DOI: 10.5748/19CONTECSI/PSE/SEC/7103

CONFIGURAÇÃO E APLICAÇÃO DE UM SOC (SECURITY OPERATION CENTER) GRATUITO: UM ESTUDO PRÁTICO PARA APLICAÇÃO DO SIEM WAZUH

Wellington Sousa Aguiar ; https://orcid.org/0000-0003-0677-5782
CENTRO UNIVERSITÁRIO ESTÁCIO DO CEARÁ: FORTALEZA

CONFIGURATION AND APPLICATION OF A FREE SOC (SECURITY OPERATION CENTER): A PRACTICAL STUDY FOR THE APPLICATION OF THE WAZUH SIEM

ABSTRACT

Attributing intelligence to the information security area has become a mandatory measure for knowing what is controlled within the organization, creating new models of cybernetic defense, not only based on the behavior of anomalies in the company, but also on what is happening around the world. This article presents an introductory SOC model capable of performing the necessary operations for monitoring threats and anomalies within an organization's network assets, emphasizing SIEM technology. For the tests with the technology, a laboratory was built so that the tests could be carried out in a practical way, assembling and simulating the SIEM Wazuh servers according to the official documentation and the good practices defined by the developers, as well as the necessary infrastructure to simulate the security incident composed of endpoint, firewall and SIEM servers (Indexer, Server and Dashboard). With the tests carried out in the laboratory, it was possible to create a monitoring environment capable of detecting anomalies as predicted by the technology, allowing the creation of new detection rules and integration of different data sources, Wazuh as a SIEM presents itself as a solution of lowcost cost effective for incident detection.

Keywords: SIEM, SOC, Wazuh, IH&R.

CONFIGURAÇÃO E APLICAÇÃO DE UM SOC (SECURITY OPERATION CENTER) GRATUITO: UM ESTUDO PRÁTICO PARA APLICAÇÃO DO SIEM WAZUH

RESUMO

Atribuir inteligência para a área de segurança da informação se tornou uma medida obrigatória para conhecimento do que está acontecendo dentro da organização, criar modelos de defesa cibernética, não baseando apenas ao comportamento de anomalias da empresa, mas também ao que está ocorrendo pelo mundo. Este artigo apresenta um modelo introdutório de SOC capaz de realizar as operações necessárias para o monitoramento de ameaças e anomalias dentro dos ativos da rede de uma organização, dando ênfase a tecnologia de SIEM. Para os testes com a tecnologia, foi realizado a construção de um laboratório para que os testes fossem realizados de forma prática, montando e simulando os servidores do SIEM Wazuh conforme a documentação oficial e as boas práticas definidas pelos desenvolvedores, assim como a infraestrutura necessária para simular o incidente de segurança composto por endpoint, firewall e os servidores do SIEM (Indexer, Server e Dashboard). Com os testes realizados no laboratório, foi possível criar um ambiente de monitoramento capaz de detectar anomalias conforme previsto pela tecnologia, possibilitando a criação de novas regras de detecção e integração de diversas fontes de dados, o Wazuh como SIEM se apresenta como uma solução de baixo custo eficaz para a detecção de incidentes.

Palavras-chave: SIEM, SOC, Wazuh, IH&R.

INTRODUÇÃO

A área de segurança da informação sempre foi uma briga sem fim do bem contra mal, ao mesmo tempo que a tecnologia avança e novos mecanismos de segurança estão sendo criados, os criminosos, hoje intitulados de várias formas, Crackers, Black Hat, Hacktivistas, Script Keddies, Carders, Spammers, criam novas formas de burlar as proteções e/ou criar novos modelos de *malwares* para diversos fins, seja para obter lucros financeiros, ações terroristas, questões políticas ou até mesmo para satisfazer o ego.

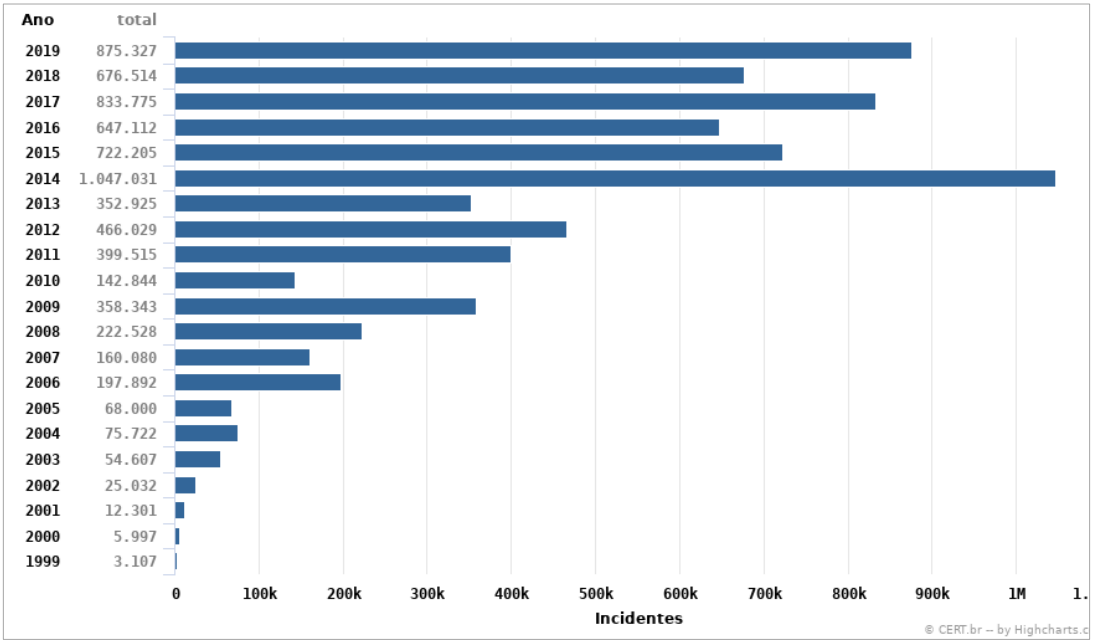
Uma pesquisa realizada pela B2B International publicada no final de 2016, envolvendo mais de 4000 empresas em 25 países, identificou que:

- 38% das empresas participantes tiveram problemas sérios com vírus/malwares;
- 21% das empresas sofreram ataques de *data loss*;
- 17% sofreram ataques de Negação de Serviço;
- 42% sofreram ataques de *Phishing*;
- 26% dos incidentes permaneceram despercebidos por semanas.

A pesquisa realizada pela B2B International aponta que as empresas que sofreram ataques de violação de dados, amargaram um prejuízo médio de US$ 891 mil, sendo esse valor a média da variação entre UU$393 mil a UU$1,1 milhão, e a variação desse custo foi resultado do quão rápido uma violação foi detectada.

Do ano de 2006 em diante, a quantidade de incidentes com cyber ataques aumentou em valores extraordinários, tornando-se cada vez mais um negócio rentável e a cada dia vem surgindo mais indivíduos com o objetivo de lucrar destas formas antiéticas. Segundo a CERT.br (Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil) somente no ano de 2019, ocorreram 875.327 incidentes reportados, aumento de 29,38% em relação ao ano de 2018, conforme apresentado no Gráfico 1, abaixo.

Gráfico 1- Relatório dos incidentes reportados ao Cert.br.



Fonte: CERT.br.

