Integração de Soluções *Open Source* para o Gerenciamento de Incidentes de Segurança da Informação

Wuarli Ceza Nunes dos Santos
Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)
Universidade de Brasília (UNB)
Brasília, DF
wuarli.santos@aluno.unb.br

Dr. Éder Souza Gualberto
Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)
Universidade de Brasília (UNB)
Brasília, DF
eder.gualberto@unb.br

Resumo: Este artigo apresenta uma proposta de integração de soluções *open source* para compor um ecossistema de SIEM (*Security Information and Event Management*), SOAR (*Security Orchestration, Automation, and Response*) e CTI (*Cyber Threat Intelligence*), voltado ao gerenciamento de incidentes de segurança da informação. A arquitetura proposta utiliza ferramentas como Wazuh, Shuffle, Cortex e MISP, selecionadas por sua flexibilidade, ausência de custos de licenciamento e suporte comunitário. A integração entre essas tecnologias é alinhada a *frameworks* e normas como NIST SP 800-61r3, ISO/IEC 27035-1, NIST CSF 2.0 e CIS *Controls* v8, visando aumentar a visibilidade, automatizar respostas e enriquecer alertas com inteligência de ameaças. O estudo inclui uma proposta de implementação em fases, iniciada em ambiente institucional na Funasa, com destaque para a instalação do Wazuh e elaboração de documentação técnica. Os resultados esperados incluem maior eficiência operacional, redução de custos e conformidade regulatória, embora desafios como suporte formal e complexidade técnica sejam reconhecidos.

Palavras-chave: SIEM. SOAR. CTI. PPSI. Segurança Cibernética. Gerenciamento de Incidentes. *Open Source*.

Abstract: This article presents a proposal for integrating open source solutions to build an ecosystem of SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and CTI (Cyber Threat Intelligence), aimed at managing information security incidents. The proposed architecture employs tools such as Wazuh, Shuffle, Cortex, and MISP, selected for their flexibility, lack of licensing costs, and community support. The integration of these technologies aligns with frameworks and standards such as NIST SP 800-61r3, ISO/IEC 27035-1, NIST CSF 2.0, and CIS Controls v8, with the goal of enhancing visibility, automating responses, and enriching alerts with threat intelligence. The study includes a phased implementation plan, initiated in an institutional environment at Funasa, highlighting the deployment of Wazuh and the development of technical documentation. Expected outcomes include improved operational efficiency, cost reduction, and regulatory compliance, although challenges such as lack of formal support and technical complexity are acknowledged.

Keywords: SIEM. SOAR. CTI. PPSI. Cybersecurity. Incident Management. Open Source.

1. INTRODUÇÃO

A segurança cibernética tem se consolidado como uma preocupação crescente para organizações de diferentes portes e setores. A complexidade e a sofisticação das ameaças digitais evoluem continuamente, exigindo soluções avançadas capazes de monitorar, detectar e responder a incidentes em tempo real [1], [2].

Nesse contexto, o Governo Brasileiro, por meio do Ministério da Gestão e Inovação em Serviços Públicos, desenvolve iniciativas e programas voltados à proteção da informação no âmbito do governo digital, como o Programa de Privacidade e Segurança da Informação (PPSI). Essas ações refletem a necessidade de fortalecer a governança e a resiliência cibernética no setor público.

Entre as tecnologias que se destacam nesse cenário, encontram-se os Sistemas de Gerenciamento de Eventos e Informações de Segurança (*Security Information and Event Management* - SIEM) e as plataformas de Orquestração, Automação e Resposta de Segurança (*Security Orchestration, Automation, and Response* - SOAR). Esses recursos são fundamentais para a construção de uma estratégia abrangente de defesa, permitindo maior visibilidade, integração e agilidade na resposta a incidentes [3], [4].

Além disso, a Inteligência de Ameaças Cibernéticas (*Cyber Threat Intelligence* - CTI) desempenha um papel essencial nesse ecossistema, fornecendo indicadores de comprometimento (IoCs), contexto sobre campanhas maliciosas e informações sobre atores de ameaça. Plataformas como o MISP (*Malware Information Sharing Platform*) possibilitam a coleta, correlação e compartilhamento colaborativo de dados de ameaças, enriquecendo alertas do SIEM e permitindo que o SOAR execute respostas mais precisas e contextualizadas [5].

A integração entre SIEM, SOAR e CTI não apenas aumenta a capacidade de detecção, mas também reduz o tempo de investigação e prioriza incidentes com base em risco real, fortalecendo a postura proativa das organizações [6][7].

As ferramentas *open source* surgem como alternativas viáveis e flexíveis às soluções proprietárias, especialmente para organizações com restrições orçamentárias[8]. Essas soluções possibilitam a implementação de mecanismos robustos de segurança, promovendo acessibilidade sem comprometer a eficácia.

Além disso, a natureza colaborativa do desenvolvimento de soluções *open source*, no caso de uma comunidade ativa, pode proporcionar constante evolução e melhoria dessas ferramentas.

A integração de soluções *open source* para SIEM, SOAR e CTI permite que as organizações personalizem suas estratégias de segurança cibernética de acordo com suas necessidades específicas. Essas soluções podem ser combinadas de forma modular, possibilitando a criação de um ecossistema de segurança adaptável e escalável.

Conforme Abreu [9], a interoperabilidade e a segurança cibernética dependem fortemente de uma visão de implementação focada como uma única camada na solução.

A interoperabilidade entre diferentes ferramentas também facilita a troca de informações e a automação de processos, resultando em uma resposta mais ágil e eficaz a incidentes de segurança.

Dessa forma, as organizações podem se beneficiar de uma abordagem holística e coordenada para a gestão de ameaças, sem incorrer em altos custos associados às soluções proprietárias.

2. FUNDAMENTOS E CONCEITOS

A Segurança Cibernética é um pilar essencial para a proteção dos ativos de informação e para a continuidade das operações institucionais, especialmente no setor público, onde a exposição a ameaças digitais pode comprometer serviços críticos e dados sensíveis da sociedade.

Tanta é a relevância do assunto que o Governo Brasileiro estabeleceu a Política Nacional de Segurança da Informação (PNSI) por meio do Decreto nº 12.752, de 4 de agosto de 2025, que define diretrizes estratégicas, princípios e objetivos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no País, garantindo a proteção das informações relevantes para a segurança nacional, a soberania e o interesse público [10].

As Políticas Nacionais sobre Segurança da Informação, alinhadas à Estratégia de Governo Digital e à Lei Geral de Proteção de Dados (LGPD), estabelecem diretrizes para que órgãos e entidades da Administração Pública adotem medidas preventivas, detectivas e corretivas, fortalecendo sua resiliência contra incidentes cibernéticos.

Nesse contexto, o PPSI funciona como instrumento normativo interno, definindo padrões, responsabilidades e controles que asseguram a governança e a conformidade em segurança da informação [11].

Além da implantação das políticas mencionadas, destaca-se a relevância do uso de soluções *open source*, que possibilitam às entidades públicas ou privadas acesso a ferramentas de segurança da informação sem a necessidade de arcar com os elevados custos de soluções proprietárias, promovendo eficiência e inclusão tecnológica.

