AVALIAÇÃO DA EFICÁCIA DO WAZUH COMO SOLUÇÃO DE SEGURANÇA PARA PEQUENAS E MÉDIAS EMPRESAS

ASSESSMENT OF WAZUH'S EFFECTIVENESS AS A SECURITY SOLUTION FOR SMALL AND MEDIUM ENTERPRISES

Allan de Sousa Monteiro
Fatec Araraquara
allandsm5@gmail.com

Maurício Turci Júnior
Fatec Araraquara
mauturj@gmail.com

Wdson de Oliveira
Fatec Araraquara
wdson.oliveira@unar.edu.br

Resumo

Este artigo analisa o uso do Wazuh como uma ferramenta de cibersegurança, especialmente voltada para pequenas e médias empresas. Em um cenário onde a tecnologia é amplamente adotada, as organizações enfrentam riscos crescentes devido à falta de recursos e soluções adequadas. A pesquisa envolveu a implementação do Wazuh em um ambiente controlado, onde foram realizados testes para avaliar sua eficácia. Os resultados mostraram melhorias significativas na detecção e mitigação de vulnerabilidades, além de proteção contra *malwares* e invasões. O estudo enfatiza a importância do Wazuh como uma solução acessível, robusta e adaptável. Isso a torna uma opção viável para atender às necessidades específicas de segurança das empresas menores. A pesquisa ressalta a necessidade urgente de soluções de segurança da informação no mercado atual.

Palavras-chave: Wazuh, cibersegurança, ferramenta.

Abstract

This article analyzes the use of Wazuh as a cybersecurity tool, especially aimed at small and medium-sized enterprises. In a scenario where technology is widely adopted, organizations face increasing risks due to a lack of resources and adequate solutions. The research involved implementing Wazuh in a controlled environment, where tests were conducted to evaluate its effectiveness. The results showed significant improvements in the detection and

mitigation of vulnerabilities, as well as protection against malware and intrusions. The study emphasizes the importance of Wazuh as an accessible, robust, and adaptable solution. This makes it a viable option to meet the specific security needs of smaller companies. The research highlights the urgent need for information security solutions in the current market.

***Keywords**: Wazuh, cybersecurity, tool.*

1. Introdução

Em um mundo cada vez mais digitalizado e interconectado, diante de diversos benefícios e facilidades operacionais, com deparamos com uma questão crucial para usuários, intsituições e, principalmente empresas: a segurança da informação. De acordo com Alarcão (2021), o avanço e facilidade de conexões realizadas através das redes e da Internet tornou este ambiente propício para agentes maliciosos, intrusões e aplicativos vulneráveis disponíveis aos consumidores. Com o aumento das ameaças cibernéticas e a sofisticação dos ataques, as organizações são constantemente desafiadas a encontrar soluções eficazes e acessíveis para garantir a integridade, confidencialidade e disponibilidade de suas informações.

Neste contexto, a utilização de ferramentas *open source* surge como uma alternativa viável e acessível para fortalecer a segurança cibernética em empresas menores. O Wazuh, uma solução de segurança *open source*, destaca-se por suas capacidades avançadas de monitoramento e resposta a incidentes, proporcionando uma solução robusta sem os altos custos associados a muitas ferramentas comerciais (Wazuh, 2024). A ferramenta oferece uma gama de funcionalidades que incluem a análise de *logs*, a detecção de intrusões e a conformidade com regulamentações, possibilitando que empresas de pequeno e médio porte implementem uma postura de segurança eficaz com um investimento reduzido.

A sua implementação pode representar uma alternativa viável e econômica para fortalecer a postura de segurança das organizações, contribuindo para a proteção de seus ativos informacionais e a continuidade de seus negócios. Considerando a acessibilidade da ferramenta, este estudo justifica-se pela necessidade de explorá-la como uma solução acessível e eficiente de segurança cibernética para empresas de pequeno e médio porte, tendo

como objetivo geral estudar a viabilidade e eficácia da implementação da ferramenta de segurança *open source*, o Wazuh, e como objetivos específicos: avaliar a eficácia da ferramenta Wazuh em termos de detecção, resposta e prevenção de incidentes cibernéticos, e realizar testes práticos para verificar seu funcionamento.

2. Referencial Teórico

2.1 Segurança da Informação

A Segurança da Informação, de forma básica, pode ser definida como uma disciplina fundamental que visa a proteção de informações. Deste modo, ela caminha lado-a-lado com os objetivos de uma organização, garantindo a proteção dados cruciais e os recursos mais valiosos para a continuidade de negócios (Blackley et al., 2024).