Portanto, com o aumento do prejuízo financeiro e o aumento de ataques cibernéticos, as empresas perceberam a necessidade de implantar não somente mais métodos de defesa e tecnologias de bloqueio de ataques, mas ferramentas e técnicas para realizar o monitoramento,

criando cada vez mais centros de operações de segurança (SOCs, Security Operations Centers) com o objetivo de combater os ataques e ter agora o conjunto de tecnologias monitoradas, com o objetivo de identificar anomalias e poder realizar uma resposta à incidentes de forma rápida e eficiente, aplicando à segurança da informação, não somente mecanismos de defesa, mas também inteligência para a operação.

> "Os centros de operações de segurança devem ser planejados visando a inteligência, adotando uma arquitetura de segurança adaptável, sendo sensíveis ao contexto e orientados por informações. Os líderes de segurança devem entender como os SOCs orientados por informações usam ferramentas, processos e estratégias para se proteger contra as ameaças modernas" (Gartner, *The Five Characteristics of an Intelligence-Driven Security Operations Center*, 2015).

Um dos maiores problemas que atinge as empresas na hora de realizar a implementação de um SOC é o alto custo das tecnologias, tornando-se as vezes impossível para empresas de pequeno e médio porte. Pensando nisso, o objetivo central deste trabalho é apresentar tecnologias suficientes e eficientes para que se tenha um SOC capaz de detectar e responder à incidentes de segurança cibernética, com foco em ferramentas gratuitas e preferencialmente *Open Source* (software de código aberto) para o desenvolvimento da estrutura por completo. Vale lembrar que para um software ser considerado *Open Source*, ele deve atender, segundo o site https://opensource.org, os seguintes critérios de forma simultânea:

a) utilização para qualquer fim e sem restrições;
b) distribuição de cópias sem restrições;
c) acesso ao código fonte e estudo do seu funcionamento;
d) adaptação às necessidades de cada um;
e) possibilidade de disponibilizar a terceiros quaisquer alterações introduzidas.

REFERENCIAL TEÓRICO

Para dar maior sustentação teórica a esta pesquisa, seguem descrições teóricas de temas relevantes para o entendimento do projeto, pesquisadas em bibliográficas relevantes.

SOC (SECURITY OPERATION CENTER)

Um centro de operações de segurança (SOC - *Security Operation Center*) é formado por um conjunto de especialistas que monitoram de forma proativa todo o ambiente da empresa, possuindo a capacidade através do auxílio da tecnologia de prever, detectar e responder a um incidente, da forma mais eficaz e rápida possível, pois essa ação é o que determinará se um atacante vai obter ou não sucesso em seu ataque.

Segundo a Kaspersky como definição o SOC é "O SOC é um departamento centralizado para o monitoramento e a análise constantes de ameaças e para a redução e prevenção de incidentes de segurança cibernética" (SOC powered by Kaspersky Lab, 2016, Pag. 2).

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Um sistema SIEM pode, de acordo com o guia da IBM:

> "Coletar dados de arquivos de log e alertas de vários componentes de infraestrutura, como firewalls, roteadores, sistemas antivírus, servidores e muitos outros. Ele pode informar as equipes de TI sobre o comportamento incomum nesses sistemas e, em seguida, essas equipes podem decidir se e que tipo de investigação adicional realizar"

(Buecker, A., Amado, J., Druker, D., Lorenz, C., Muehlenbrock, F., & Tan, R. (2010). *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*. IBM Redbooks.).

Quando citado que o SOC tem por objetivo trazer mais inteligência para a área de segurança, essa afirmativa está diretamente ligada a capacidade da equipe de SOC realizar o monitoramento de todo o ambiente e gerar regras de correlações para que seja possível a identificação de anomalias dentro da organização.

Essa afirmativa está ligada diretamente a ferramenta do SIEM, sendo essa a tecnologia responsável pela conexão dos logs de todos os ativos da empresa, gerando uma carga de informação que humanamente falando é impossível realizar a leitura, entretanto, através do SIEM é possível registrar e correlacionar regras para identificar um comportamento irregular, os chamados Casos de Uso, por exemplo: Consideramos que o SIEM da empresa X está recebendo os logs tanto da VPN quanto da catraca de entrada física na empresa, no horário de 09:00 o SIEM recebe o log da entrada do colaborador João, e às 09:15 o usuário do João realiza uma conexão na VPN, sabemos que não existe necessidade desse colaborador se conectar na VPN visto que ele está presencialmente na empresa, podendo ser um Falso-Positivo, entretanto, não deixa de ser uma anomalia, gerando um acionamento ao time de Monitoramento do SOC que irá fazer a primeira verificação, o chamado N1 do atendimento.

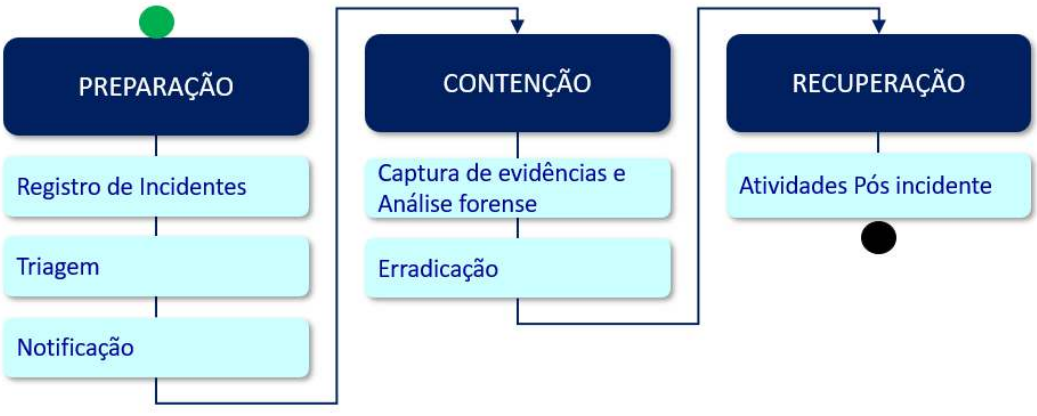
Para que um SIEM seja capaz de analisar e alertar corretamente os logs críticos, antes é imprescindível que haja ali a conexão das fontes de dados ativas na empresa, fontes essas como por exemplo os Endpoints, os Firewalls, os Proxys, os IDS/IPS, o Active Directory, o WAF, os Bancos de Dados, dentro outros, sendo possível, então, através do time de Hunting (engenharia), a realização as construções das UCs (*Use Cases* - Casos de Uso).

IH&R (INCIDENT HANDLER AND RESPONSE)

Segundo a documentação oficial da EC-COUNCIL do treinamento ECIH, o tratamento e resposta a incidentes (IH&R) "é um processo e um conjunto de procedimentos, ações e medidas - etapas organizadas e cuidadosas para reagir a um ataque cibernético de incidente de segurança ou outra ocorrência de evento inesperado."

IH&R é uma das atividades que envolvem um centro de operações de segurança, diretamente envolvida nas etapas de Resposta de um incidente cibernético, onde é definido o processo mediante um ataque cibernético, prevenindo o alastramento deste ataque ou mesmo sua efetividade. Os processos de IH&R envolvem, como mostra a Figura 1.

Figura 1 – Processo de IH&R.



Fonte: Elaborado pelo autor a partir do processo de IH&R.