"OSS - *Open Source Software offers significant benefits to organizations, including cost savings, flexibility, security, and the ability to leverage community expertise.*" [12].

As plataformas de código aberto agregam, analisam e gerenciam dados de segurança de diversas fontes em uma infraestrutura de TI, e o SIEM é uma delas.

O uso de tecnologias avançadas, como o SIEM, representa uma das medidas importantes para apoiar a operacionalização das diretrizes do PPSI. Ao combinar a gestão de informações de

segurança (SIM) e a gestão de eventos de segurança (SEM), o SIEM permite coletar *logs* de múltiplas fontes, correlacionar eventos, analisar dados em tempo real e gerar alertas proativos.

Essa capacidade possibilita detectar atividades suspeitas, responder rapidamente a incidentes e manter um nível elevado de visibilidade e controle sobre o ambiente tecnológico, atendendo tanto às demandas estratégicas definidas pelas políticas nacionais quanto às exigências técnicas previstas no PPSI. O SIEM é responsável pelo gerenciamento de eventos de segurança e desempenha papel essencial na identificação de ameaças em tempo real, por meio da correlação e análise de milhares de eventos por segundo. Essa capacidade é fundamental para aumentar a visibilidade e acelerar a resposta a incidentes em ambientes complexos [13].

O SOAR, por sua vez, é um conjunto de tecnologias que permite a orquestração e automação de processos de segurança, além de facilitar a resposta a incidentes. As principais funcionalidades de um SOAR incluem a automação de tarefas repetitivas, a coordenação de respostas a incidentes e a integração com outras ferramentas de segurança. Segundo Sampaio [14], a ferramenta possibilita identificar e mitigar ameaças críticas com maior agilidade, priorizando os alertas mais relevantes.

Nesse contexto, enquanto o SIEM se concentra na coleta e análise de dados de segurança para detectar ameaças, o SOAR foca na automação e orquestração de respostas a incidentes. A integração dessas tecnologias permite uma abordagem mais proativa e eficiente para a gestão de segurança cibernética.

Complementando SIEM e SOAR, a CTI é um componente estratégico que fornece indicadores de comprometimento (IoCs), táticas, técnicas e procedimentos (TTPs) de agentes maliciosos, além de contexto sobre campanhas e vulnerabilidades emergentes. Plataformas como o MISP (*Malware Information Sharing Platform*) permitem a coleta, correlação e compartilhamento colaborativo de dados de ameaças, enriquecendo alertas do SIEM e permitindo que o SOAR execute respostas mais precisas e contextualizadas.

Essa integração fortalece a postura proativa das organizações, reduzindo o tempo de investigação e aumentando a eficácia na mitigação de ataques. Estudos destacam que arquiteturas que combinam SIEM, SOAR e CTI, com uso do MISP, melhoram significativamente a capacidade de defesa em profundidade, permitindo correlação em tempo real e resposta baseada em inteligência [7].

3. SOLUÇÕES PROPOSTAS

Um dos fatores determinantes para a escolha das ferramentas propostas é a forte colaboração existente nas comunidades *open source* que as mantêm, garantindo constante evolução, correção de vulnerabilidades e inovação. Essa característica é estratégica para soluções críticas de segurança, pois possibilita rápida adaptação a novas ameaças e integração com diferentes ecossistemas tecnológicos.

Além disso, conforme destaca Assunção [15], a adoção de soluções *open source* é justificada pela possibilidade de auditoria do código por qualquer profissional, assegurando transparência e confiabilidade devido ao seu caráter aberto. Essa abertura é especialmente relevante em ambientes que demandam altos níveis de segurança e conformidade, pois permite verificar a integridade do software, identificar vulnerabilidades e adaptar funcionalidades às necessidades específicas da organização.

No contexto da integração entre soluções de SIEM, SOAR e CTI, a natureza colaborativa das comunidades *open source* é um diferencial. Ferramentas como Wazuh, Shuffle, Cortex e MISP são mantidas por comunidades ativas que contribuem com correções, novos módulos e integrações, além de compartilhar indicadores de comprometimento (IoCs) e boas práticas.

Essa dinâmica fortalece a interoperabilidade e a automação, pilares fundamentais para arquiteturas modernas de defesa cibernética, conforme orientam normas como NIST SP 800-61 Rev.3 e ISO/IEC 27035-1, que recomendam processos integrados de detecção, resposta e aprendizado contínuo.

3.1. SOLUÇÕES PARA O SIEM

3.1.1. ELK Stack (Elasticsearch, Logstash, Kibana)

3.1.1.1. Elasticsearch

Elasticsearch é um mecanismo de busca e análise distribuído, projetado para lidar com grandes volumes de dados em tempo real. Desenvolvido em Java, ele se baseia no motor de busca Apache Lucene. Permite a indexação e a busca eficiente de dados, tornando-se uma escolha popular para aplicações que exigem alta performance na busca e análise de grandes conjuntos de dados, conforme afirma Kathare, Reddy, Prabhu [16].

Uma das principais características do Elasticsearch é sua capacidade de distribuir dados em um cluster de nós, o que melhora a escalabilidade e a tolerância a falhas. Isso permite que ele manipule *petabytes* de dados e execute consultas complexas em milissegundos. Além disso, oferece uma *Application Programming Interface* (API) RESTful, facilitando a integração com outras aplicações e sistemas.

Amplamente utilizado em várias indústrias para casos de uso como busca de documentos, análise de *logs*, monitoramento de desempenho de aplicativos e inteligência de negócios. Sua flexibilidade e capacidade de escalar horizontalmente tornam-no uma peça central em muitas arquiteturas de dados modernas.

3.1.1.2. Logstash

Logstash é uma ferramenta para coleta, processamento e encaminhamento de dados log. Além disso, é altamente

configurável e permite que os usuários coletem dados de diversas fontes, transformem esses dados e, em seguida, enviem-nos para um destino de escolha.

Logstash suporta uma ampla variedade de entradas, filtros e saídas, o que permite manipular diferentes formatos e tipos de dados. Entradas podem incluir *logs* de servidores, *logs* de aplicativos, métricas de desempenho e dados de rede, enquanto filtros podem ser usados para transformar e formatar esses dados, tornando-os mais úteis para análise. Finalmente, as saídas podem ser configuradas para enviar os dados processados para destinos como Elasticsearch, arquivos, ou sistemas de mensagem.

O principal benefício do desenvolvimento de configurações complexas do Logstash é uma definição de consulta de pesquisa significativamente melhor e menos modificação de dados na conexão do Kibana [17].

A arquitetura modular Logstash facilita a adição de novos plugins de entrada, filtro e saída, permitindo personalizações específicas para atender às necessidades particulares de diferentes ambientes de Tecnologia da Informação e Comunicação (TIC). Dessa forma, desempenha um papel crucial na *pipeline* de dados, assegurando que informações críticas estejam prontamente disponíveis para análise e visualização.

3.1.1.3. Kibana

Kibana é uma plataforma de visualização *open source* que se integra com Elasticsearch, permitindo aos usuários explorar e visualizar dados armazenados de maneira intuitiva. Com o Kibana, as equipes podem criar e compartilhar *dashboards* dinâmicos que mostram gráficos, mapas e outras visualizações interativas.

