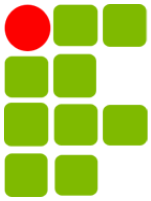


Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

DETECÇÃO E AMEAÇAS EM REDES: UMA REVISÃO SISTEMÁTICA

Davi Araujo Silva

Orientador: Prof. Dr. Éwerton Rômulo Silva Castro

Campina Grande, Abril de 2026

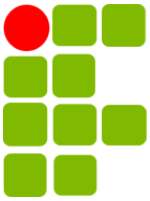
Catalogação na fonte:
Ficha catalográfica elaborada por Gustavo César Nogueira da Costa – CRB 15/479

S586d Silva, Davi Araujo.
Detecção e ameaças em redes: uma revisão sistemática / Davi Araujo Silva - Campina Grande, 2026.
48 f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2026.
Orientador: Prof.Dr. Éwerton Rômulo Silva Castro

1. Telemática. 2. Redes de computadores - Segurança. 3. Segurança de redes. 4.Gerenciamento de informações e eventos de segurança - SIEM. I. Castro, Éwerton Rômulo Silva. II Título.

CDU 004.05



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

DETECÇÃO E AMEAÇAS EM REDES: UMA REVISÃO SISTEMÁTICA

Davi Araujo Silva

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Prof. Dr. Éwerton Rômulo Silva Castro

Campina Grande, Junho de 2026

DETECÇÃO E AMEAÇAS EM REDES: UMA REVISÃO SISTEMÁTICA

Davi Araujo Silva

Prof. Dr. Éwerton Rômulo Silva Castro
Orientador

Prof. Dr. Elmano Ramalho Cavalcanti
Membro da Banca

Prof. Dr. Petrônio Carlos Bezerra
Membro da Banca

Campina Grande, Paraíba, Brasil
Junho/2026

Dedico este trabalho à Deus, meus pais e amigos, que me deram todo apoio e suporte necessário para que hoje possa concluir meu curso.

A vida é ampla, ilimitada. Não há fronteiras, não há limites
Bruce Lee

Agradecimentos

Agradeço primeiramente a Deus, que me deu a orportunidade de ingressar e concluir esse curso. Sou imensamente grato à meus pais, minha mãe Evelinne Peixoto Araujo e a meu pai, Valmir de Melo Silva, por todo o apoio e ajuda durante os momentos difícies e de alegria desses anos de estudos. Agradeço imensamente também ao Professor Dr. Éwerton Rômulo Silva Castro. Sua participação durante minha trajetória acadêmica fez toda a diferença, com seus conhecimentos e experiencias da vida. Por fim, agradeço a todos os professores do Instituto Federal da Paraíba, Campus Campina Grande, pelo compromisso, dedicação e pelos ensinamentos transmitidos ao longo da minha formação, fundamentais para o meu crescimento acadêmico e profissional.

Resumo

A segurança de redes enfrenta desafios crescentes devido à sofisticação e velocidade dos ataques modernos. A integração entre IDS (*Intrusion Detection System* - Sistemas de Detecção e Intrusão) e mecanismos de resposta automatizada, como SOAR (*Security Orchestration, Automation and Response - Orquestração, Automação e Resposta de Segurança*) e SIEM (*Security Information and Event Management - Gerenciamento de Informações e Eventos de Segurança*), surge como alternativa promissora para reduzir o tempo de mitigação e aumentar a resiliência das infraestruturas digitais. Esta RSL (Revisão Sistemática da Literatura) investiga pesquisas publicadas entre 2020 e 2025, avaliando abordagens, arquiteturas e resultados sobre a integração IDS–automação. Foram selecionados 19 estudos após triagem em bases como IEEE, Scopus, ScienceDirect e Google Scholar. Os resultados mostram avanços significativos em automação inteligente, *Zero Trust*, defesa ativa e uso de *machine learning* para aprimorar detecção e resposta. A integração reduz incidentes, acelera reações e melhora a eficiência da segurança de redes.
Palavras-chave: Segurança em Redes; Detecção de Intrusão; SOAR; SIEM; Automação de Segurança; Cibersegurança.

Abstract

Network security faces increasing challenges due to the sophistication and speed of modern attacks. The integration between Intrusion Detection Systems (IDS) and automated response mechanisms, such as SOAR and SIEM, emerges as a promising alternative to reduce mitigation time and increase the resilience of digital infrastructures. This Systematic Literature Review investigates research published between 2020 and 2025, evaluating approaches, architectures, and results on IDS-automation integration. nineteen studies were selected after screening databases such as IEEE, Scopus, and ScienceDirect. The results show significant advances in intelligent automation, Zero Trust, active defense, and the use of machine learning to improve detection and response. Integration reduces incidents, accelerates reactions, and improves the efficiency of network security.
Keywords: Network Security; Intrusion Detection; SOAR; SIEM; Security Automation; Cybersecurity.

Sumário

Lista de Abreviaturas

API	*Application Programming Interface* (Interface de Programação de Aplicações)
APT	*Advanced Persistent Threat* (Ameaça Persistente Avançada)
CIA	*Confidentiality, Integrity and Availability* (Confidencialidade, Integridade e Disponibilidade)
DDoS	*Distributed Denial of Service* (Negação de Serviço Distribuída)
EDR	*Endpoint Detection and Response* (Detecção e Resposta em Endpoints)
GDPR	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados)
HIDS	*Host-based Intrusion Detection System* (Sistema de Detecção de Intrusão baseado em Hospedeiro)
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusão)
IoT	*Internet of Things* (Internet das Coisas)
IPS	*Intrusion Prevention System* (Sistema de Prevenção de Intrusão)
MITRE	*MITRE ATT&CK – Adversarial Tactics, Techniques and Common Knowledge (Táticas, Técnicas e Conhecimento Comum de Adversários)*
MTD	*Moving Target Defense* (Defesa contra Alvos Móveis)
MTTR	*Mean Time to Repair* (Tempo Médio de Reparo)
ML	*Machine Learning* (Aprendizado de Máquina)
NIDS	*Network Intrusion Detection System* (Sistema de Detecção de Intrusão em Rede)

RAAC	*Risk-Adaptive Access Control* (Controle de Acesso Adaptável ao Risco)
SCADA	*Supervisory Control and Data Acquisition* (Supervisão e Aquisição de Dados)
SDN	*Software Defined Networking* (Rede Definida por Software)
SIEM	*Security Information and Event Management* (Gerenciamento de Informações e Eventos de Segurança)
SPIFFE	*Secure Production Identity Framework for Everyone* (Estrutura de Identidade Segura para Produção para Todos)
SOAR	*Security Orchestration, Automation and Response* (Orquestração, Automação e Resposta de Segurança)
SOC	*Security Operations Center* (Centro de Operações de Segurança)
TCP/IP	*Transmission Control Protocol / Internet Protocol* (Protocolo de controle de transmissão / Protocolo de internet)
TTP	*Tactics, Techniques and Procedures* (Táticas, Técnicas e Procedimentos)
UEBA	*User and Entity Behavior Analytics* (Análise de Comportamento de Usuários e Entidades)
VPN	*Virtual Private Network* (Rede Privada Virtual)
ZTA	*Zero Trust Architecture* (Arquitetura de Confiança zero)

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

O avanço das tecnologias de informação e comunicação impulsionou uma crescente dependência das redes de computadores em praticamente todos os setores da sociedade, incluindo ambientes corporativos, governamentais, acadêmicos e industriais. A expansão da conectividade digital, aliada ao uso de computação em nuvem, dispositivos móveis e Internet das Coisas (IoT), proporcionou maior eficiência operacional e compartilhamento de dados em larga escala. Entretanto, essa evolução tecnológica também ampliou significativamente a superfície de ataque das infraestruturas computacionais, tornando a segurança das redes um dos principais desafios da atualidade [Lee, Jang-Jaccard e Kwak 2022]

Historicamente, os mecanismos de segurança em redes eram baseados predominantemente em soluções perimetrais, como *firewalls* e controles de acesso estáticos, cuja principal função era impedir acessos não autorizados vindos de redes externas. Contudo, com o surgimento de ataques mais sofisticados, capazes de explorar vulnerabilidades internas e realizar movimentação lateral dentro das redes, tornou-se necessário o desenvolvimento de mecanismos capazes não apenas de bloquear acessos, mas também de detectar comportamentos maliciosos em tempo real. Nesse contexto, surgiram os IDS (*Intrusion Detection Systems* - Sistemas de Detecção e Intrusão), que passaram a desempenhar papel fundamental na identificação de atividades suspeitas por meio da análise de assinaturas e detecção de anomalias [Rahman e Islam 2022].

Com o aumento exponencial do volume de tráfego e eventos de segurança, os IDS passaram a gerar grandes quantidades de alertas, exigindo soluções capazes de correlacionar informações provenientes de múltiplas fontes. Assim, foram desenvolvidos os sistemas de gerenciamento e correlação de eventos de segurança SIEM (*Security Information and Event Management* - Gerenciamento de Informações e Eventos de Segurança) , que permitem centralizar *logs* e realizar análises mais abrangentes do ambiente monitorado [Ahmed e Khan 2022]. Apesar disso, a análise manual dos alertas ainda representa um gargalo operacional, especialmente diante da velocidade e da complexidade dos ataques modernos.

Mais recentemente, a evolução do estado da arte em segurança cibernética introduziu

plataformas SOAR (*Security Orchestration, Automation and Response* - Orquestração, Automação e Resposta de Segurança), que permitem automatizar processos de resposta a incidentes por meio da execução de fluxos de ações previamente definidos. Essas soluções reduzem o tempo de resposta e minimizam erros humanos, permitindo que eventos detectados por IDS resultem em ações automáticas de mitigação [Ahmed e Khan 2022]. Paralelamente, modelos modernos como o paradigma *Zero Trust* (Confiança Zero) passaram a adotar o princípio de verificação contínua de identidade e comportamento, fortalecendo a capacidade de detecção e contenção de ameaças dentro das redes corporativas [Zhang, Li e Chen 2023].

No estado da arte atual, observa-se uma tendência crescente de integração entre mecanismos de detecção, análise e resposta automatizada, frequentemente apoiada por técnicas de aprendizado de máquina e análise comportamental. Essas abordagens permitem identificar padrões complexos de ataques e executar respostas em tempo quase real, aumentando a resiliência dos sistemas frente a ameaças avançadas [Garcia e Mendes 2023]. Entretanto, ainda existem desafios relacionados à interoperabilidade entre ferramentas, redução de falsos positivos e confiabilidade das decisões automatizadas [Wang e Zhou 2024]. Diante desse cenário, este trabalho investiga o tema detecção e mitigação de ameaças em redes computacionais, com foco específico na integração entre sistemas de detecção de intrusão e mecanismos automatizados de resposta a incidentes. O problema central abordado consiste em compreender como diferentes estratégias de integração entre IDS e sistemas de resposta automatizada podem contribuir para a redução de incidentes de segurança em ambientes de rede.

Como principal contribuição, este trabalho apresenta uma análise sistemática das abordagens existentes na literatura, identificando mecanismos tecnológicos, desafios e tendências relacionadas à automação da segurança em redes. Os resultados obtidos foram alcançados por meio de uma Revisão Sistemática da Literatura, conduzida conforme diretrizes metodológicas consolidadas [Page, McKenzie e Bossuyt 2021], permitindo a seleção, análise e síntese crítica de estudos científicos relevantes na área.

1.1 Justificativa e Relevância do Trabalho

O aumento contínuo do número de ataques cibernéticos e o impacto financeiro e operacional causado por incidentes de segurança tornam a proteção das redes uma prioridade estratégica para organizações modernas. Ataques atuais são caracterizados por alta automação, rapidez de propagação e capacidade de evasão de mecanismos tradicionais de defesa, o que exige soluções igualmente dinâmicas e inteligentes.

A escolha do tema justifica-se pela necessidade crescente de integrar mecanismos de detecção e resposta automática, reduzindo o tempo entre a identificação de uma ameaça e sua mitigação efetiva. Além disso, a automação da segurança representa uma tendência

consolidada na área de cibersegurança, sendo amplamente adotada em SOC (*Security Operations Center* - Centro de Operações de Segurança). Assim, o estudo contribui para a compreensão das tecnologias emergentes e auxilia no desenvolvimento de arquiteturas mais resilientes e eficientes.