PFSENSE

Segundo o próprio site Pfsense.org, o projeto *Pfsense* "é uma distribuição de firewall de rede gratuita, baseada no sistema operacional FreeBSD com um kernel personalizado e incluindo pacotes de software gratuitos de terceiros para funcionalidade adicional".

O Firewall *Pfsense* é uma tecnologia gratuita e *Open Source*, sendo uma das mais utilizadas pela sua estabilidade e suporte oferecido na comunidade, uma das melhores soluções quando o assunto é a implantação de um sistema de segurança, isso devido ao fato de além da sua função nativa de Firewall, o *Pfsense* permite a instalação de módulos adicionais, permitindo a integração das seguintes tecnologias na mesma "caixa" de sistema operacional:

- IPS/IDS com o Snort;
- VPN com IPSec;
- Proxy com Squid ou Suricata;
- Captivel Portal.

Como mencionado anteriormente, o SOC vem para complementar as tecnologias de segurança para contenção, por isso o Projeto *Pfsense* é importante nessa etapa de projeto, pois irá permitir o controle de fluxo de comunicação, filtro de dados e conexões externas na rede de forma segura.

METODOLOGIA

Esta pesquisa utilizou a metodologia aplicada, quando a pesquisa visa a utilização dos resultados no mundo real. A pesquisa aplicada é motivada pela necessidade de resolver problemas concretos, mais imediatos ou não (VERGARA, 2010). Quanto aos meios, foi usada ainda a pesquisa bibliográfica para direcionar o trabalho, dar sustentação teórica e explicar os conceitos das técnicas utilizadas.

A principal tecnologia usada nesta pesquisa é o SIEM utilizando o sistema Wazuh. Como mencionado no capítulo anterior, o SIEM é a tecnologia principal quando falamos em aplicar inteligência no Centro de Operação de Segurança, devido a capacidade que ele possui de capturar todos os dados e criar as devidas correlações.

Conforme a própria documentação oficial do Wazuh, "o Wazuh é uma solução de monitoramento de segurança gratuita, de código aberto e pronta para empresas para detecção de ameaças, monitoramento de integridade, resposta a incidentes e conformidade."

O Wazuh não é a única tecnologia *Open Source* disponível, segue abaixo uma listagem com alguns dos mais conhecidos sistemas de SIEM: AlienVault OSSIM; Wazuh; OSSEC e Sagan.

A escolha do Wazuh como sistema para este artigo, está relacionado a algumas características que foram consideradas relevantes para o estudo e para o uso da aplicação, segue abaixo os pontos positivos apresentados nos testes para escolha do Wazuh como SIEM deste artigo:

- Documentação fácil e completo: O Wazuh conta com uma documentação rica em informação podendo ser acessada em https://documentation.wazuh.com/current/quickstart.html, que acompanha desde os requisitos necessários para instalação da aplicação, como todo o processo de configuração e utilização do sistema.
- Interface gráfica: Um grande problema enfrentado por organizações para implantar sistemas de segurança, é a necessidade da mão de obra, pois exige um conhecimento específico no uso da tecnologia. A interface é fator muito

importante para um aprendizado da tecnologia, e o Wazuh possui uma interface muito interativa com usuário, além de ser um sistema clean.

- Integrações totalmente gratuitas: Alguns dos sistemas de SIEM testados são totalmente gratuitos para uma instalação padrão, portanto, principalmente falando na parte de conexão de fontes de logs exigem a contratação de um modelo "premium" ou o pagamento de uma taxa extra. O Wazuh não pede nenhum pagamento para realizar a integração de seus plugins e portanto, essa característica se destaca como um dos pontos positivos para a utilização.

Este trabalho e os testes realizados foram baseados em um laboratório, visando sempre utilização de tecnologias gratuitas. Segue a lista dos softwares utilizados com suas respectivas funções e as configurações de hardware:

- SNORT: O Snort é um sistema gratuito de IDS (Intrusion Detect System) e IPS (Intrusion Prevent System), é um sistema que analisa o tráfego da rede em busca de assinaturas que podem corresponder a ataques cibernéticos.

Segundo o site oficial snort.org, "o Snort é o principal Sistema de Prevenção de Intrusão de Código Aberto (IPS) do mundo. Usa uma série de regras que ajudam a definir a atividade maliciosa da rede e usa essas regras para encontrar pacotes que correspondam a eles e gera alertas para os usuários."

- Squid Proxy: O Squid é um servidor proxy amplamente utilizado no Linux, utilizado para realizar o filtro de acesso na web, possui diversas características que o destacam como um dos mais utilizados sistemas Open Source do mundo, como: Armazenamento de cache; Integração com NTLM, filtro de conteúdo.

- Pfsense: O Firewall *Pfsense* como já mencionado anteriormente é uma tecnologia *Open Source* e gratuita baseado no FreeBSD, além de realizar suas funções de controle de comunicação, o *Pfsense* permite a integração de módulos para novas funcionalidades como os já citados acima:

  • Squid Proxy;
  • OpenVPN;
  • IPS/IDS com Snort;
  • Captivel Portal para controle de acesso Wireless;
  • Outros módulos (para relatórios, scan de vulnerabilidades, WAF etc.).

- Wazuh SIEM: Sendo este a tecnologia que é dado maior atenção para este artigo, o Wazuh é um sistema de SIEM que permite a integração de diversas fontes de logs e suas próprias correlações.

Para o desenvolvimento do projeto de pesquisa foi um notebook da marca Dell, como descreve o Quadro1 abaixo.

Quadro 1 – Equipamento utilizado na pesquisa.

Equipamento:	**Dell Inspiron 7472**	**CPU:**	**I7 8th Gen**
Memória RAM:	**16 GB**		
Armazenamento:	**240 GB (SSD)**		

Fonte: Elaborado pelo autor.

Os sistemas mencionados foram instalados utilizando VM's criadas e gerenciadas utilizando o *Oracle VM Virtual Box*, onde cada tecnologia possui uma configuração específica, conforme demonstrado no Quadro 2 abaixo.

Quadro 2 – Configuração específica do *Pfsense*.

Memória RAM:	**2 GB**
Armazenamento:	**30 GB (SSD)**
CPU:	**2 vCPUs**

Fonte: Elaborado pelo autor.

De acordo com o orientado pela documentação, o SIEM Wazuh foi dividido em 3 servidores separadamente, conforme o Quadro 3 abaixo:

Quadro 3 – Especificação dos servidores.