Uma das vantagens do Kibana é sua interface amigável, que permite aos usuários, sem necessidade de habilidades avançadas em programação, criar visualizações complexas e *dashboards* detalhados. Isso facilita a análise de dados e a identificação de padrões e anomalias. Souza [18] enfatiza que "devido à arquitetura baseada em plugins, o Kibana pode ser facilmente estendido para atender a necessidades específicas. ".

Além disso, oferece recursos de exploração de dados em tempo real, permitindo que os usuários filtrem e pesquisem por meio dos dados para encontrar informações específicas. Suas funcionalidades avançadas incluem a criação de alertas, integração com outros componentes do Elastic Stack, e suporte a *plugins* que estendem suas capacidades.

Em conjunto, Elasticsearch, Logstash e Kibana formam o ELK Stack, uma solução poderosa para o gerenciamento e análise de *logs*. Juntos, permitem que as organizações coletem, processem e visualizem grandes volumes de dados de maneira eficiente, fornecendo percepção valiosa e suporte à tomada de decisões informadas.

3.1.1.3. Wazuh

Wazuh é uma plataforma de monitoramento de segurança que oferece capacidades abrangentes para a detecção de ameaças, monitoramento de integridade de arquivos, análise de *logs* e resposta a incidentes. Originalmente derivado do OSSEC (*Open Source Host-based Intrusion Detection System)*, Wazuh expandiu suas funcionalidades para se tornar uma solução robusta que se integra perfeitamente com o ELK Stack (Elasticsearch, Logstash e Kibana).

> PALÁCIO [19] descreve a respeito do funcionamento técnico do Wazuh:
> O Wazuh é implementado a partir de dois principais componentes: os dispositivos monitorados e o servidor de aplicação do Wazuh, sendo o último, o que gerencia todo o processo de monitoramento. Nos hosts monitorados, há várias fontes de *logs*, tais como: arquivos do sistema, *logs* de eventos do Sistema Operacional Windows e *logs* de auditoria de aplicações. Essas fontes de dados são coletadas através do Agent Wazuh.

Dentre as funcionalidades do Wazuh, é importante destacar sua capacidade de monitorar alterações em arquivos críticos do sistema, identificando possíveis modificações não autorizadas.

Além disso, o Wazuh coleta e analisa *logs* de diversas fontes, como sistemas operacionais, aplicativos e dispositivos de rede, identificando padrões de comportamento anômalo. Ele também utiliza regras predefinidas e personalizadas para detectar atividades suspeitas e gerar alertas de segurança, proporcionando uma camada robusta de monitoramento e proteção para a infraestrutura de TIC.

A integração do Wazuh com o ELK Stack permite que os dados de segurança sejam armazenados e analisados de forma eficiente. Elasticsearch armazena e indexa os dados, Logstash processa e envia os *logs* para o Elasticsearch, e Kibana oferece visualizações interativas para monitorar e analisar os eventos de segurança.

3.2. SOLUÇÕES PARA O SOAR

3.2.2. Shuffle

Shuffle é uma plataforma de orquestração e automação de segurança cibernética que permite a criação de fluxos de trabalho personalizados para automatizar tarefas de segurança. Sua interface gráfica baseada em arrastar e soltar facilita a construção e modificação desses fluxos, mesmo por usuários sem conhecimentos avançados em programação [20].

A principal vantagem do Shuffle está em sua capacidade de integrar uma ampla gama de ferramentas de segurança e sistemas de TIC, funcionando como um hub de integração. Isso permite que as organizações automatizem processos complexos de resposta a incidentes, como coleta de dados, análise,

notificação e mitigação, de forma coordenada e eficiente. Além disso, a plataforma oferece suporte à execução de scripts personalizados, webhooks, APIs e monitoramento em tempo real, o que contribui para uma resposta mais ágil e precisa às ameaças [21].

3.3. FERRAMENTA DE CTI

3.3.1. Cortex

Cortex é uma plataforma *open source* voltada para a análise de dados e execução de respostas automatizadas em ambientes de segurança da informação. Projetada para atender às necessidades de equipes *de Security Operations Centers* (SOCs), *Computer Security Incident Response Teams* (CSIRTs) e pesquisadores, permite a análise em larga escala de observáveis como endereços IP, hashes e domínios, além de automatizar ações de resposta por meio de uma API RESTful.

Um dos principais pontos fortes do Cortex é sua integração com o MISP (*Malware Information Sharing Platform*). Essa conexão permite que os dados enriquecidos por Cortex como informações de reputação, geolocalização e histórico de ameaças sejam correlacionados com indicadores de comprometimento compartilhados por comunidades de inteligência. Isso potencializa a capacidade de detecção e resposta a incidentes, promovendo uma abordagem colaborativa e mais eficaz na defesa cibernética [22].

Além disso, Cortex é escalável, suportando a execução paralela de múltiplas análises, o que aumenta significativamente a eficiência operacional. Sua arquitetura modular e a API rica facilitam a integração com outras ferramentas de segurança e sistemas de TIC, permitindo que as respostas a incidentes sejam automatizadas de forma eficaz.

3.3.2. MISP

O MISP (*Malware Information Sharing Platform*) é uma plataforma de código aberto voltada para o compartilhamento estruturado de informações sobre ameaças cibernéticas. Seu principal objetivo é facilitar a colaboração entre organizações, permitindo a coleta, correlação, enriquecimento e distribuição de indicadores de comprometimento (IoCs), amostras de *malware*, campanhas de ataque e outros elementos relevantes para a inteligência de ameaças. A plataforma é amplamente utilizada por CSIRTs, SOCs e comunidades de segurança em todo o mundo, promovendo uma abordagem colaborativa e automatizada na resposta a incidentes [23].

No Brasil, o CERT.br tem incentivado o uso do MISP entre os CSIRTs nacionais, promovendo workshops, guias técnicos e canais de comunicação dedicados à instalação, configuração e operação da plataforma. Essa iniciativa visa automatizar o processo de compartilhamento de informações sobre ameaças, utilizando uma solução aberta, gratuita e alinhada com padrões internacionais [24].

4. INTEGRAÇÃO DO SIEM E SOAR COM MISP

A integração entre sistemas de SIEM e SOAR representa uma evolução significativa na gestão de segurança cibernética. Essa combinação une a visibilidade e correlação de eventos proporcionadas pelo SIEM com a capacidade de padronizar e automatizar respostas oferecida pelo SOAR, conectando o monitoramento contínuo à execução coordenada de ações de contenção, erradicação e comunicação.

Do ponto de vista das boas práticas, essa integração operacionaliza as funções DETECT (DE) e RESPOND (RS) do NIST *Cybersecurity Framework* 2.0 [25], estabelecendo uma ponte entre indicadores e alertas e os processos decisórios e de resposta que reduzem a exposição ao risco. O documento NIST SP 800-61 Rev. 3 [26] reforça que a incorporação de recomendações de resposta ao risco cibernético em todo o ciclo (preparação, detecção, análise, contenção, erradicação, recuperação e lições aprendidas) contribui diretamente para a eficácia da detecção e da resposta, precisamente o espaço onde a integração SIEM–SOAR agrega valor.

