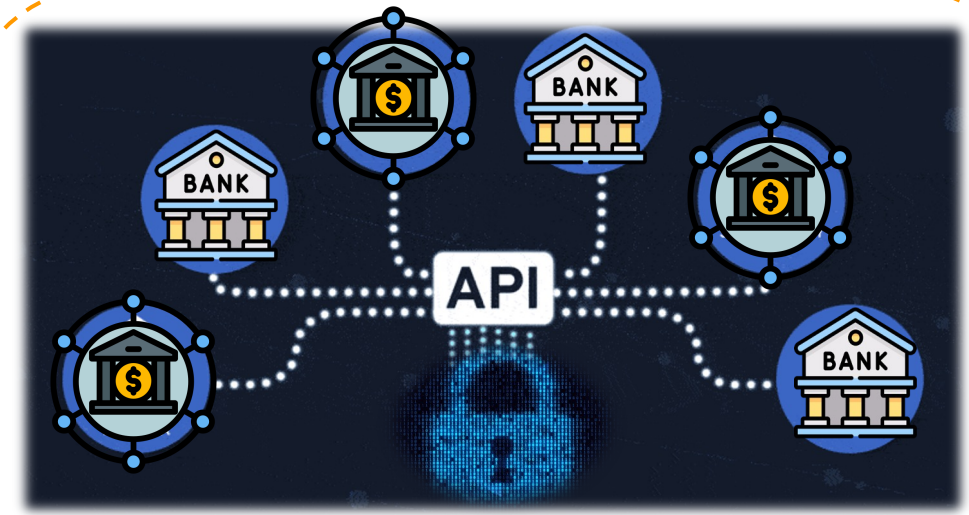
Experiência: + 20 anos

Mestrando em Computação Aplicada pelo IPT e atuo como Arquiteto de Segurança da Informação no setor financeiro, com expertise em Open Finance. Tenho especialização em Gestão de Segurança da Informação e Redes de Computadores, além de experiência no setor público e privado, focando na interoperabilidade e segurança da informação.