Com a aderência aos sistemas tecnológicos, cada vez mais sofisticados, é notável como a proteção de dados sensíveis é crucial. O cenário crítico em que se encontra a informação torna-se ainda mais evidente com o advento dos acessos online por meio da internet, quando dados começaram a ser compartilhados e vendidos. Isso elevou os riscos para o processo de tratamento de dados, visto que, agora, os cuidados para segurança cibernética se tornaram mais importantes do que nunca.

Além de cuidados com o mantimento da segurança através da tecnologia, também é essencial realizar a conscientização de todos os participantes sobre práticas seguras, ferramentas, diretrizes e políticas, fazendo com que os protocolos certos sejam empregados por quaisquer usuários envolvidos no processamento de dados, mesmo aqueles que não são especializados na área de TI (Gosenheimer; Nogueira, 2022).

O alicerce que estrutura a Segurança da Informação é a tríade CID, composta pelos pilares: Confidencialidade, que estabelece a proteção de acesso não autorizado; Integridade, para assegurar a autenticidade das informações; e a Disponibilidade, sustentando a acessibilidade consistente para usuários autorizados; ilustrados pela Figura 1. Estes são os

fundamentos mínimos de como um sistema de informação deve ser arquitetado (Yeboah-Boateng, 2013).

Figura 1 – Tríade CID

Fonte: Protiviti (2023)

2.2 Ameaças, Riscos e Vulnerabilidades Cibernéticas

Com uma quantidade cada vez maior de pessoas tendo acesso à internet, eleva-se o número de vulnerabilidades conhecidas e, ainda, de pessoas mal-intencionadas que passam a utilizá-la como ferramenta. Assim, percebe-se a importância não apenas de evoluir os sistemas de comunicação, mas também de garantir a sua segurança (Gosenheimer; Nogueira, 2022).

No estudo do ambiente de informação, passam a ser reconhecidas diversas formas, meios e atores que podem comprometer a segurança. Dentre estas destacam-se três definições:

- Ameaças: uma circunstância com o potencial de acarretar danos a um ativo.
- Vulnerabilidades: fraquezas dentro de um sistema de informação.
- Riscos: a probabilidade de um ativo ser comprometido.

2.2.1 Malware

A palavra "*malware*" é uma abreviação para *software* malicioso, aqueles produzidos com a intenção de danificar o dispositivo, roubar ou corromper arquivos (Rabia, 2018). Práticas como fazer *download* de anexos ou arquivos sem checagem e executar aplicações corrompidas são os meios mais comuns de propagação de *malware*.

Intrusões e ataques que utilizam de *malwares*, infelizmente, estão cada vez mais comuns. De acordo com a Kaspersky (2024), durante o ano de 2023 foram descobertos, em média, mais de 400 mil arquivos maliciosos por dia. O caso de ataque de *malware* mais conhecido foi o "*WannaCry*", do tipo *worm* (*malware* que se espalha em vários computadores dentro de uma rede), que em 2017, se aproveitou de uma brecha de segurança em sistemas operacionais desatualizados e, de acordo com a Cloudflare (2021), afetou mais de 200 mil computadores ao redor do mundo.

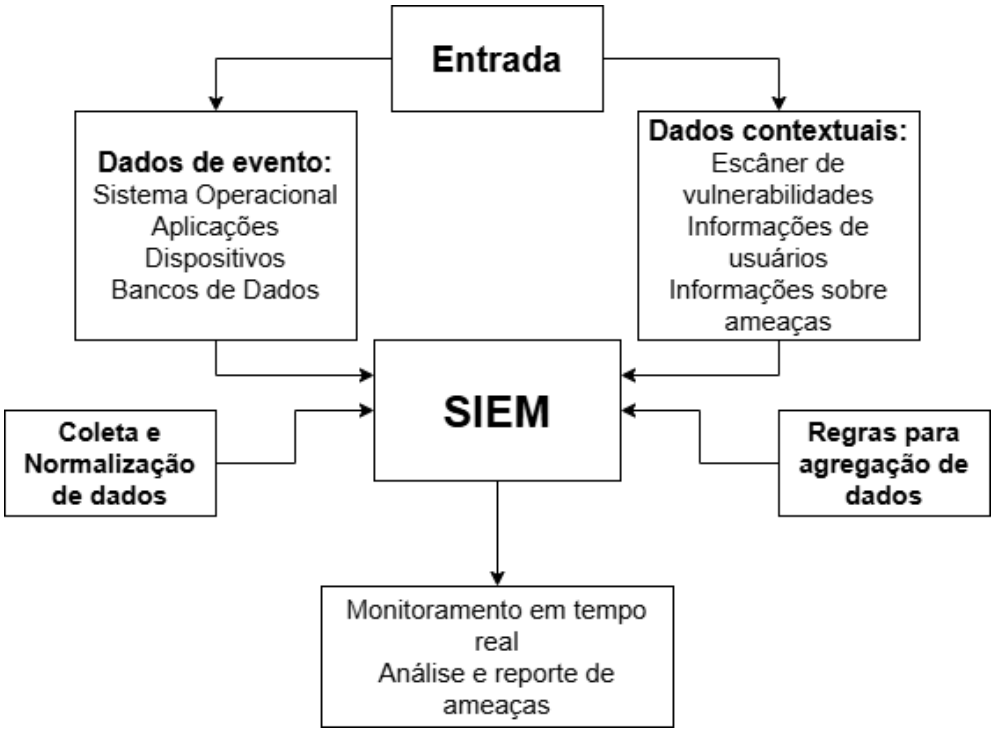
Ameaças externas, como *malwares*, podem até ser mitigadas através de boas práticas de TI e da conscientização, porém, algumas exigem tratamentos mais específicos.

