UNIVERSIDADE
LUSÓFONA

Plataforma SIEM baseada em Open Source

Trabalho Final de curso

Relatório Intercalar 2º Semestre

Cláudio Costa

Gonçalo Antunes

Orientador: Rui Ribeiro

Trabalho Final de Curso | LEI | 2022/2023

www.ulusofona.pt

Direitos de cópia

Índice

Lista de Figuras

Lista de Tabelas

Resumo

Numa era onde as empresas sofrem ciberataques constantemente, precisam de ter uma boa defesa de modo a poderem defender-se e precaver-se a estas situações.

Uma plataforma SIEM é uma solução que permite às empresas enfrentarem ciberataques e a garantirem que os seus dados estão longe de estarem comprometidos.

Um problema que as organizações têm em relação a soluções SIEM é o seu elevado preço. Este trabalho tem como objetivo o desenvolvimento de uma plataforma SIEM mais leve com o objetivo de empresas menores poderem suportar financeiramente este tipo de aplicações.

Para tal, pretendemos utilizar soluções open source de modo a este projeto poder ser desenvolvido no âmbito escolar. Exemplos destas soluções são a ferramenta Wazuh e a firewall pfSense.

Abstract

In an era where companies are constantly hacked, they need to be prepared with a lot of defenses in a way so they can defend themselves against this situations.

A SIEM platform is a solution that allows companies to fight cyberattacks e guarantee their data are far away from being compromised.

A problem companies have with SIEM solutions is its high price. This project has as objective the development of a lighter SIEM platform so smaller companies are able to afford these kind of applications.

To accomplish that, will be used open source solutions so this project can be developed in a school environment. Examples of these solutions are Wazuh and the firewall pfSense.

1 Identificação do Problema

1.1 Introdução

Atualmente vivemos numa era digital, onde bem o acesso à Internet é altamente facilitado e a informação é toda muito rápida e facilmente encontrada. É muito fácil fazermos uma pesquisa rápida num motor de busca e encontrar precisamos, ou entrar em contacto com pessoas que se encontram noutro ponto do globo.

Apesar destas vantagens, a Internet pode ser local (virtual) bastante perigoso, onde ninguém está a salvo de ser vítima de um ataque, com a consequência de ver as suas informações expostas a terceiros. Hoje em dia, as empresas são constantemente vítimas de ciberataques e necessitam de se manter protegidas (e prevenidas) destes ataques de modo a não existir uma hipótese de verem as suas informações postas em perigo.

1.2 SIEM

Uma plataforma de SIEM - Security Information and Event Management (Gestão de Informações e Eventos de Segurança) – é uma solução que facilita às empresas capacidades de deteção, análise e resposta a ameaças à sua segurança. Um SIEM recolhe dados a partir de um determinado registo de eventos e identifica, em tempo real, atividades que considera anormais.

Soluções SIEM recolhem, agregam e analisam grandes volumes de dados vindos de aplicações, dispositivos, servidores e utilizadores de uma rede de uma organização, para que as equipas de segurança possam agir perante situações de ataque.

Com alguma pesquisa, com o objetivo de analisar o mercado destas plataformas, foi possível observar o alto custo monetário que a aquisição de uma plataforma tem para as empresas. Para tal, pretende-se desenvolver uma solução SIEM "lite" que seja monetariamente acessível e de fácil utilização por parte das organizações.

Um sistema SIEM ideal tem de ser capaz de fazer uma boa análise dos dados e de demonstrar ao utilizador a sua análise. Pretende-se então desenvolver um sistema SIEM que seja user friendly, para poder ser facilmente entendido por um utilizador comum.

De modo a este projeto poder ser implementado num âmbito escolar, será implementado com base em soluções open source. Para tal, será utilizada a ferramenta Wazuh, que é composta por uma série de tecnologias open-source, como as três ferramentas ElasticSearch, Logstash e Kibana, que constituem a tecnologias ElasticStack.

A realização deste projeto terá o apoio da empresa de cibersegurança CyberS3c – uma empresa de Formação, Consultoria e Auditoria na área.

1.2.1 Funcionalidades de um SIEM

- Gestão de Requisitos: Os sistemas SIEM fazem uma agregação de uma variedade de dados num único local, organizam-nos e, então, determinam se devem ser apresentados sinais de ameaças, ataques ou falhas de segurança.
- Correlação de Dados: Depois da Gestão dos Requisitos, os dados são ordenados de modo a poderem ser identificadas padrões e relações de forma a detetar e responderrapidamente a potenciais ameaças.
- Monitorização e Resposta a Acidentes: Uma solução SIEM faz uma monitorização de incidentes de segurança na rede de uma empresa e fornece alertas e auditorias relativas a toda a atividade relacionada a um acidente.

1.2.2 Benefícios de um SIEM

- Visualização centralizada de potenciais ameaças;
- Identificação e capacidade de responder a ameaças em tempo real;
- Informações avançadas acerca de ameaças;
- Capacidade de realizar auditorias e relatórios;
- Maior transparência na monitorização de utilizadores, aplicações e dispositivos.

2 Viabilidade e Pertinência

Tal como referido na Secção 1.2, uma solução SIEM é uma tecnologia extremamente dispendiosa, com valores a rondar as dezenas de milhares de dólares. Este projeto tem o objetivo de poder ser utilizado por um utilizador cujas necessidades relativas a cibersegurança correspondam às funcionalidades que um SIEM pode fornecer.

Com a utilização desta aplicação, pequenas e médias empresas poderão:

- Detetar mais precisamente ameaças na sua rede e poderão ser alertados na eventualidade de estarem a ser vítimas de um ataque informático, pois um sistema SIEM utiliza os dados que possui para detetar e identificar ameaças. Pode também, por exemplo, correlacionar uma ameaça num log de um dispositivo com uma ameaça encontrada anteriormente noutro dispositivo diferente.
- Manter os dados seguros, pois um SIEM agrega e normaliza os dados para que possam ser analisados e reportados posteriormente. Numa rede a informação pode provir de várias fontes como dispositivos móveis, bases de dados, servidores de emails, logs da rede, entre outros, e todos estes dados têm formatos diferentes, que são então normalizados pelo sistema SIEM, para que não existam problemas na análise dos dados e na correlação dos dados. Toda esta informação é também guardada pelo SIEM para que possa então realizar uma análise e um relatório extensos.

- Ter uma maior visibilidade da rede, sendo que a agregação dos dados por parte do SIEM torna mais fácil às equipas de segurança terem uma vista completa da rede, pois atualmente, as empresas possuem uma rede muito vasta, com uma grande variedade de dispositivos, bases de dados e/ou servidores conectados. Numa rede com esta dimensão,existem espaços que, sem uma tecnologia destas, não são controlados pelas equipas de segurança. É então nestes espaços que os atacantes se escondem de modo que se possam infiltrar numa rede sem serem detetados. O SIEM alerta então as equipas de segurança na eventualidade de um atacante poder estar a esconder-se ou a tentar atacar a rede.

A partir dos resultados deste projeto, foi possível concluir o sucesso do mesmo, na medida em que foi desenvolvida uma ferramenta que permite fazer uma gestão de eventos relativos à segurança de uma infraestrutura. Para comprovar a conclusão do projeto foi realizada uma série de testes de logs no servidor da ferramenta utilizada (Wazuh) e foram obtidos resultados positivos, onde, a partir desses inputs foram outputs na ferramenta, que foram então interpretados e que nos permitiram comprovar a efetividade da solução, como é possível ver na secção 7.2.

Os objetivos definidos para a realização desta solução foram alcançados, onde, posteriormente foi definido, aconselhado pelo nosso Orientador, a realização de um ambiente de simulação empresarial à pequena escala, como pode ser visto na secção 5.4.4. Aprofundando estes objetivos, consideram-se os requisitos presentes na secção 4.1. Foi desenvolvida uma solução SIEM, utilizando a ferramenta open source Wazuh, onde foram colocadas máquinas virtuais, simulando máquinas de uma certa empresa, para a ferramenta fazer uma monitorização. Para monitorização do tráfego, foi também instalada uma Firewall, utilizando a ferramenta pfSense, que foi devidamente configurada. Com as ferramentas de monitorização a funcionar, foi então desenvolvido um ambiente virtual de simulação empresarial.

Apesar de termos disponibilizado o Wazuh na núvem, através da utilização de uma chave do GitHub Education na infraestrutura DigitalOcean, para podermos fazer implementações e testes em grupo, pois assim o serveridor não está só disponível num computador privado. Caso o objetivo fosse a implementação desta solução numa empresa, seria necessário a instalação do servidor Wazuh novamente na infraestrutura da empresa ou então a utilização de um plano do Wazuh que permite a instalação na Cloud por um preço, posteriormente adicionando as nossas configurações personalizadas.

Em todas as ferramentas utilizadas foi feita uma configuração que achámos mais apropriada para podermos fazer uma boa monitorização dos agentes.

com exceção dos requisitos marcados como “não feitos”, que foram considerados com menos importância e não foram implementados.

Este projeto tem o apoio da entidade CyberS3c (Tabela 5 - Bibliografia), uma empresa de cibersegurança que realiza Formações, Consultorias e Auditorias. O processo de implementação, bem como as tecnologias utilizadas serão revistas e aconselhadas pela CyberS3c de modo que a aplicação tenha características que pessoas com experiência na área achem que são as mais adequadas.

3 Benchmarking

Para esta secção do projeto, consultámos o site da empresa Gartner (Tabela 5 - Bibliografia) – analistas de mercado de tecnologias de informação – por sugestão do nosso orientador, para podermos ver reviews de utilizadores de aplicações SIEM que existem atualmente.

Pudemos então anotar os problemas e as vantagens da utilização de algumas aplicações.

Ao fazermos esta pesquisa anotámos várias críticas e para não tornar esta secção muito extensa apenas colocaremos aqui algumas.

Observámos com atenção as aplicações:

1. FortiSIEM
2. LogPoint
3. QRadar

Pudemos observar que a grande maioria dos comentários negativos, tinham datas de publicação mais antigos. Deduzimos então que a aplicação foi atualizada no sentido de atualizar estes problemas.

Decidimos ignorar esses problemas que foram corrigidos e apenas registámos apenas reviews mais atuais de modo a podermos focarmo-nos nas características mais recentes dos sistemas SIEM atualmente no mercado.

Nas subsecções abaixo com o nome **Review**, deixamos um resumo dos comentários de utilizadores que registámos.

3.1 FortiSIEM

O FortiSIEM é um Security Information and Event Management, ou SIEM, Sistema software da companhia de software de cibersegurança Fortinet[14]. É uma plataforma SIEM que deixa SOCs examinarem ativos à procura de dados, detetar ameaças e responder a incidentes. Está disponível para aplicações para hardware, máquinas virtuais ou na cloud pública através dos Amazon Web Services[16].

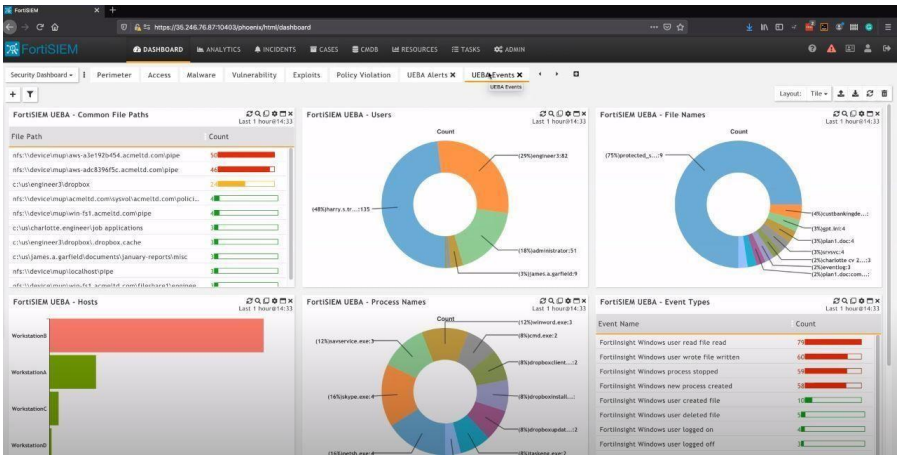

Figura 1 - Dashboard do FortiSIEM

Uma vez que os ativos estão conetados, o FortiSIEM começa a coletar logs, analisar, normalizar, indexar e a guardar tudo para análise.

A capacidade mais recente do FortiSIEM é a UEBA, ou User Entity and Behaviour Analytics. Isto permite ao FortiSIEM monitorizar processos, tanto humanos como não- humanos, tal como entidades de máquinas, especificamente o sistema coleta dados do utilizador, processos, dispositivos, recursos e comportamentos à procura de potenciais e invulgares comportamentos ameaçadores.

Quando o FortiSIEM deteta uma ameaça, envia notificações baseadas numa estrutura política de incidentes.

Tal como muitas soluções SIEM, o FortiSIEM tem uma abordagem baseada em riscos, ou seja, ameaças que o sistema consegue identificar, que representem um maior risco, são priorizadas sob ameaça que representem um risco mais baixo.

3.1.1 Review

Um sistema SIEM com muitas críticas positivas, incluindo um utilizador que denomina como "o melhor SIEM do mercado atualmente".

Os utilizadores referem o FortiSIEM como um ótimo gestor de dados, com um excelente desempenho, que fornece grande visibilidade em relação à rede, fácil de implementar e com uma user interface de fácil adaptação e navegação.

Muitos utilizadores realçam o seu poderoso real time event correlation engine[17], bem como as suas capacidades de machine learning[18] e user behaviour analytics. É uma ferramenta que pode ser integrada com outros produtos, como SOAR[19] e threat intelligence cloud[20].

O FortiSIEM vem equipado com várias opções de customização, bastante apreciadas pelos utilizadores, como, por exemplo, a possibilidade de customizar alertas e o dashboard, bem como a possibilidade de criar um CMDB[21].

Grande parte dos utilizadores criticam bastante o suporte fornecido pelo FortiSIEM, como sendo lento e de pouca confiança, bem como do seu custo elevado.

Registámos também algumas falhas relativamente à afinação de falsos alertas ser bastante complicada, algumas integrações serem complicadas de se fazer, sendo que uma pessoa sem experiência não consegue utilizar o produto. Não tem campos de threat intelligence[22], hunting playbooks[23] ou de datasheets para querries e também algumas funcionalidades inúteis.

3.2 Logpoint

O Logpoint é o criador de uma plataforma de operações de cibersegurança confiável e inovadora – empoderando organizações para entrar num mundo de ameaças constantemente em evolução.

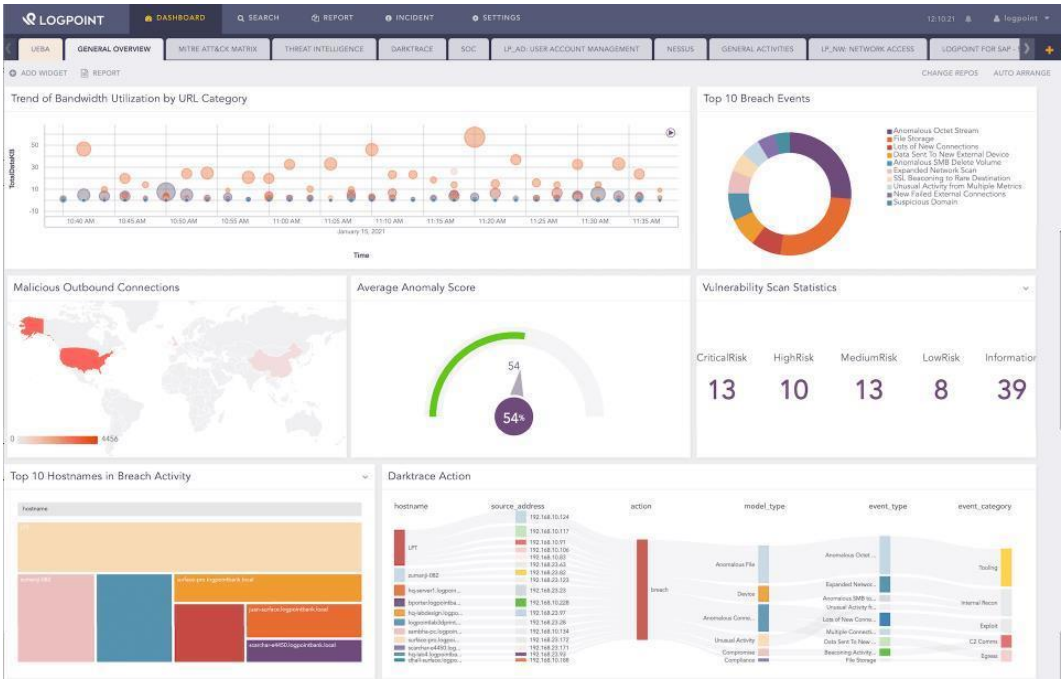

Figura 2 - Dashboard do Logpoint

Combinando tecnologia sofisticada e um conhecimento profundo em desafios dos clientes, os reforços das capacidades das equipas de segurança da Logpoint enquanto as ajudam no combate a ameaças futuras e atuais.