1.2 Objetivos

Neste tópico serão apresentados os objetivos principais desse trabalho

1.2.1 Objetivo Geral

Investigar os mecanismos de integração entre sistemas de detecção de intrusão e sistemas de resposta automatizada, analisando sua contribuição para a redução de incidentes de segurança em redes computacionais.

1.2.2 Objetivos Específicos

- Identificar os principais modelos de detecção de ameaças utilizados em redes;
- Analisar o funcionamento e as características de plataformas SIEM e SOAR;
- Avaliar abordagens de automação aplicadas à resposta a incidentes de segurança;
- Investigar desafios e limitações na integração entre IDS e sistemas automatizados;
- Sintetizar tendências e boas práticas identificadas na literatura científica.

1.3 Questão de Pesquisa

A definição da questão de pesquisa é uma etapa fundamental em uma Revisão Sistemática da Literatura, pois orienta todo o processo de busca, seleção e análise dos estudos relevantes. A partir da delimitação clara do problema investigado, torna-se possível estabelecer critérios de busca adequados e identificar trabalhos que contribuam diretamente para a compreensão do tema analisado.

Considerando o contexto atual de crescimento das ameaças cibernéticas e a necessidade de mecanismos mais eficientes para detecção e resposta a incidentes de segurança, esta pesquisa busca investigar como diferentes tecnologias de segurança da informação podem ser utilizadas de forma integrada para fortalecer a proteção de redes e sistemas computacionais.

Dessa forma, a questão de pesquisa que norteia este trabalho é definida como:

Quais os mecanismos de integração entre IDS e sistemas de resposta automatizada para a redução de incidentes de segurança?

A partir dessa questão central, a revisão sistemática busca identificar, analisar e sintetizar os estudos existentes na literatura que abordam a aplicação dessas tecnologias, suas arquiteturas, mecanismos de funcionamento e contribuições para o fortalecimento da segurança cibernética em ambientes organizacionais.

1.4 Organização do Trabalho

Para facilitar a compreensão da temática abordada e dos procedimentos adotados na pesquisa, este trabalho está estruturado em cinco capítulos, organizados da seguinte forma:

- **Capítulo 1 – Introdução**: Apresenta o contexto da segurança cibernética nas redes modernas, destacando o crescimento das ameaças digitais e a necessidade de mecanismos mais avançados de detecção e resposta a incidentes. Também são apresentados a justificativa, o objetivo geral e os objetivos específicos desta pesquisa.

- **Capítulo 2 – Fundamentação Teórica**: Apresenta os conceitos fundamentais relacionados à segurança de redes e às tecnologias utilizadas para detecção e resposta a incidentes. São discutidos os princípios e características de ferramentas e arquiteturas como SIEM, SOAR, IDS e o modelo de segurança *Zero Trust*, além de suas aplicações na proteção de infraestruturas digitais.

- **Capítulo 3 – Metodologia**: Descreve os procedimentos metodológicos utilizados para a realização da Revisão Sistemática da Literatura. Neste capítulo são apresentados os critérios de busca, as bases de dados utilizadas, os critérios de inclusão e exclusão dos estudos, bem como o processo de seleção e análise dos artigos científicos.

- **Capítulo 4 – Resultados**: Apresenta os resultados obtidos a partir da Revisão Sistemática da Literatura. Neste capítulo são discutidos os principais achados dos estudos selecionados, destacando as contribuições relacionadas ao uso de SIEM, SOAR, IDS e do modelo *Zero Trust* para aprimorar a detecção, análise e resposta a incidentes de segurança cibernética.

- **Capítulo 5 – Considerações Finais**: Apresenta a síntese das principais conclusões obtidas a partir da análise dos estudos selecionados, verificando o atendimento aos objetivos propostos. Também são discutidas as limitações da pesquisa e apresentadas sugestões para trabalhos futuros relacionados à evolução das soluções de segurança cibernética.

Capítulo 2

Fundamentação Teórica

Este capítulo apresenta os conceitos fundamentais necessários para a compreensão do tema abordado neste trabalho, bem como os principais avanços tecnológicos relacionados à detecção e mitigação de ameaças em redes computacionais. Inicialmente são discutidos os conceitos de segurança em redes e evolução das ameaças cibernéticas, seguidos pela descrição dos IDS, SIEM, plataformas SOAR e modelos modernos de segurança, como o paradigma *Zero Trust*. Por fim, são apresentados os avanços recentes relacionados à automação e ao uso de técnicas inteligentes na defesa cibernética.

2.1 Segurança em Redes de Computadores

A segurança em redes de computadores tem como objetivo proteger dados, sistemas e serviços contra acessos não autorizados, alterações indevidas e interrupções de funcionamento. Tradicionalmente, a proteção das redes era baseada em mecanismos perimetrais, como *firewalls* e sistemas de autenticação, que buscavam impedir acessos externos maliciosos. Contudo, a crescente complexidade das infraestruturas digitais e a evolução das ameaças tornaram essas abordagens insuficientes [Mukhopadhyay *et al.* 2011]. Ataques modernos exploram vulnerabilidades internas, utilizam técnicas de evasão e frequentemente permanecem ocultos por longos períodos dentro das redes comprometidas. Dessa forma, tornou-se necessário o desenvolvimento de mecanismos capazes de monitorar continuamente o ambiente e identificar comportamentos suspeitos em tempo real [Lakbabi, Orhanou e Hajji 2013].

2.2 Sistemas de Detecção e Intrusão

Os IDS (Intrusion Detection System - Sistemas de Detecção e Intrusão), são ferramentas responsáveis por monitorar atividades em redes e sistemas computacionais com o objetivo de identificar possíveis violações de segurança. Esses sistemas analisam pacotes de rede, registros de eventos e padrões de comportamento em busca de atividades

maliciosas [Mukhopadhyay *et al.* 2011].
Os IDS podem ser classificados em três categorias principais:

- Baseados em assinatura: detectam ataques conhecidos por meio da comparação com padrões previamente catalogados;
- Baseados em anomalia: identificam desvios em relação ao comportamento considerado normal;
- Sistemas híbridos: combinam múltiplas técnicas para aumentar a precisão da detecção.

Apesar de sua importância, IDS tradicionais apresentam limitações, como elevado número de falsos positivos e dependência de análise humana para resposta aos incidentes detectados. Esse fator motivou o desenvolvimento de soluções complementares capazes de correlacionar e automatizar ações de segurança [Lakbabi, Orhanou e Hajji 2013].
A Figura **??** ilustra o funcionamento de um Sistema de Detecção de Intrusão em conjunto com um *firewall* no processo de monitoramento do tráfego de rede. Inicialmente, as conexões que chegam à rede passam pelo *firewall*, responsável por aplicar regras de filtragem e decidir se o tráfego deve ser bloqueado ou permitido com base em políticas de segurança previamente definidas.
Quando uma conexão é permitida, o IDS atua analisando o tráfego que circula na rede com o objetivo de identificar comportamentos suspeitos ou padrões associados a ataques cibernéticos. A partir dessa análise, o sistema é capaz de classificar o tráfego como legítimo ou suspeito, permitindo a identificação de possíveis tentativas de intrusão.
Além da detecção, o IDS também auxilia no processo de análise de eventos de segurança e pode gerar alertas para administradores ou outros sistemas de segurança. Em arquiteturas modernas de segurança, essas informações podem ser utilizadas por plataformas de gerenciamento e resposta a incidentes, como sistemas SIEM e SOAR, possibilitando ações de resposta mais rápidas e eficientes diante de ameaças identificadas.

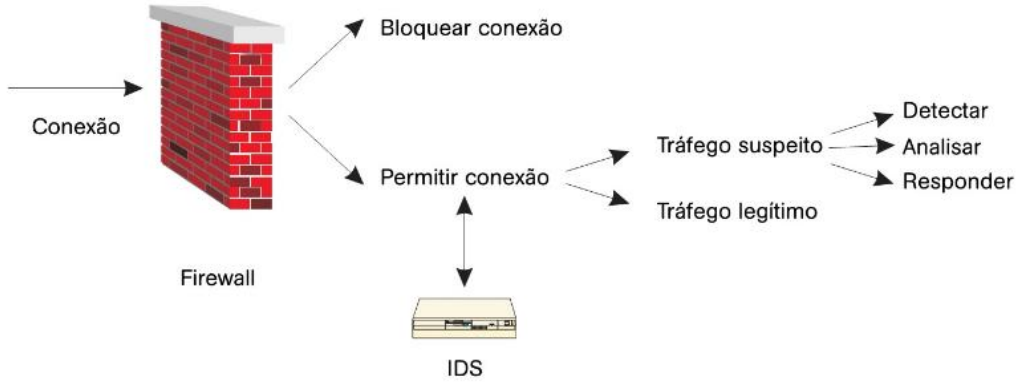


Figura 2.1: *Funcionamento de um Sistema de Detecção de Intrusão (IDS) em conjunto com um firewall. Fonte: [Tinoco 2026]*

2.3 Gerenciamento de Informações e Eventos de Segurança

Os sistemas SIEM (*Security Information and Event Management* - Gerenciamento de Informações e Eventos de Segurança) surgiram como uma evolução dos mecanismos de monitoramento de segurança, permitindo a coleta, armazenamento e correlação de eventos provenientes de diversas fontes, incluindo IDS, *firewalls*, servidores e aplicações corporativas [Vazão *et al.* 2023].

A principal função do SIEM é fornecer visibilidade centralizada do ambiente de segurança, permitindo identificar padrões complexos de ataque por meio da correlação de eventos distintos. Dessa forma, os analistas conseguem compreender melhor o contexto dos incidentes e priorizar respostas.

Entretanto, embora o SIEM melhore significativamente a análise de eventos, sua eficácia ainda depende da intervenção humana para tomada de decisão, o que pode gerar atrasos em cenários de ataques rápidos e automatizados [Sridharan e Kanchana 2022].

A Figura 2.2 apresenta a arquitetura conceitual de um sistema SIEM. Esse tipo de sistema tem como principal função coletar, normalizar, armazenar e analisar dados de segurança provenientes de diferentes fontes presentes na infraestrutura de tecnologia da informação.

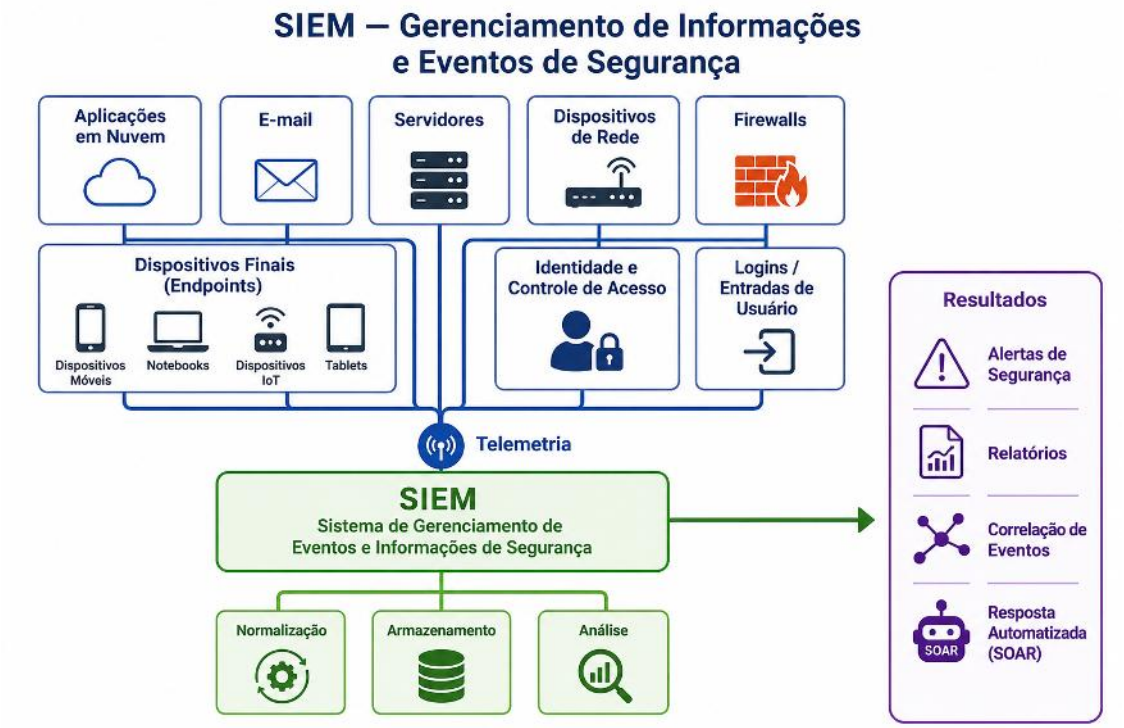


Figura 2.2: *Arquitetura conceitual de um sistema SIEM. Fonte: [M 2026]. (Adaptada pelo autor com auxilio de IA).*

No modelo apresentado, o SIEM recebe telemetria de diversos componentes do ambiente computacional, incluindo dispositivos de rede como *firewalls*, servidores, serviços de *e-mail*,

aplicações em nuvem e dispositivos finais, como *laptops, smartphones, tablets* e dispositivos de Internet das Coisas. Além disso, informações relacionadas à gestão de identidade e controle de acesso, como registros de autenticação e *login* de usuários, também são utilizadas como fonte de dados.