AGENDA

1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

Introdução

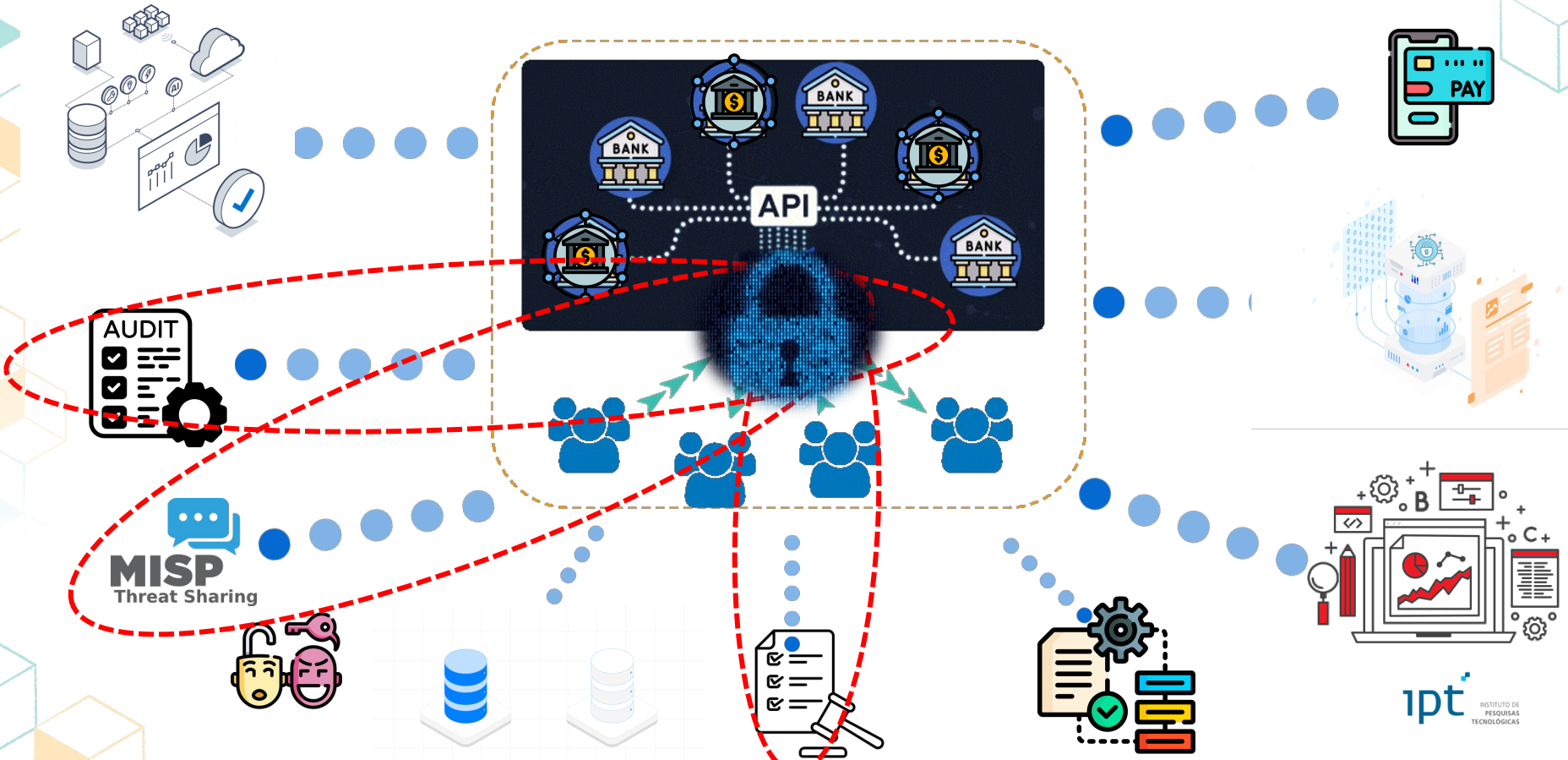


Fonte: Elaborado pelo Autor

O Open Finance, ou sistema financeiro aberto, é a possibilidade de clientes de produtos e serviços financeiros permitirem o compartilhamento de suas informações entre diferentes instituições autorizadas pelo Banco Central e a movimentação de suas contas bancárias a partir de diferentes plataformas e não apenas pelo aplicativo ou site do banco, de forma segura, ágil e conveniente.

Fonte: Banco Central do Brasil

Introdução



Fonte: Elaborado pelo Autor

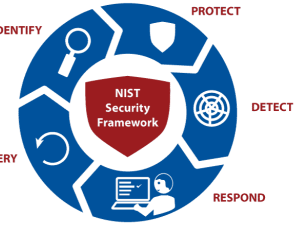
Introdução

MITRE ATT&CK

NIST National Institute of Standards and Technology

openfinance

CVE Common Vulnerabilities and Exposures



Security Operation Center
(Centro de Operação de Segurança)

SIEM

SOAR
Security Orchestration, Automation, Response

Security Information and Event Management
(Gerenciamento e Correlação de Eventos de Segurança)

Segurança em Camadas!

Fonte: Adaptado de Mediatesterling (2023).

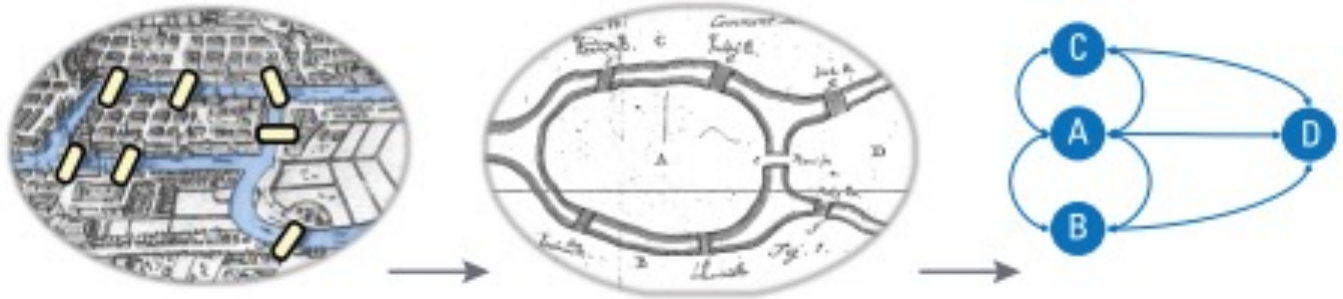
ansible-log-collection-playbook.yml

```yaml
---
# Nome do playbook e descrição geral
- name: Playbook para coleta de logs e gravação em CSV
  # Define que o playbook será executado em todos os hosts do inventário
  hosts: all
  # Habilita a elevação de privilégios (equivalente a usar sudo)
  become: yes
  # Inclui variáveis de um arquivo externo para melhor organização
  vars_files:
    - vars/log_vars.yml

  # Lista de tarefas a serem executadas
  tasks:
    # Tarefa para criar o diretório onde os logs serão armazenados
    - name: Criar diretório para armazenar os logs
      file:
        # Usa a variável definida no arquivo vars/log_vars.yml
        path: "{{ log_directory }}"
        # Garante que o diretório existe
        state: directory
        # Define permissões mais restritas (apenas o proprietário e grupo podem ler/executar)
        mode: '0750'
      # Tag para permitir a execução seletiva desta tarefa
      tags:
        - setup

    # Tarefa para coletar logs do serviço MISP
    - name: Coletar logs do serviço MISP
      # Usa 'command' em vez de 'shell' por segurança, e 'tail' para limitar a quantidade de dados
      command: tail -n 1000 /var/log/misp.log
      # Armazena a saída do comando na variável 'misp_logs'
      register: misp_logs
      # Continua a execução mesmo se houver erro na leitura do log
      ignore_errors: yes
      tags:
        - logs

    # Tarefa para coletar logs da API
    - name: Coletar logs da API
      command: tail -n 1000 /var/log/api.log
```

