INSTITUTO DE PESQUISAS TECNOLÓGICAS

COMUNICAÇÃO TÉCNICA

Nº 179373

Estabelecendo bases: estudo preliminar de ameaças baseado em grafos no Open Banking/Open Finance

Paulo Henrique Bessani Salkys
Olga Satomi Yoshida

Palestra apresentada INTERNATIONAL CENFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, 20, 2024, São Paulo. 8 slides.

Instituto de Pesquisas Tecnológicas do Estado de São Paulo S/A - IPT
Av. Prof. Almeida Prado, 532 | Cidade Universitária ou
Caixa Postal 0141 | CEP 01064-970
São Paulo | SP | Brasil | CEP 05508-901
Tel 11 3767 4374/4000 | Fax 11 3767-4099

www.ipt.br

Estabelecendo Bases: Estudo Preliminar de Ameaças Baseado em Grafos no Open Banking / Open Finance

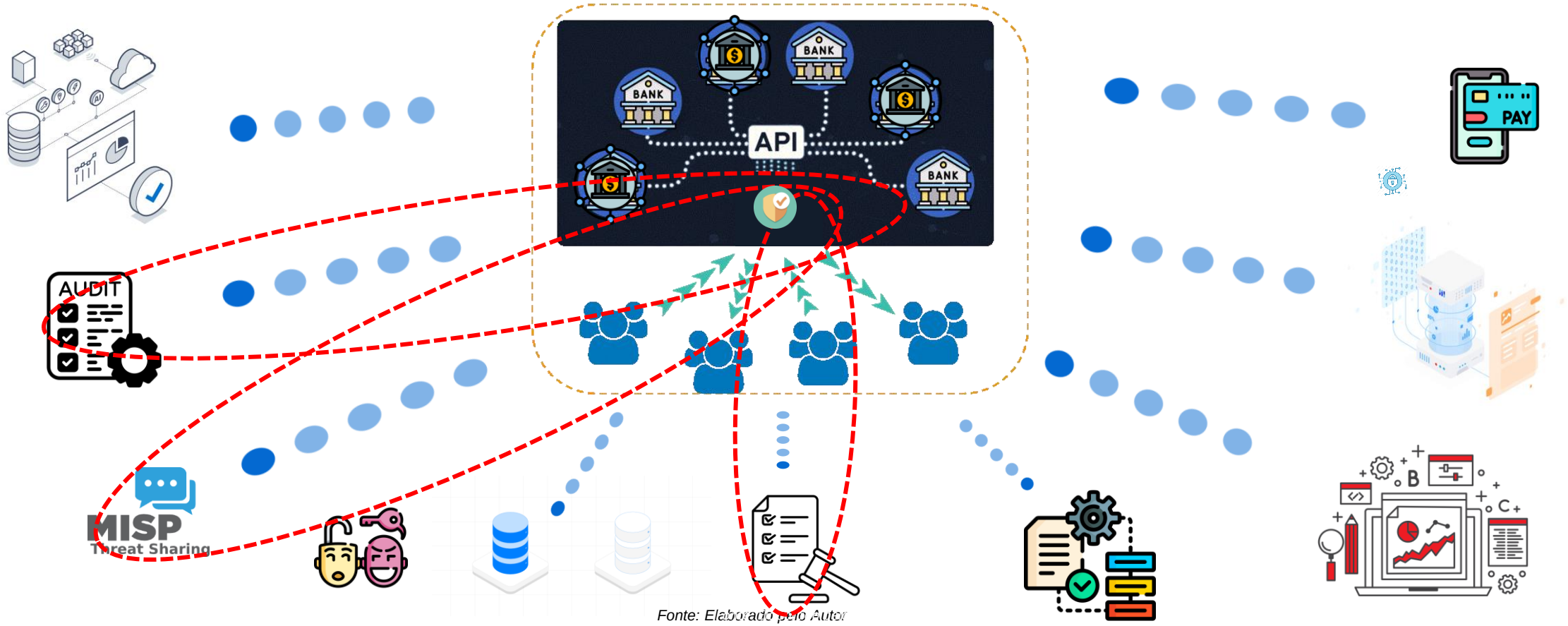
Autor 1: Paulo Henrique Bessani Salkys

Instituição: IPT - Instituto de Pesquisas Tecnológicas

Autor 2 Dra. Olga Satomi Yoshida

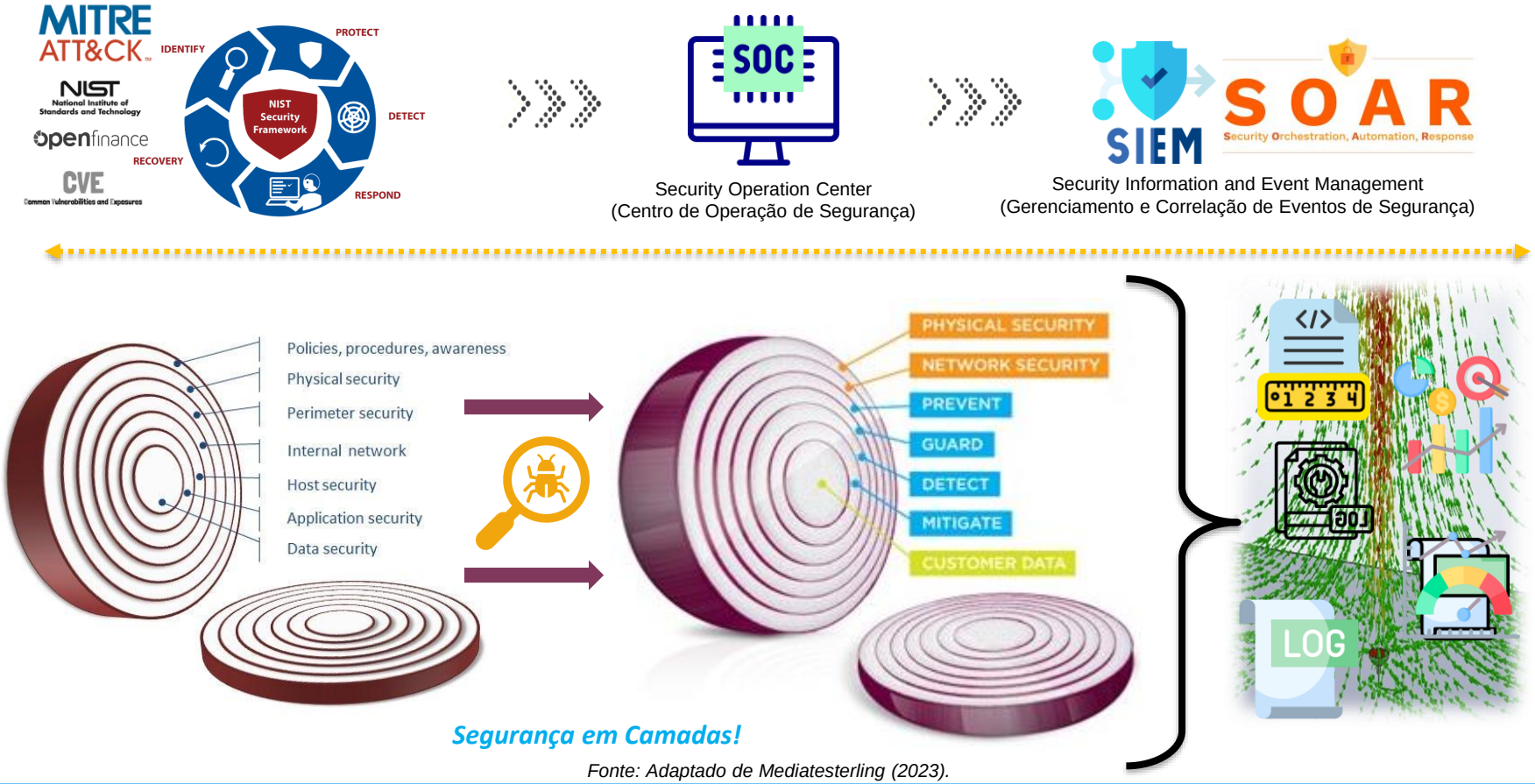
Instituição: IPT - Instituto de Pesquisas Tecnológicas