A partir da análise desses registros, o sistema é capaz de correlacionar eventos de segurança, gerar alertas, produzir relatórios e apoiar processos de resposta a incidentes. Em ambientes modernos de segurança cibernética, os dados processados pelo SIEM também podem ser utilizados por plataformas de automação e orquestração, como sistemas SOAR, permitindo a execução de respostas automatizadas a ameaças detectadas [Sridharan e Kanchana 2022].

2.4 Orquestração, Automação e Resposta de Segurança

As plataformas SOAR (*Security Orchestration, Automation and Response* - Orquestração, Automação e Resposta de Segurança) representam uma evolução na área de segurança cibernética ao introduzir automação e orquestração nos processos de resposta a incidentes. Essas soluções integram diferentes ferramentas de segurança e permitem a execução automática de ações por meio de fluxos operacionais denominados *playbooks* (roteiros) [Waelchli e Walter 2025].

Entre as principais funcionalidades dos sistemas SOAR destacam-se:

- automação da análise de alertas;
- execução automática de respostas a incidentes;
- integração entre múltiplas ferramentas de segurança;
- redução do tempo de resposta e da carga operacional dos analistas.

Figura 2.3: *Arquitetura conceitual do sistema SOAR. Fonte [Islam 2026]. (Adaptado pelo autor com auxilio de imagem).*

A Figura **??** ilustra uma visão conceitual da arquitetura de uma plataforma SOAR. Nesse modelo, a organização utiliza uma plataforma SOAR para integrar diferentes ferramentas de segurança responsáveis pelas etapas de detecção, análise e resposta a incidentes.

A plataforma executa e gerencia processos de orquestração, os quais coordenam atividades e tarefas específicas relacionadas ao tratamento de eventos de segurança. Essas atividades são suportadas pelas capacidades fornecidas pelas ferramentas de segurança integradas ao sistema.

Além disso, o modelo destaca a utilização de roteiros, que representam fluxos estruturados de resposta a incidentes. Esses roteiros são projetados por especialistas e implementam planos de resposta automatizados, permitindo que a plataforma execute ações de forma coordenada, padronizada e com menor intervenção humana. Dessa forma, o SOAR contribui para aumentar a eficiência operacional, reduzir o tempo de resposta a incidentes e melhorar a integração entre diferentes soluções de segurança. A integração entre IDS , SIEM e SOAR possibilita que eventos detectados sejam automaticamente analisados e mitigados, reduzindo significativamente o impacto dos ataques [Bridges *et al.* 2023].

O que o SOAR não é ?

De acordo com [Kallimath e Savalagimath 2020], uma solução SOAR não substitui analistas qualificados. Implantar uma solução SOAR para substituir analistas inevitavelmente criará mais riscos em vez de mitigá-los. Em vez disso, uma solução SOAR deve ser vista como um facilitador tanto para o programa de segurança quanto para os analistas de segurança.

O SOAR é uma solução para mitigar ameaças à segurança por meio da automação, que é programada para coletar dados sobre ameaças à segurança de várias fontes e responder rapidamente a eventos de segurança de baixo nível sem intervenção humana.
As soluções SOAR não são projetadas para ingerir um grande volume de eventos brutos. Em vez disso, as soluções SOAR são projetadas para detectar o incidente onde a funcionalidade do SIEM termina, fornecendo uma resposta automatizada e orquestrada durante a fase de identificação, bem como nas fases de contenção, erradicação e recuperação.

2.5 Modelo Confiança Zero

O modelo de segurança *Zero Trust* (Confiança Zero) surgiu como resposta às limitações das arquiteturas tradicionais baseadas em perímetro. Seu princípio fundamental consiste em assumir que nenhuma entidade deve ser automaticamente confiável, independentemente de sua localização na rede [Narasappa 2025].
Nesse modelo, cada acesso é continuamente validado com base em identidade, comportamento e contexto operacional. Essa abordagem reduz a movimentação lateral de atacantes e melhora a capacidade de detecção de atividades suspeitas.
A integração do *Zero Trust* com sistemas de detecção e automação fortalece a segurança ao permitir respostas dinâmicas baseadas no nível de risco identificado.
A Figura 2.4 ilustra a arquitetura conceitual do modelo de segurança *Zero Trust*, que se baseia no princípio de que nenhum usuário, dispositivo ou sistema deve ser automaticamente confiável, independentemente de estar dentro ou fora da rede organizacional. Nesse modelo, todas as requisições de acesso são continuamente verificadas antes de serem autorizadas.

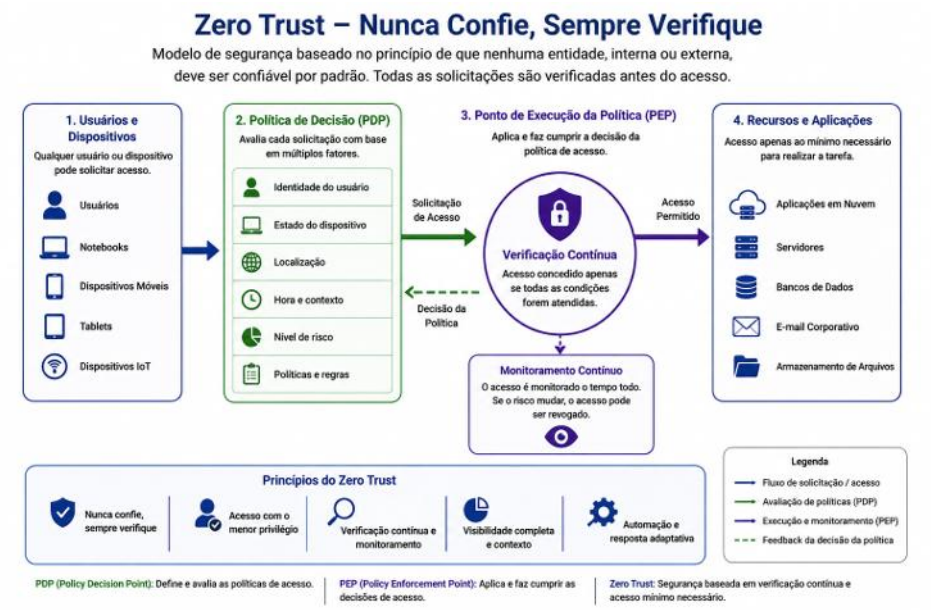


Figura 2.4: *Arquitetura conceitual do modelo de segurança Zero Trust. Fonte: [Narasappa 2025] (Adaptada pelo autor com auxilio de IA).*

A arquitetura é composta por três elementos principais: o (PDP) *Policy Decision Point* (Ponto de Decisão de Política), responsável por analisar políticas de segurança e tomar decisões de acesso; o (PEP) *Policy Enforcement Point* (Ponto de Aplicação de Política), que aplica as decisões de segurança permitindo ou bloqueando conexões; e o *Data Plane* (Plano de dado)s, que representa o ambiente onde estão localizados os sistemas, usuários e recursos da rede. O processo de decisão utiliza diversas fontes de informação, como políticas de acesso a dados, gerenciamento de identidade, sistemas SIEM, inteligência de ameaças e registros de atividades. Com base nesses dados, o sistema avalia continuamente o contexto das requisições e determina se o acesso deve ser autorizado ou bloqueado. Dessa forma, o modelo *Zero Trust* fortalece a segurança das redes ao reduzir riscos associados a acessos indevidos e movimentação lateral dentro da infraestrutura [Narasappa 2025].

2.6 Automação e Inteligência Artificial na Segurança de Redes

O aumento do volume de dados gerados nas redes modernas tornou inviável a análise manual de eventos de segurança. Como consequência, técnicas de aprendizado de máquina e análise comportamental passaram a ser aplicadas na detecção de ameaças.

Essas técnicas permitem:

- Identificação de padrões anômalos complexos;
- Detecção de ameaças desconhecidas;
- Análise preditiva de ataques;

- Redução de falsos positivos.

Quando combinadas com plataformas SOAR, essas abordagens possibilitam respostas automatizadas em tempo quase real, aumentando significativamente a capacidade defensiva das organizações [Vast *et al.* 2021]. A figura 2.5 ilustra a arquitetura de um ecossistema moderno de Orquestração, Automação e Resposta de Segurança (SOAR) integrado com capacidades de Inteligência Artificial (IA) e Inteligência de Ameaças (Threat Intelligence). O fluxo demonstra o ciclo de vida de um incidente, iniciando-se na coleta massiva de dados brutos provenientes de ferramentas de detecção e armadilhas (Suricata e TPOT) e seu posterior tratamento via pipeline de logs (Elastic Stack)

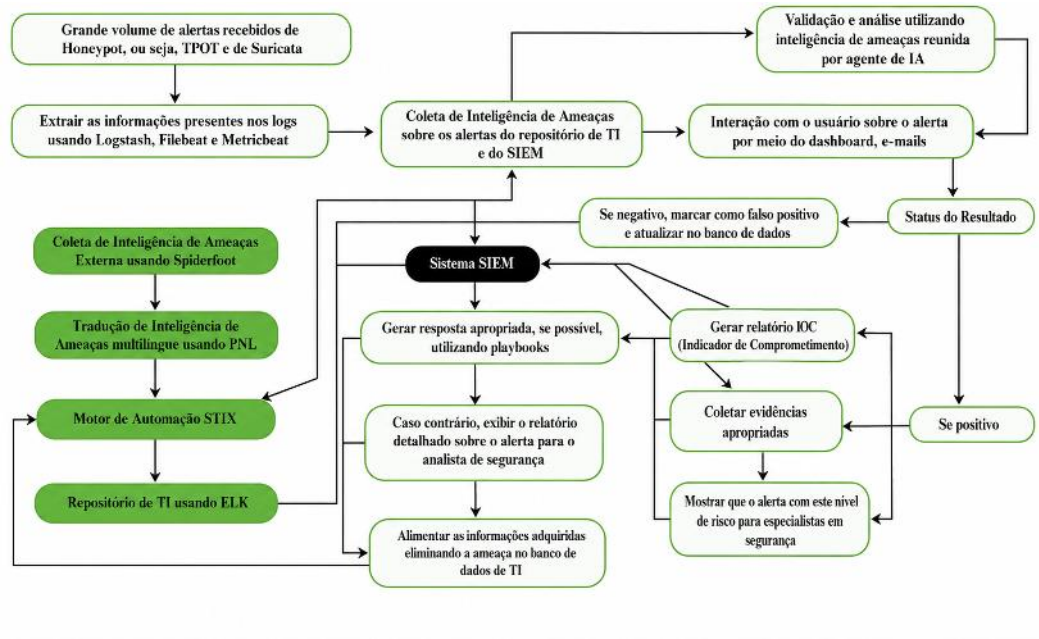


Figura 2.5: *Diagrama de um sistema de orquestração, automação e resposta de segurança baseado em inteligência artificial. Fonte: [Vast* et al. *2021] (Adaptado pelo autor com auxilio de IA).*

O grande diferencial do modelo está na automação dos processos analíticos: um agente de IA valida as ameaças em tempo real e consulta repositórios enriquecidos por ferramentas externas (como o Spiderfoot, processados via NLP e padronizados em STIX). A partir da classificação do status do alerta, o sistema bifurca sua execução: falsos positivos alimentam a base de conhecimento para calibração, enquanto ameaças reais disparam playbooks de resposta automatizada, geram relatórios de Indicadores de Comprometimento (IOC) e notificam os especialistas humanos apenas com alertas de alto risco filtrados. Esse modelo mitiga diretamente o problema da "fadiga de alertas"em Centros de Operações de Segurança (SOC), otimizando o tempo de resposta a incidentes críticos [Vast *et al.* 2021].