O Logpoint oferece SIEM, UEBA SOAR e tecnologias de segurança SAP[24] convergem numa plataforma completa que deteta eficientemente e respondem às ameaças.

3.2.1 Review

O LogPoint é uma solução SIEM denominada como "out of the box", que coneta os dados numa única plataforma, com uma utilização bastante fácil para um utilizador comum. É user friendly e escalável, e com uma configuração muito simples, apesar de termos registarmos várias críticas relativas à sua user interface.

Uma característica muito elogiada pelos utilizadores é o facto de receberem SOAR, bem como o facto de o LogPoint fazer uma classificação e uma priorização dos incidentes com base no risco. É possível adicionar novas funcionalidades e o LogPoint já inclui várias integrações de pesquisa.

Alguns clientes queixam-se da má gestão de notificações que lhes são apresentadas, pois dizem que acontece regularmente aparecerem várias notificações em simultâneo e não conseguem tratar de todas em pouco tempo. O sistema não se gere sozinho, então precisa de várias revisões constantemente.

3.3 QRadar

A IBM QRadar é um Security Information and Event Management, ou SIEM, uma Plataforma da empresa IBM.

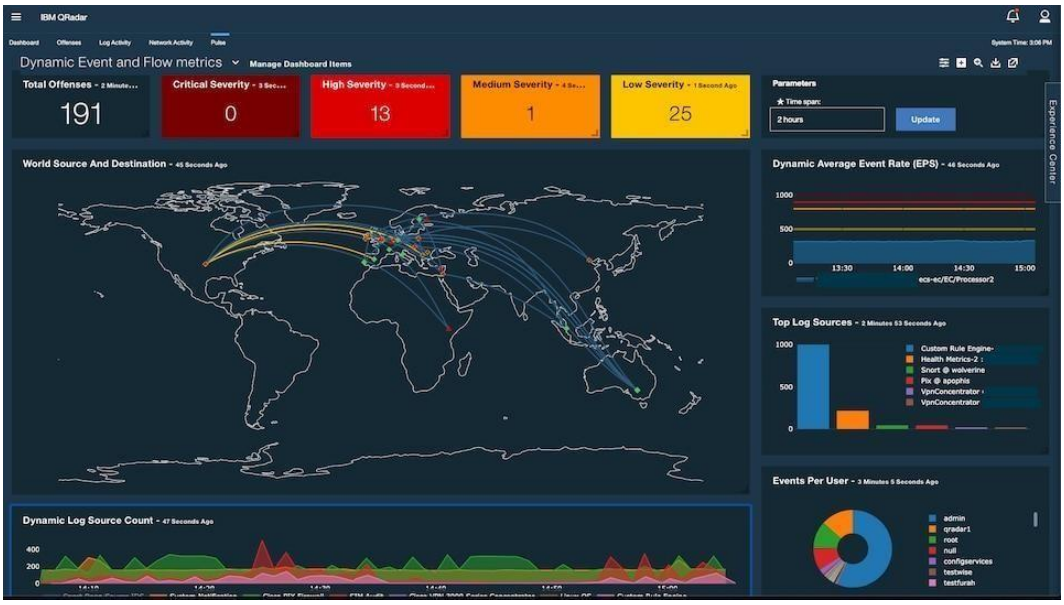

Figura 3 - Dashboard do QRadar

A IBM QRadar é uma solução SIEM poderosa para empresas médias e grandes que inclui todas as core SIEM funcionalidades que se podem encontrar nos produtos da competição, com funcionalidades adicionais de segurança e reporting.

A QRadar bloqueia um número de malwares comuns, incluindo, cavalos de Tróia[26], rootkits[27] e ransomwares[28], bem como ameaças particularmente perigosas, como Zero Day Attacks[29].

O preço para a IBM QRadar é fixo e o sistema não oferece um free trial. Apesar de ser possível requisitar uma demonstração grátis, este é um produto SaaS[30], então não é necessário instalar nos próprios servidores.

A habilidade de conectar o sistema a centenas de endpoints[31] faz uma deteção de ameaças compreensiva e o número de eventos que o sistema consegue coletar e processar por segundo é extremamente rápido.

Para as ameaças que passem pelas suas defesas, a QRadar vem com ferramentas de investigação poderosas que utilizam a Watson[32], a inteligência artificial para business program da IBM. Isto permite para visões mais rápidas e acelerar tempos de resposta para SOCs.

A facilidade da implementação depende do número de fatores, mas a maior parte dos utilizadores relatam que a IBM QRadar é relativamente de fácil implementação.

A IBM QRadar é robusta e sensível, e requere afinação para reduzir falsos positivos. Utilizadores de SIEM com experiência e conhecimento são essenciais para a utilização desta plataforma.

3.3.1 Review

Muitos utilizadores consideram o QRadar como um sistema SIEM bastante completo e com uma ótima performance, com um modelo de cibersegurança Zero Trust[33], que fornece visibilidade aos seus utilizadores, bem como flexível e escalável, sendo possível conetar com terceiros, como, por exemplo, SOAR. A quantidade de falsos positivos é bastante baixa, facilitando as equipas de segurança a não perderem muito tempo com estas situações.

Relativamente à equipa de suporte, houve elogios por parte de quase todos os utilizadores, adjetivando-os de bastante responsivos e úteis.

Apesar de muitos utilizadores elogiarem a GUI, dizendo que é bastante user friendly, observámos também algumas queixas, como considerarem pouco intuitiva e dizendo que a interface é um pouco antiga.

A criação de reports é bastante fácil e a visualização de eventos em tempo real é bastante útil. Foram referidas várias vezes duas ferramentas de inteligência artificial que podem ser utilizadas, por aquisição, nomeadas Watson e X-Force[34], que referem serem bastante úteis para threat hunting e post incident analysis[35].

Registámos queixas relativas ao preço do produto, por ser bastante dispendioso, e de exigir bastante formação para um utilizador poder utilizar o QRadar, sendo que um utilizador novato não consegue utilizá-lo. Alguns utilizadores queixam-se de a documentação ser escassa. Observámos um utilizador criticar que o não existe um acompanhamento por parte do QRadar para os tipos de logs atuais, e que não é possível distinguir fontes de logs, o que leva a um unparsed logging[36].

3.4 Conclusões

Tabela 1 - Comparação dos três produto

	FortiSIEM	LogPoint	QRadar
VANTAGENS	Poderoso real time event engine	O cliente recebe SOAR	Suporte responsivo e útil
	User Interface user friendly	Escalável	GUI user friendly
	O CMDB é uma boa ideia e bastante útil	User Friendly	Flexível e escalável
	Utiliza Machine Learning e User Behaviour Analytics	Ocorrências baseadas no seu risco	Fácil pesquisa
	Capacidade de fazer várias customizações	Gestão e configuração simples	Boas opções de filtragem
	Possível ver dados de outros dispositivos fora da Fortinet	Possível adicionar funcionalidades	Boa visualização de eventos
	---	Grandes capacidades de pesquisa	Deteção de ameaças completa e rápida
	---	Possível fazer scan a várias fontes de logs para uma string específica	Inteligência Artificial Watson muito útil para deteção de ameaças
	---	---	Baixa qualidade de falsos positivos
	---	---	Fácil manipulação de regras e eventos
DESVANTAGENS	User interface falha por vezes	Custo alto	Produto caro
	Integrações complicadas	User interface complicada	Utilização impossível sem treino
	Tem funcionalidades inúteis	Muitos alertas em simultâneo	Ocorrência de falsos positivos
	Custo alto	Deployment e configuração complexos	User interface pouco intuitiva, que podia ser renovada
	Suporte fraco	Sintaxe de pesquisa complicada	Não houve um acompanhamento das fontes de logs atuais pela IBM
	Documentação fraca	Tem funcionalidades escondidas	---
	Afinação de falsos alertas complicada	Necessário fazer revisões regularmente	---
	Requere muita formação para poder utilizar o produto	Necessário muito conhecimento técnico	---

Embora a ferramenta Wazuh seja também um SIEM, bem como estas três soluções existentes no mercado presentes acima, são todas bastante diferentes, com funcionalidades diferentes.

Começando pela *user interface*, o Wazuh é essencialmente acedido através de um dashboard fornecido pelo Kibana (5.3.3), enquanto que o QRadar fornece uma interface *user friendly* com dashboards costumizáveis, a Longpoint e o FortiSIEM oferecem uma interface intuitiva para visualização e navegação dos eventos.

Relativamente à escalabilidade, todas as ferramentas aguentam um número relativamente elevado de eventos e são adequadas para uma pequena a uma grande escala. Todas têm uma arquitetura que permite um aumento da escala conforme necessário.

As capacidades de integração são bastante diferentes entre todas. O Wazuh faz a integração com o ElasticStack, um sistema de *ticketing* e através de *feeds* de reconhecimento de ameaças. O QRadar funciona através de integrações provenientes de terceiros e é possível integrar várias outras ferramentas de segurança. O LogPoint apresenta uma integração com *scanners* de vulnerabilidades, *firewalls*, entre outras ferramentas. O FortiSIEM integra ferramentas pertencentes à Fortinet.

O Suporte e a comunidade variam também entre todas. O Wazuh tem uma comunidade open-source. Um exemplo desta comunidade é o Google Groups “Wazuh Mailing List” (Tabela 5 - Bibliografia), onde pudemos colocar algumas dúvidas que tivemos e obtivemos sempre respostas bastante úteis. O QRadar recebe suporte técnico da IBM, o LogPoint fornece suporte técnico e serviços profissionais e o FortiSIEM auxilia os seus clientes com o suporte da Fortinet.

4 Engenharia

4.1 Levantamento e Análise de Requisitos

Para iniciar a realização de um projeto de software, é necessário realizar um levantamento dos requisitos, antes de começar qualquer implementação. Esta fase "traça um caminho" relativo às funcionalidades que o projeto deve ter. Nesta secção é feito o levantamento de requisitos para a implementação do SIEM. Considerando a existência de vários sistemas SIEM no mercado, para o preenchimento deste campo, realizámos pesquisas sobre requisitos de uma solução SIEM, e adicionámos alguns requisitos que já pertencem ao Wazuh.

Importância	Secção	Esforço (Pontos 1-64)	Descrição dos Requisitos	Feito
Mandatory	Análise de Segurança	4	Coletar, agregar, indexar e analisar dados de segurança	Sim
		8	O Agente fornece os recursos necessários de monitorização e resposta	Sim
		8	A componente servidor fornece informações de segurança	Sim
		16	A componente servidor analisa os dados	Sim
	Deteção de Intrusões	32	O Agente procura malwares, rootkits e anomalias suspeitas nos sistemas monitorizados	Sim
		32	O Agente deteta arquivos ocultos, processos ocultos e ouvintes na rede não registados	Sim
		32	A componente servidor deteta intrusos	Sim
		16	A componente servidor analisa os dados de registos coletados e procura indicadores de estar comprometido	Sim
	Análise dos Dados dos Registos	2	Os Agentes leem os registos do sistema operativo e encaminham a um gestor central	Sim
		2	Os Agentes encaminham os registos do sistema para um gestor central	Sim
		4	O gestor central analisa e armazena os registos do sistema operativo	Sim
	Monitorização da Integridade de Ficheiros	8	Monitorização do sistema de arquivos, identificando alterações no conteúdo, permissões e propriedades	Sim
		2	Identificação dos utilizadores e aplicativos utilizados para criar ou modificar arquivos	Sim
	Deteção de Vulnerabilidades	2	Os Agentes enviam os dados do inventário do software para o servidor	Sim
		4	O servidor correlaciona os dados enviados pelo agente com o banco de dados CVE	Sim
	Avaliação da Configuração	2	Monitorização das definições de configuração do sistema para verificar se estão em conformidade com as políticas de segurança	Sim
		2	Personalizar as verificações de configuração	Sim

Tabela 2 - Levantamento e Análise de Requisitos

Mandatory		8	Os agentes realizam varrimentos para detetar aplicações que são geralmente vulneráveis, sempatches ou configuradas de forma insegura	Não
	Resposta a Incidentes	32	Responder ativamente a ameaças ativas, como bloquear o acesso a um sistema	Sim
		16	Executar comandos remotamente, identificando indicadores de comprometimento (IOCs)	Sim
	Conformidade Regulamentar	2	Fornecer controlos de segurança de modo a estar emconformidade com os padrões e regulamentos do setor	Sim
		4	A interface do utilizador fornece relatórios e painéis que ajudam com certos regulamentos, como GDPR, NIST 800-53, TSC SOC2 e HIPAA	Sim
	Segurança na Cloud	8	Monitorizar uma infraestrutura na cloud a nível da API	Sim
		16	Fornecer de regras para avaliar a configuração do ambiente na cloud, identificando pontos fracos	Sim
	Segurança de Contentores	8	Fornecer visibilidade da segurança nos hosts e contentores do Docker, monitorizando o seu comportamento e detetando ameaças, vulnerabilidades e anomalias	Sim
		4	Coletar e analisar informações detalhadas do tempo de execução	Sim
	Arquitetura Hierárquica Modular/ Escalável	4	O software tem uma estrutura hierárquica, onde as diferentes componentes e funcionalidades são organizadas de forma lógica e ordenada	Sim
		8	Capacidade de escalar facilmente	Sim
		4	O software tem um design modular, onde diferentes funcionalidades podem ser adicionadas ou removidas	Sim
Nice To Have	Scanerização de Vulnerabilidades	8	Identificar, avaliar e relatar vulnerabilidades em sistemas computacionais, redes e aplicativos	Sim
		32	Identificar possíveis vulnerabilidades que podem serexploradas por um invasor	Sim
		16	Verificar vulnerabilidades para identificar e priorizar riscos	Sim
	Deteção de Intrusões naRede	16	Utilização da medida de Deteção de Intrusões naRede (NID – Netword Intrusion Detection) para detetar e alertar atividade não autorizada num computador ou numa rede	Sim
		8	Monitorizar tráfego numa rede	Sim
		8	Identificar padrões em atividade maliciosa ou ataquesque indiquem indicativos de falhas na segurança	Sim
		32	Detetar e responder ameaças à segurança em tempo real	Sim

4.2 Diagrama de Casos de Uso

O Wazuh, a plataforma utilizada para o desenvolvimento deste projeto, é uma ferramenta que já existe, tem a sua própria arquitetura e já tem definidas as suas componentes centrais.