1 - Introdução



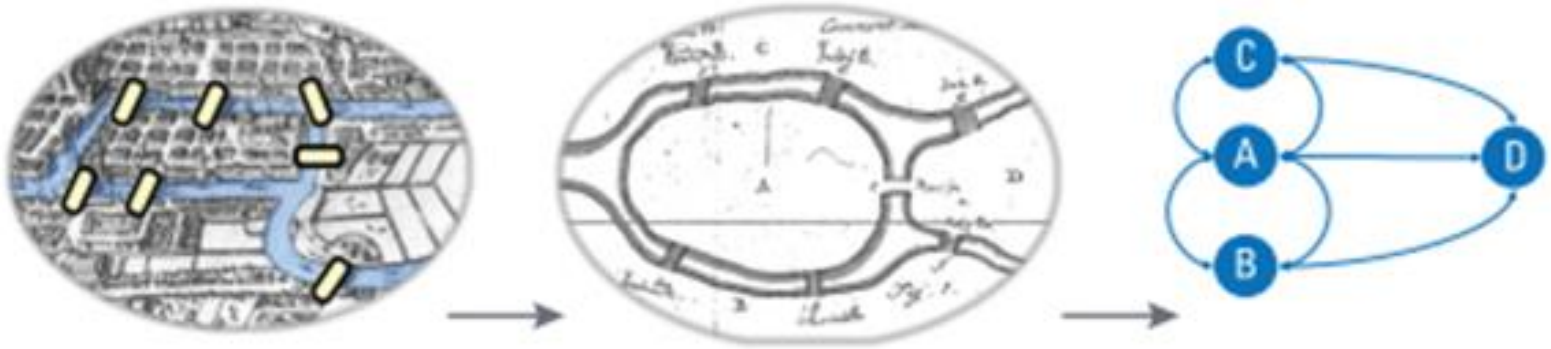
Fonte: Elaborado pelo Autor

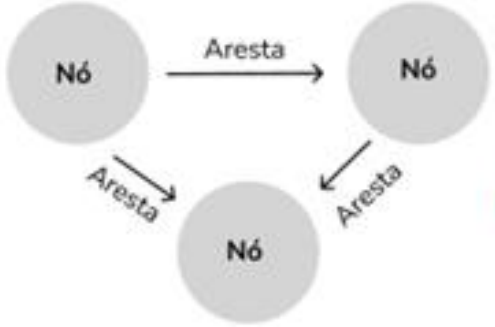
1 - Introdução



Fonte: Adaptado de Mediatesterling (2023).

2- Referencial Teórico





← Grafo

Com base no entendimento do livro "Introduction to Algorithms", de Cormen, um grafo é definido como "uma estrutura de dados composta por um conjunto finito de vértices e por uma coleção de pares não ordenados desses vértices, chamados de arestas

Fonte: Adaptado de Mediatesterling (2023).

2- Referencial Teórico

Modelagem de ameaças: Modelagem dos dados ou de ameaças de segurança da informação com grafos, pode incluir a representação de entidades como usuários, dispositivos, recursos e permissões como nós do grafo, e as relações entre eles como arestas, como demonstrado por Cao et al. (2022)