2.7 Integração entre Detecção e Resposta Automatizada

A literatura recente aponta que a integração entre mecanismos de detecção e sistemas automatizados de resposta representa uma das principais tendências da segurança

cibernética moderna. Arquiteturas integradas permitem que alertas gerados por IDS sejam correlacionados por sistemas SIEM e transformados em ações automáticas por plataformas SOAR [Mala *et al.* 2025]. A Figura 2.6, ilustra a integração entre os principais mecanismos modernos de segurança em redes computacionais, destacando a relação entre sistemas IDS, SIEM, SOAR e o modelo Zero Trust.

Figura 2.6: *Arquitetura Integrada entre IDS, SIEM, SOAR e Zero Trust. Fonte: (Elaborado pelo autor com auxilio de IA).*

Inicialmente, o IDS é responsável por monitorar o tráfego da rede e identificar atividades suspeitas ou comportamentos anômalos. Os eventos detectados são enviados ao SIEM, que centraliza, correlaciona e analisa logs provenientes de diferentes dispositivos e serviços da infraestrutura.

Em seguida, as informações processadas pelo SIEM são utilizadas pelo SOAR, responsável por automatizar processos de resposta a incidentes, executando ações como bloqueio de conexões, isolamento de dispositivos comprometidos e aplicação de políticas de contenção.

Paralelamente, o modelo *Zero Trust* atua de forma integrada, aplicando autenticação contínua, segmentação de rede e validação permanente de usuários e dispositivos, reduzindo a confiança implícita na infraestrutura.

A integração dessas tecnologias proporciona maior visibilidade da rede, redução do tempo de resposta a incidentes, automação de processos de segurança e fortalecimento da resiliência cibernética em ambientes corporativos modernos. Essa integração reduz o tempo entre detecção e mitigação, fator crítico para minimizar danos causados por ataques. Além disso, abordagens baseadas em automação contribuem para maior escalabilidade e eficiência operacional em ambientes complexos.

2.8 Síntese da Fundamentação Teórica

A análise dos conceitos apresentados demonstra uma evolução clara das arquiteturas de segurança: de mecanismos estáticos e isolados para ecossistemas integrados, automatizados e inteligentes. O IDS continuam desempenhando papel central na detecção de ameaças, porém sua eficácia é ampliada quando integrados a sistemas SIEM e SOAR, aliados a modelos modernos como *Zero Trust* e técnicas de inteligência artificial.
Essa base teórica sustenta a investigação proposta neste trabalho, que busca compreender como diferentes mecanismos de integração contribuem para a redução de incidentes de segurança em redes computacionais.

2.9 Revisão Sistemática da Literatura

É descrito a seguir, os procedimentos metodológicos adotados na condução da Revisão Sistemática da Literatura, utilizada para investigar mecanismos de IDS e sistemas automatizados de resposta a incidentes de segurança em redes computacionais.
Esta pesquisa foi conduzida por meio de uma Revisão Sistemática, um método escolhido por permitir a síntese e análise de um grande volume de informações sobre um determinado tema. De acordo com [Sampaio e Mancini 2007], esse tipo de revisão possibilita a incorporação de uma variedade maior de resultados relevantes, em vez de restringir as conclusões à leitura de um número limitado de estudos. [Silva 2019] destaca que a publicação de revisões sistemáticas pode servir como um meio para a disseminação contínua de contribuições significativas para a academia.

Tabela 2.1: *Principais referências metodológicas utilizadas para a condução da Revisão Sistemática.*

Referência	**Tipo de Estudo**	**Contribuição para o TCC**
Sampaio e Mancini (2007)	Guia Metodológico	Forneceu o roteiro para a síntese criteriosa da evidência científica e estruturação das etapas da revisão.
Silva (2019)	Artigo Editorial	Fundamentou a distinção entre revisões narrativas e sistemáticas, validando o rigor científico do método escolhido.

A Tabela 2.1 apresenta a caracterização dos estudos selecionados para esta Revisão Sistemática da Literatura, estruturada conforme o rigor metodológico sugerido por [Sampaio e Mancini 2007] e [Silva 2019] para garantir a transparência e a reprodutibilidade do processo de coleta. Os artigos foram analisados sob a ótica de suas contribuições para a detecção de ameaças e automação de respostas, abrangendo desde

soluções consolidadas de SIEM e IDS até arquiteturas emergentes como o framework SMASH (SDN-MTD) e modelos adaptativos de *Zero Trust*. A síntese desses estudos revela uma tendência clara de integração entre tecnologias como a convergência de SOAR com *Machine Learning* e inteligência artificial visando mitigar vulnerabilidades críticas e reduzir a carga operacional em ambientes de rede complexos.

Capítulo 3

Desenvolvimento

3.1 Fundamentação Teórica

A metodologia empregada neste trabalho baseia-se na realização de uma Revisão Sistemática da Literatura, seguindo diretrizes metodológicas amplamente utilizadas em pesquisas científicas. Inicialmente, foi definida uma questão de pesquisa voltada à integração entre mecanismos de detecção e resposta automatizada em segurança de redes. Em seguida, foram elaboradas termos de busca contendo palavras-chave relacionadas ao tema, aplicadas em bases científicas reconhecidas, como Scopus, IEEE Xplore e ScienceDirect, por meio do Portal de Periódicos CAPES. Após a etapa de busca, foram aplicados critérios de inclusão e exclusão para seleção dos estudos relevantes, considerando período de publicação, idioma, tipo de documento e aderência ao tema da pesquisa. Os artigos selecionados passaram por análise qualitativa, permitindo a extração e síntese das principais contribuições, tecnologias utilizadas, desafios identificados e resultados apresentados pelos autores.

3.2 Etapas da Revisão Sistemática

Neste estudo, a pesquisa segue as diretrizes do método PRISMA para revisar a literatura e orientar futuras pesquisas sobre o tema "Detecção e Ameaças em Redes". O processo de Revisão Sistemática incluiu as seguintes etapas:

- Definição da questão de pesquisa;
- Seleção das bases: Scopus, IEEE Xplore e ScienceDirect (via Portal CAPES);
- Definição de strings de busca;
- Aplicação de critérios de inclusão/exclusão;
- Triagem dos artigos;

- Síntese dos resultados.

A pergunta central foi "Quais mecanismos de integração entre IDS e sistemas de resposta automatizada ajudam a reduzir incidentes de segurança em redes?" A busca foi realizada por meio de *keyword strings* nas bases IEEE Xplore, Scopus e ScienceDirect. As buscas também foram realizadas na base Google Scholar, utilizando termos adaptadas, devido às limitações de operadores booleanos da plataforma. Foram utilizadas combinações de termos relacionados a IDS, SIEM, SOAR e *Zero Trust*, com o objetivo de ampliar a cobertura da literatura e identificar estudos relevantes não indexados em outras bases. Os termos selecionadas foram: (("intrusion detection system "OR" "IDS") AND ("security orchestration and automated response "OR" "SOAR") AND ("security information and event management "OR" "SIEM") AND ("zero trust")). Os resultados obtidos na primeira etapa, incluindo a definição dos termos e a escolha das fontes de busca podem ser vistos na Tabela 1. Foram criados filtros para selecionar os artigos (etapa 3) que trariam informações mais relevantes ao estudo (Tabela 3). O segundo filtro foi a seleção pelo idioma inglês e o terceiro, por tipo de produção acadêmica. Foram selecionados apenas artigos científicos e conferências enquanto outras formas textuais foram desconsideradas. Esta metodologia assegurou a identificação de estudos relevantes e consistentes, que permitiram a análise aprofundada do tema, conforme será apresentado nas seções subsequentes.

Tabela 1 — Termos de busca e quantidade obtida

Termos de busca aplicadas nas bases — valores de artigos encontrados.

String de Pesquisa	**Scopus**	**IEEE Xplore**	**ScienceDirect**	**Google Scholar**
(("intrusion detection system"“OR” "IDS") AND ("security orchestration and automated response"“OR” "SOAR") AND ("security information and event management"“OR” "SIEM") AND ("zero trust"))	17	18	13	67
Total (indicativo)	**125**			

A seleção foi fundamentada na relevância e qualidade dos resultados obtidos, com ênfase em estudos relacionados a tecnologias voltadas à detecção de ameaças em redes ou temas correlatos. A Tabela 2 ilustra a quantidade obtida de artigos nas bases de dados, após os filtros de pesquisa.

Tabela 2 — Quantidade obtida de artigos após os filtros de pesquisa em cada base

Plataforma	**Quantidade obtida**
Scopus	5
IEEE Xplore	16
ScienceDirect	4
Google Scholar	45
Total (indicativo)	**70**

Tabela 3 — Filtros aplicados e justificativa

Filtros aplicados na triagem e respectiva justificativa.

Filtro	**Justificativa**
Período: 2020–2025	Selecionar estudos recentes, acompanhando a evolução moderna dos sistemas IDS e das plataformas de resposta automatizada (SOAR, SIEM, automação de incidentes).
Idioma: Inglês	Estudos em inglês abrangem a maior parte da produção científica internacional.
Tipo de documento: Artigos científicos e artigos de conferências	Garante que somente estudos revisados por pares e tecnicamente validados façam parte da síntese.
Área de conhecimento: Computer Science, Engineering	Restringe a literatura às áreas diretamente relacionadas à segurança de redes e automação de resposta.
Disponibilidade de texto completo	Assegura possibilidade de leitura integral e extração metodológica dos dados.

Foi realizada a criação de filtros para seleção dos artigos que trariam informações mais relevantes ao estudo (Tabela 3). Selecionou-se inicialmente os artigos de 2020 até 2025, pois devido a atualidade das tecnologias, ainda não existem artigos em quantidade significativa que as avaliem, outra coisa importante foi o inico das buscas, que ocorreram em fevereiro de 2026.. O segundo filtro foi a seleção por idioma (inglês) e o terceiro, por produção literária. Foram selecionados apenas artigos científicos, incluindo os de revisão; capítulos de livros e outras formas textuais foram desconsideradas.

3.3 Fluxograma PRISMA

No quarto filtro foi realizada a seleção dos artigos. Os critérios de elegibilidade foram (i) a identificação da palavras "IDS", "SOAR", "Security orquestration,automation and response" explícita no resumo e (ii) Termos que remetessem ao universo que abrange segurança de redes e ameaças, tais como: intrusion detection, security networks, Internet das Coisas. Ao final, conforme Figura 3.1, restaram 39, dos quais foram lidos apenas 19 para verificar se abrangiam o tema escolhido: Detecção e ameaças em redes. As etapas 4, 5, 6 e 7 – coleta de dados, análise e apresentação dos dados, interpretação dos dados e análise crítica, respectivamente – serão apresentadas e discutidas nas seções seguintes.