Para a realização deste ponto, foi utilizado como modelo, um diagrama disponibilizado pelo site oficial do Wazuh, que se encontra no seguinte link:

https://wazuh.com/platform/

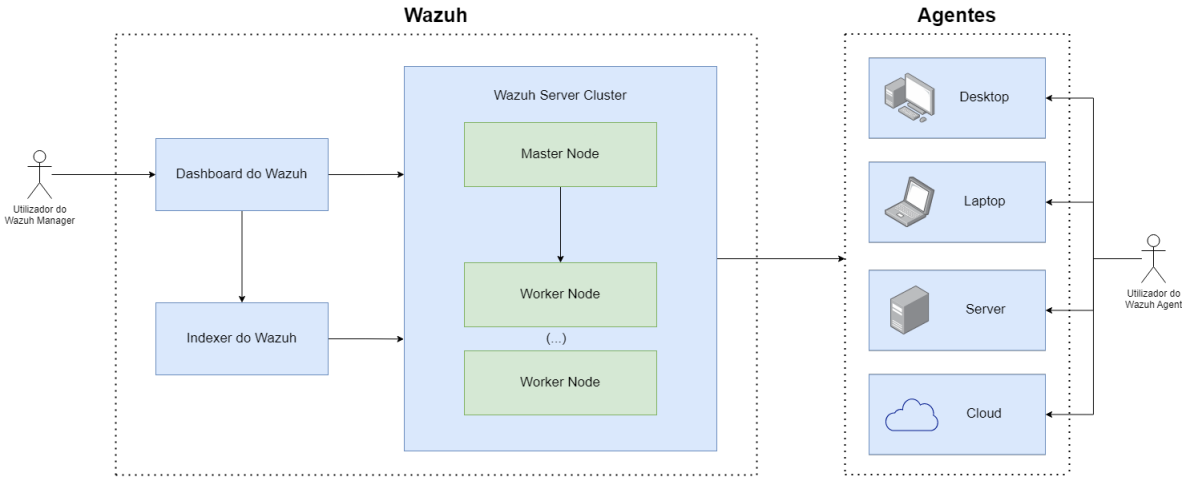

Figura 4 - Arquitetura do Wazuh

Neste diagrama, um utilizador acede ao Wazuh e utiliza as suas funcionalidades a partir de um dashboard (painel de controlo) intuitivo, a partir de uma interface web. Este dashboard pode ser utilizado para visualização e análise dos dados.

O dashboard pode visualizar os alertas gerados, através do indexador do Wazuh, que tem como função armazenar e indexar os alertas que o servidor do Wazuh gera.

O servidor do Wazuh é responsável por gerir os agentes e fazer configurações quando necessário. É também responsável por analisar os dados provenientes dos agentes e processar esta informação à procura de indicadores de compromisso (IOCs).

5 Solução Desenvolvida

5.1 Introdução

De modo a obter alguma orientação relativamente ao ambiente onde é implementada a nossa solução SIEM, baseada em componentes open source, foi marcada uma reunião com dois membros da empresa de cibersegurança CyberS3c (Tabela 5 - Bibliografia). Na reunião foi recomendada a utilização da ferramenta Wazuh – uma plataforma open source que contempla características de um sistema SIEM, e que é extremamente útil na implementação de um sistema SIEM open source.

Toda a implementação deste projeto ser realizada utilizando a plataforma Wazuh, hospedando-a na cloud, com o objetivo de agregar mais soluções e regras às já implementadas por defeito no Wazuh, para tornar a nossa implementação de SIEM mais personalizada e segura, como por exemplo o ElastickStack, que combina três tecnologias open source – ElasticSeach, Logstash e Kibana, referidos detalhadamente na secção 5.3.

Para podermos melhorar a monitorização do tráfego decidimos também implementar uma firewall. Após alguma pesquisa sobre estas ferramentas que fossem gratuitas, decidimos utilizar a firewall pfSense, detalhada na secção 5.3.12.

De modo a demonstrar o ambiente onde este trabalho foi desenvolvido, no nosso caso, a plataforma Wazuh, foi gravado e disponibilizado um link (abaixo) de demonstração do ambiente de trabalho, bem como algumas funcionalidades que achámos pertinentes demonstrar.

https://www.youtube.com/watch?v=OOoSG9l7S3Y&ab_channel=Ku7u2ioK0st4

5.2 Arquitetura

Uma solução SIEM é constituída por várias componentes que auxiliam as equipas de segurança na deteção de data breaches e atividades maliciosas, monitorizando e analisando constantemente os dispositivos e eventos de uma rede.

Para conseguirmos desenvolver um sistema SIEM, necessitamos de entender primeiro a sua arquitetura e os componentes que o constituem.

As nove componentes da arquitetura de um sistema SIEM são:

5.2.1 Agregação de Dados

É a componente responsável por coletar log data[1] gerados por várias fontes dentro de uma rede corporativa, tal como servidores, bases de dados, aplicações. Firewalls, routers, sistemas cloud, etc. Estes logs contêm um registo de todos os eventos que acontecem num determinado dispositivo ou aplicação e são coletados e armazenados num local centrado ou num data store.

Existem três técnica de coletar logs:

- **Agent-based Log Collection:** Um agente é instalado em todos os dispositivos da rede que geram logs. Este agente é responsável por coletar os logs dos dispositivos e enviá-los para o servidor SIEM central. Este método é geralmente utilizado em zonas fechadas e seguras, onde a comunicação é restrita.
- **A Agentless Log Collection:** Esta técnica não envolve agentes em nenhum dispositivo da rede. Em vez disso, mudanças da configuração têm de ser feitas no dispositivo para que possa enviar qualquer log gerado para o servidor SIEM central de uma forma segura.
- **API-based Log Collection:** Os logs podem ser coletados diretamente dos dispositivos da rede com a ajuda de APIs (Application Programming Interfaces).

5.2.2 Análise da Segurança dos Dados (Relatórios e Dashboards)

As soluções SIEM incluem uma componente de análise de segurança, que inclui maioritariamente live dashboards, que apresentam intuitivamente dados de segurança sob a forma de gráficos. Estes dashboards são atualizados em tempo real e automaticamente, ajudando assim a equipa de segurança a identificar atividades maliciosas e resolver estes problemas de segurança rapidamente. As soluções SIEM geralmente fornecem uma opção aos utilizadores de criarem os seus próprios dashboards.

Outra funcionalidade deste componente são relatórios predefinidos. Geralmente, as soluções SIEM incluem centenas de reports predefinidos que auxiliam a fornecer visibilidade a eventos de segurança, detetar ameaças, etc. Estes relatórios, que são, na maior parte, construídos sob indicadores de compromisso (IoCs – Indicators of Compromise2[2]), podem também ser customizados para atenderem a necessidades da segurança interna.

As soluções SIEM fornecem ao utilizador opções de filtragem, pesquisa, e detalhe destes reports, gerar horários para gerir reports, dependendo das necessidades do utilizador, visualizar dados sob a forma de tabelas e gráficos e exportar os reports em diferentes formatos.

5.2.3 Correlação e Monitorização de Eventos

Um motor de correlação é uma das componentes mais importantes de uma solução SIEM. Utilizando regras predefinidas, ou definidas pelo utilizador, os log data coletadossão analisados para quaisquer relações existentes entre diferentes atividades da rede, atributos comuns, ou padrões que possam ser apresentados. Motores de correlação possuem a habilidade de juntar diferentes incidentes de segurança de modo a fornecer uma visão global de ataques de segurança. São capazes de detetar sinais de atividade suspeita ou potenciais falhas de segurança na rede, e o sistema SIEM vai gerar alertas para essas atividades

Grande parte dos Sistemas SIEM vêm com regras predefinidas construídas baseando-se em IoCs, mas os atacantes utilizam constantemente técnicas cada vez mais avançadas para hackear um sistema. Então as regras têm de ser modificadas e melhoradas regularmente, ou então tornar-se-ão obsoletas. A construção de regras de correlação requere um conhecimento profundo do comportamento e das táticas dos atacantes.

5.2.4 Análise Forense

Esta componente é utilizada para executar uma análise da causa principal, gerar um report de incidentes e fornecer uma análise detalhada, da tentativa de um atacante ou de um ataque a decorrer, que ajuda a empresa a tomar as medidas adequadas de imediato.

Uma empresa pode executar análises forenses de modo a reconstruir cenas de crime e verificar a principal causa de uma falha. Sendo que os log data comprometem um registo de todos os eventos que aconteceram num determinado dispositivo ou aplicação, podem ser analisados para perseguir os rastos deixados pelos atacantes maliciosos.

Soluções SIEM ajudam as equipas de segurança a pesquisar os logs, gerar reports forenses e descobrir o tempo que uma falha de segurança particular ocorreu, os sistemas e os dados que foram comprometidos, os hackers por detrás da atividade, tal como o ponto de entrada.

5.2.5 Deteção e Resposta a Incidentes

Esta componente tem a função de detetar incidentes de segurança, ou seja, uma tentativa invasão ou uma invasão bem-sucedida na rede por alguém não autorizado, ou uma infração das políticas de segurança de uma empresa.

Ataques DoS, mau uso de dados ou recursos, aproveitamento de privilégios, ataques de phishing são exemplos de incidentes de segurança. Estes incidentes têm de ser detetados e analisados, e têm de ser tomadas as ações apropriadas para cada um de modo a resolver o problema de segurança, assegurando em simultâneo a continuidade das operações da empresa.

Durante a deteção de incidentes, as empresas esforçam-se para um manter o mean time to detect[3] (MTTD) o mais baixo possível de modo a tentar reduzir os danos causados pelos atacantes.

Incident Response: Este módulo é responsável por ter uma ação imediata para resolver um incidente de segurança mal seja detetado. Reduzir o mean time to resolve[4] (MTTR) é uma prioridade para todas as empresas.

5.2.6 Resposta em Tempo Real ou Consola de Alerta

As soluções SIEM realizam atividades de coleta de logs e correlação em tempo real. Se alguma atividade suspeita for detetada, um alerta é lançado instantaneamente e a equipa de resposta a incidentes irá atuar de imediato de modo a mitigar o ataque ou impedi-lo de acontecer.

As notificações de alerta podem ser enviadas via email ou SMS em tempo real, e podem também ser categorizadas com base na prioridade que lhe foi atribuída: Alta, Média ou Baixa.

5.2.7 Threat Intelligence

As soluções SIEM realizam atividades de coleta de logs e correlação em tempo real. Se alguma atividade suspeita for detetada, um alerta é lançado instantaneamente e a equipa de resposta a incidentes irá atuar de imediato de modo a mitigar o ataque ou impedi-lo de acontecer.

As notificações de alerta podem ser enviadas via email ou SMS em tempo real, e podem também ser categorizadas com base na prioridade que lhe foi atribuída: Alta, Média ou Baixa.

5.2.8 User and Event Behaviour Analytics (UEBA)

Esta componente ajuda na deteção de incidentes de segurança. Com os atacantes a desenvolverem constantemente novas técnicas para hackearem redes, sistemas de segurança convencionais tornam-se rapidamente obsoletos. Porém, as organizações podem defender-se de quaisquer tipos de ciberataques com a ajuda de técnicas de machine learning.

Componentes UEBA adotam técnicas de machine learning de modo a poderem desenvolver um modelo comportamental baseado no comportamento normal de utilizadores e das máquinas de uma empresa. Este modelo comportamental é desenvolvido para cada utilizador e entidade, processando grandes quantidades de dados obtidos de vários dispositivos da rede.

Qualquer evento que se desvie deste modelo comportamental será considerado uma anomalia, e será revisto como uma potencial ameaça.

Uma taxa de risco é atribuída para o utilizador ou entidade. Quanto maior for a taxa de risco, maior a sua suspeita. Com base na taxa de risco, uma análise é feita e certas medidas são tomadas.

A diferença entre um Correlation Engine e um UEBA, é que enquanto um Correlation Engine é um sistema com regras utilizado para detetar incidentes e ameaças, um UEBA, como indica o nome, identifica eventos baseados numa análise de comportamentos.

5.2.9 IT Compliance Management

De modo a uma organização atender a todos os requisitos definidos para a proteção de dados sensíveis, as soluções SIEM incluem uma componente de compliance management.

Medidas proativas tal como adotar várias técnicas de identificação de anomalias, padrões, e ciber ameaças são essenciais para proteger dados sensíveis de serem comprometidos.

As soluções SIEM têm a capacidade de armazenar e arquivar log data por um período para que possam ser realizadas auditorias. Podem também gerar compliance reports como HIPAA, SOX, PCI DSS, GDPR, ISSO 27001 pela coleta e análise de logs, bem como reports fora da caixa atendendo a requisitos específicos do mandato.

5.3 Tecnologias e Ferramentas Utilizadas

Como referido na Secção 1.2, a implementação deste projeto será realizada com a utilização da plataforma Wazuh (5.3.4), uma ferramenta open source com grande escalabilidade, constituída por várias tecnologias, inclusive o Elastic Stack, composto por três tecnologias:

1. **Logstash (5.3.1):** Solução de agregação de logs;
2. **ElasticSearch (5.3.2):** Solução de armazenamento;
3. **Kibana (5.3.3):** Solução de visualização.

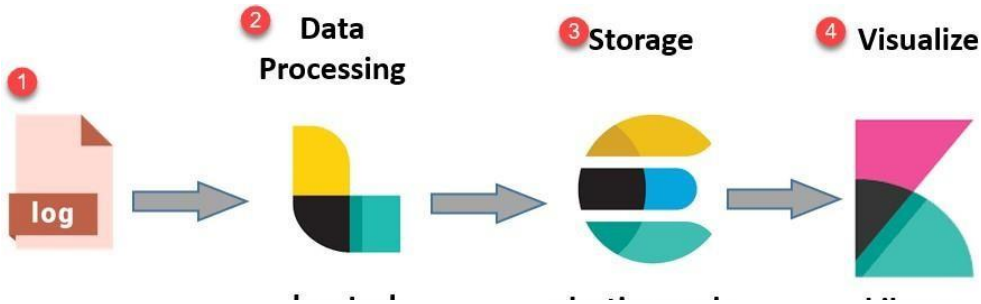

Figura 5 - Três ferramentas open-source que fazem parte do Wazuh

© guru99.com

Para esta secção utilizámos vários sites e vídeos, que estão disponibilizados na Secção **Erro! A origem da referência não foi encontrada.**.

De seguida serão enumeradas e brevemente descritas as três tecnologias que serão utilizadas.

5.3.1 Logstash

O Logstash é uma solução que fica entre os dados e o local onde se pretende que os dados fiquem localizados.

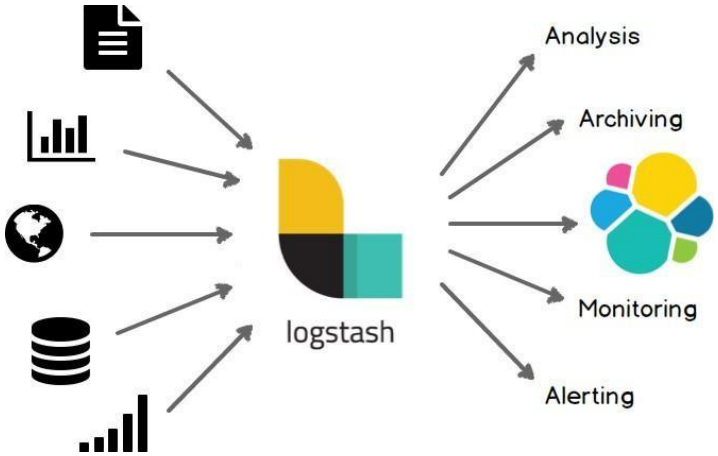

Figura 6 - Logstash

Os dados podem ser importados de praticamente qualquer lado, não sendo necessário serem unicamente ficheiros locais, podem ser de outro sistema e os podem ser colocados em outros locais simultaneamente no ElasticSearch. Pode também importar dados de mais que uma fonte ao mesmo tempo e gerar um output para mais que um destino ao mesmo tempo.

O Logstash tem funcionalidades como derivar estruturas de dados que não estão previamente estruturados e pode anonimizar dados pessoais quando os vê ou até mesmo excluí-los de todo. Pode também fazer visualizações de geolocalização, como por exemplo, ver logs de acesso a um servidor web e relacionar automaticamente a origem desse log, com base no endereço IP.

5.3.2 ElasticSearch

O ElasticSearch é uma ferramenta utilizada para Big Data[5] e é denominada como uma base de dados NoSQL[6].