2.3 Soluções para as ameaças à segurança cibernética

2.3.1 SIEM

A detecção de anomalias em tempo real é essencial para uma administração adequada dentro dos sistemas de informação. Para isso, são utilizados os sistemas SIEM, *Security Information and Event Management* (em português, Gerenciamento de Informações e Eventos de Segurança), que fornecem a análise em tempo real de eventos de segurança gerados por dispositivos dentro de uma determinada rede (González-Granadillo et al, 2021).

Figura 2 – SIEM.



Fonte: Os autores (2024), baseado em Intelipaat (s.d.)

Conforme ilustrado na Figura 2, o sistema SIEM é estruturado em blocos, cada um desempenhando uma função específica. O processo inicia-se com a coleta de dados provenientes de diversas fontes, como aplicações, dispositivos ou sistemas operacionais. Em seguida, ocorre a etapa de correlação e normalização dos dados, que organiza e correlaciona os eventos para facilitar a análise. Com os dados já normalizados e centralizados, torna-se possível realizar o monitoramento em tempo real, permitindo a identificação e análise de possíveis ameaças de forma eficiente. Dessa forma, esta ferramenta se qualifica como uma ferramenta de monitoramento ágil e eficiente para a administração de sistemas de informação (Bhatt et al, 2014).

2.3.2 XDR

A ferramenta XDR corresponde *a Extended Detection and Response* (em português, Detecção e Resposta Estendidas), atuando na correlação de dados e registros de *log*

apreendidos entre as camadas de rede, como: nuvem, servidores, e-mail e *endpoints*, que são as máquinas finais, chamadas de “extremidades da rede” (Soleman; Soewito, 2023).

Figura 3: XDR

Fonte: Os autores (2024), traduzido de OpenEDR (s.d.)

Como mostra a figura 3, o XDR (*Extended Detection and Response*) opera em três etapas principais: análise de dados, que consiste em agregar informações de diversas fontes e correlacionar contextos para identificar anomalias; detecção de ameaças, que prioriza e examina os alertas mais críticos; e resposta a ataques, que executa ações para eliminar ameaças detectadas e atualizar políticas de segurança.

Uma de suas funcionalidades é a Resposta Automatizada, onde é possível aplicar e planejar ações pré-definidas que o XDR irá executar em um cenário de alertas, como filtros, bloqueios de IP ou interrupção de processos. Além disso, a ferramenta conta com funcionalidades de investigação de ataques, que analisa dados, escaneia portas para identificar a raiz dos problemas, e a caça de ameaças, que consiste na busca de atividades suspeitas dentro do sistema (Soleman; Soewito, 2023).

2.4 Wazuh (SIEM/XDR)

O Wazuh é uma plataforma de segurança gratuita e de código aberto que unifica as capacidades de XDR e SIEM. Ele protege cargas de trabalho em ambientes locais, virtualizados, conteinerizados e baseados em nuvem. Seu funcionamento é baseado em 4 módulos:

- Wazuh *Indexer:* mecanismo de busca e análise de texto, responsável por indexar e armazenar alertas gerados pelo Wazuh.
- Wazuh *Dashboard:* interface *web* para visualização e análise dos dados.
- Wazuh *Server:* analisa os dados recebidos dos agentes.
- Wazuh *Agent: software* instalado nos *endpoints*, responsáveis pela coleta de dados e prevenção contra ameaças.

O Wazuh conta com diversas funcionalidades disponíveis por padrão, como Análise de Vulnerabilidades, auditoria baseada em regulamentações internacionais, como HIPAA, GDPR e PCI DSS, avaliação das configurações de segurança dos *hosts* baseado no CIS (*Center For Internet Security*) *benchmarks*, detecção de *malware* e monitoramento de integridade de diretórios e arquivos (Wazuh, 2024). Combinando essas funcionalidades, é possível obter uma postura de segurança robusta e proteger os ativos de segurança da empresa.