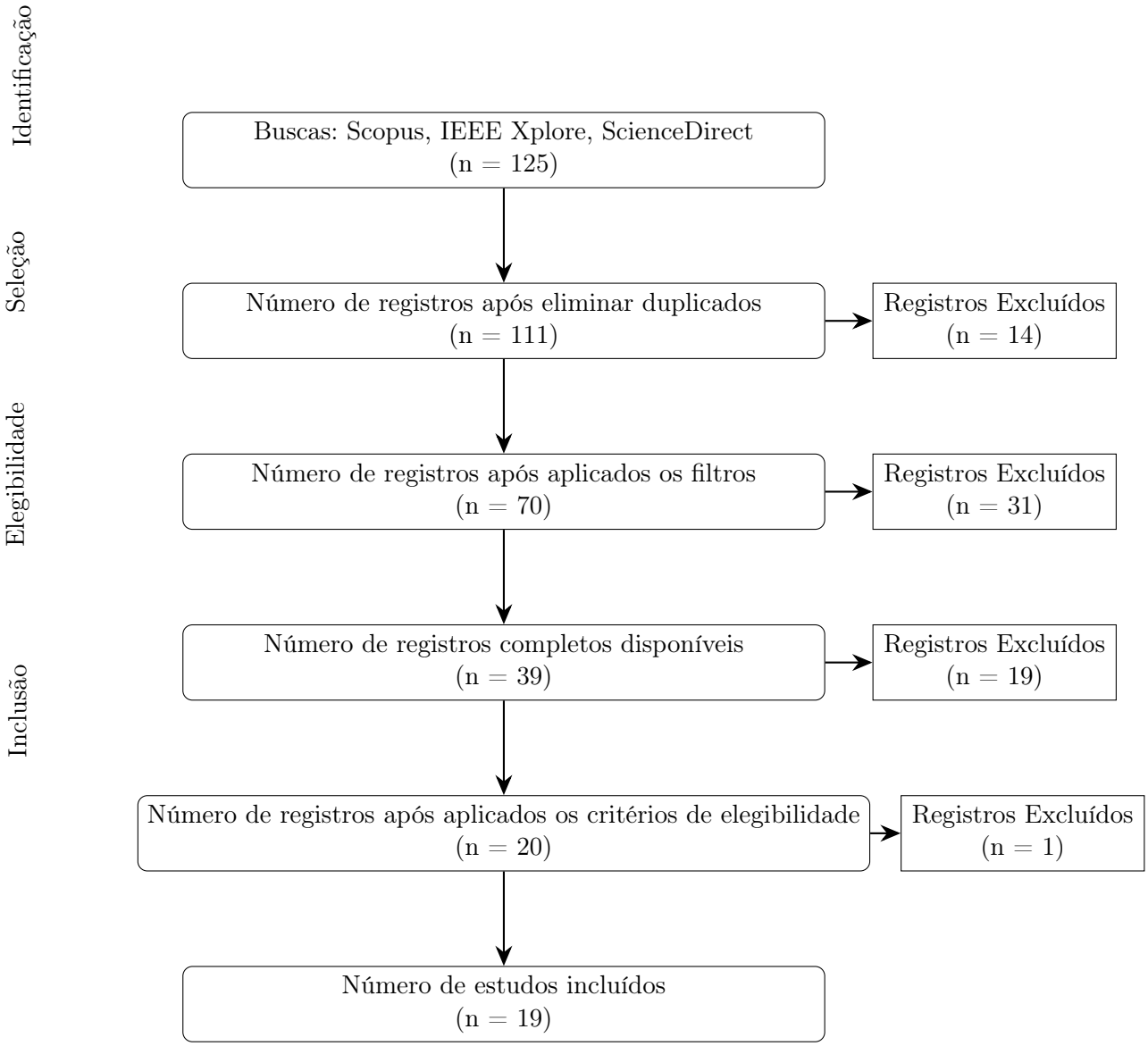


Figura 3.1: *Fluxograma PRISMA da revisão sistemática. Fonte: (Elaborado pelo autor)*

A Figura 3.1 ilustra o fluxograma do processo de seleção dos estudos incluídos nesta Revisão Sistemática da Literatura, seguindo a lógica do protocolo PRISMA. Inicialmente, foram coletados 125 artigos nas bases de dados consultadas. Após a aplicação de critérios

iniciais de relevância, 39 estudos foram considerados potencialmente relacionados ao tema da pesquisa.

Na etapa seguinte, após a análise dos títulos, resumos e critérios de elegibilidade, os 39 artigos foram selecionados para avaliação mais detalhada. Por fim, após a leitura completa e aplicação dos critérios de inclusão e exclusão definidos na metodologia, 19 artigos foram efetivamente escolhidos para compor a análise final da revisão sistemática.

Esse processo estruturado de filtragem permitiu reduzir gradualmente o conjunto inicial de estudos, garantindo que apenas pesquisas relevantes e alinhadas aos objetivos do trabalho fossem incluídas na análise.

3.4 Distribuição de artigos pesquisados

A Figura 3.2 apresenta a distribuição dos artigos coletados nas bases de dados utilizadas na pesquisa, totalizando 125 trabalhos.

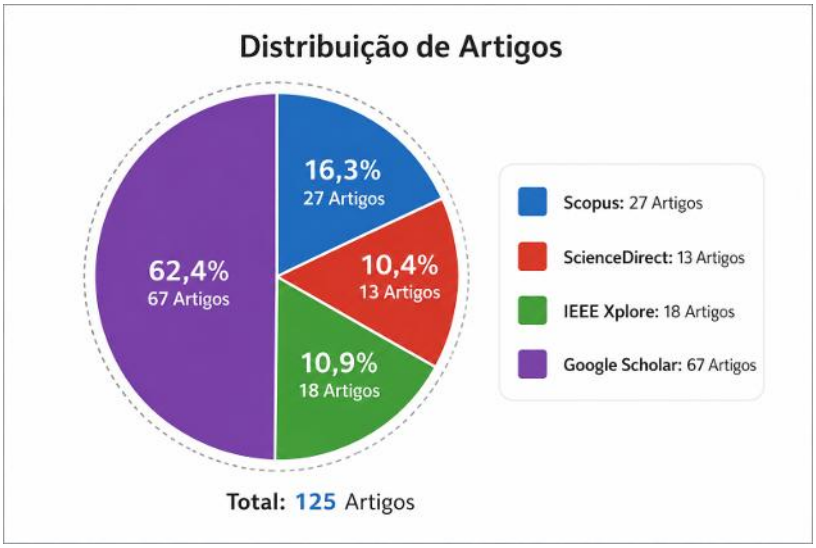


Figura 3.2: *Distribuição dos artigos encontrados nas bases de dados. Fonte: (Elaborado pelo autor com auxilio de IA).*

Observa-se que o Google Scholar concentrou a maior quantidade de publicações, com 67 artigos (62,4%), demonstrando sua relevância como fonte complementar de estudos científicos na área de segurança em redes. Em seguida, a base Scopus apresentou 27 artigos (16,3%), enquanto a IEEE Xplore contribuiu com 18 artigos (10,9%). A menor participação foi identificada na ScienceDirect, com 13 artigos (10,4%). Esses resultados demonstram que a maior parte dos estudos relacionados ao tema foi encontrada no Google Scholar, enquanto as demais bases contribuíram de forma complementar para a composição da revisão sistemática da literatura.

Capítulo 4

Resultados

Este capítulo apresenta os resultados obtidos a partir da Revisão Sistemática da Literatura, conduzida conforme o protocolo PRISMA descrito no Capítulo anterior. A análise dos estudos selecionados teve como objetivo identificar como a integração entre Sistemas de Detecção de Intrusão (IDS) e mecanismos automatizados de resposta contribui para a redução de incidentes de segurança em redes computacionais.
Os resultados são apresentados de forma analítica, destacando tendências observadas, tecnologias empregadas e contribuições identificadas nos artigos analisados.

4.1 Resultados da Revisão Sistemática

A busca, triagem e análise dos estudos permitiu identificar um conjunto de 20 artigos relevantes relacionados aos mecanismos de integração entre Sistemas de Detecção de Intrusão e Sistemas de Resposta Automatizada, tais como SOAR, SIEM e arquiteturas *Zero Trust* - (Confiança Zero). Após a remoção de duplicados, leitura de títulos, resumos e, posteriormente, leitura completa, 19 estudos atenderam integralmente aos critérios de inclusão estabelecidos na etapa de planejamento da revisão.
Os resultados são apresentados a seguir por meio de uma caracterização geral dos estudos selecionados, seguida de análises estruturadas que incluem: classificação metodológica, distribuição temporal da produção científica, categorização temática e síntese comparativa das contribuições.
A Tabela 4.1 ilustra informações essenciais dos cinco estudos incluídos, já as tabelas 4.2 e 4.3 são apenas as continuações da tabela. Contendo autor, ano, objetivo, abordagem aplicada e principais contribuições para o tema de integração entre IDS e sistemas de resposta automatizada.

Tabela 4.1: *Caracterização dos estudos selecionados na Revisão Sistemática da Literatura.*

Artigo	Autor(es)/Ano	Tecnologias	Objetivo do Estudo	Principais Contribuições
SIEM Integration with SOAR for Automated Incident Response	Ahmed e Khan (2022)	SIEM, SOAR, Automação	Integrar plataformas SIEM e SOAR para automatizar processos de resposta a incidentes.	Redução do tempo de resposta (MTTR), automação de playbooks e melhoria da correlação de eventos de segurança.
SIEM integration with SOAR	Sridharan e Kanchana (2022)	SIEM, SOAR, IDS, IPS	Propor integração entre SIEM e SOAR para lidar com grandes volumes de dados e ameaças avançadas[cite: 505, 508].	Redução do volume de alertas no SOC através da identificação de casos duplicados e diminuição do tempo de resposta[cite: 508].
Integration of Intrusion Detection Systems with Automated Response Mechanisms	Garcia e Mendes (2023)	IDS, Resposta Automatizada	Investigar integração entre IDS e mecanismos automatizados de resposta.	Mitigação dinâmica de ameaças e melhoria da eficiência operacional.
Autonomous Intrusion Detection and Response using Machine Learning Techniques	Rahman e Islam (2022)	IDS, Machine Learning	Desenvolver modelo autônomo de detecção utilizando aprendizado de máquina.	Redução de falsos positivos e aumento da precisão da detecção de ameaças.
Integrating Zero Trust Architecture with Automation and Analytics for Resilient Cybersecurity	Narasappa (2025)	Zero Trust (ZTA), SOAR, ML	Propor um framework unificado que integra ZTA com automação adaptativa ao risco e análise baseada em Machine Learning[cite: 2].	Desenvolvimento do sistema RAAC para decisões de acesso dinâmicas e uso de Isolation Forests para detecção de anomalias com 96,4% de precisão[cite: 3, 6].
A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems	Mukhopadhyay et al. (2011)	IDS, IPS, Firewall	Realizar estudo comparativo entre tecnologias de detecção e prevenção de intrusão.	Definição do IPS como controle ativo e evolução tecnológica sobre firewalls tradicionais.

Tabela 4.2: *Continuação da caracterização dos estudos selecionados.*

Artigo	Autor(es)/Ano	Tecnologias	Objetivo do Estudo	Principais Contribuições
Moving Target Defense and Honeypots for Adaptive Cyber Defense	Wang e Zhou (2024)	MTD, Honeypots	Aplicar técnicas adaptativas para mitigação de ameaças avançadas.	Maior resiliência da infraestrutura e aumento da dificuldade de exploração por atacantes.
Towards Automatic Detection and Mitigation of High-Risk Cybersecurity Vulnerabilities at Networked Systems	Polónio, Moura e Marinheiro (2025)	SOAR, SDN, VLAN	Propor arquitetura automatizada para mitigação de vulnerabilidades críticas.	Descoberta automática de dispositivos, classificação de riscos e mitigação dinâmica baseada em VLANs.
Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment	Lee, Jang-Jaccard e Kwak (2022)	SOAR, IoT	Propor arquitetura SOAR aplicada a ambientes conectados e IoT.	Integração entre automação e análise de ameaças em ambientes híbridos.
Automating Security Incident Response in SCADA Systems through SIEM-ML Integration	Al-Dahasi e Khan (2024)	SIEM, Machine Learning, SCADA	Automatizar resposta a incidentes em sistemas SCADA.	Aplicação de aprendizado de máquina para acelerar detecção e mitigação de ameaças industriais.
Artificial Intelligence based Security Orchestration, Automation and Response System	Vast et al. (2021)	IA, SOAR, Deep Learning	Propor um sistema SOAR baseado em IA com perfil de eventos individual usando detecção por Deep Learning[cite: 917].	Padronização de dados de múltiplas fontes (firewalls, IDS) e geração automática de relatórios de Indicadores de Comprometimento (IoC)[cite: 918, 919].