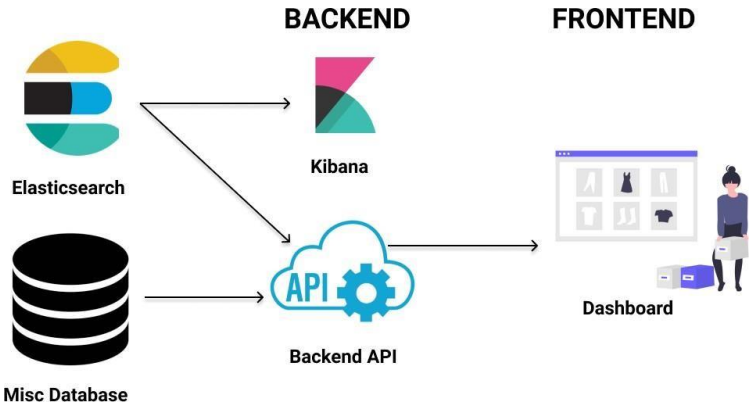

Figura 7 - Utilização do ElasticSearch

Tem sido utilizado para fazer pesquisas num website ou num determinado documento, coletar e analisar log data e para análise e visualização de dados. Uma grande vantagem da utilização do ElasticSearch é a possibilidade de armazenar dados em qualquer formato, utilizando ficheiros JSON, e atribui um index para cada registo. É uma tecnologia facilmente escalável, para vários servidores.

O ElasticSearch possui um motor de pesquisa e de análise escaláveis, open-source e distribuídos. Fornece uma análise e umes pesquisa em tempo real. É uma base de dados orientada a objetos.

5.3.2.1 Onde utilizar o ElasticSearch?

- Application, Website and Enteprise Search
- Análise de Logging e de Logs
- Monitorização de containers
- Métricas de Infraestruturas
- Análise de Negócios
- Análise de Segurança

As Bases de Dados Relacionais demoram bastante em comparação a bases de dados muito grandes. Isto leva a poor user experience.

5.3.3 Kibana

O Kibana é uma ferramenta de interface visual que permite a exploração, visualização e construção de um dashboard com base em dados vindos do ElasticSearch, que fornece dados semiestruturados.

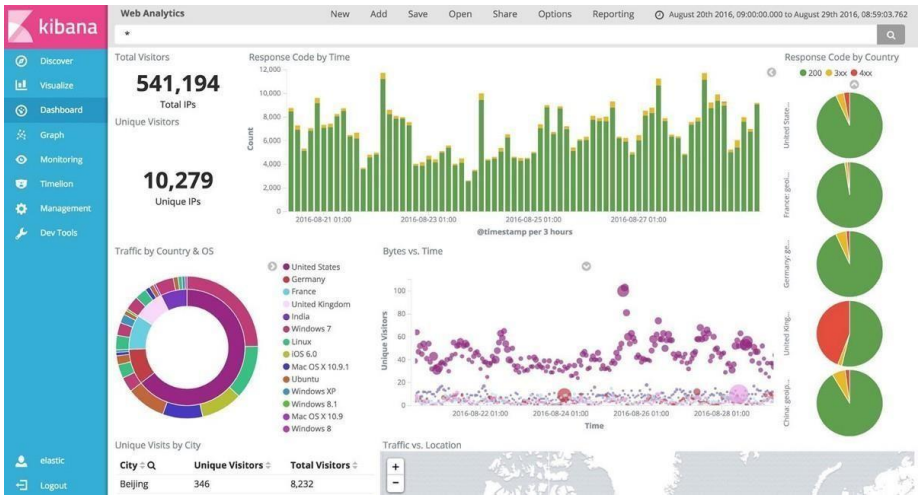

Figura 8 - Kibana

A funcionalidade principal do Kibana é análise e data querying, e permite também que um utilizador possa visualizar os dados de várias formas:

- Heat Maps;
- Gráficos Lineares;
- Histogramas;
- Pie Charts;
- Entre outros.

Através dos dashboards que se atualizam em tempo real, é bastante fácil fazer uma compreensão dos dados.

5.3.3.1 Para que utilizamos o Kibana?

- **Deteção de Anomalias:** o Kibana é equipado com funcionalidades de machine-learning que permitem detetar anomalias nos dados.
- **Agregações e Filtragem:** Com o Kibana, um utilizador é capaz de correr análises como, por exemplo, Histogramas.
- **Gráficos Interativos:** O Kibana contém gráficos interativos e relatórios que percorrem a grande quantidade de dados.
- **Kibana Search:** O Kibana vem incluído com métodos de pesquisa nos dados pré- concebidos.
- **Partilha e Colaboração Seguras:** Segurança na partilha de visualizações e de dashboards, mas também existe uma opção de limitar a visualização. Os dados podem ser partilhados com várias pessoas, como, por exemplo, uma equipa de segurança.
- **Suporte em Mapeamento:** O Kibana possui capacidades geoespaciais que permitem ao utilizador visualizar informação geográfica dos dados e observá-la num mapa.

5.3.4 Wazuh

Wazuh é uma solução de monitorização de segurança open source composta por várias ferramentas que realizam análise de registos, deteção de ameaças e resposta a incidentes de segurança.

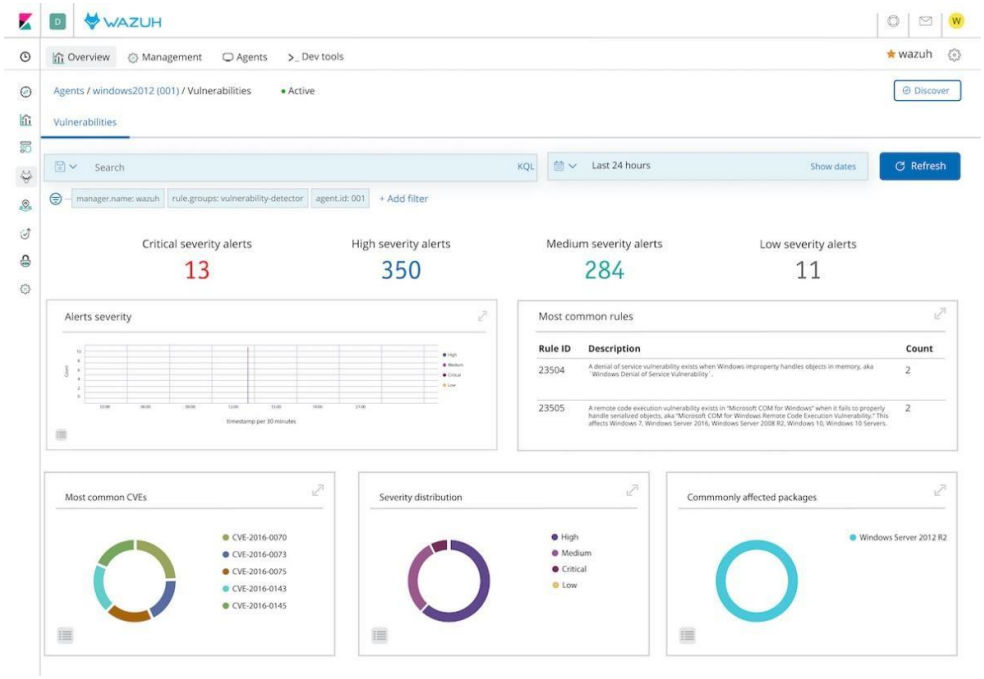

Figura 9 - Menu do Wazuh

Tem como base a tecnologia, mencionada anteriormente, Elastic Stack (conhecida como ELK stack e composta pelo ElasticSearch, Logstash e Kibana) e fornece uma plataforma para monitorização e análise de dados de várias fontes provenientes de uma determinada rede.

O Wazuh contém uma variedade de funcionalidades, como por exemplo, alerta em tempo-real, resposta ativa e reporting. Na realização deste projeto pretende-se implementar também outras tecnologias que o Wazuh permita adicionar. Por defeito, é constituído pelas seguintes tecnologias e componentes:

- **OSSEC (5.3.5):** O Wazuh é baseado no sistema de deteção de intrusões host based (HIDS – Hostbased Intrusion Detection System) OSSEC. Utiliza o seu motor para analisar registos e detetar ameaças.
- **Elastic Stack:** O Wazuh utiliza o Elastic Stack para armazenamento e análise dos dados obtidos. Estes dados são então enviados para o ElasticSearch (5.3.2) e então armazenados. O Kibana (5.3.3) é utilizado para visualização e alertas.
- **Logstash (5.3.1):** O Logstash é utilizado para coleta, análise e transformação dos registos e dos eventos antes de serem armazenados pelo ElasticSearch (5.3.2).
- **OpenSCAP (5.3.6):** O módulo OpenSCAP também é incluído no Wazuh. Este módulo permite a realização de auditorias de conformidade, utilizando padrões SCAP (Security Content Automation Protocol – Protocolo de Automação de Conteúdos de Segurança).

- **Suricata (5.3.7) e Snort (5.3.8):** Estas duas ferramentas podem ser configuradas para prevenção e deteção de intrusos.
- **Docker (5.3.9):** O Wazuh pode monitorizar e assegurar Dock containers[7].
- **Syslog-ng, Rsyslog e Fluentd (5.3.10):** A integração destes coletores de registos faz uma centralização dos registos e dos eventos.
- **Active Directory (5.3.11):** O Wazuh pode ser configurado para utilizar Active Directory[8] para autenticação e autorização de utilizadores.

O Wazuh inclui também uma *RESTful API*[9] que permite uma fácil integração com outras plataformas e ferramentas de segurança. Esta mesma API foi utilizada para testes da ferramenta e como protótipo do projeto.

O Wazuh foi desenhado de modo a ser altamente escalável e pode perfeitamente ser implementado numa arquitetura distribuída de modo a gerir grandes quantidades de dados. Fornece também uma consola central de gestão e monitorização de múltiplos agentes, e alertas e relatórios pré-definidos e configurados de modo a ser possível identificar e responder facilmente a ameaças.

5.3.4.1 Utilizadores

É possível criar vários utilizadores no Wazuh através de uma autenticação centralizada[37]. Pode ser configurado para integrar sistemas de autenticação já existentes como Active Directory, como referente na secção 5.3.11.

Também é possível criar utilizadores e senhas diretamente no sistema, caso não seja desejado utilizar autenticações externas. Estas informações são guardadas diretamente na Base de Dados do Wazuh.

Existem três tipos de utilizadores que podem ser criados, com diferentes permissões:

1. **Administrador:** Tem um total acesso ao sistema, podendo visualizar todas as funcionalidades do Wazuh e executar todo o tipo de ações.
2. **Gerente:** Pode gerenciar agentes, políticas de segurança, regras, configurações, mas não possui um total acesso ao sistema
3. **Utilizador:** Apenas consegue visualizar informações e relatórios específicos, não conseguindo alterar configurações ou executar ações no sistema.

5.3.4.2 CVEs

O Wazuh tem conhecimentos relativamente a Wazuh a CVEs (Common Vulnerabilities and Exposures), onde mantém estas informações numa Base de Dados, sempre atualizada, de CVEs, que contém informações sobre estas vulnerabilidades conhecidas.

Com base nos CVEs, o Wazuh consegue detetar vulnerabilidades em tempo real nos sistemas que monitoriza, comparando as versões do sistema operativo com as informações de vulnerabilidades que possui.

Podem ser consultadas mais informações relativamente a este assunto na secção Bibliografia.

5.3.5 OSSEC

OSSEC é um poderoso motor HIDS open source que realiza várias funções de segurança informática, tais como verificação de integridade, deteção de rootkits, alertas em tempo-real, análise de registos, entre outras.

Tem funcionalidades como:

- **Resposta Ativa:** Resposta a ataques e mudanças numa rede em tempo real.
- **Auditoria Conformada:** Aplicação e auditoria de sistemas para respeitar padrões, tais como PCI-DSS[10].
- **Monitorização de Integridade de Ficheiros:** Deteção de alterações em ficheiros de um sistema e cópia dos dados, que se altera ao longo do tempo.
- **Inventário do Sistema:** Conjunto de informação coletada, tal como serviços da rede, hardware, software instalado, entre outros.
- **Deteção de Intrusões Baseada em Registos (LIDs – Log Based Intrusion Detection):** Monitorização ativa e análise de dados de várias fontes de dados em tempo real.
- **Deteção de Rootkits e Malwares:** Análise de ficheiros com o objetivo de detetar aplicações maliciosas rootkits.

5.3.6 OpenSCAP

OpenSCAP é um conjunto de ferramentas open-source para validação da conformidade de segurança. Contém várias bibliotecas para análise e avaliação de conteúdos de segurança.

O OpenSCAP pode ser utilizado para avaliar a conformidade de sistemas e aplicações, de modo a verificar se estes respondem a padrões de segurança, como PCI-DSS. Pode também utilizado para fazer scans automáticos de vulnerabilidades e gerar reports.

5.3.7 Suricata

Suricata é um detetor open-source de intrusões a sistemas, que pode ser utilizado na plataforma Wazuh, com o objetivo de fornecer capacidades de análise de tráfego e alertas em tempo real, permitindo assim detetar ameaças à segurança. Tem uma alta performance e consegue detetar novas ameaças utilizando vários métodos, como signature-based detection[11] e protocol anomaly detection[12].

5.3.8 Snort

Snort é um detetor e preventor open-source de intrusões a sistemas utilizado para detetar e prever ataques a uma rede. É utilizado no Wazuh como um motor de deteção de intrusões com o objetivo de detetar e alertar relativamente a atividade maliciosa numa rede.

O Snort utiliza um conjunto de regras que podem ser customizadas, dependendo da situação, e podem ser utilizadas para detetar uma grande variedade de ameaças.

O Wazuh utiliza o Snort para efetuar deteção de intrusos em tempo real, monitorizando o tráfego de uma rede e alertando qualquer tráfego que combine com as regras configuradas.

5.3.9 Docker

Docker é a plataforma que permite a criação e implementação de aplicações em ambientes fechados. No caso do Wazuh, o Docker é utilizado para a criação de ambientes leves e portáteis para poder correr as componentes do Wazuh.

Com o Docker é possível instalar o Wazuh em qualquer outro sistema, sem quaisquer preocupações com dependências ou outras configurações, permitindo assim correr o Wazuh em outros ambientes, como na Cloud ou em ambientes híbridos.

O Docker permite uma escalabilidade das componentes do Wazuh, aumentando assim a performance da ferramenta.

5.3.10 Syslog-ng, Rsyslog e Fluentd

Três ferramentas open-source de gestão de registos que podem ser utilizadas para coletar, analisar e enviar mensagens de registos[13] de várias fontes. O Wazuh utiliza estas ferramentas para enviar mensagens de registos de várias fontes para o Wazuh Manager para processo e análise futuros. Com estes dados, o Wazuh Manager pode então detetar e alertar ameaças à segurança, bem como fornecer informação.

5.3.11 Active Directory

Active Directory é uma tecnologia da Microsoft utilizada para gerir e organizar um grande número de dispositivos e utilizadores numa rede. O Wazuh utiliza esta ferramenta para centralizar a autenticação e autorização dos gestores e agentes do Wazuh. Pode também integrar o Active Directory com o objetivo de autenticar utilizadores que pretendem aceder à interface web do Wazuh.

5.3.12 pfSense

A pfSense é uma firewall open-source cujo sistema operativo é o FreeBSD. Fornece funcionalidades de segurança, como proteção firewall, conetividade Virtual Private Network (VPN), deteção de intrusões, etc.