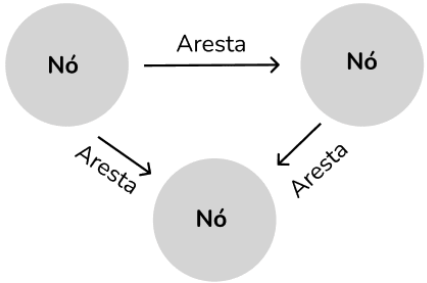
AGENDA

1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

Teorias e Tecnologias Fundamentais



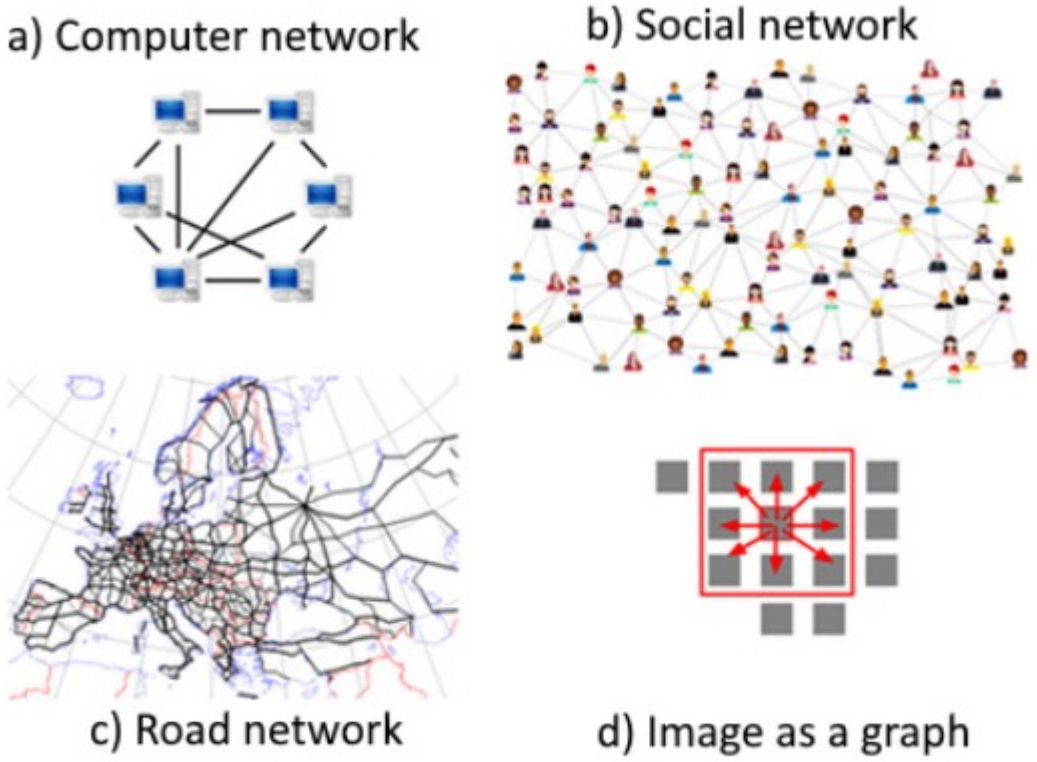
Fonte: PIERSON, L.. Data Science For Dummies.