Tabela 4.3: *Continuação da caracterização dos estudos selecionados.*

Artigo	Autor(es)/Ano	Tecnologias	Objetivo do Estudo	Principais Contribuições
Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots	Bartwal et al. (2022)	SOAR, Honeypots	Implementar honeypots comportamentais integrados ao SOAR.	Aprimoramento da detecção e análise automatizada de ataques.
Testing SOAR Tools in Use	Bridges et al. (2023)	SOAR	Avaliar ferramentas SOAR utilizadas em ambientes reais.	Identificação de limitações e benefícios operacionais das plataformas SOAR.
Reducing the Risk of Social Engineering Attacks Using SOAR Measures in a Real World Environment	Waelchli e Walter (2025)	SOAR, Engenharia Social	Propor medidas de SOAR para reduzir a suscetibilidade humana a ataques de engenharia social em ambientes reais[cite: 2532].	Redução do risco através de playbooks que forçam troca de senhas ou bloqueio de contas após detecção de incidentes[cite: 2537].
Implementing and evaluating a GDPR-compliant open-source SIEM solution	Vazão et al. (2023)	SIEM, GDPR, Elastic Stack	Definir e validar uma solução SIEM de código aberto que garanta conformidade com o GDPR através de medidas técnicas[cite: 1338].	Desenvolvimento de algoritmo de pseudonimização de logs em tempo real e avaliação de desempenho em ambiente real[cite: 1341, 1342].
SPIFFE-Based Zero-Trust Authentication for AI Agent Ecosystems	Pappu, Bhushan e Mittal (2025)	Zero Trust, Autenticação	Implementar autenticação Zero Trust para ecossistemas baseados em IA.	Fortalecimento da autenticação contínua e proteção de agentes inteligentes.
SMASH: An SDN-MTD framework for efficient honeypot deployment	d'Ambrosio et al. (2025)	SDN, MTD, Honeypots	Mitigar ameaças internas e automatizar a implementação de honeypots.	Uso de Redes Definidas por Software (SDN) para criar defesas proativas e enganar atacantes.
Network Access Control Technology Proposition	Lakbabi, Orhanou e El Hajji (2012)	NAC, Firewall, IDS/IPS	Analisar a interação entre NAC e outros componentes para uma postura de segurança centralizada.	Proposta de um servidor de política central (PDP) atuando como ponto de orquestração da rede.
The Complete Guide to Security Orchestration, Automation and Response (SOAR)	Kallimath e Savalagimath (2023)	SOAR, Threat Intelligence	Definir as funções críticas do SOAR e o alinhamento de workflows a procedimentos operacionais.	Sistematização dos componentes do SOAR: orquestração, automação, gestão de casos e inteligência de ameaças.

4.1.1 Principais tecnologias e aplicações relacionadas à detecção de ameaças em redes, segundo os estudos analisados.

A Figura 4.1 ilustra uma organização visual das principais tecnologias, componentes e aplicações associadas à detecção de ameaças em redes encontradas nos estudos analisados. O diagrama evidencia como diferentes mecanismos trabalham de forma integrada para compor uma arquitetura moderna de segurança cibernética.

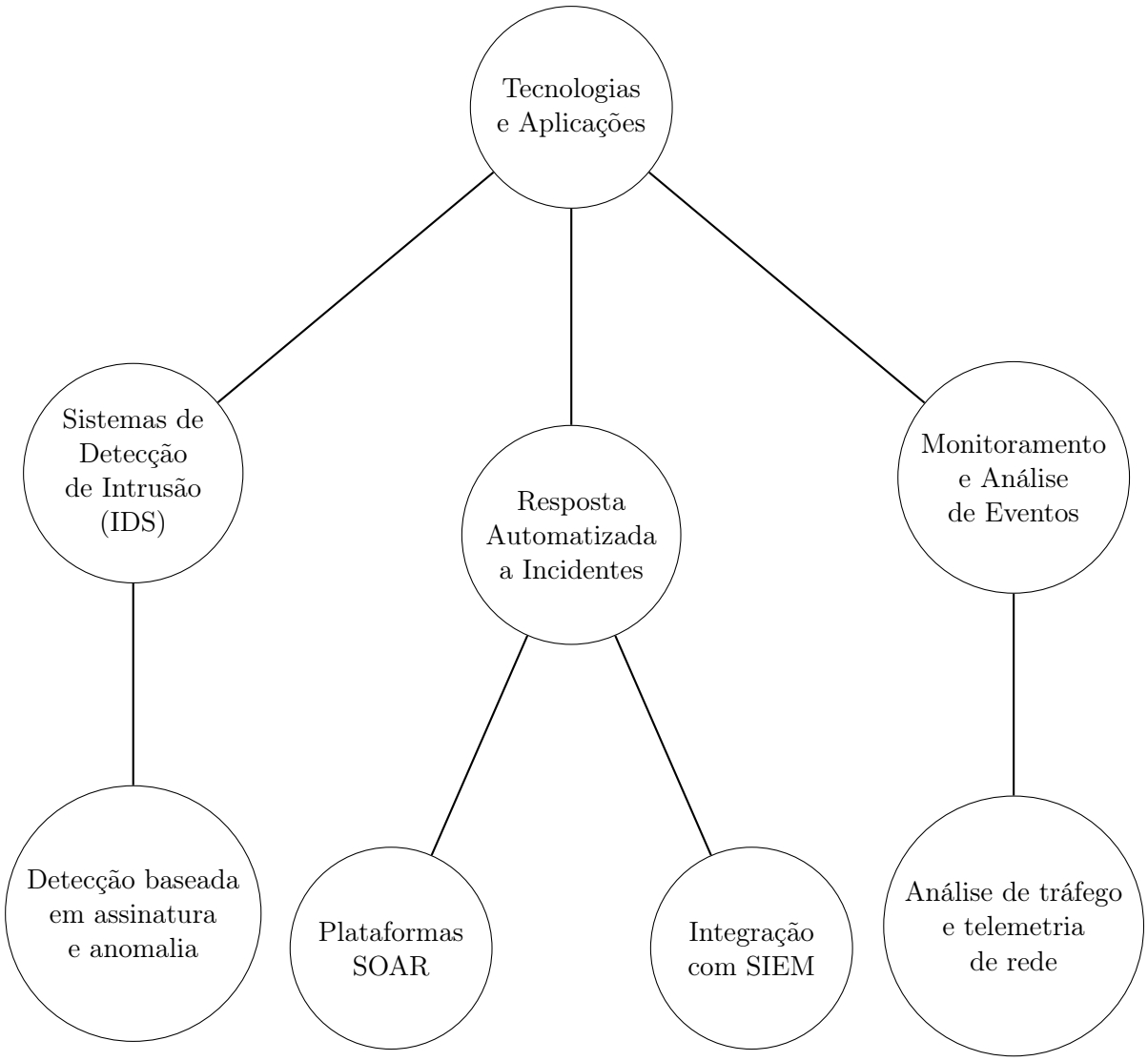


Figura 4.1: *Principais tecnologias e aplicações relacionadas à detecção de ameaças em redes, segundo os estudos analisados. Fonte:(Elaborado pelo autor).*

A Figura 4.1 ilustra inicialmente o papel dos Sistemas de Detecção de Intrusão, que empregam métodos baseados em assinatura, anomalia ou modelos híbridos para identificar atividades suspeitas no tráfego de rede. Esses sistemas funcionam como o núcleo da detecção, alimentando os demais componentes com informações essenciais.

Em seguida, observa-se a integração direta com plataformas de Resposta Automatizada, principalmente soluções SOAR, que executam ações de mitigação definidas em roteiros, permitindo redução de tempo de resposta e menor dependência de intervenção humana. A figura 4.1 também ilustra a interação com sistemas SIEM, responsáveis pela coleta, normalização e correlação de *logs* provenientes de diversas fontes, ampliando a visibilidade sobre o ambiente e fornecendo dados ricos para automação.

Além disso, a figura 4.1 ilustra tecnologias complementares como análise de tráfego, telemetria e monitoramento contínuo, que sustentam uma abordagem mais robusta de detecção e resposta. Em síntese, a Figura 4.1 ilustra que a efetividade na detecção de ameaças depende da combinação entre monitoramento, análise e automação, reforçando a

importância do alinhamento entre IDS, SIEM e SOAR.

4.1.2 Os desafios associados à integração entre sistemas de detecção de intrusão e resposta automatizada.

A figura 4.2 resume os principais desafios identificados nos estudos quanto à integração entre sistemas de detecção de intrusões e mecanismos automatizados de resposta. O diagrama retrata como cada obstáculo impacta diretamente a eficácia e a escalabilidade das soluções.

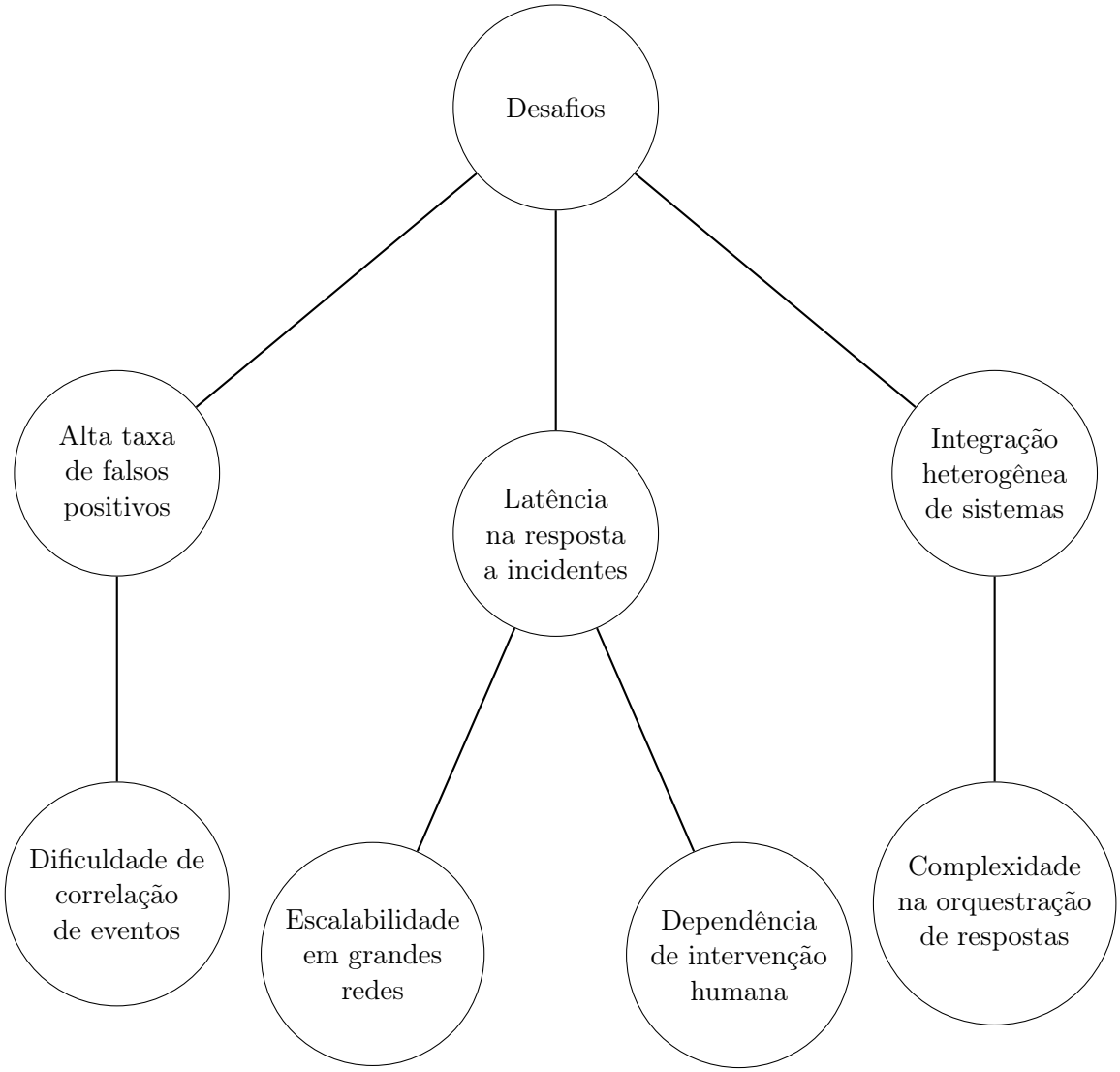


Figura 4.2: *Principais desafios associados à integração entre sistemas de detecção de intrusão e resposta automatizada. Fonte: (Elaborado pelo autor).*

Entre os desafios mais recorrentes, destaca-se a alta taxa de falsos positivos, que compromete a precisão das decisões automatizadas e pode levar à execução indevida de ações corretivas. Outro ponto crítico é a latência na resposta, especialmente em ambientes distribuídos ou com grande volume de tráfego, dificultando a contenção rápida de incidentes.