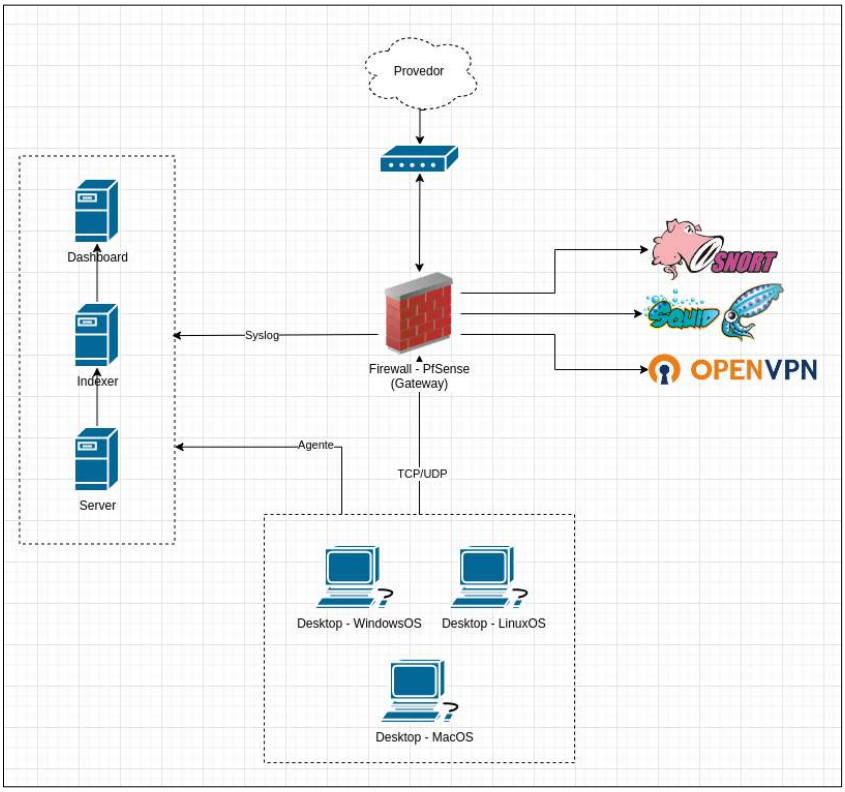
HARDWARE	INDEXER	SERVER	DASHBOARD
Memória RAM:	**4 GB**	**2 GB**	**4 GB**
Armazenamento:	**50 GB (SSD)**	**30 GB (SSD)**	**30 GB (SSD)**
CPU:	**2 vCPUs**	**2 vCPUs**	**3 vCPUs**

Fonte: Elaborado pelo autor.

RESULTADOS

Como resultado, será apresentado a interface e funcionamento pós instalação do SIEM Wazuh, apresentando os dados que foram gerados e o evento correlacionado devido a regra construída no SIEM. A arquitetura que seŕa apresentada de forma acadêmica, segue conforme a Figura 2 abaixo.

Figura 2 – Arquitetura utilizada.

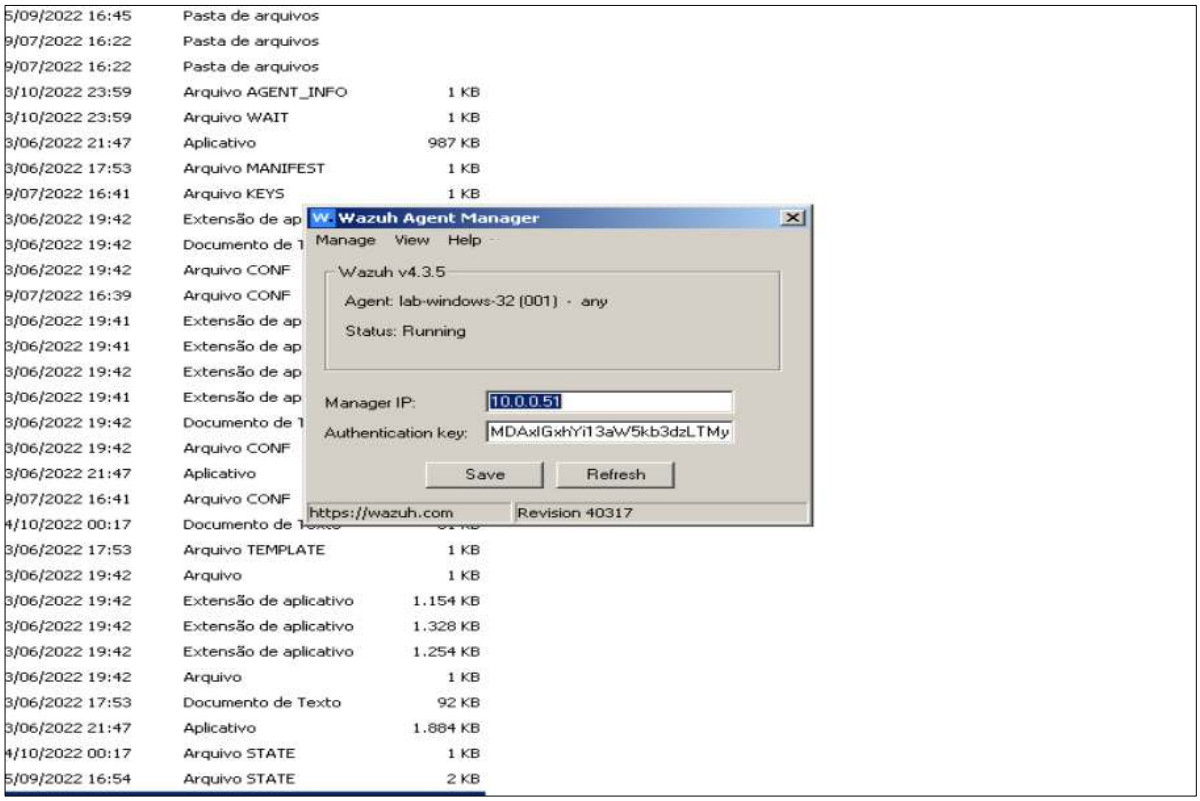


Fonte: Elaborado pelo autor.

Os computadores Windows/Linux/MacOS podem enviar os dados para o SIEM de forma direta via agent instalado no computador, dessa forma todos os eventos locais são registrado no Wazuh. Tecnologias que não possuem suporte ao agente, como o o Firewall *Pfsense* que é baseado no FreeBSD, pode ser configurado o redirecionamento de logs via protocolo Syslog.

Após o agente instalado no sistema operacional, é apontado para o Server do Wazuh, que é responsável pelo gerenciamento dos eventos, conforme apresenta a Figura 3.

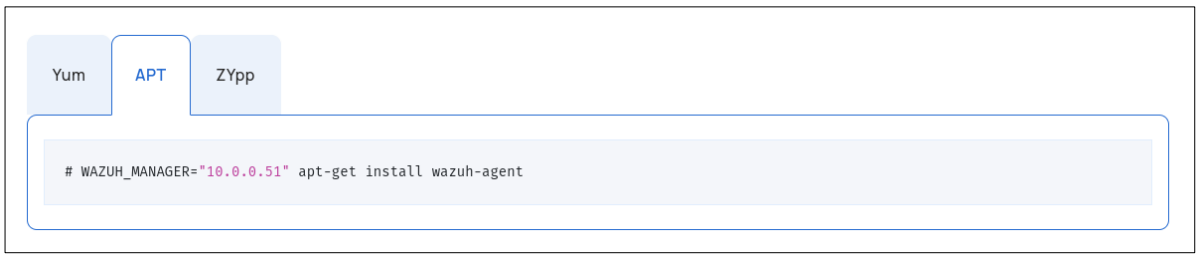
Figura 3 – Configuração do agente para conexão e autenticação do servidor.



Fonte: Capturado pelo autor.

Para o sistema operacional Linux é também realizado o mesmo procedimento de apontamento de servidor, entretanto utilizando uma variável de ambiente na hora da instalação, como apresenta a Figura 4.

Figura 4 – Comando de instalação do agente no Linux.