← **Grafo**

Conforme explicado no livro "Algoritmos em Grafos" do Cormen et al. (2009), o grafo é definido como "uma estrutura de dados composta por um conjunto finito de vértices e por uma coleção de pares não ordenados de vértices, chamados arestas".

Teorias e Tecnologias Fundamentais



Fonte: SCIFO, E. Graph Data Science with Neo4j. [s.l.] Packt Publishing Ltd, 2023.

Teorias e Tecnologias Fundamentais

O MISP é uma solução de software de código aberto para coleta, armazenamento, distribuição e compartilhamento de indicadores e ameaças de segurança cibernética. É projetado para analistas de incidentes, profissionais de segurança e profissionais de TIC para apoiar suas operações diárias de compartilhamento de informações estruturadas de forma eficiente

A Instrução Normativa BCB Nº 305 é uma instrução regulatória emitida pelo Banco Central do Brasil. Anuncia o lançamento da versão 4.0 do Manual de Segurança do Open Finance.

O manual é obrigatório para todas as instituições participantes. A instrução é baseada no art. 3º, inciso IV, da Resolução BCB nº 32, de 29 de outubro de 2020. A instrução foi emitida em 15 de setembro de 2022.

Teorias e Tecnologias Fundamentais

O Neo4j é uma forma de implementação prática e aplicada da teoria de grafos, permite modelar e armazenar dados em forma de grafos e manipulá-los de forma eficiente e intuitiva.

Ao usar o Neo4j, o objetivo é aproveitar os conceitos e as técnicas da teoria de grafos para solucionar problemas de segurança da informação do ecossistema Open Finance, realizando análise, relacionamentos e correlacionamento, além da modelagem dos dados e consultas complexas demandadas por esse grandes conjuntos de dados.

A combinação do Python com APIs é a forma escolhida para a integração de dados. As APIs facilitam o acesso a informações em tempo real de diferentes fontes, enquanto o Python permite o processamento desses dados, podendo incluir limpeza, transformação, análise e visualização. Essa união resulta em uma poderosa ferramenta para extrair insights e valor dos dados, possibilitando a tomada de decisões e a integração com o Neo4j.