A figura também evidencia a heterogeneidade dos sistemas, que torna complexa a orquestração entre ferramentas distintas, como IDS, SIEM e SOAR. A correlação de eventos surge como outro problema relevante, já que a fusão de dados de múltiplas fontes exige modelos avançados de análise para evitar interpretações equivocadas.
Outros desafios incluem questões de escalabilidade, principalmente em redes amplas ou de alta criticidade, e a dependência de intervenção humana, ainda necessária em cenários que exigem julgamento contextual. A complexidade da orquestração de respostas automatizadas reforça a necessidade de arquiteturas mais adaptativas e soluções baseadas em *Machine Learning* (Aprendizado de Máquina).
Assim, a figura sintetiza os principais entraves práticos para a adoção plena de automação na segurança de redes, servindo como base para discussão de soluções emergentes e lacunas da literatura.

4.2 Visão Geral dos Estudos Selecionados

Após a aplicação dos critérios de seleção, os artigos científicos considerados diretamente relacionados à questão de pesquisa proposta,foram incluídos para a síntese dos resultados. Esses estudos abordam diferentes perspectivas da segurança em redes, incluindo integração SIEM-SOAR, arquiteturas *Zero Trust*, automação de resposta a incidentes e uso de inteligência artificial na detecção de ameaças. As Tabelas 4.4 e 4.5, apresentam uma visão geral dos trabalhos analisados.

Tabela 4.4: *Artigos selecionados na Revisão Sistemática (Parte 1)*

Autor/Ano	**Tema Principal**	**Contribuição**
Kallimath e Savalagimath (2023)	Definição e Funções do SOAR	Guia completo sobre orquestração, automação e gestão de incidentes.
Ahmed e Khan (2022)	Integração SIEM-SOAR	Automação da resposta a incidentes e redução do MTTR.
Bridges et al. (2023)	Orquestração de Segurança	Metodologias para automação de fluxos de trabalho em operações de segurança.
Bartwal et al. (2022)	Frameworks de Resposta	Análise de eficácia de sistemas de resposta a incidentes em tempo real.
Lee, Jang-Jaccard e Kwak (2022)	Detecção de Ameaças	Uso de técnicas avançadas para identificação proativa de vetores de ataque.
Sridharan e Kanchana (2022)	SIEM e SOAR	Gestão de grandes volumes de dados e redução de alertas duplicados.
Narasappa (2025)	Zero Trust e SOAR	Framework RAAC para decisões de acesso dinâmicas com 96,4% de precisão.
d'Ambrosio et al. (2025)	SDN e MTD (SMASH)	Automação de honeypots para mitigação de ameaças internas.
Lakbabi et al. (2012)	NAC e IDS/IPS	Proposta de servidor de política central (PDP) para orquestração de rede.
Mukhopadhyay et al. (2011)	IDS e IPS	Estudo comparativo definindo o IPS como controle ativo sobre firewalls.

Tabela 4.5: *Artigos selecionados na Revisão Sistemática (Continuação)*

Autor/Ano	**Tema Principal**	**Contribuição**
Vast et al. (2021)	IA e SOAR	Uso de Deep Learning para perfil de eventos e geração de IoCs.
Vazão et al. (2023)	SIEM e GDPR	Pseudonimização de logs em tempo real para conformidade de dados.
Waelchli e Walter (2025)	SOAR e Eng. Social	Playbooks automatizados para mitigação de riscos do fator humano.
Wang e Zhou (2024)	MTD e Honeypots	Aumento da resiliência da infraestrutura via defesa adaptativa.
Polónio et al. (2025)	SOAR e SDN	Mitigação dinâmica de vulnerabilidades através de isolamento por VLAN.
Al-Dahasi e Khan (2024)	SIEM e SCADA	Automação de resposta em sistemas críticos industriais usando ML.
Pappu et al. (2025)	Zero Trust e IA	Autenticação baseada em SPIFFE para ecossistemas de agentes de IA.
Garcia e Mendes (2023)	Detecção Inteligente	Investigação de mecanismos automatizados integrados ao IDS.
Rahman e Islam (2022)	IDS e ML	Redução de falsos positivos através de modelos autônomos de detecção.

Observa-se que todos os estudos convergem para a necessidade de automatizar o processo de resposta a incidentes, reduzindo a dependência da intervenção humana.

4.2.1 Integração entre IDS, SIEM e SOAR

Um dos principais resultados identificados foi a consolidação da integração entre IDS, SIEM e plataformas SOAR como abordagem central para segurança moderna em redes. Os artigos analisados demonstram que o IDS atua como mecanismo inicial de detecção, responsável por monitorar o tráfego e identificar comportamentos suspeitos. Em seguida, sistemas SIEM realizam a correlação de eventos provenientes de múltiplas fontes, permitindo contextualizar o incidente detectado.

Por fim, plataformas SOAR executam respostas automatizadas, como bloqueio de endereços IP, isolamento de dispositivos comprometidos e geração automática de alertas operacionais.

Os estudos indicam que essa integração reduz significativamente o MTTR (Mean Time to Repair - tempo médio de resposta a incidentes), fator considerado crítico na contenção de ataques cibernéticos.

4.2.2 Automação da Resposta a Incidentes

Os resultados apontam que a automação é um dos elementos mais relevantes para a evolução da segurança em redes. A literatura evidencia que Centros de Operações de

Segurança enfrentam grande volume de alertas diários, tornando inviável a análise manual de todos os eventos.

A utilização de roteiros automatizados em plataformas SOAR permite executar ações previamente definidas assim que determinados padrões são identificados pelo IDS ou SIEM. Essa abordagem reduz erros humanos e aumenta a velocidade de mitigação de ameaças. Além disso, os estudos mostram que a automação contribui para padronizar processos de resposta, garantindo maior consistência nas ações executadas.

4.2.3 Uso de Inteligência Artificial na Detecção

Outro resultado relevante identificado foi o crescente uso de técnicas de aprendizado de máquina para aprimorar a detecção de intrusões.

Os artigos analisados indicam que modelos inteligentes conseguem identificar padrões anômalos em grandes volumes de tráfego de rede, aumentando a capacidade de detecção de ataques desconhecidos *Zero-day*. Essas técnicas também auxiliam na redução de falsos positivos, um dos principais desafios enfrentados por sistemas IDS tradicionais.

A combinação entre detecção baseada em inteligência artificial e resposta automatizada foi apontada como tendência dominante na literatura recente.

4.2.4 Arquiteturas *Zero Trust* e Segurança Contínua

Os estudos também destacam a adoção crescente do modelo *Zero Trust*, no qual nenhuma entidade da rede é considerada confiável por padrão.

Nesse modelo, mecanismos de detecção e resposta operam continuamente, validando acessos e monitorando comportamentos em tempo real. A integração com sistemas automatizados permite respostas imediatas diante de atividades suspeitas, reduzindo movimentações laterais de atacantes dentro da rede.

Essa abordagem reforça a importância da integração entre monitoramento contínuo e automação de segurança.

4.2.5 Síntese dos Resultados

De forma geral, os principais resultados da Revisão Sistemática indicam que:

- A integração IDS–SIEM–SOAR representa a arquitetura predominante em segurança moderna;
- A automação reduz significativamente o tempo de resposta a incidentes;
- Técnicas de aprendizado de máquina aumentam a eficiência da detecção;
- O modelo Zero Trust fortalece estratégias de monitoramento contínuo;

- A combinação entre detecção inteligente e resposta automatizada aumenta a resiliência das redes.

Esses resultados demonstram que a evolução da segurança em redes está diretamente associada à automação e à integração de múltiplas camadas de defesa, consolidando uma abordagem mais adaptativa frente às ameaças cibernéticas atuais.

4.2.6 Discussão dos Resultados

A análise conjunta dos estudos demonstra que a segurança em redes está evoluindo de modelos reativos para arquiteturas proativas e automatizadas. Enquanto soluções tradicionais dependiam majoritariamente da análise humana, os sistemas atuais combinam detecção inteligente, correlação de eventos e resposta automatizada.

Os resultados indicam que a integração entre IDS e sistemas automatizados responde diretamente à questão de pesquisa deste trabalho, evidenciando que mecanismos de orquestração e automação são capazes de reduzir o impacto de incidentes de segurança ao diminuir o tempo de resposta e aumentar a precisão das ações de mitigação.

Entretanto, os estudos também apontam desafios importantes, como a complexidade de integração entre ferramentas heterogêneas, necessidade de ajuste contínuo dos modelos inteligentes e riscos associados à automação excessiva sem supervisão adequada. A análise integrada dos estudos selecionados revela que a segurança de redes contemporânea está deixando de ser uma estrutura baseada em perímetros estáticos para se tornar um ecossistema dinâmico e adaptativo. A convergência entre monitoramento, inteligência e resposta automática emerge como a principal tendência para lidar com a sofisticação das ameaças cibernéticas.

Orquestração e Definição Funcional do SOAR

A base da resposta moderna a incidentes reside na integração entre SIEM e SOAR. De acordo com [Kallimath e Savalagimath 2020], o SOAR redefine a operação de segurança ao permitir a ingestão de dados de fontes heterogêneas e a aplicação de fluxos de trabalho alinhados a procedimentos operacionais padrão. Essa definição é corroborada por [Ahmed e Khan 2022], que demonstram que tal integração é vital para a redução do Tempo Médio de Reparo, permitindo que processos que antes levavam horas sejam executados em segundos via *playbooks*.

[Sridharan e Kanchana 2022] complementam essa visão ao destacar que o uso do SOAR auxilia na gestão da fadiga de alertas no *Security Operations Center* - (Centro de Operações de Segurança), filtrando eventos duplicados. [Kallimath e Savalagimath 2020] reforçam que o valor central do SOAR não é apenas a automação, mas a assistência "potencializada por máquinas"aos analistas humanos, garantindo consistência e visibilidade em paineis de controles centralizados de gerenciamento de casos.

Defesa Proativa, Decepção e SDN

Uma das contribuições mais inovadoras encontrada nesta revisão é o uso de SDN (*Software Defined Networking* - Rede Definida por Software) para defesas proativas. O framework *SMASH*, proposto por [d'Ambrosio *et al.* 2025], utiliza a flexibilidade da SDN para implementar o conceito de *Honeypot as a Service*. Ao integrar técnicas de MTD (*Moving Target Defense* - Defesa contra Alvos Móveis), o sistema consegue enganar atacantes e mitigar ameaças internas de forma automática. Esta abordagem é reforçada por [Wang e Zhou 2024], que argumentam que a resiliência da infraestrutura aumenta exponencialmente quando o atacante é confrontado com um ambiente cujas propriedades mudam constantemente.

A mitigação técnica em nível de rede também é abordada por [Polónio, Moura e Marinheiro 2025], que demonstram como o SOAR interage com controladores SDN para realizar o isolamento imediato de *hosts* comprometidos através da reconfiguração dinâmica de VLANs. Essa interação entre orquestração de segurança e controle de acesso é um conceito que remonta aos trabalhos de [Lakbabi, Orhanou e Hajji 2013] e [Mukhopadhyay *et al.* 2011], que já discutiam a importância de sistemas de prevenção (IPS) e controle de acesso (NAC) atuarem como braços executores de políticas centralizadas.

Inteligência Artificial e a Arquitetura Zero Trust

A Inteligência Artificial atua como o motor dessa automação. [Vast *et al.* 2021] propõem um sistema SOAR que utiliza *Deep Learning* para criar perfis de eventos individuais, permitindo a geração automática de Indicadores de Comprometimento. No campo da detecção, [Rahman e Islam 2022] provam que o aprendizado de máquina é essencial para reduzir a taxa de falsos positivos em IDS. Essa capacidade inteligente torna-se crítica em ambientes de alta complexidade, como os sistemas SCADA (*Supervisory Control and Data Acquisition* - Supervisão e Aquisição de Dados) analisados por [Al-Dahasi e Khan 2024], onde a automação pode prevenir danos físicos em infraestruturas industriais.

No topo dessa pirâmide tecnológica, a arquitetura *Zero Trust* redefine o acesso. [Narasappa 2025] propõe o sistema RAAC (*Risk-Adaptive Access Control* - Controle de Acesso Adaptável ao Risco), que utiliza modelos de *Isolation Forests* para detectar anomalias com 96,4% de precisão, adaptando as permissões de acesso em tempo real. Essa segurança contínua é estendida para ecossistemas de agentes de IA por [Pappu, Bhushan e Mittal 2025], que utilizam identidades baseadas no protocolo SPIFFE (*Secure Production Identity Framework for Everyone* - Estrutura de Identidade Segura para Produção para Todos) para garantir a autenticidade em ambientes de nuvem.