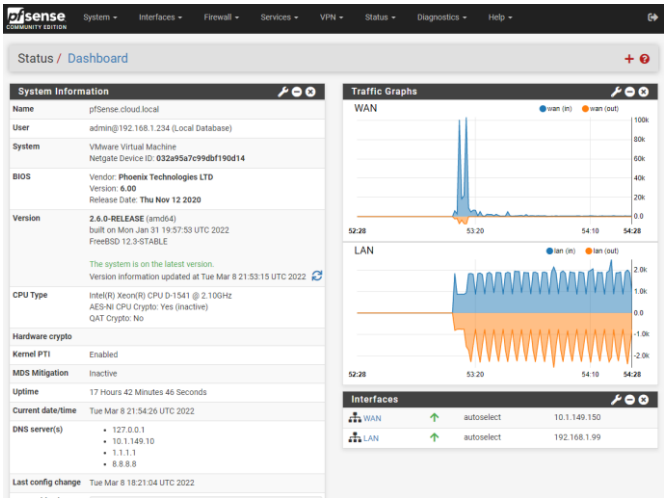

Figura 10 - pfSense

Devido a ser uma firewall open-source foi-nos bastante útil no contexto da implementação de um SIEM baseado em open-source.

5.4 Implementação

Para a implementação deste trabalho, primeiramente é necessário efetuar a implementação da plataforma Wazuh, processo descrito na secção 5.4.1. Essencialmente toda a implementação é feita com esta ferramenta, acrescentando posteriormente algumas ferramentas adicionais e conjuntos de regras personalizáveis.

Posteriormente, para garantirmos uma maior monitorização do tráfego da rede, decidimos também acrescentar a Firewall open-source pfSense.

Para a testagem desta plataforma foi utilizada um ficheiro .ISO numa máquina virtual, para a instalação do Wazuh Manager e para a testagem do Wazuh Agent, outra máquina virtual configurada para ser analisada pelo Manager. Este processo pode ser visto no vídeo encontrado na secção 5.1.

5.4.1 Implementação do Wazuh

Para a implementação deste trabalho, primeiramente é necessário efetuar a implementação da plataforma Wazuh, que segue os seguintes passos:

- **Instalar o Wazuh Manager no host que serve de gestor central para a monitorização:** O Wazuh Manager é a componente central do sistema que faz a coleta e análise dos dados provenientes dos agentes. Pode ser instalado em vários sistemas operativos, como Windows, Linux e macOS. Pode ser instalado utilizando um package manager, ou instalando a partir do seguinte link:

https://documentation.wazuh.com/current/installation-guide/index.html

- **Instalar o Wazuh Agent em cada host que se pretende monitorizar:** Ao correr esta ferramenta no host que se quer monitorizar, os dados dos registos são coletados. Bem como o Wazuh Manager, o Wazuh Agent pode ser instalado em vários sistemas operativos e pode ser instalado com um package manager ou através do seguinte link:

https://documentation.wazuh.com/current/installation-guide/wazuh- agent/index.html

- **Configurar o Wazuh Manager e o Wazuh Agent para poderem comunicar:** Depois de estas ferramentas estarem instaladas, é necessário comunicarem. Este processo é geralmente especificando o IP e a port do Wazuh Manager no agente e vice-versa.
- **Configurar o Wazuh Manager para coletar e analisar os registos dos Agentes:** O Manager analisa os registos que coleta e deteta eventos de segurança. É necessário configurar o Wazuh Manager para coletar os registos mais adequados dos Agentes e configurar regras para análise e deteção dos eventos mais relevantes.

- **Utilizar a API do Wazuh e a Interface Web para acessar e analisar os dados coletados pelo Wazuh Manager:** Como referido na secção 3.3.4, o Wazuh Manager utiliza uma API RESTful e uma interface web que permite acessar e analisar os dados coletados pelo sistema. A API pode ser utilizada para acessar os dados e a interface web para interagir com os dados de uma forma mais user-friendly.
- **Configurar e utilizar as várias regras para detetar e alertar eventos específicos:** Através das regras preconfiguradas no Wazuh, é possível detetar eventos de segurança. É também possível criar regras personalizadas de modo a detetar eventos que se considerem específicos para um determinado ambiente.
- **Afinação das configurações e certificação de que o sistema funciona corretamente:** Este processo envolve afinação das configurações, tal como definir as regras das análises e monitorizar o sistema de modo a certificar que o sistema coleta e analisa os dados dos registos pretendidos.

5.4.1.1 Instalação de um Agente

Para podermos adicionar agentes ao Wazuh Manager, começámos por instalar máquinas virtuais nos nossos computadores, uma máquina com o sistema operativo Windows 10, e quatro com Linux: uma delas com Kali Linux, duas com Ubuntu e uma com o sistema operativo Fedora.

Depois, no Wazuh Manager, para cada uma destas VMs, acedemos ao ecrã dos agentes e selecionámos a opção de adicionar um agente, que mostra um ecrã bastante interativo:

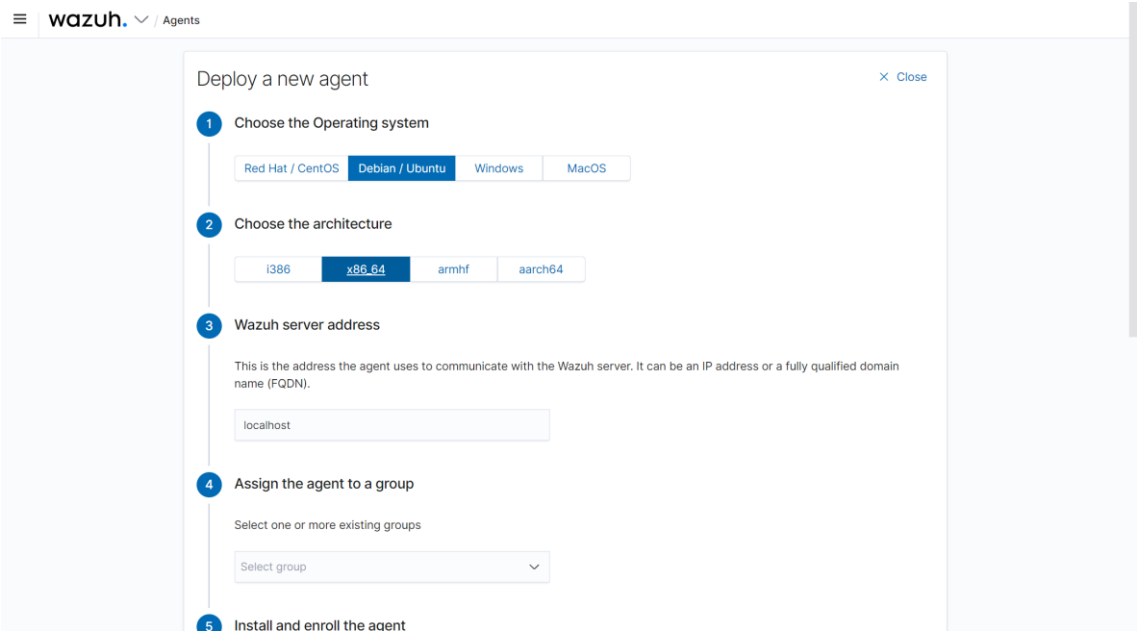

Figura 11 - Adicionar Agente no Wazuh

Ao selecionarmos as opções relativas ao sistema operativo que pretendemos monitorizar, são-nos então dados comandos que teremos de introduzir na linha de comandos (por motivos de segurança, o IP do Manager está escrito como “localhost”):

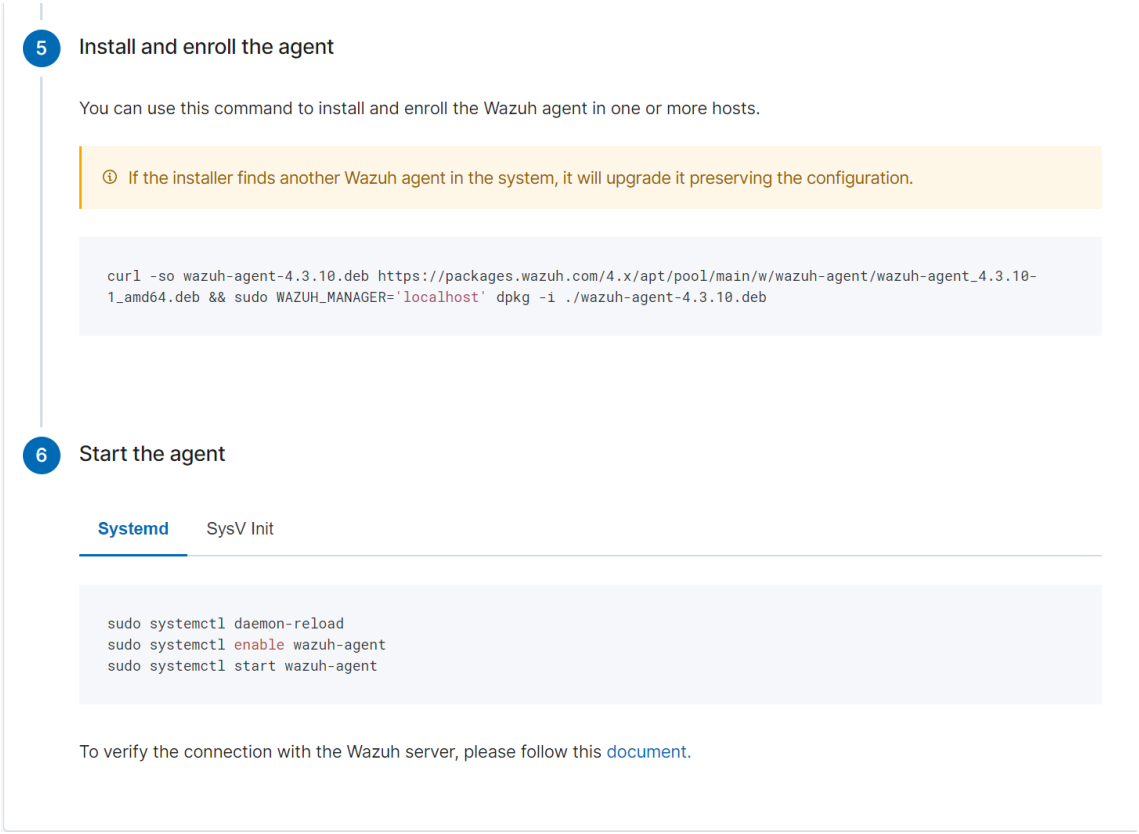

Figura 12 - Comandos para a instalação de um agente

Depois deste passo, de correrm os estes comandos, a VM passa a ser monitorizada pelo Wazuh Manager cada vez que se encontra conectada à Internet.

5.4.1.2 Deteção de Processos Ocultos

Esta operação foi feita numa máquina virtual com o sistema operativo Ubuntu. Esta configuração no agente permite a deteção de um processo oculto criado por um rootkit.

Para permitir a visualização mais rápida, alterámos a latência dos rootchecks – processo que verifica processos a correr e a presença de ficheiros – de 12 horas (default) para 2 minutos, em segundos:

```
<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>43200</frequency>

  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>
</rootcheck>
```

Figura 13 - Deteção de Processos Ocultos

Como teste, importamos um rootkit do GitHub, fornecido pelo Wazuh e corremos o ficheiro.

Através da linha de comandos, executamos o comando "kill", para terminar processos, num processo aleatório. No nosso caso, para teste, terminámos o processo 509.

Ao correrrmos o comando "lsmod", que tem como função a visualização dos módulos do Kernel que estão atualmente carregados, juntamente com o módulo do rootkit, não vemos alterações, pois é escondido pelo rootkit.

Corremos então o comando "ps auxw | grep rsyslogd | grep -v grep" que tem como função visualizarmos o PID dos processos de Syslogs. Obtivemos então o seguinte output:

Como podemos observar, o PID é 932. Com esta informação terminamos então este processo também, através do comando "kill -31 932". Ao correrrmos de novo o comando de visualização do PID dos syslogs, não vamos obter nenhum output. Se correrrmos o comando kill de novo, o processo torna-se, de novo, visível. Porém, como é possível observar na Figura 37 - Teste 5, esta eliminação dos processos é detetada pelo Manager.

```
ronaldo@ronaldo-virtual-machine:~$ ps auxw | grep rsyslogd | grep -v grep
syslog       932  0.0  0.1 222400  5592 ?        Ssl  04:04   0:00 /usr/sbin/rsyslogd -n -iNONE
ronaldo@ronaldo-virtual-machine:~$ S
```

Figura 14 - Output do PID dos Syslogs

5.4.1.3 Monitorização da Integridade de Ficheiros

Esta configuração foi efetuada numa máquina virtual, cujo sistema operativo é Ubuntu.

Esta configuração tem como objetivo permitir ao Wazuh Manager verificar que ficheiros são alterados e removidos de uma determinada máquina. Para tal, começamos por aceder ao ficheiro das configurações do Agente e adicionámos a seguinte linha (Assinalada a vermelho):

```
<!-- File integrity monitoring -->
<syscheck>
  <!-- ADICIONADO PARA TESTE -->
  <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
```

Figura 15 – Monitorização da Integridade de Ficheiros

A partir desse momento, podemos monitorizar o diretório "root" – determinado por nós – na medida em que quando um ficheiro que é alterado e/ou apagado, um alerta é enviado para o Wazuh Manager.

5.4.1.4 Personalizar Configurações

Com o objetivo de tornarmos o Wazuh Manager mais personalizado a nosso gosto, acedemos ao seu ficheiro de configuração e fizemos algumas alterações:

Começámos por alterar os níveis a partir dos quais queríamos receber alertas (nível 5) e quando queríamos ser alertados pelo email (nível 11):

```
<alerts>
  <!-- Vai mandar alertas a partir do nível 5 -->
  <log_alert_level>5</log_alert_level>
  <!-- Vai mandar emails a partir do nível 11 -->
  <email_alert_level>11</email_alert_level>
</alerts>
```

Figura 16 - Nível de Alertas

Para podermos visualizar a integridade de ficheiros (mostrado em 5.4.1.3) ativámos essa funcionalidade no Manager:

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
```

Figura 17 - Integridade de Ficheiros

5.4.1.5 Bloquear o SSH quando uma Brute Force é tentada

Com o objetivo de prevenir que atacantes acedam ao Wazuh Manager através de ataques Brute Force, bloqueamos o acesso do IP do atacante. Esta configuração é um método de **resposta ativa**.

Primeiramente acedemos ao ficheiro de configuração do Wazuh Manager e acrescentamos o bloco abaixo, que nos vai permitir este inicializar o bloqueio:

```
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

Figura 18 - SSH Block

Neste caso aceitamos timeout, pois após duas tentativas falhadas, o IP é então bloqueado, e como por vezes já nos aconteceu errarmos a palavra-passe duas vezes, não ficarmos sem acesso total ao Manager.

Por fim, adicionámos o bloco abaixo, que tem como função bloquear o SSH durante 10 minutos:

```
<active-response>
  <command>firewall-drop</command>
  <location>localhost</location>
  <rules_id>5710</rules_id>
  <timeout>600</timeout>
</active-response>
```

Figura 19 - Timeout

5.4.1.6 Instalação do Suricata

Como referido no ponto 5.3.7, o Suricata é uma ferramenta de monitorização do tráfego da rede. Esta ferramenta foi implementada numa máquina virtual com o sistema operativo Ubuntu.