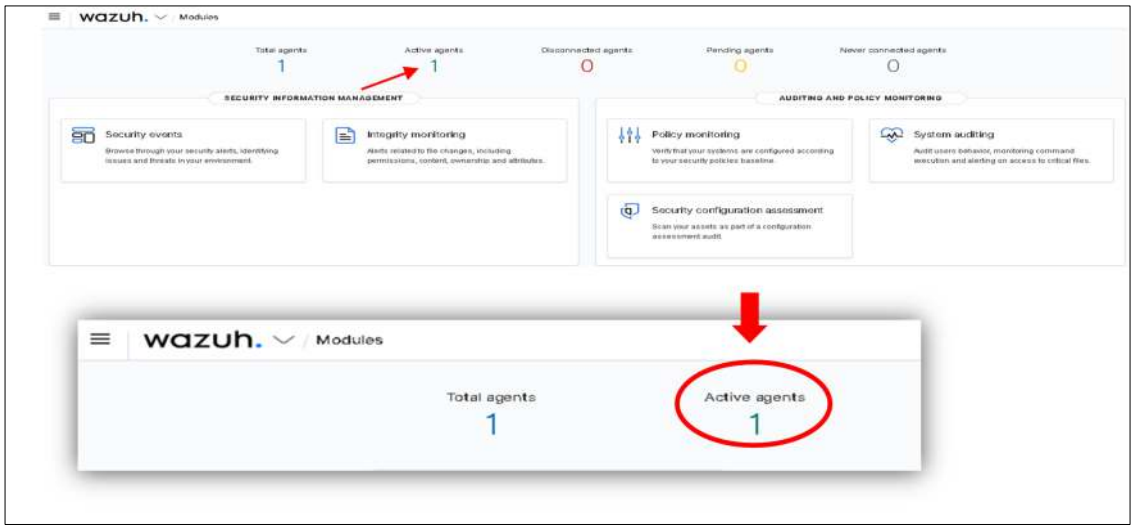


Fonte: Elaborado pelo autor.

Como mencionado, o envio de logs para o Wazuh pode ser configurado tanto via agente instalado em sistemas que utilizam Windows, Linux, MacOS, Solaris, AIX e HP-UX quanto o envio por protocolo Syslog.

Com o agente instalado na máquina, utilizando como exemplo o host windows da imagem acima, podemos acompanhar no Wazuh que ele registrou que existe uma quantidade total de agentes, agentes ativos, desconectados e pendentes conforme Figura 4, e verificando os agentes mais específicos podemos ver que se trata da mesma Máquina Windows que está sendo utilizada na Figura 5 abaixo.

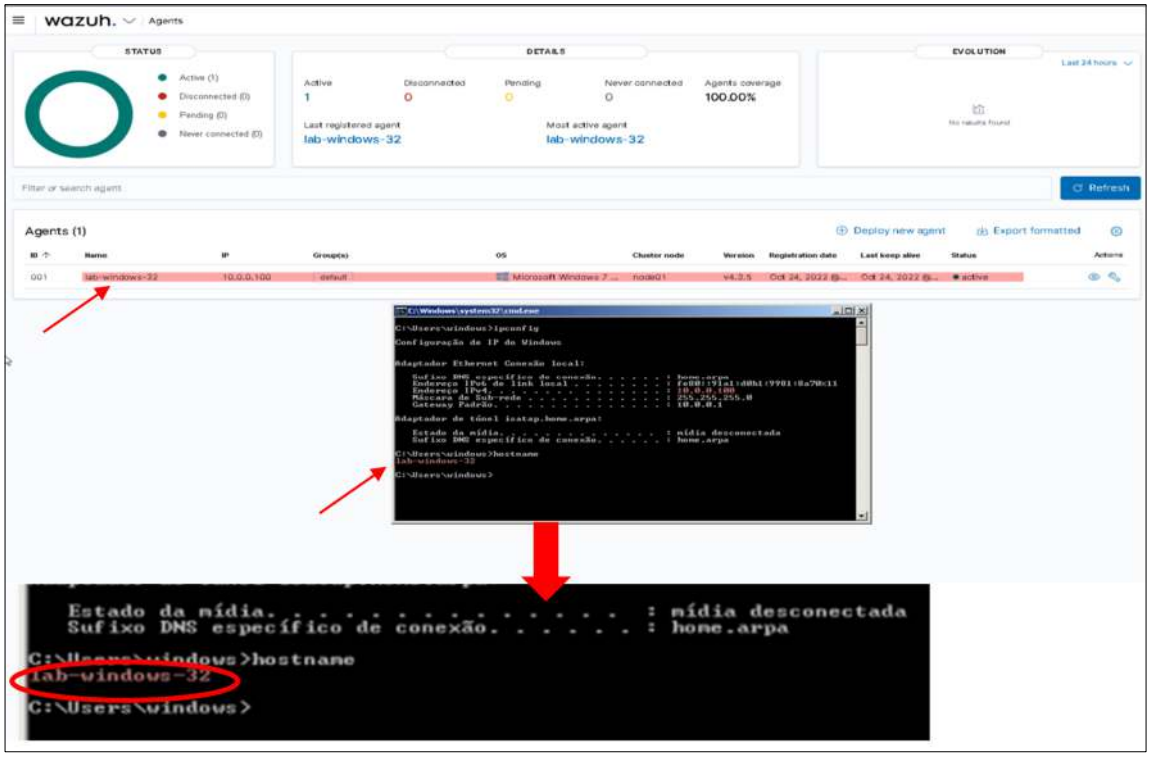
Figura 5 – Quantidade de agentes reconhecidos pelo Wazuh.



Fonte: Elaborado pelo autor.

A Figura 6 apresenta a confirmação de máquina instalada.

Figura 6 – Confirmação de Máquina instalada.



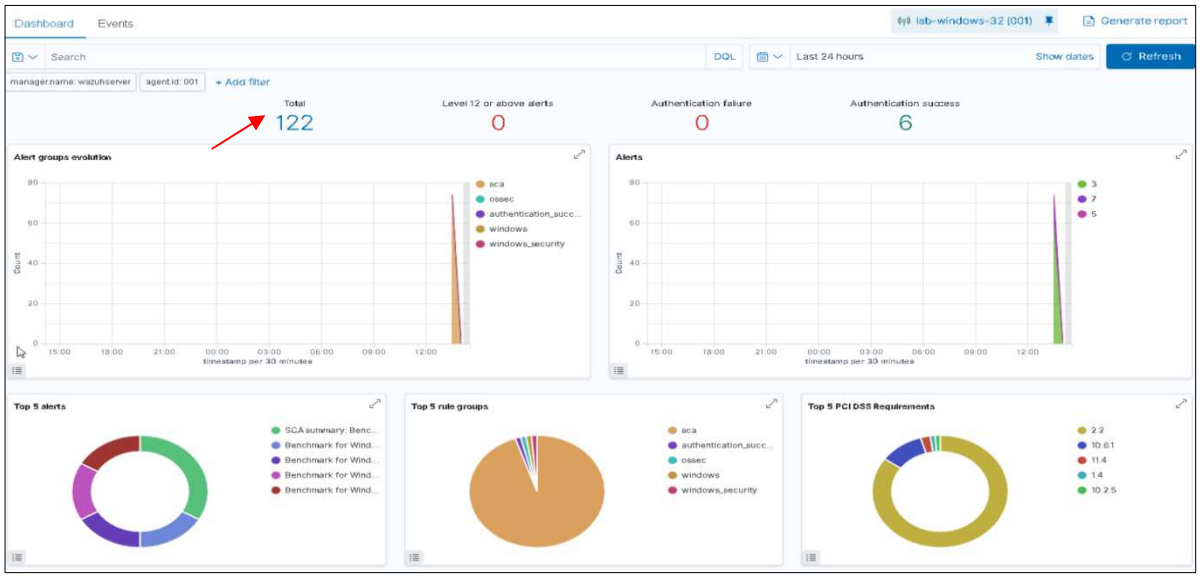
Fonte: Elaborado pelo autor.