Além disso, a inclusão de *Threat Intelligence* por meio do MISP amplia a eficácia da integração, fornecendo indicadores de comprometimento (IoCs) atualizados e contextualizados para enriquecer alertas e *playbooks*.

Do ponto de vista técnico, SIEMs modernos evoluíram para tratar grandes volumes de dados e apoiar detecções em cenários críticos, ao passo que SOARs reduzem o esforço manual e o *alert fatigue*, padronizando *playbooks* e coordenando múltiplas ferramentas. Em conjunto, resultam em ganhos mensuráveis de eficiência e capacidade analítica da operação de segurança.

4.1. BENEFÍCIOS DA INTEGRAÇÃO SIEM–SOAR-CTI

Ao automatizar processos como triagem, enriquecimento de dados e ações iniciais, como o isolamento de hosts ou o bloqueio de indicadores de comprometimento (IoCs), a integração entre SIEM e SOAR reduz significativamente a janela entre o alerta e a resposta. Práticas como priorização de *logs*, normalização de eventos e uso de *playbooks* contribuem para tempos de resposta mais ágeis e consistentes.

O acoplamento entre SIEM e SOAR transfere tarefas repetitivas da equipe de segurança para fluxos de trabalho automatizados. Essa abordagem reduz erros operacionais e promove consistência por meio de trilhas de auditoria, que são elementos essenciais para a governança de incidentes e para a conformidade regulatória. Segundo Mir e Ramachandran [27], a implementação de SOAR em ambientes críticos permite que equipes de segurança lidem de forma mais eficiente com o

volume crescente de alertas, automatizando processos como análise de incidentes, resposta a ameaças e integração com ferramentas diversas. Isso resulta em redução do tempo médio de resolução e maior eficácia operacional.

A integração facilita aderência a marcos como o NIST SP 800-61 Rev. 3 (integração da resposta ao risco) e ao NIST CSF 2.0 (DE/RS), além de apoiar ISO/IEC 27035-1:2023 (gestão estruturada de incidentes), que preconiza preparação, detecção, reporte, avaliação, resposta e lições aprendidas.

4.2. DESAFIOS E RISCOS

Correlações imprecisas e a ingestão de *logs* heterogêneos aumentam o ruído nos sistemas de monitoramento e comprometem a eficácia da automação em plataformas SIEM. Para mitigar esse problema, recomenda-se a adoção de práticas como pré-processamento de dados, mapeamento de campos e definição de fontes prioritárias antes da ingestão, conforme orientações técnicas para profissionais de segurança da informação [28]

A automação de bloqueios pode introduzir riscos operacionais, como indisponibilidade de serviços, caso não seja calibrada adequadamente. Por isso, boas práticas sugerem a presença de um *human in the loop* em ações de alto impacto, permitindo validação manual antes da execução automática. À medida que a maturidade operacional aumenta, é possível promover gradualmente a automação plena, alinhando eficiência com controle [29].

Orquestrações complexas exigem funcionalidades avançadas, como controle de estado, gerenciamento de dependências entre fluxos e compartilhamento de recursos. Essas capacidades são típicas de plataformas SOAR e vão além das funcionalidades oferecidas por *frameworks* tradicionais de automação de TI, conforme destacado por Watson [30] em estudo sobre orquestração de segurança.

4.3. BOAS PRÁTICAS E *FRAMEWORKS*

4.3.1. NIST CSF 2.0 (DE/RS)

Mapear casos de uso às categorias e subcategorias de DETECT e RESPOND ajuda a priorizar fontes de log, casos de automação e integrações essenciais (SIEM, EDR, IAM, e-mail, rede) [25].

4.3.2. NIST SP 800-61 Rev. 3

Derivar *runbooks* e *playbooks* alinhados às fases de resposta (preparação → detecção/análise → contenção/erradicação/recuperação → lições aprendidas) garantindo métricas, documentação e comunicação [26].

4.3.3. NIST SP 800-53 Rev.

A publicação é estruturada em famílias de controles (como *Access Control, Incident Response*, *Audit and Accountability*), permitindo que as organizações selecionem e implementem medidas de acordo com seu perfil de risco e requisitos regulatórios. Além disso, está alinhada ao NIST *Cybersecurity Framework* (CSF), facilitando a integração com estratégias de gestão de riscos cibernéticos [31].

4.3.4. CIS *Controls* v8

CIS *Controls* v8 é um conjunto de 18 controles críticos desenvolvidos pelo *Center for Internet Security* para ajudar organizações a reduzir riscos cibernéticos de forma prática e priorizada. Esses controles são baseados em ameaças reais e incidentes observados globalmente, oferecendo um roteiro claro para fortalecer a postura de segurança [32].

4.3.5. MITRE ATT&CK

Usar a taxonomia de táticas/técnicas para orientar regras de detecção (SIEM) e passos de resposta (SOAR), rastreando cobertura e lacunas [33].

4.3.6. ISO/IEC 27035-1:2023

Implantar processo formal de gestão de incidentes com papéis definidos (*incident coordinator*, *incident management team*), entrada/saída de cada fase e registro de lições aprendidas [34].

4.3.7. ISO/IEC 27035-2:2023

Complementa a parte 1, detalhando planejamento, preparação e resposta a incidentes [35].

4.3.8. Conformidade no Brasil.

LGPD (Lei 13.709/2018) demanda medidas técnicas/administrativas proporcionais ao risco, incluindo capacidade de detectar e responder a incidentes envolvendo dados pessoais. O PPSI/SGD/MGI orienta elevar maturidade em governança, metodologia, pessoas e tecnologia na APF, enquanto o CTIR Gov coordena recomendações e alertas, todos beneficiados por capacidades integradas SIEM-SOAR-CTI.

4.4. FLUXO DE INTEGRAÇÃO

4.4.1. Coleta e correlação (Wazuh + Logstash)

- Agentes → Wazuh: coleta de *logs* de endpoints, servidores e dispositivos de rede.
- Wazuh → Logstash: normalização e enriquecimento dos dados antes da indexação.
- Correlação por regras + match com IoCs (feeds do MISP e listas internas).
- Integração com Elasticsearch: armazenamento estruturado e indexação para consultas rápidas.

4.4.2. Observabilidade e Monitoramento (Kibana)

- *Dashboards* interativos para análise de eventos, alertas e indicadores de risco.
- Visualização de métricas de segurança (*Mean Time To Detect* - *MTTD*, *Mean Time To Repair* - MTTR, volume de alertas, top IoCs).
- Alertas visuais e relatórios executivos para apoiar decisões estratégicas.

4.4.3. Envio ao SOAR (Shuffle)

- Alertas relevantes via *webhook* → início do workflow no Shuffle.
- Normalização de campos e deduplicação para evitar redundâncias.

4.4.4. Enriquecimento (Cortex + MISP + fontes externas)

- *Analyzers* (VirusTotal, Whois, GeoIP) + consulta ao MISP (sightings, taxonomias, galaxies).
- Integração com Elasticsearch para correlação histórica e análise de tendências.