Começámos por instalar o Suricata através da linha de comandos:

```
ronaldo@ronaldo-virtual-machine:~$ sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
```

Figura 20 - Suricata Terminal

Depois instalamos as regras pertencentes ao Suricata:

```
ronaldo@ronaldo-virtual-machine:~$ cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```

Figura 21 - Comando Suricata

Com as configurações instaladas, alterámos algumas variáveis sugeridas na instalação do Suricata.

Por fim, acedemos ao ficheiro de configurações do Agente para que o Agente consiga ler os ficheiros de log do Suricata:

```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
```

Figura 22 - Configuração Suricata

5.4.1.7 Feedback da Instalação

Todo este processo envolveu bastante pesquisa, no sentido de conseguirmos avaliar as melhores e possíveis configurações que pudéssemos aplicar, tanto no Wazuh Manager, como nos Agentes. Foi um processo um tanto complicado, pois muitas vezes encontrámos configurações que não funcionavam para a nossa arquitetura (muitas vezes por terem dependências de outras funcionalidades ou configurações), ou que simplesmente não se aplicavam ou achámos que não seriam adequadas. Apesar disso, tentámos ter um ficheiro de configuração compacto em termos de conteúdo.

Se quiséssemos, agora, criar a ferramenta do 0, já tendo conhecimento de funcionalidades que podemos adicionar aos ficheiros de configuração, seria um processo muito mais rápido. Simplesmente seria necessário instalar um novo servidor Wazuh (Manager) e adicionar os novos agentes. Após isso, para a configuração normal (sem a firewall, apenas com Wazuh Manager e agentes) seria apenas necessário, como referido acima, modificar os ficheiros de configuração de todos.

A partir do momento que temos uma configuração default, podemos, depois de conectar com o agente, simplesmente fazer um cópia e colagem de um dos ficheiros ossec.conf para o novo agente, simplesmente mudando o valor do endereço IP do novo agente.

5.4.2 Firewall pfSense

5.4.2.1 O que é o Pfsense

PfSense é uma firewall open source e a plataforma de routing que se tornou muito conhecida no mundo da segurança e administração de redes. Ela destaca se como uma solução confiável e rica em recursos, o que o torna uma ótima opção para implantações de pequena escala e grandes redes empresariais. Os seus recursos de segurança são um dos principais fatores na escolha do pfSense. Os recursos avançados de segurança que ela oferece incluem filtragem de pacotes com informações de estado, deteção e prevenção de invasões, suporte para redes privadas virtuais (VPNs) e proxies da Web seguros. Além disso, o pfSense oferece muita flexibilidade e opções de personalização, permitindo que os utilizadores ajustem a configuração para atender às suas necessidades exclusivas. Tanto os administradores de rede experientes quanto os novatos podem usá-lo graças à sua interface amigável baseada na web, que facilita as tarefas de gerenciamento e monitoramento. No geral, o pfSense capacita as organizações com uma solução poderosa, econômica e facilmente implantável para proteger e controlar o tráfego de rede.

5.4.2.2 Porquê da escolha do Pfsense

- Integração de log do Wazuh: escolhi o pfSense por causa de sua integração perfeita com o Wazuh, permitindo o envio remoto e análise de logs eficiente e deteção de ameaças.
- Interface amigável: A interface amigável baseada na Web do pfSense foi um fator importante na nossa decisão, facilitando a navegação e o gerenciamento das configurações de rede.
- Extensas opções de personalização: optei pelo pfSense devido às suas amplas opções de personalização, permitindo adaptar a configuração aos nossos requisitos específicos de rede.
- Solução Open Source: o pfSense sendo uma solução open source foi um fator chave na nossa escolha, pois fornece transparência, suporte da comunidade e liberdade para modificar e estender suas funcionalidades.
- É gratuito: O facto do pfSense ser gratuito desempenhou um papel significativo no meu processo de tomada de decisão, tornando-o uma opção económica para implementar uma segurança de rede robusta.

5.4.2.3 Instalação e configuração do Pfsense

1. Entrar em Download pfSense Community Edition e colocar as seguintes opções:
    - Arquitetura -> AMD64(64-bit)
    - Installer-> Dvd Image
    - Mirror-> Frankfurt, Germany
2. Quando criarmos a máquina virtual escolher o sistema operativo BSD versão FreeBSD e continuar com a instalação normal escolhendo as características da máquina virtual.
3. Abrir as settings da firewall e selecionar em network e habilitar os 3 adapters, 1 em Bridged adapter para ter conexão à internet e os outros dois em internal network, 1 para a vlan e o outro para a DMZ
4. Em seguida abrir a máquina virtual e selecionar o ISO do pfsense e continuar com a instalação default

5. Vamos ter um ecrã de menu e vamos criar as interfaces (carregamos 2) e vamos configurar a interface LAN
6. Escrever o IPV4 da LAN neste caso escolhemos o ipv4 172.16.1.254 e escolhemos 24 de subnet bit count
7. Em seguida passamos à frente das duas próximas opções
8. Quando pedem para ativar o DHCP escrevemos y
9. Depois escolhemos o range de ipv4 no nosso caso é do ip 172.16.1.100 ao 172.16.1.150
10. Escrever y e agora já temos a instalação do Pfsense concluída.

Quando abrimos o Pfsense pede nos password e nome do user, como abrimos pela primeira vez o username é admin e a password é pfsense e logo em seguida aparece uma tela de setup onde podemos mudar o hostname mas mais importante vamos usar o dns da google 8.8.8.8 e como dns secundário 8.8.4.4, carregamos em next e escolhemos a hora, carregando next novamente deixamos tudo por padrão e vamos até ao fim da página, no final temos 2 checkbox's que não vamos selecionar neste caso porque estamos a fazer um teste à solução Pfsense mas em contexto real temos de as deixar habilitadas.

Para enviar os logs da firewall para o wazuh vamos carregar na opção estado->logs do sistema ->configurações e quanto às configurações deixamos o seguinte.

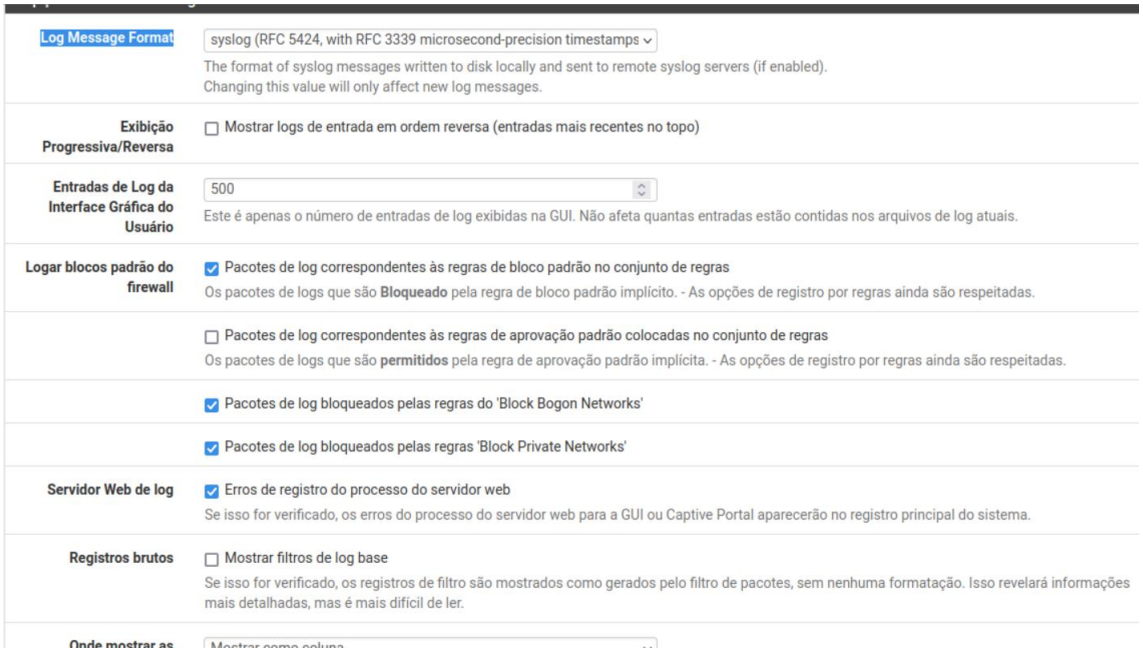

Figura 23 - pfSense print 1

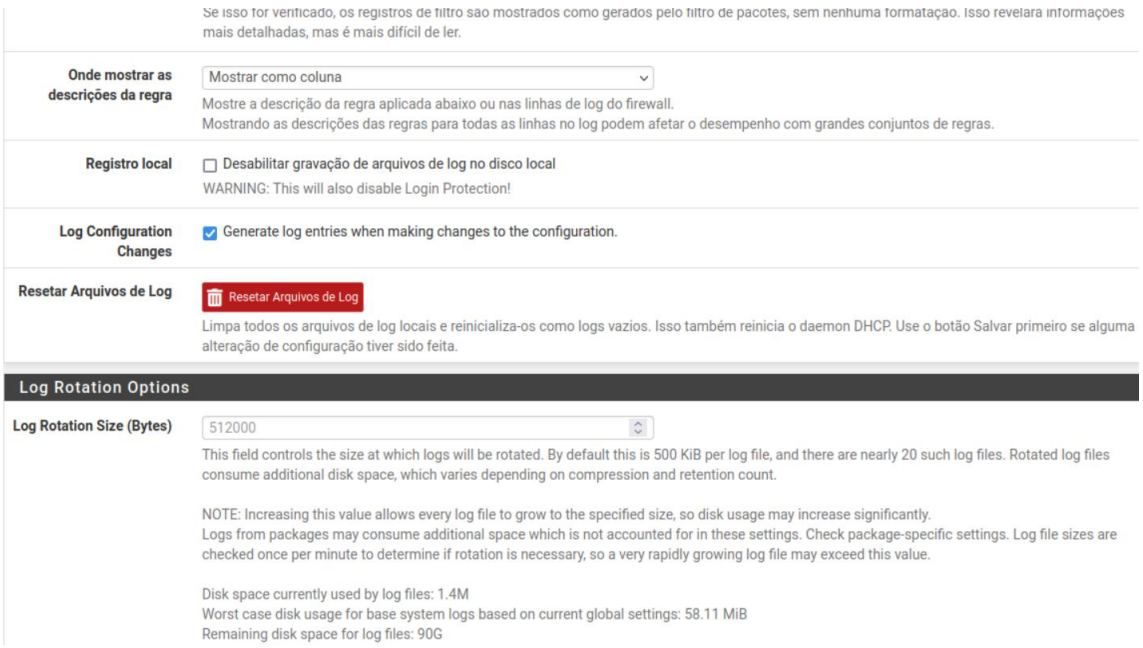

Figura 24 - pfSense print 2

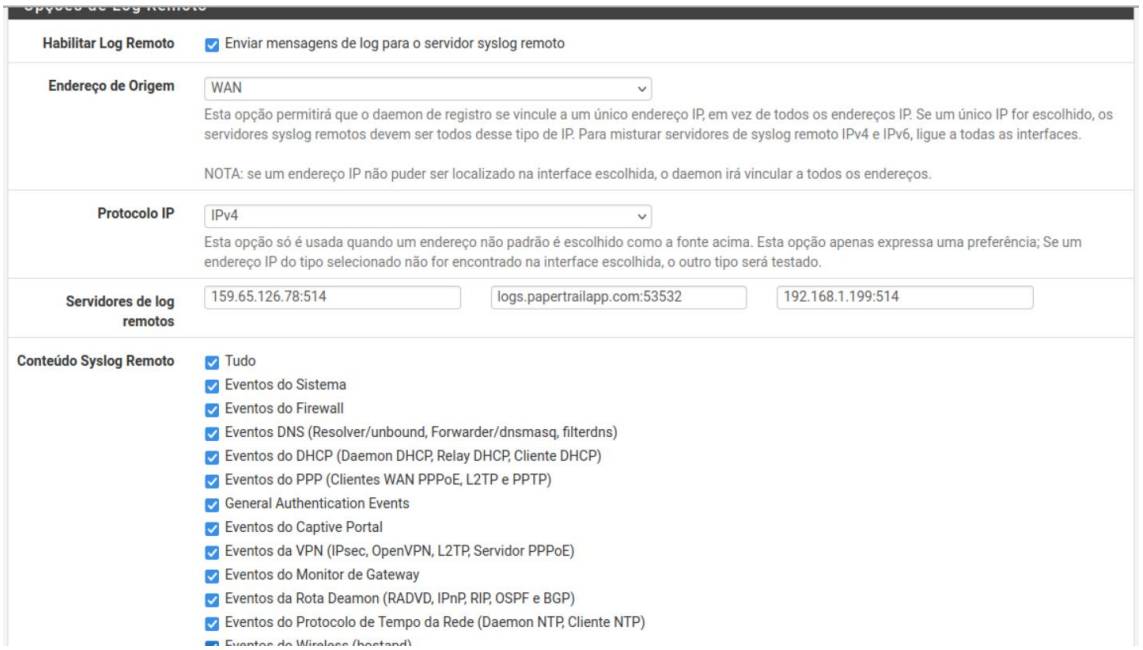

Figura 25 - pfSense print 3

Onde diz servidores de log remotos é onde vamos escrever o ip do wazuh e vamos usar a porta 514.

5.4.3 DMZ

DMZ significa “Demilitarized Zone” (Zona Desmilitarizada) e no contexto de segurança informática funciona como uma zona entre as redes interna e externa de uma organização, geralmente, a Internet.

O seu propósito é fornecer uma camada adicional de segurança, isolando o acesso público aos serviços ou aos sistemas da rede interna.

No nosso caso, só usamos uma firewall que apesar de proteger menos fica muito mais simples, para criarmos uma dmz precisamos de fazer o seguinte:

1. Adicionamos uma nova interface DMZ

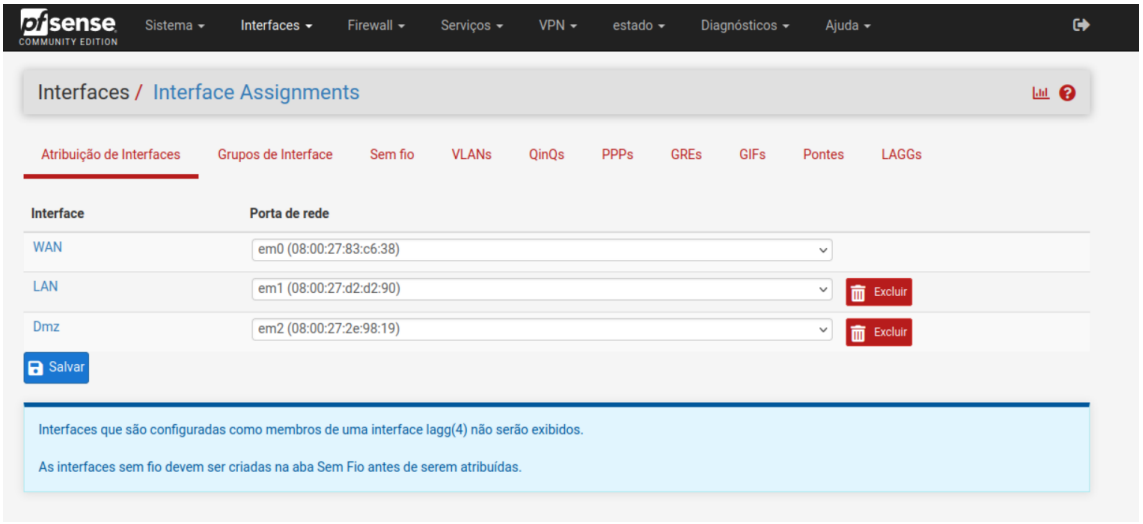

Figura 26 - DMZ print 1

2. Nas configurações da DMZ temos de ativar a interface e carregar em ipv4 estático e adicionar o ip do da interface, neste caso usamos o 172.16.0.1
3. Adicionar as regras da imagem abaixo

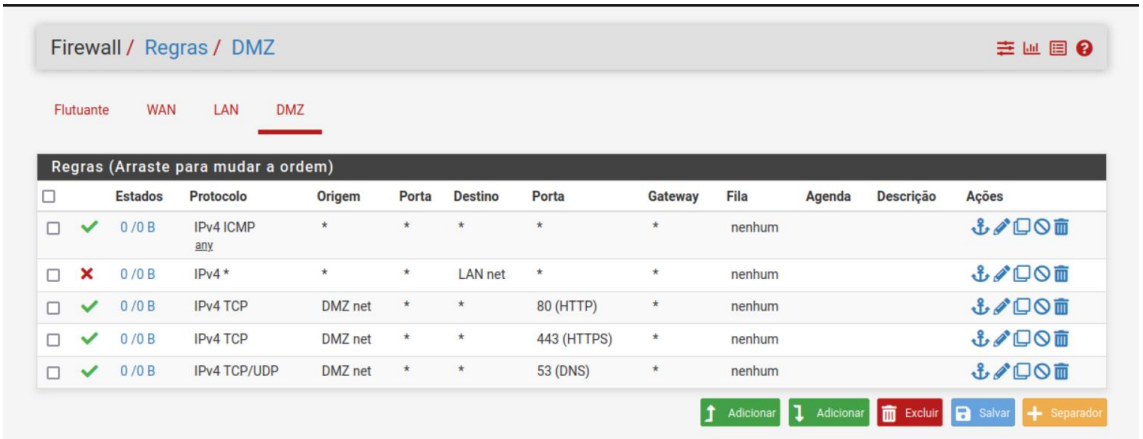

Figura 27 - DMZ print 2

Figura 28 - DMZ print 3

4. Em sistema->avançado clicar nas opções que estão marcadas na imagem e salvar

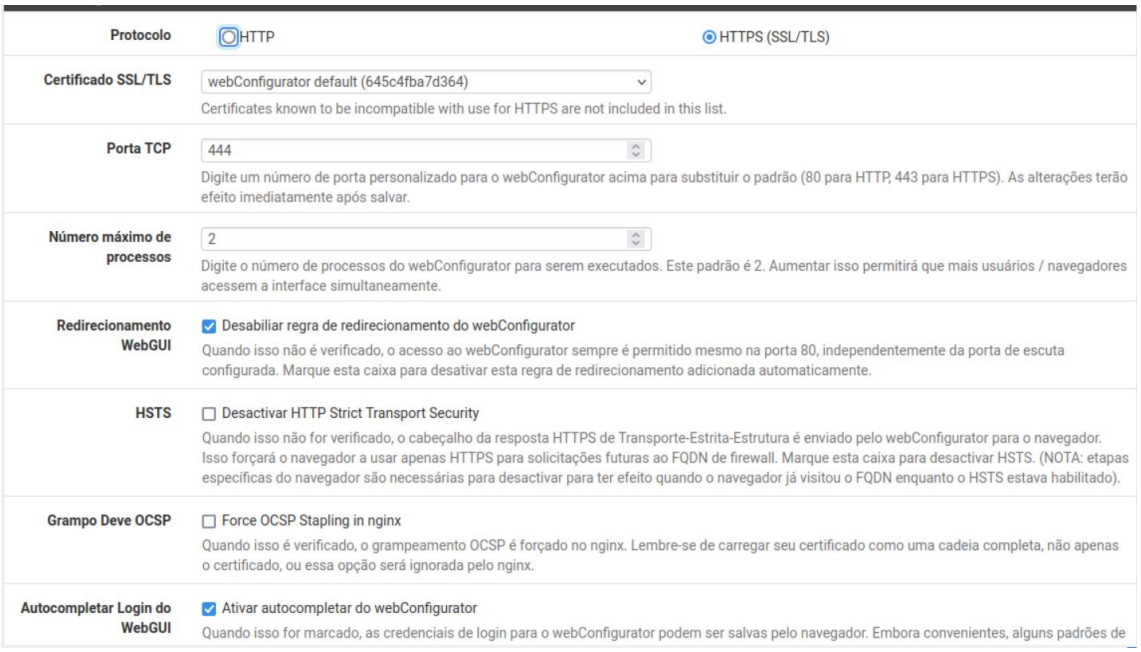