Todos os eventos gerados por essa máquina serão encaminhados para o SIEM do Wazuh, que já possui Interpretadores e Regras definidas. O Wazuh possui uma característica

muito importante que é: Todos os eventos que são enviados ao SIEM, se não possuir um interpretador para aquele log ele será descartado, portanto, caso ocorra uma conexão de um sistema, em que o formato de log não é reconhecido pelo Wazuh ele irá descartar aquela informação, podendo ser construído de forma manual um interpretador para cada fonte de log desejada.

A Figura 7 abaixo, apresenta os eventos que estão chegando ao SIEM do Host lab-windows-32 enviados pelo agente instalado.

Figura 7 – Visualização dos eventos no Wazuh.

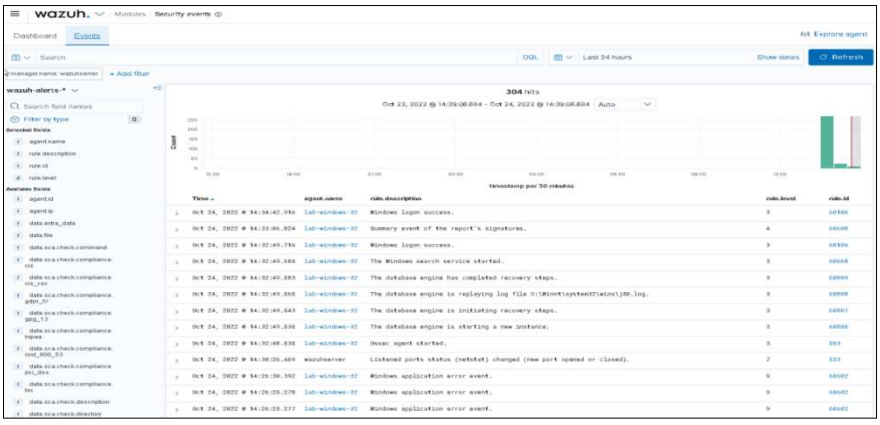


Fonte: Elaborado pelo autor.

Conforme figura acima, nas últimas 24h foram registrados 122 eventos, envolvendo sucesso de autenticação, events do Windows e Windows Security, navegando até o Menu: Modulos > Security Events, é visualizado agora todos os eventos envolvendo todas as tecnologias conectadas ao SIEM, sendo eles os servidores Wazuh, Host Windows e o Firewall *Pfsense*.

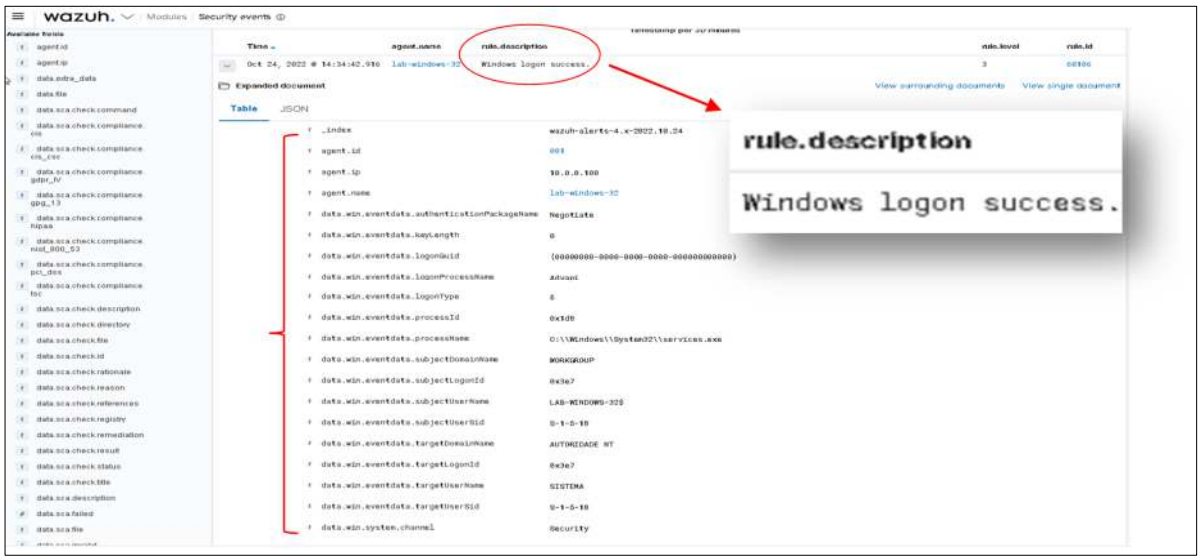
Alterando a aba de Dashboard para Events, é possível ver os eventos agora de forma mais detalhada conforme Figura 8 e clicando em um dos eventos serão apresentadoa todos os metadados envolvendo a ofensiva na Figura 9.

Figura 8 – Listagem dos eventos reportados no Wazuh.



Fonte: Elaborado pelo autor.

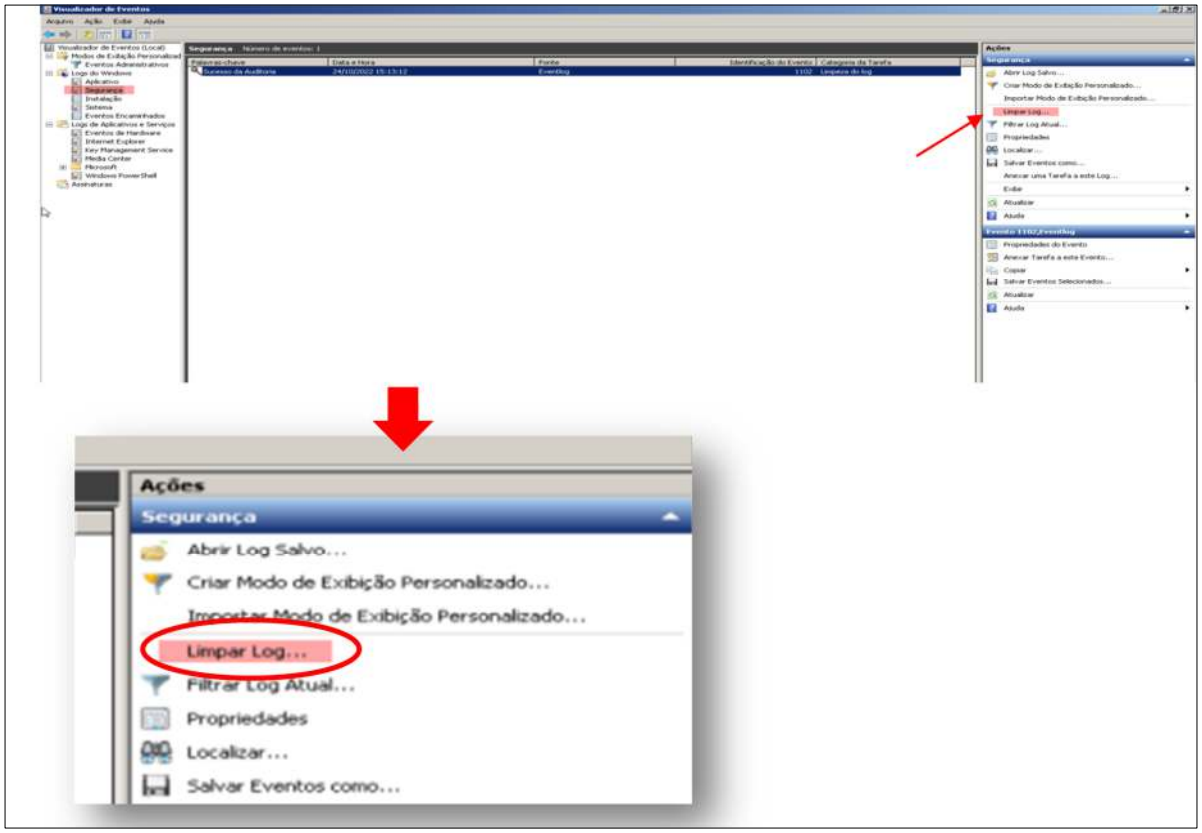
Figura 9 – Propriedades de um evento de login no Windows.