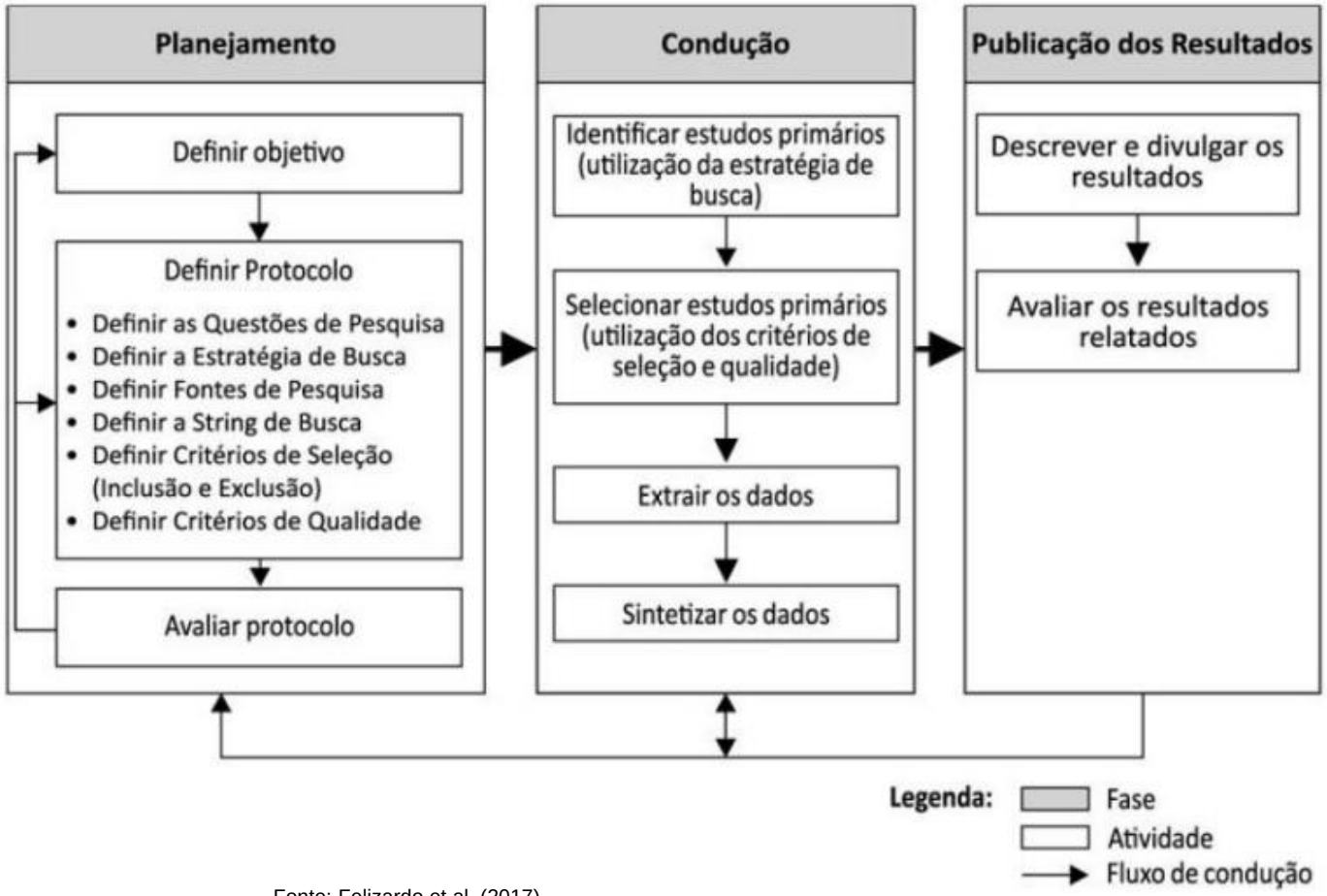
Análise de padrões: Li et al. (2021) demonstraram que, após a modelagem dos dados em um grafo, é possível identificar padrões e anomalias.

Detecção de ameaças: A análise de grafos também pode ser usada para detectar ameaças à segurança da informação. Por exemplo, pode-se procurar por atividades suspeitas ou tentativas de exploração de vulnerabilidades. Mavroeidis et al. (2018) apresentaram um framework ontológico para melhorar a segurança e a detecção de ameaças, que pode ser aplicado para detectar desvios de políticas de segurança organizacional.

Prevenção de ameaças: Pirbhulal et al. (2021) revisaram como a análise de dados do grafo pode informar a implementação de medidas preventivas de segurança da informação.