4.4.5. Decisão por risco (Shuffle)

- Cálculo do risk score (alerta + confiança do IoC + criticidade do ativo).
- Alto risco: auto-contenção (bloqueio FW/EDR/IAM) + notificação.
- Médio risco: semi-automação com aprovação humana.
- Baixo risco: revisão manual completa.

4.4.6. *Feedback* e Lições Aprendidas

- Publicação de sightings/status no MISP.
- Atualização de blocklists/regras no Wazuh.
- Pós-incidente conforme NIST SP 800-61r3 e ISO/IEC 27035-1 (lições aprendidas e melhoria contínua).

4.4.7. Fluxo Visual

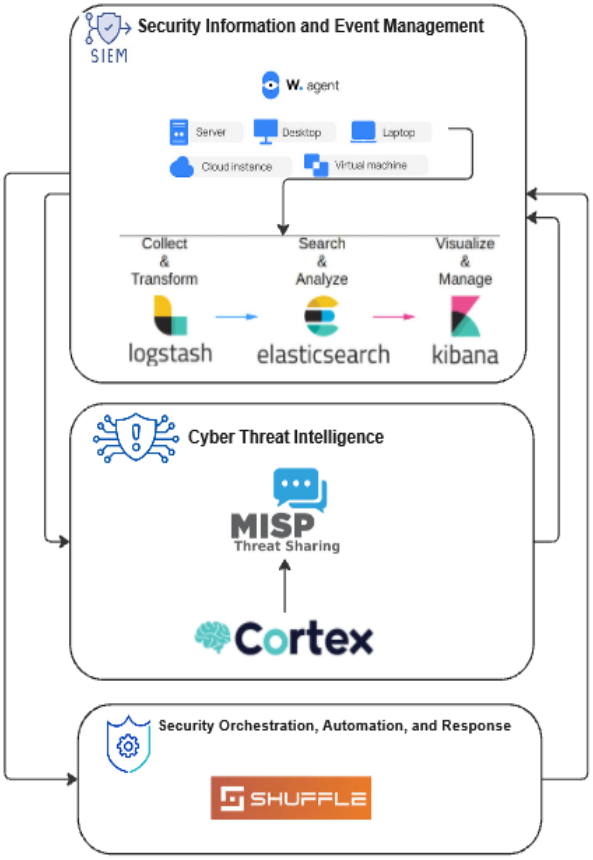

Figura 1: Fluxo de integração.

4.5. PROPOSTA DE IMPLEMENTAÇÃO EM FASES

4.5.1. Fase 1 - Fundamentos, SIEM e Observabilidade

Objetivo: Estabelecer visibilidade centralizada, coleta confiável de eventos e capacidade de análise em tempo real.
Ações:

- Implantar Wazuh como SIEM:
  - Configurar agentes em *endpoints* e servidores;
  - Definir fontes prioritárias: Active Directory, firewall, proxy, EDR e sistemas críticos;
  - Ajustar regras e decoders para reduzir falsos positivos.
- Integrar com ELK Stack:
  - Logstash: pipeline para ingestão e normalização dos *logs* do Wazuh;
  - Elasticsearch: indexação e armazenamento estruturado para consultas rápidas;
  - Kibana: criação de *dashboards* interativos para monitoramento, análise e relatórios executivos.
- Criar painéis e alertas básicos (ex.: autenticações suspeitas, escalonamento de privilégios);
- Integrar *feeds* do MISP no Wazuh (IoCs para correlação);
- Métricas: cobertura de *logs*, taxa de falsos positivos, MTTD (*Mean Time To Detect*) inicial.
- Elaboração de documentação detalhada dos processos de instalação, configuração e integração.

4.5.2. Fase 2 - Gestão de Incidentes

Objetivo: Padronizar processos e centralizar casos.
Ações:

- Estabelecer processo manual de resposta com base no NIST SP 800-61r3.
- Métricas: tempo de abertura de caso, taxa de incidentes tratados.

4.5.3. Fase 3 - Enriquecimento e Inteligência

Objetivo: Aumentar contexto e reduzir tempo de análise.
Ações:

- Implantar Cortex e configurar *analyzers* essenciais (VirusTotal, Whois, GeoIP).
- Implantar MISP:
  - Configurar *feeds* confiáveis e taxonomias.
  - Estabelecer política de *sightings* e compartilhamento.
- Integração com Elasticsearch: correlação histórica e análise de tendências.
- Métricas: tempo médio de análise, taxa de falsos positivos após enriquecimento.
- Atualização da documentação detalhada dos processos de instalação, configuração e integração.

4.5.4. Fase 4 - Automação Parcial (SOAR)
Objetivo: Reduzir esforço manual em tarefas repetitivas. Ações:

- Implantar Shuffle:
  - Criar workflows para: normalização de alertas, enriquecimento.
  - Implementar *gate* humano para ações críticas (bloqueio, isolamento).
- Automatizar notificações (Telegram, WhatsApp, e-mail) e coleta de evidências.
- Métricas: redução de MTTR, número de tarefas automatizadas.
- Atualização da documentação detalhada dos processos de instalação, configuração e integração.

4.5.5. Fase 5 - Automação Avançada e Feedback
Objetivo: Orquestração completa e melhoria contínua. Ações:

- Implementar *risk scoring* (alerta + confiança IoC + criticidade do ativo).
- Automatizar contenção para casos de alto risco (com *rollback* seguro).
- Criar ciclo de feedback:
  - Atualizar regras no Wazuh com IoCs confirmados.
  - Publicar *sightings* no MISP.
- Implantar KPIs e relatórios (MTTD, MTTR, taxa de automação, cobertura ATT&CK).
- Métricas: redução global de MTTR, aumento da taxa de resposta automatizada.
- Atualização da documentação detalhada dos processos de instalação, configuração e integração.

4.5.6. Governança e segurança em todas as fases

- Segregação de funções (Wazuh, Cortex, Shuffle, MISP).
- TLS e API Keys seguras para integrações.
- Auditoria e conformidade (LGPD, PPSI, ISO 27035).
- Documentação detalhada dos processos de instalação, configuração e integração.
- Treinamento contínuo da equipe SOC.

4.5.7. Benefícios da abordagem gradativa

- Reduzirá riscos operacionais e indisponibilidades, ao permitir validações e correções em cada etapa antes da próxima implantação.
- Medição e maturidade, por meio de métricas específicas em cada fase, como MTTD, MTTR e taxa de automação.
- Permitirá ajustes contínuos, conforme mudanças no cenário de ameaças, requisitos regulatórios ou evolução tecnológica.
- Aprimorará a gestão de mudanças, promovendo maior aceitação organizacional e capacitação gradual das equipes envolvidas.
- Fortalecerá a governança e a segurança, com aplicação progressiva de controles e conformidade com normas.
- Estimulará a melhoria contínua, por meio de ciclos de *feedback* e atualização de regras, indicadores e processos com base em incidentes reais.
- Contribuirá para maior previsibilidade e controle, reduzindo impactos negativos e promovendo uma evolução segura e sustentável da operação de segurança.

4.6. SIEM e SOAR e sua vinculação ao PPSI e Cis Controls V8

Outro ponto a ser ressaltado é a relação das ferramentas com os *frameworks* PPSI e Controles Críticos de Segurança do CIS (CIS *Controls*), o PPSI do Governo Digital utiliza os Controles Críticos de Segurança do CIS (CIS *Controls*) como referência e guia para a implementação de medidas de segurança.