Fonte: Elaborado pelo autor.

Como modelo de simulação de um incidente, no mesmo host utilizado neste laboratório (lab-windows-32) foi realizado um procedimento de evasão que é a limpeza de Logs do Windows, procedimento comumente utilizado, visando apagar qualquer rastro da movimentação ou processo realizado. Conforme veremos na Figura 10 abaixo, foi realizada a limpeza do Security Event do Windows.

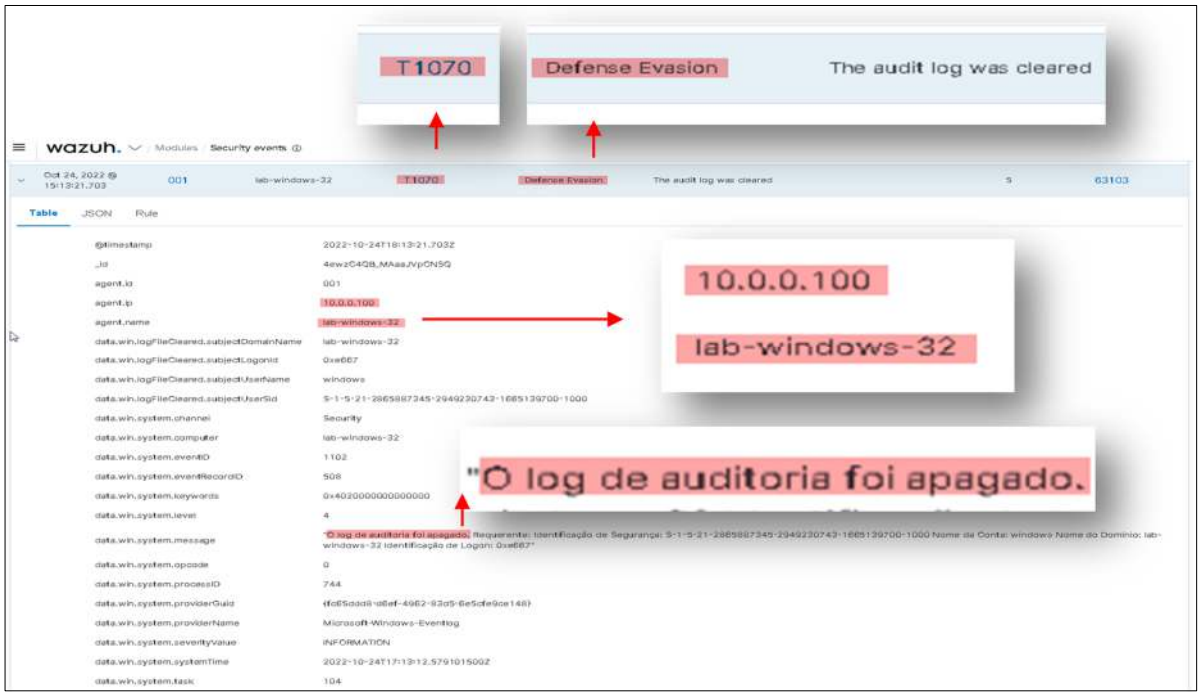
Figura 10 - Limpeza do Security Log Windows.



Fonte: Elaborado pelo autor.

Após a limpeza do Log, o evento é então encaminhado SIEM pelo agente instalado, apresentado na tela de *event* na Figura 11.

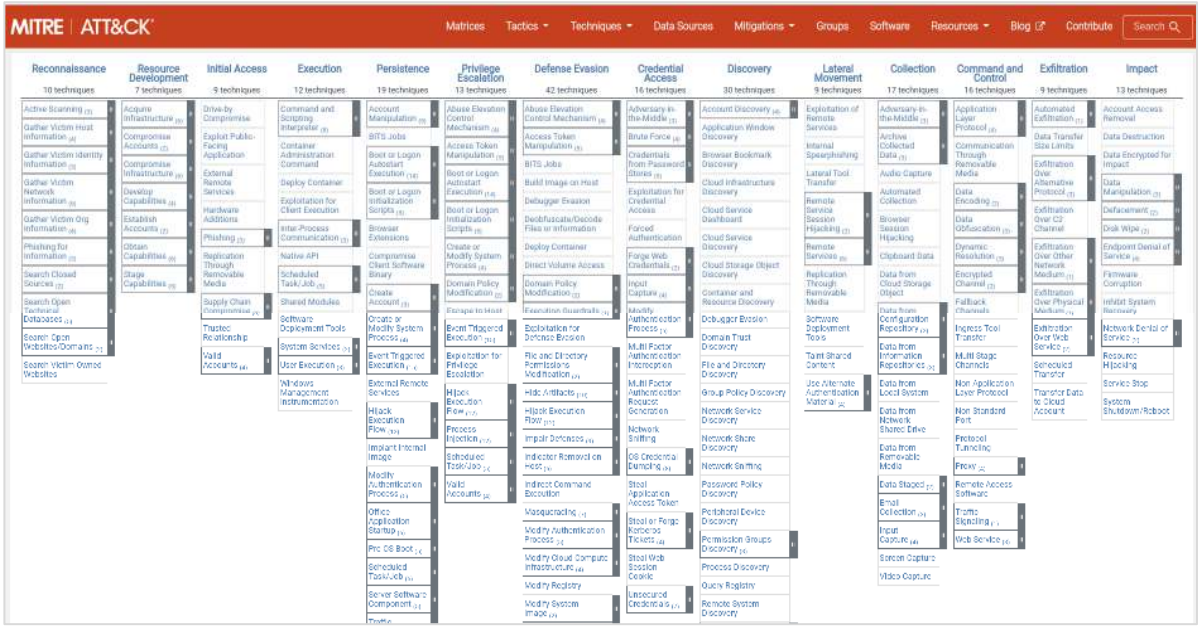
Figura 11 – Propriedades do evento de limpeza de Log.



Fonte: Elaborado pelo autor.

Além de trazer os detalhes do evento, o Wazuh registra o incidente baseado no MITRE ATT&CK, que é um framework comumente utilizado para verificação de técnicas de táticas de ataque, abaixo segue uma imagem com a listagem que pode ser consultada também em https://attack.mitre.org , como apresenta a Figura 12.