Conformidade e o Fator Humano

Por fim, a discussão aponta que a automação não deve negligenciar a privacidade e o fator humano. [Vazão *et al.* 2023] trazem uma contribuição prática essencial ao demonstrar que

soluções de monitoramento podem ser *compliant* com o GDPR (*General Data Protection Regulation* - Regulamento Geral sobre a Proteção de Dados) através de algoritmos de pseudonimização de logs. Paralelamente, [Waelchli e Walter 2025] abordam a vulnerabilidade humana, demonstrando que o SOAR pode combater a Engenharia Social ao automatizar o bloqueio preventivo de credenciais e forçar a troca de senhas após a detecção de incidentes suspeitos.

Em suma, os resultados indicam que o futuro da defesa de redes reside na integração profunda: a visibilidade do SIEM, a inteligência da IA, a flexibilidade da SDN e o rigor do Zero Trust, todos orquestrados por plataformas SOAR que, como definido por [Kallimath e Savalagimath 2020], unem pessoas, processos e tecnologia em um fluxo de trabalho unificado.

Capítulo 5

Considerações Finais e Sugestões para Trabalhos Futuros

Este capítulo apresenta, primeiramente, as considerações finais obtidas a partir da Revisão Sistemática. Permite concluir que integrar IDS e sistemas de resposta automatizada reduz significativamente incidentes de segurança. Plataformas SOAR e SIEM desempenham função central na coordenação e execução de ações rápidas, combinando múltiplas tecnologias em uma arquitetura moderna e eficaz.

5.1 Considerações Finais

O presente trabalho teve como objetivo investigar as abordagens relacionadas à detecção e mitigação de ameaças em redes computacionais, com foco específico na integração entre IDS e mecanismos automatizados de resposta a incidentes, como plataformas SIEM e SOAR. A motivação para este estudo esteve associada ao crescimento da superfície de ataque das infraestruturas digitais e à necessidade de reduzir o tempo de resposta diante de ameaças cada vez mais sofisticadas.

Por meio da Revisão Sistemática da Literatura, conduzida conforme protocolo metodológico estruturado, foi possível identificar as principais estratégias adotadas na literatura para integração entre mecanismos de detecção e resposta. Os resultados evidenciam que a automação de processos de segurança, aliada à correlação inteligente de eventos e ao uso de técnicas de aprendizado de máquina, contribui significativamente para a redução do Tempo Médio de Detecção e do Tempo Médio de Resposta, além de diminuir a dependência de intervenção humana em tarefas repetitivas.

Observou-se também que plataformas SIEM desempenham papel central na consolidação e análise de grandes volumes de *logs*, enquanto soluções SOAR ampliam a capacidade operacional ao permitir a execução automatizada de *playbooks* de resposta. A integração eficiente entre essas ferramentas possibilita respostas mais rápidas e consistentes, aumentando a resiliência organizacional frente a ataques avançados.

Entretanto, a análise dos estudos selecionados revelou desafios relevantes, como a alta taxa de falsos positivos em sistemas de detecção, dificuldades de interoperabilidade entre

ferramentas heterogêneas, complexidade na orquestração de respostas automatizadas e questões relacionadas à confiabilidade das decisões baseadas em inteligência artificial. Esses fatores demonstram que, embora a automação represente um avanço significativo, sua implementação exige planejamento estratégico, padronização e governança adequada.
Como principal contribuição, este trabalho sistematiza o estado da arte sobre a integração entre detecção e resposta automatizada, organizando as evidências científicas disponíveis, identificando lacunas e apontando tendências tecnológicas emergentes, como o uso de arquiteturas *Zero Trust* e modelos baseados em análise comportamental.
Como limitações, destaca-se a restrição às bases de dados selecionadas e ao período definido no protocolo da RSL, o que pode ter excluído estudos relevantes publicados fora desse escopo. Além disso, por se tratar de uma pesquisa de natureza teórica, não foram realizados experimentos práticos ou implementações em ambiente real para validação empírica das abordagens identificadas.
Para trabalhos futuros, sugere-se a realização de estudos experimentais que avaliem, em ambientes controlados ou corporativos, o impacto quantitativo da integração entre IDS, SIEM e SOAR na redução de incidentes de segurança. Recomenda-se ainda investigar modelos híbridos que combinem automação com supervisão humana inteligente, bem como explorar técnicas avançadas de aprendizado de *Explainable AI* - (Máquina Explicável) aplicadas à segurança de redes.

5.2 Conclusão

Conclui-se que a integração entre mecanismos de detecção e resposta automatizada representa uma evolução necessária na defesa de infraestruturas digitais modernas. Embora desafios técnicos e operacionais ainda persistam, a consolidação dessas tecnologias tende a fortalecer significativamente a postura de segurança das organizações, tornando-as mais preparadas para enfrentar ameaças cibernéticas cada vez mais complexas e dinâmicas. Os estudos selecionados convergem ao apontar que: Automação é indispensável para lidar com o volume e velocidade dos ataques modernos. SOAR, quando conectado a SIEM e IDS, transforma alertas brutos em ações imediatas, reduzindo o tempo de contenção de minutos para segundos. *Zero Trust* complementa IDS ao validar continuamente identidades e comportamentos, criando um ambiente menos permissivo e mais seguro. *Machine learning* emerge como pilar da detecção moderna, reduzindo falsos positivos e permitindo resposta preditiva. Defesa ativa (*honeypots* + MTD) adiciona camadas estratégicas que confundem atacantes e geram sinais úteis para o IDS.
Portanto, a literatura demonstra que a integração entre, IDS, SIEM, SOAR, *Zero Trust* e *Machine Learning*. Constitui hoje o caminho mais promissor para reduzir incidentes, aumentar a precisão da detecção e fortalecer a resiliência cibernética ddetectar correlacionar analisar responder tudo de forma automatizada e contínua, com mínima intervenção humana.

Referências Bibliográficas

[Ahmed e Khan 2022] AHMED, M.; KHAN, S. Siem integration with soar for automated incident response. *Journal of Cybersecurity and Information Security*, v. 10, n. 2, p. 45–58, 2022. 1, 2, 29

[Al-Dahasi e Khan 2024] AL-DAHASI, E.; KHAN, F. A. Automating security incident response in scada systems through siem-ml integration. In: IEEE. *2024 29th International Conference on Automation and Computing (ICAC)*. [S.l.], 2024. p. 1–10. 30

[Bridges *et al.* 2023] BRIDGES, R. A. *et al.* Testing soar tools in use. *Computers & Security*, Elsevier, v. 129, p. 103201, 2023. 9

[d'Ambrosio *et al.* 2025] D'AMBROSIO, N. *et al.* Smash: An sdn-mtd framework for efficient honeypot deployment and insider threat mitigation. *Computer Networks*, Elsevier, p. 111327, 2025. 30

[Garcia e Mendes 2023] GARCIA, L.; MENDES, R. Integration of intrusion detection systems with automated response mechanisms. *Computers & Security*, Elsevier, v. 125, p. 103012, 2023. 2

[Islam 2026] ISLAM, C. *Conceptual map of security orchestration and automation*. 2026. Acessado em: 28 maio 2026. Disponível em: <https://www.researchgate.net/figure/Conceptual-map-of-security-orchestration-and-automation_fig1_344260727>. xiv, 9

[Kallimath e Savalagimath 2020] KALLIMATH, V.; SAVALAGIMATH, C. *The Complete Guide to Security Orchestration, Automation and Response (SOAR)*. [S.l.], 2020. Disponível em: <https://happiestminds.com>. Acesso em: 20 mai. 2026. 9, 29, 31

[Lakbabi, Orhanou e Hajji 2013] LAKBABI, A.; ORHANOU, G.; HAJJI, S. E. Network access control technology-proposition to contain new security challenges. *arXiv preprint arXiv:1304.0807*, 2013. 5, 6, 30

[Lee, Jang-Jaccard e Kwak 2022] LEE, M.; JANG-JACCARD, J.; KWAK, J. Novel architecture of security orchestration, automation and response in internet of blended environment. Tech Science Press, 2022. 1

[M 2026] M, C. *Security Information and Event Management (SIEM) for businesses*. 2026. Acessado em: 28 maio 2026. Disponível em: <https://www.businessbroadbandhub.co.uk/blog/siem/>. xiv, 7

[Mala *et al.* 2025] MALA, K. *et al.* Ai-enhanced cloud security: A dynamic framework for adaptive threat intelligence. In: IEEE. *2025 International Conference on Computing Technologies (ICOCT)*. [S.l.], 2025. p. 1–7. 13

[Mukhopadhyay *et al.* 2011] MUKHOPADHYAY, I. *et al.* A comparative study of related technologies of intrusion detection & prevention systems. *J. Information Security*, v. 2, n. 1, p. 28–38, 2011. 5, 6, 30

[Narasappa 2025] NARASAPPA, D. Integrating zero trust architecture with automation and analytics for resilient cybersecurity. In: IEEE. *2025 3rd International Conference on Data Science and Network Security (ICDSNS)*. [S.l.], 2025. p. 1–6. xiv, 10, 11, 30

[Page, McKenzie e Bossuyt 2021] PAGE, M. J.; MCKENZIE, J. E.; BOSSUYT, P. M. The prisma 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, v. 372, p. n71, 2021. 2

[Pappu, Bhushan e Mittal 2025] PAPPU, K.; BHUSHAN, B.; MITTAL, A. Spiffe-based zero-trust authentication for ai agent ecosystems. In: IEEE. *2025 International Conference on Computer and Applications (ICCA)*. [S.l.], 2025. p. 1–7. 30

[Polónio, Moura e Marinheiro 2025] POLÓNIO, J.; MOURA, J.; MARINHEIRO, R. N. Towards automatic detection and mitigation of high-risk cybersecurity vulnerabilities at networked systems. *IEEE Access*, IEEE, 2025. 30

[Rahman e Islam 2022] RAHMAN, A.; ISLAM, M. Autonomous intrusion detection and response using machine learning techniques. *Computers, Materials & Continua*, v. 71, n. 3, p. 4951–4968, 2022. 1, 30

[Sampaio e Mancini 2007] SAMPAIO, R. F.; MANCINI, M. C. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. *Revista Brasileira de Fisioterapia*, v. 11, n. 1, p. 83–89, 2007. 14

[Silva 2019] SILVA, W. Mendes-da. Contribuições e limitações de revisões sistemáticas e meta-análises na área de administração. *Revista de Administração Contemporânea*, v. 23, n. 2, p. 1–11, 2019. 14

[Sridharan e Kanchana 2022] SRIDHARAN, A.; KANCHANA, V. Siem integration with soar. In: IEEE. *2022 International Conference on Futuristic Technologies (INCOFT)*. [S.l.], 2022. p. 1–6. 7, 8, 29

[Tinoco 2026] TINOCO, C. *Modo de operação IDS*. 2026. Acessado em: 28 maio 2026. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/Sistemas-de-Deteccao-e-Intrusao/Modo-de-Operacao.html>. xiv, 6

[Vast *et al.* 2021] VAST, R. *et al.* Artificial intelligence based security orchestration, automation and response system. In: IEEE. *2021 6th International Conference for Convergence in Technology (I2CT)*. [S.l.], 2021. p. 1–5. xiv, 12, 30

[Vazão *et al.* 2023] VAZÃO, A. P. *et al.* Implementing and evaluating a gdpr-compliant open-source siem solution. *Journal of Information Security and Applications*, Elsevier, v. 75, p. 103509, 2023. 7, 30

[Waelchli e Walter 2025] WAELCHLI, S.; WALTER, Y. Reducing the risk of social engineering attacks using soar measures in a real world environment: A case study. *Computers & Security*, Elsevier, v. 148, p. 104137, 2025. 8, 31

[Wang e Zhou 2024] WANG, T.; ZHOU, Q. Moving target defense and honeypots for adaptive cyber defense. *Symmetry*, v. 16, n. 4, p. 859, 2024. 2, 30

[Zhang, Li e Chen 2023] ZHANG, Y.; LI, H.; CHEN, X. Integrating zero trust architecture with automation and analytics for resilient cybersecurity. *IEEE Access*, v. 11, p. 10234–10250, 2023. 2