Com a funcionalidade de XDR, o Wazuh consegue responder a ameaças em tempo real e minimizar danos potenciais. O sistema utiliza regras de detecção baseadas em comportamento para identificar *malware*, em vez de se basear apenas em assinaturas pré-definidas. Isso permite a detecção tanto de ameaças conhecidas quanto desconhecidas, proporcionando uma defesa proativa e adaptável contra ataques cibernéticos (Wazuh, 2024).

Além disso, o Wazuh possui a funcionalidade de SIEM, que centraliza e correlaciona *logs* de dispositivos na rede. Isso simplifica a supervisão da rede sem a necessidade de

acessar diretamente os dispositivos para ler os *logs*. É possível criar regras para identificar atividades anômalas e gerar alertas para que a equipe de segurança possa investigar e agir conforme necessário.

2.4.1 Integrações

O Wazuh possui diversas integrações que permitem estender as funcionalidades padrões e compensar por algumas funções que ele não é capaz de fazer nativamente. Ele recebe telemetria via *syslog* ou APIs de aplicativos de terceiros, dispositivos e cargas de trabalho, como provedores de nuvem e fornecedores de SaaS (Wazuh, 2024).

Um exemplo delas é o *Shuffle*, um SOAR (*Security Orchestration, Automation and Response) open source* que permite automatizar ações e respostas a incidentes baseados em eventos do Wazuh, como isolar uma máquina, enviar um alerta ou realizar uma análise automatizada. Também é possível integrar com diversos outros sistemas, como o VirusTotal e AbuseIPDB para análise de reputação de arquivos e indicadores de compromisso (IOCs), integração com Inteligências Artificiais, sistemas de chamados como Jira e envio de mensagens através de email, Microsoft Teams e Slack.

2.4.2. Comparativo do Wazuh com outras ferramentas do mercado

2.4.2.1 Comparativo com o Splunk SIEM

O Splunk é uma plataforma comercial de análise e monitoramento de dados, conhecida por sua capacidade de lidar com grandes volumes de informações em tempo real. Utilizada para segurança, operações de TI e inteligência de negócios, ela oferece recursos avançados de pesquisa, visualização e integração com várias fontes de dados (Splunk, 2024).

A comparação com o Wazuh é relevante para destacar as diferenças entre uma solução comercial (Splunk) e uma *open source* (Wazuh). Ambas são utilizadas para monitoramento de segurança, mas atendem a diferentes necessidades, desde o custo e a escalabilidade até a abordagem de implementação e personalização.

Tabela 1: Comparativo Wazuh vs Splunk

Critério	Wazuh	Splunk
Licenciamento	*Open source*	Comercial
Custo	Baixo *(open source)*	Alto, baseado em volume de dados
Escalabilidade	Escalável, com limitações para ambientes grandes	Altamente escalável, ideal para grandes ambientes
Configuração	Requer conhecimento técnico	Fácil configuração e uso
XDR	Integrado nativamente	Não possui

Fonte: Os autores (2024)

Como mostrado na tabela 1, o Wazuh é uma solução *open source* e acessível, focada em segurança e monitoramento de ameaças, sendo ideal para empresas com orçamentos limitados. Já o Splunk é uma plataforma comercial, mais cara, mas oferece uma abordagem mais ampla e escalável. O Wazuh é mais técnico e exige mais configuração, enquanto o Splunk é mais fácil de implementar e escalável, mas com custos mais altos (Infoprotect, s.d.). A escolha depende das necessidades específicas de custo, escalabilidade e abrangência funcional.

2.4.2.2 Comparativo com o Microsoft Defender XDR

O Microsoft Defender é uma plataforma XDR incluído nas licenças avançadas do pacote Microsoft 365, que oferece investigação e resposta, fornecendo a proteção nativa contra ataques cibernéticos em dispositivos IoT, servidores, *email*, aplicações e na nuvem.

A comparação com o Wazuh é pertinente para demonstrar as diferenças entre uma solução comercial (Microsoft Defender) e uma *open source* (Wazuh). Ambas são utilizadas para a proteção, mas atendem a diferentes necessidades, desde o custo, desempenho, e sua implantação.

Tabela 2: Comparativo Wazuh vs Microsoft Defender

Critério	**Wazuh**	**Microsoft Defender XDR**
Licenciamento	*Open source*	Comercial
Custo	Baixo *(open source)*	Alto, baseado em volume de dados
Desempenho	Personalização de recursos, mais leve.	O uso de recursos do sistema impacta muito sobre o desempenho.
Implantação e Suporte	O *software* possui boa adaptabilidade, porém demanda conhecimento do usuário para implementação. Sem suporte.	Fácil implantação em ambientes da Microsoft, com suporte e atendimento ao cliente.
SIEM	Integrado nativamente.	Não possui.