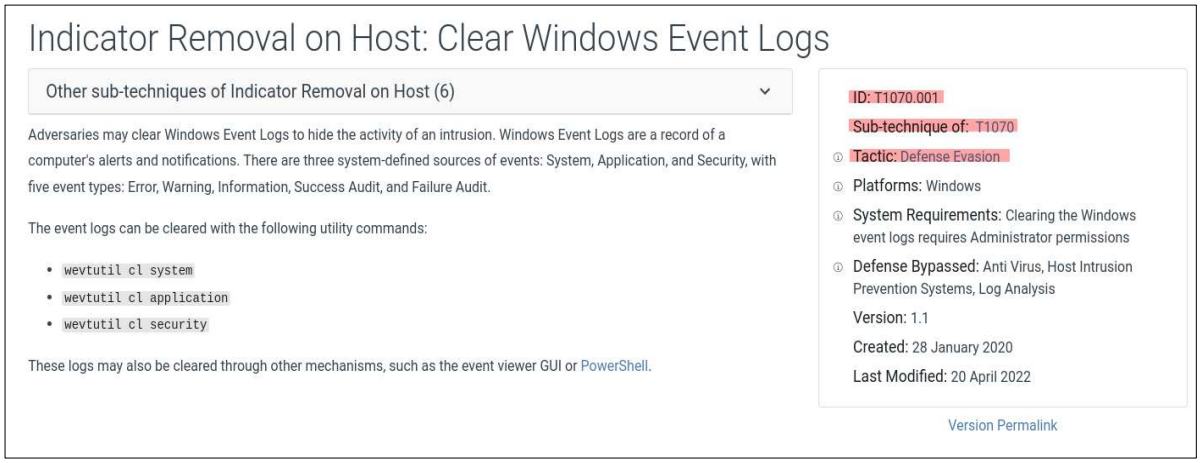
Figura 12 - Técnicas e táticas do framework MITRE Attack.



Fonte: Elaborado pelo autor.

O incidente gerado no SIEM para a limpeza de log é registrado com o código T1070 da tática de Defense Evasion, verificando junto ao MITRE é possível ver que o evento condiz com o framework, sendo a técnica T1070 - Impair Defenses, e T1070.001 se refere especificamente a “Clear Windows Event Logs”, apresentado na Figura 13.

Figura 13 - Definição da sub técnica T1070.001 do MITRE Attack.



Fonte: Elaborado pelo autor.

O exemplo mostrado acima são para eventos enviados pelo agente, porém a utilização é a mesma se tratando de outras formas de ingestão de logs como o protocolo Syslog. O Wazuh permite a construção de novos Interpretadores e Regras conforme regra de negócio para o solicitante, todos esses procedimentos podem ser acessados no canal da documentação do Wazuh: https://documentation.wazuh.com/current/quickstart.html.

CONCLUSÃO

Utilizar sistemas que atribuem inteligência para o processo de segurança da informação se torna algo indispensável para uma organização, o SIEM sendo uma das principais ferramentas para essa integração de inteligência, comumente apresenta valores altíssimos quando falamos de pequenas e médias empresas. O Wazuh se apresenta portanto como uma solução capaz de realizar a função de correlação e inteligência na análise dos logs, permitindo a integração de diversos ativos de diferentes sistemas e a integração de plugins adicionais.

Foram realizados testes envolvendo a integração de logs de agentes Windows e Linux, além do envio via protocolo Syslog do *Pfsense*, em ambos os casos o comportamento dos enventos no SIEM foram iguais, sendo possível criar novas regras ou monitorar apenas um nível de críticidade específico.

Um ponto a ser enfatizado nesta pesquisa é quanto a tratativa do Wazuh para fontes de dados a qual não é reconhecido o formato por nenhum interpretador, citando como exemplo a atualização do *Pfsense* que alterou o formato de escrita dos logs enviados, essa atualização fez com que, os até então interpretadores do *Pfsense* não fossem mais capazes de reconhecer o log e portanto, por padrão, realizar o descarte do evento. Para sanar este problema, é possível criar o próprio interpretador utilizando regex conforme modelo apresentado na Figura 14 abaixo.

Figura 14 - Modelo de decodificador para Firewall Pfsense.

```
<!--
  -  PfSense Syslog decoders
  -  Created by Alexandre Bonadiman Angeli.
  -  This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
-->

<decoder name="pfSense-Syslog">
        <prematch>filterlog\S*</prematch>
</decoder>

<!-- Jul 22 16:00:49 filterlog[28296]: 80,,,1658440156,em1,match,block,in,4,0x0,,128,2211,0,DF,6,tcp,52,
10.0.0.100,8.8.8.8,49548,80,0,S,1314666264 -->

<decoder name="pfSense-Syslog-Fields">
        <parent>pfSense-Syslog</parent>
        <regex offset="after_parent">\S*,\S*,\S*,(\S*),\S*,\S*,(\S*),(\S*),\S*,\S*,\S*,\S*,\S*,\S*,\S*,(\S*),(\S*),\S*,(\S*),(\S*),(\S*),(\S*),\S*</regex>
        <order>id,action,direction,protocol_code,protocol,srcip,dstip,srcport,destport</order>
</decoder>
```

Fonte: Elaborado pelo autor.

Após ser capaz de decodificar o log enviado, os eventos são registrados normalmente pelo SIEM, seguindo os mesmos moldes apresentados neste artigo.

O SIEM, sendo ele pago ou gratuito ainda é uma tecnologia nova e portanto, exige dedicação e conhecimento para trabalhar com essa ferramenta, não somente para nível de arquitetura e estruturação, mas para compreensão de técnicas de segurança e construção de regras conforme a necessidade de cada negócio. O Wazuh possui tecnologia suficiente, que quando bem configurado, irá permitir não somente a correlação de regras padrões, mas personalizadas e utilizando tecnologias de Threat Intelligence como MISP e canais de conhecimento como Virus Total.

REFERÊNCIAS BIBLIOGRÁFICAS

BROWN, L., & Stallings, W. (2017). Segurança de Computadores: Princípios e Práticas. (E. Brasil, Ed.). Elsevier Editora Ltda. Retrieved from https://books.google.pt/books?id=y2DcAwAAQBAJ

BASSETT, S., & Paquette, M. (2018). Melhore a análise de segurança com o Elastic Stack, Wazuh e IDS | Elastic Blog. Retrieved June 6, 2019, from https://www.elastic.co/pt/blog/improve-security-analytics-with-the-elastic-stackwazuh-and-ids

DANTAS, Marcus Leal. (2011) Segurança da informação: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido.

FERNANDES, A. J. C. (2021). Implementação de um Security Operations Center (Doctoral dissertation).

GALVÃO, Michele C. (2015). Fundamentos em Segurança da Informação. Pearson: São Paulo.

Kaspersky Lab. (2016). SOC powered by Kaspersky Lab.

MONTEIRO, A. D. A. (2020). Detecção e tratamento de incidentes de cibersegurança (Doctoral dissertation).

MUNIZ, J., McIntyre, G., & AlFardan, N. (2015). Security operations center: Building, operating, and maintaining your SOC. Cisco Press.

NATHANS, D. (2014). Designing and Building Security Operations Center. Syngress.

VAZÃO, A. P. H. (2021). Implementação de sistema SIEM open-source em conformidade com o RGPD (Doctoral dissertation).

VERGARA, Sylvia C., Métodos de Pesquisa em Administração. Editora Atlas, 4ª Edição, São Paulo - SP, 2010.