Figura 29 - DMZ print 4

5. Por fim em firewall e nat selecionar o seguinte

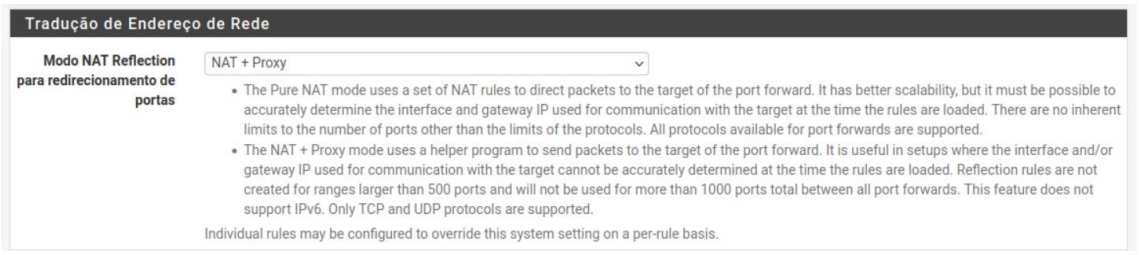

Figura 30 - DMZ print 5

A dzm já está configurada e a funcionar, assim dividimos a vlan e a dmz que pode conter o site da empresa e o servidor de emails, neste caso não usamos um servidor web para conseguirmos mostrar.

5.4.4 Criação de um ambiente de Simulação Empresarial

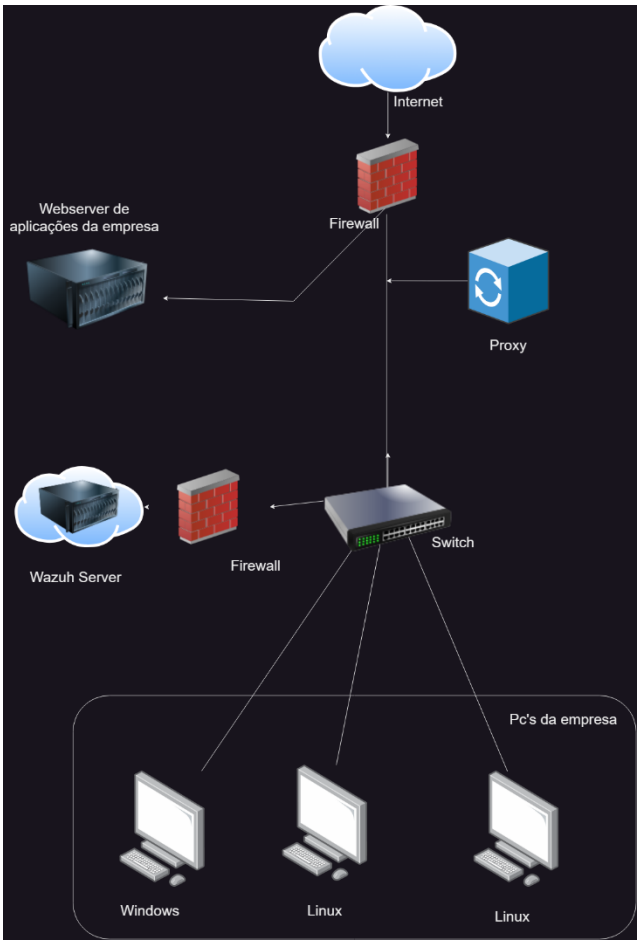

Figura 31 - SImulação de Ambiente

5.4.4.1 Descrição dos componentes

Incluímos vários elementos na construção do ambiente empresarial para garantir a segurança e o bom funcionamento da infraestrutura. A nossa configuração consiste em:

Switch: Um switch é usado para ligar elementos da rede local, incluindo computadores e servidores. Ele permite a comunicação entre eles e garante uma transferência efetiva de dados em toda a rede.

Firewalls: Para aumentar a segurança do ambiente, decidimos instalar dois firewalls. Um dos firewalls serve como um servidor proxy, além de proteger a rede de ameaças externas. Com essa configuração, podemos gerenciar o acesso à Internet e monitorar o comportamento do utilizador para proteger os dados corporativos.

Servidor Proxy: Para mediar as conexões entre o hardware da rede local e a internet, utilizamos um servidor proxy. Ao filtrar o tráfego da Web e impedir o acesso a sites prejudiciais ou não autorizados, ele adiciona uma camada extra de segurança. Além disso, o servidor proxy permite que consigamos acompanhar e registar a atividade do utilizador, o que ajuda na análise de possíveis ameaças.

Servidor Web para Aplicações Internas da Empresa: Montamos um servidor web específico para as aplicações internas da empresa. Abriga os serviços e software necessários para a

operação dos processos de negócios. As firewalls que protegem esse servidor garantem a segurança dos dados e a disponibilidade do serviço.

LAN com Computadores da Empresa: Utilizando computadores que correspondem ao hardware utilizado pela empresa, montamos uma rede local (LAN). Esses computadores são representados no ambiente de simulação por máquinas virtuais. Isso permite nos simular o ambiente de negócios com segurança sem ter um efeito adverso na infraestrutura real.

Montámos uma zona DMZ com uma firewall que se encarrega de reencaminhar o tráfego para o servidor web da aplicação. Os serviços públicos serão alojados nesta DMZ, acrescentando mais um nível de segurança entre a rede interna e a internet. O acesso é restrito e as conexões seguras com o servidor web são feitas graças à firewall na DMZ.

Utilizámos a firewall oferecida pela plataforma de nuvem que selecionamos para implementar o servidor (Digital Ocean) para o servidor Wazuh. O servidor Wazuh é ainda mais protegido por essa firewall, que o protege contra possíveis ameaças externas.

Para garantir a segurança dos dados e a continuidade dos processos internos do negócio, essa configuração do ambiente de negócios é fundamental. Além disso, permite a simulação de cenários e testes de segurança, o que ajuda a equipa de TI a aprimorar suas habilidades e encontrar possíveis vulnerabilidades antes que elas se manifestem no mundo real.

5.4.4.2 Porque fizemos um ambiente de simulação

Um ambiente de simulação utilizando a ferramenta Wazuh é um projeto que vale a pena por vários motivos. Podemos primeiro treinar e melhorar as habilidades da nossa equipa de cibersegurança simulando o ambiente empresarial. Podemos representar cenários do mundo real em um ambiente de simulação e avaliar a nossa aptidão para detetar ameaças em potencial e tomar as medidas apropriadas. Além de aprender sobre os recursos e funcionalidades da ferramenta Wazuh, isso permite que melhoremos as nossas habilidades de análise e resposta. Além disso, ao simular o ambiente Wazuh, podemos confirmar em um ambiente controlado a eficácia das políticas de segurança e configurações de ferramentas.

Diferentes cenários de ataques informáticos podem ser testados e explorados e podemos encontrar buracos na nossa infraestrutura de segurança. Com a ajuda desses testes, podemos ajustar e aprimorar as configurações do Wazuh para garantir que o programa esteja pronto para identificar e responder a ameaças no mundo real. Avaliar a eficácia das estratégias de resposta a incidentes é uma das principais vantagens de simular o ambiente empresarial. Podemos simular incidentes de segurança e testar as nossas estratégias de resposta, incluindo medidas de mitigação, comunicação interna e externa e recuperação do sistema, simulando incidentes de segurança reais. Ao identificar áreas para melhoria nos nossos procedimentos de resposta a incidentes por meio desses exercícios de treinamento, podemos ter a certeza de que estamos prontos para lidar com qualquer incidente de segurança real.

Em conclusão, desenvolver um ambiente de simulação para a ferramenta Wazuh é crucial para treinamento, confirmação de configurações de segurança e aprimoramento contínuo dos procedimentos de resposta a incidentes. Por meio dessa simulação, melhoramos o nosso trabalho, a ferramenta e a segurança da organização, dando mais segurança e segurança aos nossos sistemas e dados.

5.5 Abrangência

- **Bases de Dados:** Será necessário criar uma base de dados de modo a poder organizar toda a informação que o SIEM irá recolher.
- **Linguagens de Programação:** Todo o processo será feito através de linguagens de programação.
- **Engenharia de Requisitos e Testes:** Antes de se começar qualquer passo, teremos de levantar os requisitos para esta aplicação e definir bem os seus limites.
- **Programação Web:** O dashboard será demonstrado no formato web.
- **Redes de Computadores:** Temos de ter uma noção de redes de computadores para podermos ter noção de certas especificidades que o SIEM terá.
- **Sistemas de Suporte à Decisão:** O dashboard terá de ser tanto intuitivo como informativo.
- **Computação Distribuída:** Sendo que o SIEM também irá recolher dados de servidores, bem como de variadas fontes, é importante termos noções de software distribuído.
- **Segurança Informática:** Estando a desenvolver uma aplicação de cibersegurança, é crucial existir conhecimento na área.
- **Sistemas de Informação na Nuvem:** A ferramenta Wazuh tem uma versão na cloud, com a qual estamos também a trabalhar.

6 Método e planeamento

Tabela 3 - Calendário

ID	NOME	INÍCIO	FIM
0	Pesquisa sobre SIEM	19/10/2022	24/11/2022
1	Reunião com o Orientador para fazer um ponto de situação e apresentar as pesquisas	27/10/2022	27/10/2022
2	Construção do Relatório Intercalar 1º Semestre	17/11/2022	24/11/2022
3	Entrega do Relatório Intercalar 1º Semestre	24/11/2022	24/11/2022
4	Reunião online com a empresa de cibersegurança CyberS3c para obter algumas recomendações para a implementação do projeto	13/01/2023	13/01/2023
5	Construção do Relatório Intermédio	13/01/2023	27/01/2023
6	Reunião online com o Orientador para demonstrar o trabalho realizado até ao momento	23/01/2023	23/01/2023
7	Entrega do Relatório Intermédio 1º Semestre	27/01/2023	27/01/2023
8	Apresentação do TFC	30/01/2023	30/01/2023
9	Implementar o SIEM na cloud	02/02/2023	07/02/2023
10	Adicionar sistema de deteção de intrusões na rede	09/02/2023	13/02/2023
11	Implementar o scan de vulnerabilidades	15/02/2023	22/02/2023
12	Configuração de alguns agentes	01/03/2023	20/04/2023