Center for Internet Security [32] menciona que os "Controles Críticos de Segurança do CIS (CIS *Controls*) são um conjunto priorizado de salvaguardas para mitigar os ataques cibernéticos mais comuns contra sistemas e redes. Eles são mapeados e referenciados por vários *frameworks* legais, regulatórios e políticos".

A tabela a seguir apresenta as atuações do SIEM e do SOAR nos respectivos *frameworks* mencionados.

PPSI	Controle CIS v8	Atuação do SIEM	Atuação do SOAR
1.1 a 1.5	*Control 1: Inventory and Control of Enterprise Assets*	Identifica ativos não autorizados via *logs* de rede	Automatiza abertura de incidentes para ativos suspeitos
2.1 a 2.7	*Control 2: Inventory and Control of Software Assets*	Correlaciona execução de softwares não autorizados	Abre tickets automáticos para softwares não autorizados
4.1 a 4.12	*Control 4: Secure Configuration of Enterprise Assets and Software*	Detecta desvios de configuração em ativos/sistemas	Executa scripts de correção ou aciona equipes técnicas
6.1 a 6.8	*Control 6: Access Control Management*	Monitora e alerta sobre acessos fora do padrão	Bloqueia automaticamente credenciais comprometidas

8.1 a 8.12	*Control 8: Audit Log Management*	Coleta, centraliza e analisa *logs* de segurança	Orquestra resposta automática a alertas críticos
13.1 a 13.11	*Control 13: Network Monitoring and Defense*	Correlaciona tráfego malicioso e anomalias de rede	Isola hosts automaticamente ao detectar ataque
16.1 a 16.14	*Control 16: Application Software Security*	Monitora *logs* de aplicações críticas	Aciona resposta automática em pipeline DevSecOps
17.1 a 17.9	*Control 17: Incident Response Management*	Gera alertas de incidentes detectados em tempo real	Executa *playbooks* de resposta (ex.: bloqueio em firewall, desativação de conta)
18.1 a 18.5	*Control 18: Penetration Testing*	Registra *logs* de testes de intrusão e simulações	Gera relatórios automáticos de ações corretivas

Tabela 1 : SIEM and SOAR e sua vinculação ao PPSI and Cis Control V8

Desta forma, ficando evidenciado o potencial das ferramentas aqui apresentadas para atender os *frameworks* de referência do Governo e o Controles Críticos de Segurança do CIS (CIS *Controls*).

5. RESULTADOS

5.1. BENEFÍCIOS DAS SOLUÇÕES

5.1.1 Custo

Ferramentas *open source* são geralmente mais acessíveis do que soluções proprietárias. Elas eliminam os custos de licenciamento, permitindo que organizações de todos os tamanhos, especialmente aquelas com orçamentos limitados, implementem soluções robustas de segurança cibernética.

Freitas [36] enfatiza sobre os custos na TI “A análise de custo em Tecnologia da Informação às vezes não é uma tarefa simples, ainda mais quando se trata da segurança da informação. Nem todos os custos são diretos. ”.

Optar por ferramentas proprietárias, desconsiderando o estudo de ferramentas *open source* eliminam a curva de aprendizado de uma equipe técnica e potencializam os custos operacionais e de dependência. Conforme enfatiza Saleh [37] “os softwares proprietários são prejudiciais ao desenvolvimento do conhecimento, e por consequência a sociedade como um todo”.

5.1.2 Flexibilidade

A natureza *open source* dessas ferramentas permite customizações específicas para atender às necessidades únicas de cada organização. Isso significa que as empresas podem adaptar as ferramentas para se integrarem perfeitamente com sua infraestrutura existente e processos operacionais.

Os pioneiros do movimento *open source*, como Eric S. Raymond e Bruce Perens, foram fundamentais para estabelecer os princípios que sustentam esse modelo de desenvolvimento colaborativo de acordo com Zwirtes [38].

Entre os aspectos mais relevantes do software *open source*, destaca-se a flexibilidade, que permite adaptações conforme as necessidades dos usuários e contextos específicos.

> ZWIRTES [38] flexibilidade: com o código fonte disponível, qualquer programa pode ter centenas ou milhares de desenvolvedores. Cada comunidade de código aberto tem uma tremenda flexibilidade em modificar o programa. Os desenvolvedores podem modificar o software para atender às suas necessidades, ou às necessidades de suas empresas, clientes ou comunidades. A estabilidade e consistência do software de código aberto são tipicamente mantidas pelo criador ou uma equipe de desenvolvimento que controla a versão principal do software. Entidades comerciais geralmente não podem se dar ao luxo de gastar recursos em mercados de nicho, dos quais pode haver milhares, mas os desenvolvedores que trabalham por conta própria podem fazer com mais facilidade.

5.1.3 Comunidade

Uma comunidade ativa de desenvolvedores e usuários contribui para a melhoria contínua das ferramentas. Essa colaboração comunitária acelera o desenvolvimento de novos recursos, correções de bugs e melhorias na segurança, garantindo que as ferramentas estejam sempre atualizadas e evoluindo conforme as necessidades do mercado.

É por meio da comunidade que a segurança é garantida, os códigos e rotinas de processamento de um software livre são liberados a toda comunidade, um grande número de pessoas, ornando mais fácil de descobrir qualquer problema, e antecipando e garantindo mais integridade, segundo LIMA JUNIOR [39].

5.2. DESAFIOS DAS SOLUÇÕES

5.2.1 Suporte

A ausência de suporte formal pode ser um desafio para algumas organizações. Enquanto muitas ferramentas *open source* possuem documentação extensiva e comunidades de suporte ativas, a falta de suporte técnico oficial pode ser um

obstáculo para empresas que necessitam de assistência imediata e especializada.

Saleh [40] realizou uma pesquisa com gestores de TI, que envolvia a disponibilidade do suporte para ferramentas *open source*, as respostas dos seus entrevistados enfatizavam termos como: “afirmou que não existe suporte” em outro caso que: “o suporte existe, mas é insuficiente para atender as necessidades do mercado.”.

Fica evidenciado que apesar do potencial das ferramentas, o desafio do suporte após a implementação, e até mesmo para o início da implantação precisa ser uma barrarei vencida.

5.2.2 Complexidade

A configuração e integração dessas ferramentas podem exigir um alto nível de conhecimento técnico. Organizações podem enfrentar desafios ao implementar e manter essas soluções, especialmente se não possuírem equipes de TIC com a expertise necessária.

Apesar das vantagens em se ter uma comunidade colaborativa, também existem também as desvantagens [40] enfatiza “vai aumentar a complexidade e a as extensões podem não oferecer atualizações ao mesmo tempo que a solução disponibiliza uma nova versão. ”.

6. TRABALHOS FUTUROS

Como trabalho futuro, propõe-se a implementação prática da arquitetura integrada de SIEM, SOAR e CTI abordada neste artigo, acompanhada da elaboração de um manual técnico-operacional com procedimentos detalhados de implantação. Essa abordagem permitirá que organizações realizem a implementação de ferramentas sem custo de licenciamento, promovendo maior acessibilidade e eficiência.