Fonte: Os autores (2024)

Como mostrado na figura 2, o Wazuh é uma solução mais acessível, sendo ideal para empresas com orçamentos limitados, principalmente considerando seu desempenho. Já o Microsoft Defender XDR é uma plataforma comercial, mais cara, porém, oferece suporte ao

cliente, sem o usuário precisar ter conhecimento sobre a ferramenta para instalação, e por conta de seus recursos, é indicado para empresas e companhias de grande porte. A escolha depende das necessidades específicas de custo e desempenho da empresa.

2.4.3 Pontos negativos

Apesar de seus diversos pontos positivos, o Wazuh apresenta algumas limitações que devem ser consideradas. Conforme avaliações do Gartner entre 2022 e 2024, uma das principais dificuldades relatadas pelos usuários é o processo de implementação e configuração. Determinados recursos, como integrações, exigem ajustes manuais nos arquivos de configuração, em vez de uma configuração facilitada via dashboard. Essa abordagem aumenta o tempo e o esforço necessários para sua utilização.

Outro ponto destacado é a limitação do suporte na versão gratuita. O suporte oferecido pela comunidade pode ser útil para questões básicas, mas, em casos mais complexos que demandam assistência especializada, pode não atender às necessidades dos usuários.

Além disso, a PeerSpot (2022) ressalta que a escalabilidade da solução pode ser um desafio. Quando exposta a grandes volumes de dados, a ferramenta pode apresentar instabilidades, afetando a eficiência e a confiabilidade em cenários mais robustos.

3. Materiais e Métodos

3.1 Instalação e implementação do Wazuh

O Wazuh pode ser instalado facilmente utilizando o seguinte comando, que executa uma instalação automática através do script *wazuh-install.sh*. Este script é responsável pela instalação do *Indexer, Dashboard, Manager* e *Agent* no servidor. Após a execução do comando, o Wazuh estará disponível na porta 443.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i
```

3.2 Instalação dos Agentes

Nesta seção, será descrito o processo de instalação dos agentes utilizados para monitoramento e coleta de dados no ambiente de estudo.

3.2.1 Windows

No Windows, o agente do Wazuh pode ser instalado automaticamente utilizando o PowerShell. Este processo baixa o instalador do repositório do Wazuh e o instala como um serviço. Durante a instalação, é necessário configurar dois campos: *WAZUH_MANAGER*, onde deve ser inserido o IP do servidor do Wazuh, e *WAZUH_AGENT_NAME*, que define o nome de identificação do agente. O comando para realizar a instalação é:

```
# Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.2-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='IP_SERVER' WAZUH_AGENT_NAME='NOME_AGENTE'
```

Após a instalação, inicie o serviço do agente com o seguinte comando:

```
# NET START WazuhSvc
```

3.2.2 Linux

A instalação do agente do Wazuh no Linux é semelhante ao processo no Windows. O agente deve ser baixado do repositório do Wazuh e configurado conforme necessário:

```
# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-1_amd64.deb && sudo WAZUH_MANAGER='IP_SERVIDOR' WAZUH_AGENT_NAME='NOME_AGENTE' dpkg -i ./wazuh-agent_4.9.2-1_amd64.deb
```

Após a instalação, inicie e habilite o serviço do agente com os seguintes comandos:

```
# sudo systemctl daemon-reload

# sudo systemctl enable wazuh-agent

# sudo systemctl start wazuh-agent
```

4. Resultados e Discussões

Este capítulo descreve os testes realizados durante o estudo e os resultados obtidos. A partir desses testes, é possível validar as hipóteses iniciais e avaliar a eficácia das metodologias propostas.

4.1 Ambiente de testes

Os testes foram realizados em um ambiente virtual controlado. Tanto o agente quanto o *server* foram instalados no sistema operacional *Ubuntu Server* 22.04 LTS sem configurações adicionais. A versão do Wazuh utilizada é a 4.9, em conjunto com o agente na versão 4.9.2. No *endpoint* de testes, foi utilizado o Apache na versão 2.4.58. Todas as máquinas utilizadas possuíam 2GB de RAM e 2 vCPUs.

4.2 Testes realizados

4.2.1 Teste 1 - *Scanner* de vulnerabilidades

Com o agente instalado e iniciado nos *hosts*, ele começa automaticamente a buscar vulnerabilidades nos pacotes instalados, sem necessidade de configuração adicional. O agente compara as versões dos pacotes instalados no host com bancos de dados de vulnerabilidades, como o CVE (*Common Vulnerabilities and Exposures*). Os resultados da varredura são exibidos na seção "*Vulnerability Scanning*", conforme a Figura 4, e incluem informações sobre o pacote vulnerável, a versão instalada, uma descrição da vulnerabilidade, a severidade e o CVE relacionado.

Figura 4 – Resultados do *scan*

nano	7.2-2ubuntu0.1	A vulnerability...	Medium	CVE-2024-57...
git	1:2.43.0-1ubu...	GIT version 2....	Medium	CVE-2018-10...
setuptools	68.1.2	A vulnerability...	High	CVE-2024-63...
Jinja2	3.1.2	Jinja is an ext...	Medium	CVE-2024-34...

Fonte: Os autores (2024)

O teste foi realizado com o pacote "*setuptools*", relacionado a CVE “CVE-2024-6345” que apresenta uma criticidade alta, é relativamente recente e permitiria um atacante realizar a execução de código remoto na máquina. Inicialmente, foi verificada a versão instalada, conforme a Figura 5, a qual, conforme indicado pelos resultados da varredura, é a versão "68.1.2".

Figura 5 – Verificação da versão instalada