AGENDA

1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

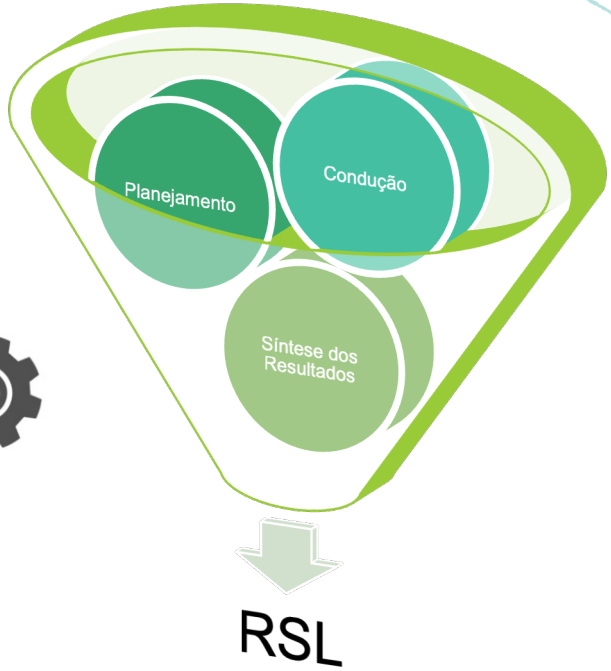
Trabalhos Correlatos

arXiv.org

WEB OF SCIENCE

Scopus

IEEE Xplore DIGITAL LIBRARY



Trabalhos Correlatos

Artigo (ID)	Título	Contribuições
1	A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems	Ao usar a teoria dos grafos para modelar nossa infraestrutura de segurança, podemos antecipar e mitigar riscos, otimizando recursos de defesa.
2	AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports	Auxiliar na identificação de potenciais ameaças à segurança da informação.
3	Platform for Connected Data Enhancing AI with Context & Connections.	Grafos podem ser utilizados para armazenar, mapear e visualizar conexões entre diferentes componentes de um sistema.
4	A framework for conceptual characterization of ontologies and its application in the cybersecurity domain	Reunindo perspectivas de diversos frameworks, podemos produzir resultados como os mostrados na Figura, que apresenta o conceito de análise cruzada de risco.
5	Securing Open Banking with Model-View-Controller Architecture and OWASP	O artigo mostra a metodologia para aplicar o OWASP Top 10 ao aplicativo e sua arquitetura, o que implica percorrer sistematicamente a lista da ameaça mais crítica à menos crítica.
6	Cybersecurity Knowledge Graph Improvement with Graph Neural Networks	Diagrama de arquitetura de alto nível para o modelo de gráfico de conhecimento. A entrada para o gráfico contém informações incorretas destacadas em vermelho. Através do "aprendizado de máquina" é produzido uma saída que contém pontuações probabilísticas para todos os relacionamentos. As pontuações podem ser interpretadas como o quanto nós 'confiamos' em cada relacionamento.

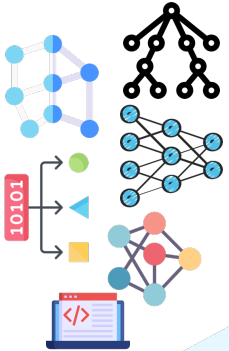
AGENDA

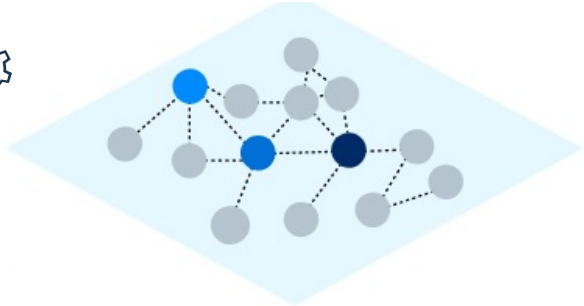
1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

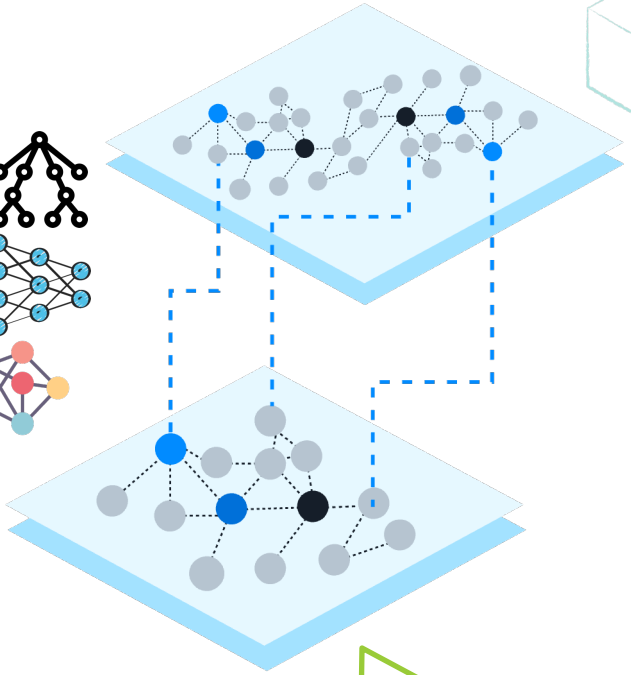
Pesquisa, Desenvolvimento & Inovação

(GRIGORIADIS et al., [s.d.])

(HOPPA, 2020)







(MARTINS et al., 2022)

Fonte: Adaptado de "Graph Database Use Cases: Neo4j Knowledge Graph for Total Visibility", [s.d.])