Ressalta-se que a aplicação prática deste artigo já foi iniciada em um ambiente de instituição pública, especificamente na Fundação Nacional de Saúde (Funasa), e atualmente encontra-se na fase de instalação e configuração dos agentes da solução Wazuh. O objetivo final é superar as complexidades intrínsecas de projetos dessa magnitude, fornecendo documentação técnica abrangente e exemplos práticos que sirvam como referência para outras organizações.

Com uma visão empreendedora, este projeto poderá, por meio de cooperação técnica entre órgãos, viabilizar o fornecimento do ambiente implantado como serviço, tornando-o economicamente competitivo em relação às soluções privadas disponíveis no mercado.

Essa implementação permitirá validar os benefícios das ferramentas *open source*, como custo reduzido, flexibilidade de customização e suporte de uma comunidade ativa de desenvolvedores e usuários. Ao mesmo tempo, enfrentará os desafios inerentes a essas ferramentas, incluindo a ausência de suporte formal e a complexidade na configuração e integração das soluções.

A realização deste projeto fornecerá subsídios sobre a eficiência operacional da integração e oferecerá diretrizes práticas para outras organizações que buscam fortalecer suas capacidades de segurança cibernética por meio de soluções abertas.

7. CONCLUSÃO

Este estudo demonstrou que a integração de soluções *open source* para SIEM, SOAR e CTI constitui uma abordagem estratégica e economicamente viável para fortalecer a segurança cibernética, especialmente em ambientes institucionais com restrições orçamentárias. A arquitetura proposta, composta por Wazuh, Shuffle, Cortex e MISP, mostrou-se aderente às melhores práticas e *frameworks* internacionais, como NIST SP 800-61r3, ISO/IEC 27035-1, NIST CSF 2.0 e CIS *Controls* v8, garantindo alinhamento normativo e suporte à governança.

O artigo abordou benefícios significativos, incluindo redução de custos, flexibilidade para customizações e suporte comunitário contínuo, fatores que ampliam a acessibilidade e a capacidade de evolução das soluções. Além disso, a integração entre SIEM, SOAR e CTI potencializa a detecção e resposta a incidentes, reduzindo o tempo médio de resolução (MTTR) e promovendo maior eficiência operacional por meio da automação e do enriquecimento de alertas com inteligência de ameaças.

Por outro lado, foram identificados desafios relevantes, como a ausência de suporte formal e a complexidade técnica na configuração e integração das ferramentas, exigindo equipes capacitadas e processos bem estruturados para mitigação de riscos. Tais aspectos reforçam a necessidade de uma implementação gradual, conforme a proposta em fases apresentada, que contempla desde a coleta e correlação de eventos até a automação avançada e ciclos de melhoria contínua.

Conclui-se que a adoção da arquitetura integrada não apenas atende às exigências regulatórias e às diretrizes do Programa de Privacidade e Segurança da Informação (PPSI), mas também contribui para elevar a maturidade em segurança cibernética no setor público. Como trabalhos futuros, recomenda-se a validação prática completa da solução, acompanhada da elaboração de guias técnicos e métricas de desempenho, visando consolidar um modelo replicável e sustentável para outras organizações.

REFERÊNCIAS

[1] A. Dhanaraj, “The Evolution of Cyber Threats: From Traditional Attacks to AI-Powered Challenges,” European Journal of Computer Science and Information Technology, vol. 13, no. 36, pp. 50–61, Jun. 2025. Acessado em: 14 de outubro de 2025. Disponível em: https://eajournals.org/wp-content/uploads/sites/21/2025/06/The-Evolution-of-Cyber-Threats.pdf

[2] M. Danish, “Enhancing Cyber Security Through Predictive Analytics: Real-Time Threat Detection and Response,” arXiv preprint, arXiv:2407.10864, Jul. 2024. Acessado em: 14 de outubro de 2025. Disponível em: https://arxiv.org/pdf/2407.10864

[3] National Cyber and Information Security Agency, “Implementing SIEM and SOAR Platforms: Practitioner Guidance,” May 2025. Acessado em: 14 de outubro de 2025. Disponível em: https://media.defense.gov/2025/May/27/2003722066/-1/-1/0/IMPLEMENTING-SIEM-AND-SOAR-PLATFORMS-PRACTITIONER-GUIDANCE.PDF

[4] S. Ramakrishnan and D. R. Chittibala, “Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024,” Cyber Defense Operations, Mar. 2024. Jul. 2024. Acessado em: 14 de outubro de 2025. Disponível em: https://pdfs.semanticscholar.org/fca6/a6b23bf675d86fa0fb651f986e3c4d3e1d4e.pd

[5] H. Wang et al., “CLEVER: Crafting Intelligent MISP for Cyber Threat Intelligence,” in *Proc. 49th IEEE Conf. on Local Computer Networks (LCN)*, Caen, France, Oct. 2024. DOI: 10.1109/LCN60385.2024.10639749. Acessado em: 14 de outubro de 2025. Disponível em: https://ri.diva-portal.org/smash/record.jsf?pid=diva2:1932092

[6] Cyber Advisory. Automating Threat Intelligence Enrichment in Your SIEM with MISP. 2025. Acessado em: 30 de agosto de 2025. Disponível em: https://cybersecuritynews.com/automating-threat-intelligence-enrichment-in-your-siem-with-misp

[7] Ammi, M., & Jama, Y. (2023). Cyber Threat Hunting Case Study using MISP. Journal of Internet Services and Information Security (JISIS), 13(2), 1-29. DOI: 10.58346/JISIS.2023.I2.001. Acessado em: 30 de agosto de 2025. Disponível em: https://jisis.org/wp-content/uploads/2023/06/2023.I2.001.pdf

[8] I. P. Pinzegher, “O uso de ferramentas open source no compliance ao princípio de segurança da LGPD,” in *Temas Atuais de Direito Digital*, F. Palhares and D. S. L. Francoski, Eds., JusBrasil, 2024. Acessado em: 14 de outubro de 2025. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/1-introducao-capitulo-21-o-uso-de-ferramentas-open-source-no-compliance-ao-principio-de-seguranca-da-lgpd-temas-atuais-de-direito-digital-ed-2024/2485212471

[9] ABREU, M. (2020). Segurança e Interoperabilidade na indústria 4.0. II Simpósio Internacional de Inovação. Acessado em: 05 de agosto de 2025. Disponível em: https://www.researchgate.net/profile/Marcus-Abreu-3/publication/336000244SEGURANCAEINTEROPERABILIDADENAINDUSTRIA40/links/5ee782b892851ce9e7e3da10/SEGURANCA-E-INTEROPERABILIDADE-NA-INDUSTRIA-40.pdf

[10] BRASIL. (2025). Decreto Nº 12.573, de 4 de agosto de 2025. Acessado em: 05 de julho de 2024 Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784

[11] BRASIL. (2023). Portaria SGD/MGI Nº 852, de 28 de março de 2023. Acessado em: 05 de agosto de 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908

[12] LINUX FUNDATION – The Value of Open Source Software (2023). Acessado em: 07 de agosto de 2025. Disponível em: https://www.linuxfoundation.org/blog/the-value-of-open-source-software-is-more-than-cost-savings