```
root@user:/home/user# pip show setuptools
Name: setuptools
Version: 68.1.2
```

Fonte: Os autores (2024)

Em seguida, atualizamos o pacote utilizando o comando “`pip install --upgrade setuptools`”, seguindo a Figura 6, que irá remover a versão vulnerável e instalar a versão mais recente.

Figura 6 – Atualização da versão do pacote

```
Collecting setuptools
  Downloading setuptools-73.0.1-py3-none-any.whl.metadata (6.6 kB)
Downloading setuptools-73.0.1-py3-none-any.whl (2.3 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.3/2.3 MB 8.5 MB/s eta 0:00:00
Installing collected packages: setuptools
  Attempting uninstall: setuptools
    Found existing installation: setuptools 68.1.2
    Uninstalling setuptools-68.1.2:
      Successfully uninstalled setuptools-68.1.2
Successfully installed setuptools-73.0.1
```

Fonte: Os autores (2024)

Como esperado, agora a versão instalada é a versão mais atual do pacote, sem vulnerabilidades conhecidas, de acordo com a Figura 7.

Figura 7 – Verificação da nova versão

```
root@user:/home/user# pip show setuptools
Name: setuptools
Version: 73.0.1
```

Fonte: Os autores (2024)

Ao consultar a aba *"Vulnerability Scanner"* novamente, observa-se na Figura 8, que a vulnerabilidade foi marcada como "*Solved*" (Resolvida).

Figura 8 – Novo status da vulnerabilidade.

data.vul...	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability
High	CVE-2024-6345	setuptools	Solved

Fonte: Os autores (2024)

Esta função desempenha um papel crucial na identificação de *softwares* vulneráveis presentes nos *hosts*, os quais podem servir como portas de entrada para ameaças externas e internas. A presença de vulnerabilidades em *softwares* pode resultar em graves consequências para os ativos da empresa, incluindo a execução não autorizada de código, a exfiltração e o roubo de dados, e a instalação de *malwares*. Através de uma visualização centralizada, é possível monitorar e reagir a essas vulnerabilidades de forma proativa, permitindo a implementação de medidas preventivas e mitigadoras antes que uma ameaça se concretize.

4.2.2 Teste 2 - Detecção de ataques à *websites*

O agente é responsável por coletar *logs* dos *hosts* e enviá-los para o SIEM. Por padrão, ele é capaz de coletar *logs* de acesso e erros de servidores web como Apache e NGINX, e possui regras nativas para detectar tentativas de exploração, como *SQL Injection* e XSS *(Cross-site Scripting)*. A detecção desses ataques ocorre através da identificação de padrões específicos nos *logs* coletados.

O teste foi realizado utilizando a ferramenta Nikto, um *scanner open source* de servidores *web* que procura por falhas de segurança através de diversos tipos de ataque. O alvo do *scan* foi um servidor Apache padrão, sem configurações adicionais. O Nikto pode ser instalado e iniciado com os seguintes comandos:

```
# apt install nikto
# nikto -host IP-ALVO
```

Após iniciar o *scan*, o usuário receberá os *logs*, conforme a Figura 9.

Figura 9 – Detecção do *scanner*.

Nov 15, 2024 @ 18:55:54.490	Host	XSS (Cross Site Scripting) attempt.
Nov 15, 2024 @ 18:55:54.490	Host	XSS (Cross Site Scripting) attempt.
Nov 15, 2024 @ 18:55:54.123	Host	Multiple XSS (Cross Site Scripting) attempts from same source ip.
Nov 15, 2024 @ 18:55:54.046	Host	SQL injection attempt.

Fonte: Os autores (2024)

Como mostrado na figura, as regras padrões de detecção do Wazuh foram eficazes em identificar a tentativa de ataque rapidamente. Aproximadamente 10 segundos após o início do *scan, f*oram detectadas diversas tentativas de *SQL Injection* e XSS (*Cross-site Scripting*) ocorrendo em um curto intervalo de tempo. Esta alta concentração de ataques sugere o uso de uma ferramenta automatizada. Com base nessa análise, é possível configurar alertas para notificar quando esses ataques forem detectados, permitindo uma resposta rápida e mitigando potenciais problemas.

5. Considerações Finais

Este artigo destacou a eficácia do Wazuh como uma solução robusta para a segurança cibernética. Suas funcionalidades, como monitoramento em tempo real, detecção de anomalias e geração de alertas, oferecem uma resposta rápida a incidentes e uma proteção abrangente contra ameaças. Além disso, sua flexibilidade permite a adaptação a diferentes contextos organizacionais, o que aumenta seu valor como ferramenta de segurança.

No entanto, é importante considerar as limitações identificadas, como a necessidade de configurações manuais em alguns recursos e desafios na escalabilidade em ambientes que lidam com grandes volumes de dados. Essas questões podem demandar maior esforço e planejamento durante a implementação e operação da solução.

Mesmo com essas limitações, os benefícios proporcionados pelo Wazuh são evidentes, especialmente para organizações que buscam uma ferramenta eficiente e acessível para fortalecer sua postura de segurança. Com a devida análise das necessidades

específicas e o investimento em um ambiente bem estruturado, o Wazuh pode se tornar uma peça-chave na proteção contra ameaças cibernéticas.

5.1 Trabalhos futuros

Como trabalhos futuros, sugere-se aprofundar os testes envolvendo diferentes tipos de ataques para avaliar como o Wazuh se comporta em situações mais complexas e variadas. A criação de cenários controlados que simulem ataques reais e sustentados por um período prolongado pode oferecer dados mais detalhados sobre sua resiliência e capacidade de resposta. Além disso, há a possibilidade de ampliar o ambiente de testes, incorporando redes mais robustas e sistemas operacionais alternativos, como Mac ou FreeBSD, o que permitirá verificar a compatibilidade e eficácia da ferramenta em plataformas diversificadas.

Outro aspecto a ser explorado é a integração de novas ferramentas complementares, possibilitando o desenvolvimento de um ecossistema de segurança mais abrangente e eficiente. Por exemplo, seria interessante criar um sistema integrado que automatize processos de análise, resposta e recuperação, tornando o ambiente mais proativo diante de ameaças. Essas iniciativas não só ampliariam o alcance dos estudos sobre o Wazuh, como também contribuiriam para o avanço da segurança cibernética em geral, promovendo soluções mais completas e adaptáveis às demandas do mercado.

Referências

ALARCÃO, Ana Paula de Aguiar. **Implementação e análise de resultados de ferramenta de detecção e resposta para proteção de endpoints em ambiente controlado.** 2021. 144 f. Tese (Doutorado em Ciência da Computação) - Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/bitstream/10483/34490/1/2021_AnaPaulaDeAguiarAlarcao_tcc.pdf. Acesso em: 3 mar. 2024.

BHATT, Sandeep; MANADHATA, Pratyusa K.; ZOMLOT, Loai. **The operational role of security information and event management systems**. IEEE security & Privacy, v. 12, n.

5, p. 35-41, 2014. Disponível em: https://www.researchgate.net/publication/273394505_The_Operational_Role_of_Security_Information_and_Event_Management_Systems. Acesso em: 15 ago. 2024.

BLACKLEY, John A.; PELTIER, Thomas R.; PELTIER, Justin. **Information Security Fundamentals**. (1st ed.). Auerbach Publications. 2004. Disponível em: https://www.taylorfrancis.com/books/mono/10.1201/9780203488652/information-security-fundamentals-john-blackley-thomas-peltier-justin-peltier. Acesso em: 9 mai. 2024.

Cloudflare. **O que foi o ataque de ransomware WannaCry?** Disponível em: https://www.cloudflare.com/pt-br/learning/security/ransomware/wannacry-ransomware/. Acesso em: 12 ago. 2024.