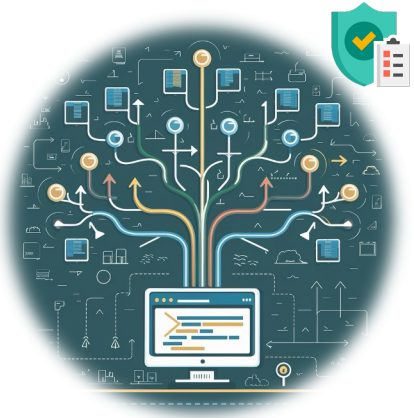
AGENDA

1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

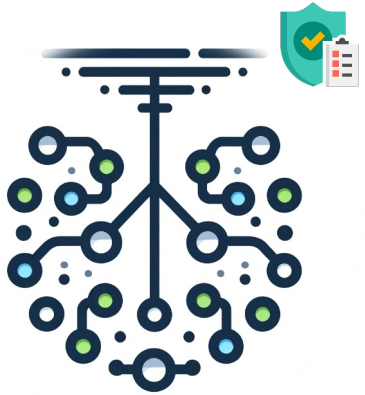
Prova de Conceito

Caso 1

Caso 2



Caso 3



openfinance

BACEN

MISP Threat Sharing

CVE Common Vulnerabilities and Exposures

OWASP Open Web Application Security Project

NIST Cybersecurity Framework

MITRE ATT&CK

ipt Instituto de Pesquisas Tecnológicas

Fonte: Elaborado pelo Autor

AGENDA

1. Introdução
2. Teorias e Tecnologias Fundamentais
3. Trabalhos Correlatos
4. Pesquisa, Desenvolvimento & Inovação
5. Prova de Conceito
6. Contribuições e Agradecimentos
7. Referências

Contribuições e Agradecimentos

Carlos Shigueo Urata

Edna Baptista Dos S Gubitoso

Dr. Eduardo Takeo Ueda

Dra. Olga Satomi Yoshida

Dr. Roni Francis Shigueta

Talita Rodrigues

Dr. Vagner Luiz Gava

Referências

- GRIGORIADIS, C. et al. A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems. [s.l: s.n.].
- KAUFMAN, C.; PERLMAN, R.; SPECINER, M. Network security : private communication in a public world. Uttar Pradesh, India: Pearson, 2018.
- MAARTEN VAN STEEN. Graph theory and complex networks : an introduction. [s.l.] Maarten Van Steen, 2010.
- BRASIL. Instrução Normativa nº 305, de 15 de setembro de 2022. Divulga a versão 4.0 do Manual de Segurança do Open Finance, e dá outras providências. Diário Oficial da União, Brasília, 19 stembro. 2022.
- CORMEN, T. H. et al. Introduction to algorithms. [s.l.] MIT Press, 2009. BRASIL. Resolução Conjunta nº 5, de 20 de maio de 2022. Dispõe sobre a interoperabilidade no Open Finance, e dá outras providências. Diário Oficial da União, Brasília, 24 mai. 2022.
- BRASIL. Instrução Normativa nº 134, de 22 de julho de 2021. Divulga a versão 3.0 do Manual de Segurança do Open Banking, e dá outras providências. Diário Oficial da União, Brasília, 27 julho. 2021.
- Referência: KELLEZI, Deina; BOEGELUND, Christian; MENG, Weizhi. Securing Open Banking with Model-View-Controller Architecture and OWASP. Wireless Communications And Mobile Computing, [S.L.], v. 2021, p. 1-13, 21 set. 2021. Hindawi Limited. http://dx.doi.org/10.1155/2021/8028073.
- Referência: KHAN, Saad; PARKINSON, Simon. Discovering and utilising expert knowledge from security event logs. Journal Of Information Security And Applications, [S.L.], v. 48, p. 102375, out. 2019. Elsevier BV. http://dx.doi.org/10.1016/j.jisa.2019.102375.
- TSOULIAS, Konstantinos; PALAIOKRASSAS, Georgios; FRAGKOS, Georgios; LITKE, Antonios; VARVARIGOU, Theodora A.. A Graph Model Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems. Ieee Access, [S.L.], v. 8, p. 130952-130965, 2020. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2020.3006383.
- PURIFICATO, Erasmo; WEHNERT, Sabine; LUCA, Ernesto William de. Dynamic Privacy-Preserving Recommendations on Academic Graph Data. Computers, [S.L.], v. 10, n. 9, p. 107, 25 ago. 2021. MDPI AG. http://dx.doi.org/10.3390/computers10090107.
- GRIGORIADIS, Christos; BERZOVITIS, Adamantios Marios; STELLIOS, Ioannis; KOTZANIKOLAOU, Panayiotis. A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems. Computer Security. Esorics 2021 International Workshops, [S.L.], p. 23-39, 2022. Springer International Publishing. http://dx.doi.org/10.1007/978-3-030-95484-0_2.

Contato

Paulo Henrique Bezzani Salkys

Especialista em Segurança da Informação

https://www.linkedin.com/in/phsalkys/