[13] S. Jangampeta, “AI and Machine Learning in SIEM: Enhancing Threat Detection and Response with Predictive Analytics,” *International Journal of Artificial Intelligence & Machine Learning (IJAIML)*, vol. 1, no. 1, pp. 10–14, 2022. Acessado em: 17 de outubro de 2025. Disponível em: https://www.academia.edu/114500435/AI_AND_MACHINE_LEARNING_IN_SIEM_ENHANCING_THREAT_DETECTION_AND_RESPONSE_WITH_PREDICTIVE_ANALYTIC

[14] SAMPAIO, Inês Paiva. (2024). Automação de Processos de Resposta a Eventos de Segurança. Acessado em: 05 de agosto de 2025. Disponível em: https://repositorio.ulisboa.pt/handle/10451/41411

[15] R. Assunção, “A transparência e confiabilidade na adoção de soluções open source em ambientes críticos,” *Anais do XLII Encontro Nacional de Engenharia de Produção*, Foz do Iguaçu, PR, Brasil, pp. 41, 2015

[16] Kathare, N., Reddy, OV, & Prabhu, V. (2020). Um estudo abrangente do Elasticsearch. Revista internacional de ciência e pesquisa (IJSR). Acessado em: 07 de agosto de 2025. Disponível em: https://bryanhousepub.org/src/static/pdf/JRSE-2022-4-117.pdf

[17] ELASTIC. ELK Logstash. 2021. Acessado em: 10 de agosto de 2025. Disponível em: https://www.elastic.co/logstash/

[18] Souza, J. M. G. D. (2024). Visualização e análise de dados para cidades inteligentes: um estudo comparativo entre Grafana e Kibana (Bachelor's thesis, Universidade Tecnológica Federal do Paraná). Acessado em: 10 de agosto de 2025. Disponível em: http://riut.utfpr.edu.br/jspui/bitstream/1/35633/1/visualizaodadosgrafanakibana.pdf

[19] Palácio, L. G. (2024). Implantação de SIEM de código aberto em um ambiente corporativo: um estudo de caso. Acessado em: 10 de agosto de 2025. Disponível em: https://repositorio.ufc.br/bitstream/riufc/79253/3/2024_tcc_lgpalacio.pdf

[20] LINUX SOLUTIONS. Shuffle – Automação SOAR para um Futuro Mais Seguro. Acessado em: 31 de agosto de 2025. Disponível em: https://linuxsolutions.com.br/shuffle/

[21] SHUFFLE LLC. Shuffle Automation – An Open Source SOAR Solution. Acessado em: 31 agosto de 2025. Disponível em: https://shuffler.io/.

[22] STRANGEBEE. Cortex: Powerful observable analysis and active response engine. Acessado em: 31 agosto de 2025. Disponível em: https://www.strangebee.com/cortex

[23] ACADEMIA DE FORENSE DIGITAL. MISP no combate ao cibercrime. Acessado em: 31 de agosto de 2025. Disponível em: https://academiadeforensedigital.com.br/misp-no-combate-a-cibercrime.

[24] CERT.br. MISP – Plataforma de Compartilhamento de Informações de Ameaças Acessado em: 31 de agosto de 2025. Disponível em: https://www.cert.br/misp.

[25] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. Feb. 2024. Acessado em: 30 agosto de 2025. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[26] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Computer Security Incident Handling Guide (SP 800-61 Rev. 3). 2025. Acessado em: 30 agosto de 2025. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[27] MIR, Abdul Wahid; RAMACHANDRAN, Ramkumar Ketti. Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems. In: Sixth International Conference on Intelligent Computing and Applications. Springer, 2021. p. 157–169. Acessado em: 31 de agosto de 2025. Disponível em: https://link.springer.com/chapter/10.1007/978-981-16-1335-7_14.

[28] NATIONAL CYBER AND INFORMATION SECURITY AGENCY. Priority Logs for SIEM Ingestion: Practitioner Guidance. 2025. Acessado em: 31 agosto de 2025. Disponível em: https://media.defense.gov/2025/May/27/2003722069/-1/-1/0/PRIORITY-LOGS-FOR-SIEM-INGESTION-PRACTITIONER-GUIDANCE.PDF

[29] NEUMANN, Felix; WEBER, Claudia. Automated Security Operations: Scaling Threat Response with SOAR and AI-Driven Playbooks. International Journal of Trend in Scientific Research and Development, v. 5, n. 2, p. 1317–1323, 2021. Acessado em: 31 de agosto de 2025. Disponível em: https://www.ijtsrd.com/papers/ijtsrd38541.pdf.

[30] WATSON, Kimberly K. Orchestration of Information Technology Automation Frameworks. Cybersecurity and Threat Intelligence Sharing Best Practices, CISA, 2021. Acessado em: 31 de agosto de 2025. Disponível em: https://www.cisa.gov/sites/default/files/publications/Orchestration%20of

%20Information%20Technology%20Automation%20Frameworks_508c.pdf.

[31] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5, set. 2020. Acessado em: 30 de agosto de 2025. Disponível em: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[32] CENTER FOR INTERNET SECURITY (CIS) (2025). CIS Critical Security Controls v8. Acessado em: 15 de setembro de 2025. Disponível em: https://www.cisecurity.org/controls/.

[33] MITRE Corporation, *MITRE ATT&CK®: A Framework for Cyber Adversary Behavior*. Acessado em: 15 de setembro de 2025. Disponível em: https://attack.mitre.org

[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27035-1:2023 – Information security incident management — Part 1: Principles and process. Acessado em: 30 de agosto de 2025. Disponível em: https://www.iso.org/standard/78973.html.

[35] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Genebra: ISO, 2022. Acessado em: 15 de setembro de 2025. Disponível em: https://www.iso.org/standard/82875.html.

[36] Freitas, E. A. M. (2009). Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação. Acessado em: 07 de agosto de 2025. Disponível em: https://www.academia.edu/download/34979046/gestaoriscosfreitas.pdf

[37] Saleh, A. M. Adoção de Tecnologia: Um estudo sobre o uso de software livre nas empresas. 2004, pp. 18, 68. Acessado em: 07 de agosto de 2025. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12139/tde-06122004-123821/publico/Dissertacao-SWLivrenasempresas-AmirSaleh-Internet-040421.pdf

[38] Zwirtes, J. D. O. (2025). Open source e inovação: lições organizacionais da inovação aberta e do desenvolvimento colaborativo, p.27. Acessado em: 07 de agosto de 2025. Disponível em: https://lume.ufrgs.br/handle/10183/294739

[39] LIMA JUNIOR, T. A. DE S. 2006. ACEITAÇÃO DE TECNOLOGIA: UMA ABORDAGEM COGNITIVA SOBRE O USO DE SOFTWARE LIVRE. Acessado em: 07 de agosto de 2025. Disponível em: https://repositorio.ufba.br/bitstream/ri/8966/1/111j.pdf

[40] Vazão, A. P. H. (2020). Implementação de sistema SIEM open-source em conformidade com o RGPD. Acessado em: 10 de agosto de 2025. Disponível em: https://core.ac.uk/download/pdf/395660824.pdf