FERREIRA, A. J. L. **Open Source Software**. Departamento de Engenharia Informática. Universidade de Coimbra, 2005. Disponível em: https://student.dei.uc.pt/~ajfer/CP/CP%20Artigo%20-%20Open%20Source%20Software.pdf. Acesso em: 20 ago. 2024.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação: o fator humano**. Pontifícia Universidade Católica do Paraná. Curitiba, p. 10, 2009. Disponível em: https://www.cursosavante.com.br/cursos/curso533/conteudo7486.pdf. Acesso em: 15 mai. 2024.

Gartner. **Wazuh - The Open Source Security Platform Likes and Dislikes.** Disponível em: https://www.gartner.com/reviews/market/security-information-event-management/vendor/wazuh/product/wazuh-the-open-source-security-platform/likes-dislikes. Acesso em: 16 nov. 2024.

GONZÁLEZ-GRANADILLO, Gustavo; GONZÁLEZ-ZARZOSA, Susana; DIAZ, Rodrigo. **Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures.** Sensors, v. 21, n. 14, p. 4759, 2021. Disponível em: https://www.mdpi.com/1424-8220/21/14/4759. Acesso em: 7 mar. 2024.

GOSENHEIMER, Ana Clara Custódio; NOGUEIRA, Felipe Lopes Gurgel. **Avaliação e teste de ataques cibernéticos via ferramenta de EDR.** 2022. 122 f. Tese (Mestrado em Ciência da Computação) - Universidade de Brasília, Brasília, 2022. Disponível em: https://bdm.unb.br/bitstream/10483/35638/1/2022_AnaClaraCustodioGosenheimer_FelipeLopesGurgelNogueira_tcc.pdf. Acesso em: 8 mar. 2024.

GULYÁS, Oliver; KISS, Gabor. **Impact of cyber-attacks on the financial institutions**. Procedia Computer Science, v. 219, p. 84-90, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050923002752. Acesso em: 27 mai. 2024.

Infoprotect. **Wazuh vs. Splunk: Explorando as Diferenças entre Duas Poderosas Soluções de Segurança.** Disponível em: https://infoprotect.com.br/wazuh-vs-splunk-explorando-as-diferencas-entre-duas-poderosas-solucoes-de-seguranca/. Acesso em: 15 nov. 2024.

Intellipaat. **What is SIEM? Security Information & Event Management**. Disponível em: https://intellipaat.com/blog/what-is-siem/. Acesso em: 11 ago. 2024.

Kaspersky. **Kaspersky: mais de 400 mil malware foram descobertos por dia em 2023**. Disponível em: https://www.kaspersky.com.br/about/press-releases/2024_kaspersky-mais-de-400-mil-malware-foram-descobertos-por-dia-em-2023. Acesso em: 15 mai. 2024.

Microsoft. **Microsoft Defender XDR.** Disponível em: https://www.microsoft.com/pt-br/security/business/siem-and-xdr/microsoft-defender-xdr. Acesso em: 10 jun. 2024.

OpenEDR. **What is XDR Explained? An overview of Extended Detection and Response Technology.** Disponível em: https://www.openedr.com/blog/xdr-explained/. Acesso em: 18 nov. 2024.

PeerSpot. **Microsoft Defender XDR vs Wazuh comparison.** Disponível em: https://www.peerspot.com/products/comparisons/microsoft-defender-xdr_vs_wazuh. Acesso em: 11 nov. 2024.

PeerSpot. **Wazuh pros and cons.** Disponível em https://www.peerspot.com/products/wazuh-pros-and-cons. Acesso em: 16 nov. 2024.

Protiviti. **Conheça os Pilares da Segurança da Informação.** Disponível em: https://www.protiviti.com.br/cybersecurity/pilares-seguranca-da-informacao/. Acesso em: 3 ago. 2024.

SOLEMAN, Dedi; SOEWITO, Benfano. **Information Security System Design Using XDR And EDR.** Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, v. 9, n. 1, p. 51-57, 2023. Disponível em: https://ejournal.unitomo.ac.id/index.php/inform/article/view/7331/3660. Acesso em: 13 abr. 2024.

Splunk. **What Is Splunk & What Does It Do? A Splunk Intro.** Disponível em: https://www.splunk.com/en_us/blog/learn/what-splunk-does.html. Acesso em 14 nov. 2024.

Wazuh. **Active XDR protection from modern threats.** Disponível em: https://wazuh.com/platform/xdr/. Acesso em: 16 nov. 2024.

Wazuh. **Wazuh - The Open Source Security Platform**. Disponível em: https://wazuh.com/. Acesso em: 11 mai 2024.

Wazuh Documentation. **Architeture - Getting started with Wazuh**. Disponível em: https://documentation.wazuh.com/current/getting-started/architecture.html. Acesso em: 9 jun. 2024.

World Economic Forum. **After reading, writing and arithmetic, the 4th "r" of literacy is cyber-risk**. World Economic Forum. Disponível em: https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/. Acesso em: 14 ago. 2024.

YEBOAH-BOATENG, Ezer Osei. **Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)**. 1 ed. Institut for

Elektroniske Systemer, Aalborg Universitet, 2013. Disponível em: https://vbn.aau.dk/ws/portalfiles/portal/549483575/PhD_Thesis_Boateng_Final_for_print.pdf. Acesso em: 10 mai. 2024.