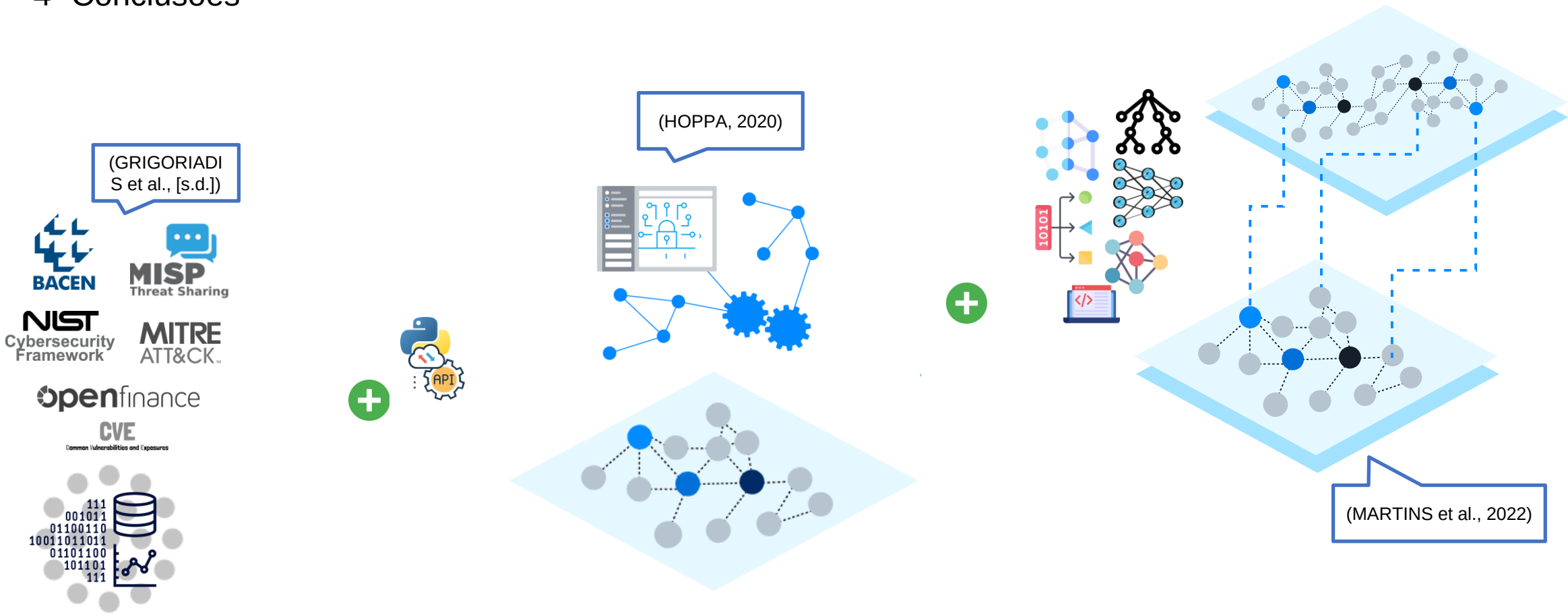
3- Metodologia

Fases e atividades do processo da Revisão Sistemática da Literatura



Fonte: Felizardo et al. (2017).

4- Conclusões



Fonte: Elaborado pelo autor com dados de Barrasa e Webber (2023), Grigoriadis et al. (2022), Martins et al. (2022), Neo4j. (2022).

4- Conclusões

Retomada dos Objetivos: Revisão do objetivo original do estudo, que é desenvolver um framework para a aplicação da teoria dos grafos para a análise e mitigação de ameaças à segurança da informação no contexto do Open Finance/Open Banking.

Resposta à pergunta de pesquisa: O artigo mostra a viabilidade do desenvolvimento de um motor/framework que emprega a teoria dos grafos para avaliar e mapear as ameaças à segurança da informação dentro do ecossistema do Open Finance/Open Banking, incluindo arquitetura, ferramentas e soluções propostas.

Contribuições Esperadas

Para a academia:
Revisar as práticas recomendadas na literatura.
Ampliar o entendimento sobre o tema.
Discutir com maior profundidade sobre o tema.

Para a indústria:
Mapear as melhores práticas para tomada decisão.
Solução de detecção de ameaças, que utiliza como base a correlação de dados, por meio de Grafos.
Diminuir a complexidade das análises.
Atender a demandas regulatórias.
PD&I.