13	Testagem das configurações efetuadas nos agentes	01/03/2023	20/04/2023
14	Reunião com o Orientador	22/03/2023	22/03/2023
15	Estudo de como funcionam algumas arquiteturas de SIEMs em empresas	24/03/2023	23/04/2023

16	Realização do Relatório Intercalar do 2º Semestre	16/04/2023	23/04/2023
17	Entrega do Relatório Intercalar do 2º Semestre	23/04/2023	23/04/2023
18	Compreensão de como funciona uma Firewall	27/04/2023	02/05/2023
19	Instalação de uma firewall	03/05/2023	08/05/2023
20	Testagem da Firewall	08/05/2023	12/05/2023
21	Implementar um ambiente, de forma a simular uma pequena empresa	14/05/2023	19/05/2023
22	Testar ataques nesse ambiente criado	20/05/2023	25/05/2023
23	Realização do Relatório Final	18/06/2023	30/06/2023
24	Entrega do Relatório Final	30/06/2023	30/06/2023

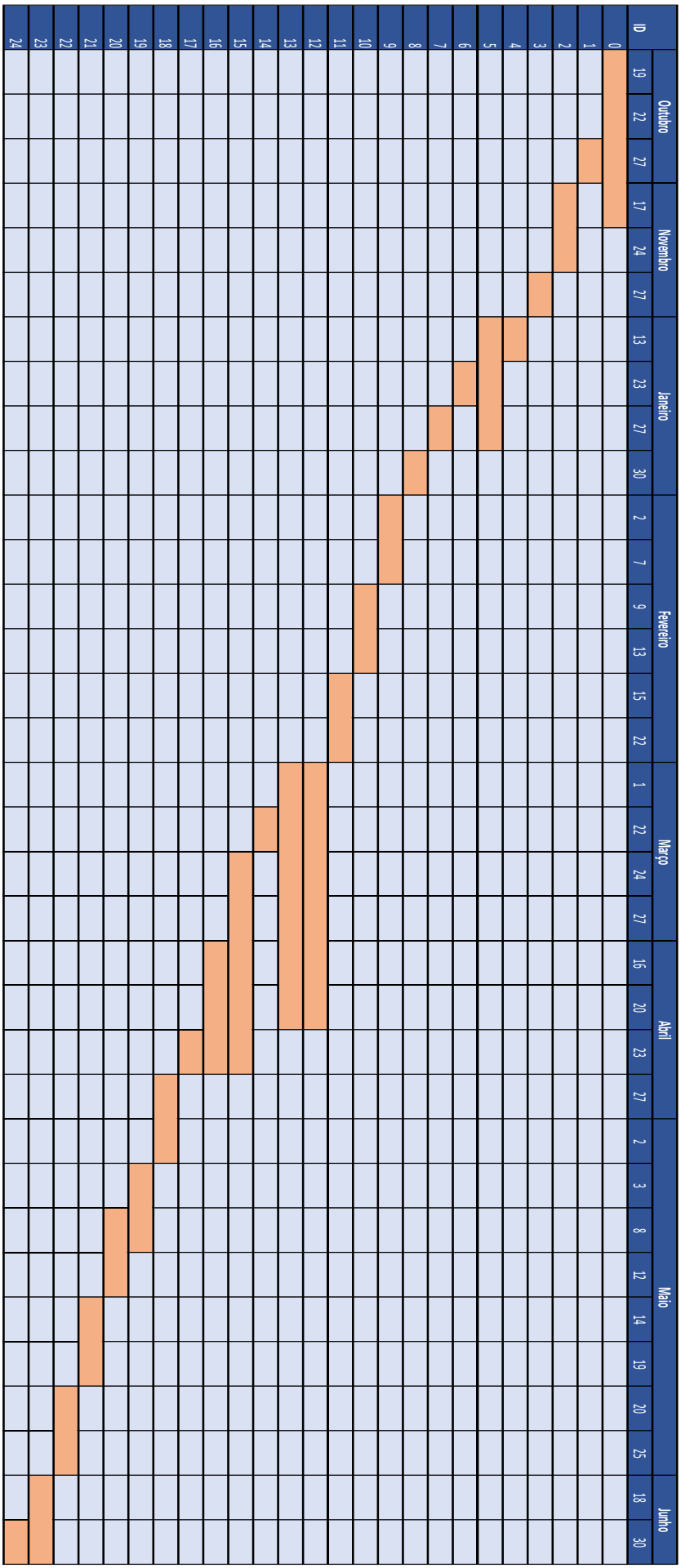

Figura 32 - Mapa de Gantt

O desenvolvimento deste projeto consistiu em 5 fases essenciais:

- A primeira fase diz respeito a toda a pesquisa feita para obtermos um maior conhecimento de o que é uma plataforma SIEM, como é utilizada, em que situações, entre outras perguntas que achámos pertinentes. Esta fase foi, talvez, a mais demorada, porque queríamos tentar consolidar os nossos conhecimentos neste assunto.
- Na segunda fase, já tendo alguns conhecimentos teóricos e do Wazuh, tentámos então começar a conhecer melhor esta ferramenta e a alocá-la, tanto numa máquina, como através do DigitalOcean, disponibilizarmo-la na Internet. Nesta fase existe também pesquisa, bem como na fase anterior.
- Com o Wazuh pronto a utilizar, passámos então para a terceira fase, onde conectámos o primeiro agente e testámos e observámos outputs obtidos, ao falharmos palavras-passe, não termos permissões, etc. Sendo o Wazuh uma ferramenta com muitas funcionalidades, esta fase foi também bastante demorada, na medida em quisemos ter uma perceção das variadas coisas que podemos testar.
- Na quarta fase implementámos uma firewall, de modo a termos também uma ferramenta de monitorização do tráfego. Fizemos uma pesquisa sobre Firewalls que pudéssemos utilizar sem qualquer tipo de pagamento e tentámos algumas, até conseguirmos fazer a configuração com o pfSense.
- Na quinta, e última, fase elaborámos um ambiente virtual de simulação empresarial para podermos fazer uma boa representação do objetivo deste projeto.

O calendário demonstrado na Figura 32 foi maioritariamente cumprido, com exceção das datas apresentadas, que, algumas vezes, se tivéssemos acabado um item antes da data, começávamos o seguinte, também ocorrendo alguns atrasos, o que acabava por equilibrar o tempo do processo de desenvolvimento.

7 Resultados

7.1 Testes no Wazuh

Como o Wazuh é uma framework já inclui várias funcionalidades de uma plataforma SIEM, a fase de testes foi bastante útil para aprendermos mais sobre como trabalhar com uma plataforma destas.

Para tal, consultámos os requisitos referidos na Tabela 2, e para alguns conseguimos efetuar alguns testes, abaixo referidos. Para a realização destes testes foi consultado o website do Wazuh, bem como a sua documentação.

Tabela 4 - Tabela de Testes

Test Case	Test Title	Test Summary	Test Steps	Expected Result	Actual Result
1	Coletar Dados	Verificar se é possível coletar dados de um Wazuh Agent	Instalar o Wazuh Agent no host que pretendemos monitorizar. Aceder ao menu dos Agentes no Wazuh Manager e ver se o Agente foi adicionado. Entrar na opção desse agente no Wazuh Manager e visualizar as informações disponíveis.	O host foi adicionado ao Wazuh Manager e é possível visualizar informações.	O host foi adicionado ao Wazuh Manager e foi possível visualizar informações.
2	Correlação com CVEs	Verificar se o Wazuh Manager disponibiliza uma lista com CVEs – uma vulnerabilidade que foi encontrada e exposta	Aceder à página de um agente registado no Wazuh Manager. Na página do agente, aceder à opção "Vulnerabilities".	São mostrados os CVEs encontrados no agente.	Foi mostrada uma lista dos CVEs encontrados do agente.
3	Intrusão - Brute Force	Inserir várias vezes uma palavra passe errada num utilizador de uma máquina	Numa máquina que já esteja registada como agente no Wazuh Manager, inserir uma palavra-passe errada várias vezes, não sendo necessário ser	É detetada uma tentativa de brute force a um agente.	Foi detetada a tentativa de brute force a um agente.

		registada como agente.	sempre a mesma palavra-passe. Aceder ao Wazuh Manager, e ir à página do agente em que as palavras-passe foram introduzidas corretamente. Aceder à opção "Security Events" e de seguida a "Events". Adicionar o filtro de uma rule.id com o valor "2501".		
4	Deteção de Rootkits	Verificar se o Wazuh Manager consegue detetar um rootkit que esteja num agente.	Seguir os passos no seguinte hyperlink: https://documentation.wazuh.com/current/proof-of-concept-guide/poc-detect-hidden-process.html	O Wazuh Manager consegue detetar com sucesso a existência de um rootkit.	O rootkit foi detetado.
5	Modificação de Ficheiros	Verificar se o Wazuh Manager regista ficheiros modificados e eliminados.	Seguir os passos no seguinte hyperlink: https://documentation.wazuh.com/current/proof-of-concept-guide/poc-file-integrity-monitoring.html	O Wazuh Manager regista a eliminação de um ficheiro.	O Wazuh Manager registou a eliminação de um ficheiro.
6	Personalizar Configuraçõ es	Personalizar a configuração do Wazuh.	No menu principal do Wazuh Manager, na secção "Management" aceder a "Configuration". Neste menu, clicar em "Edit configuration". Depois de fazer algumas alterações a gosto, clicar em "Save" e de seguida	A configuração do Wazuh Manager foi alterada.	A configuração do Wazuh Manager foi alterada.

			em "Restart manager".		
7	Bloquear SSH	Efetuar brute force no Manager e verificar se o SSH é bloqueado	Seguir os passos no seguinte hyperlink: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html	O SSH é bloqueado.	O SSH foi bloqueado.
8	IOCs	Verificar se é possível identificar IOCs e executar comandos remotamente.	Seguir os passos no seguinte hyperlink: https://wazuh.com/blog/detecting-and-responding-to-malicious-files-using-cdb-lists-and-active-response/	O ficheiro é eliminado e foi efetuada uma resposta ativa.	O ficheiro foi eliminado com resposta ativa.
9	Conformidade Regulamentar	Verificar se são fornecidos relatório e painéis que ajudam com certos regulamentos	No dashboard do Wazuh Manager, "Modules", aceder às opções: PC DSS (regulamentos para pagamentos online), NIST 800-53 (regulamentos para sistemas de informação) e GDPR (proteção de dados) e visualizar as informações em cada uma destas opções.	Em cada uma destas opções são mostrados gráficos com informação sobre cada um dos regulamentos.	Em todas as opções são demonstradas informações visualmente sobre cada um dos regulamentos.
10	NID	Num agente com o Suricata configurado, verificar se, por exemplo, um ping é detetado pelo Wazuh Manager.	Num agente com o Suricata configurado, efetuar um ping através do comando: ping -c 20 "<UBUNTU_IP>"	No Wazuh Manager é detetado e alertado esse ping.	No Wazuh Manager foi detetado e alertado esse ping.

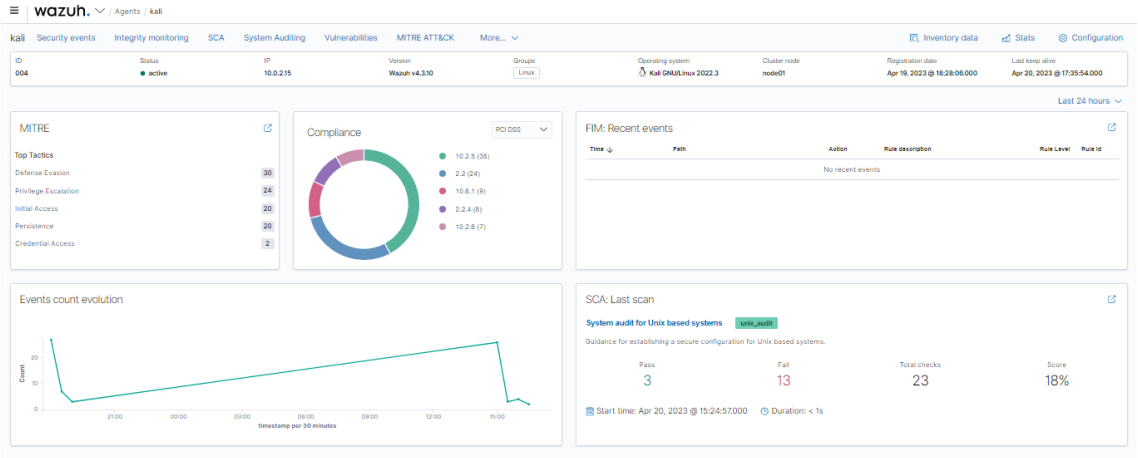

Figura 33 - Teste 1

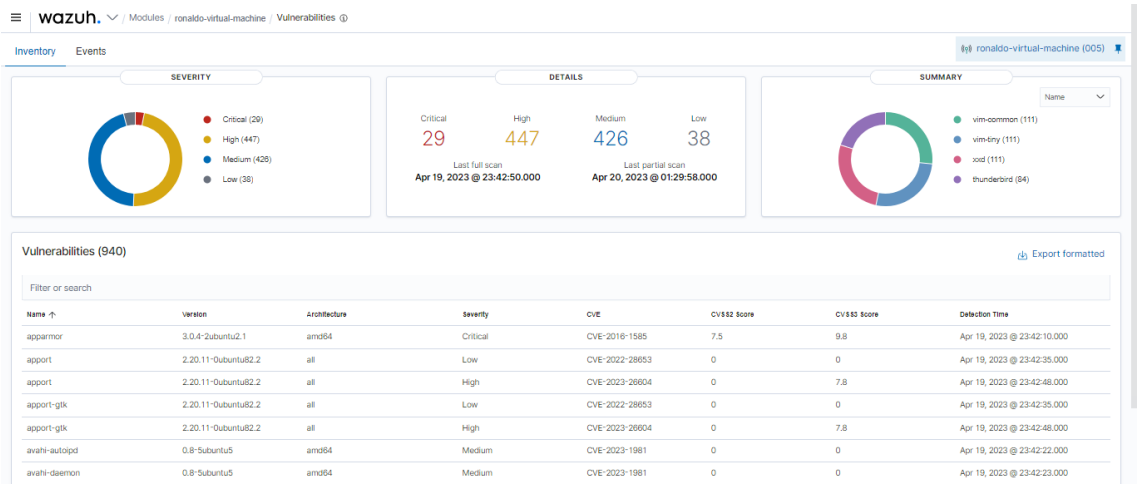

Figura 34 - Teste 2

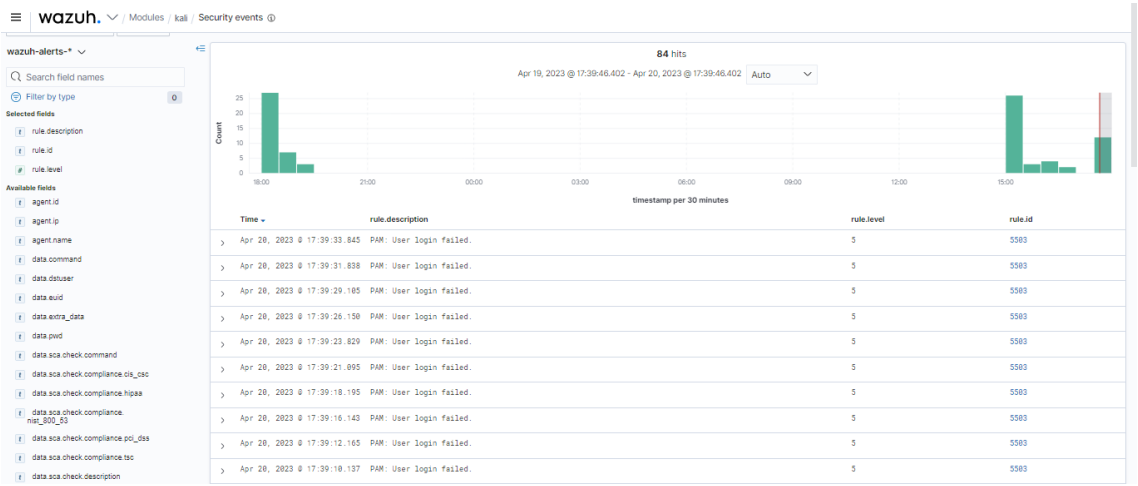

Figura 35 - Teste 3

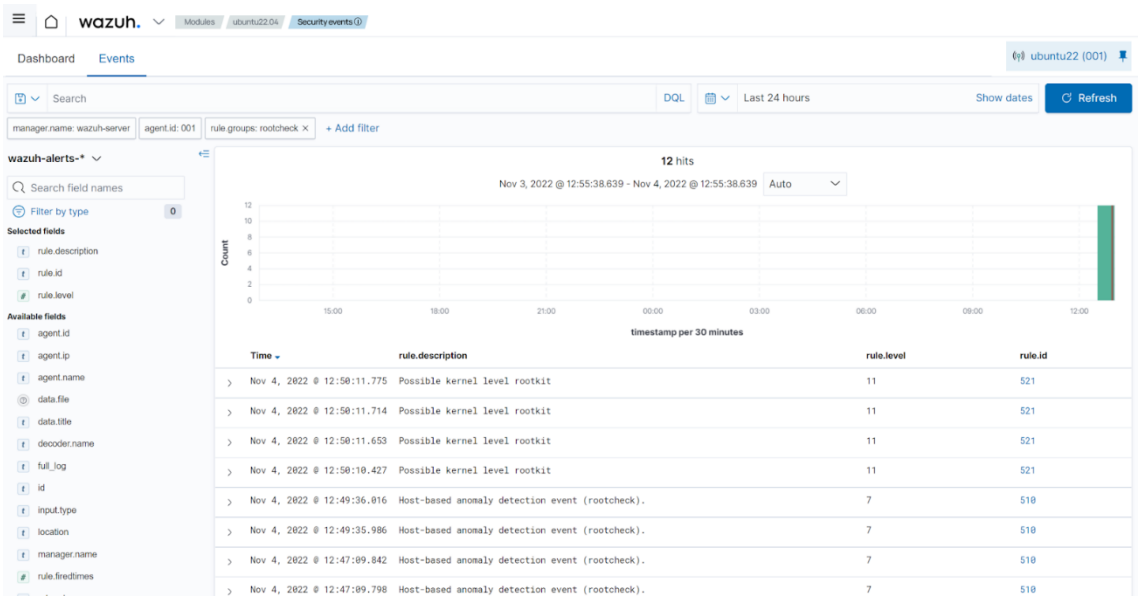

Figura 36 - Teste 4

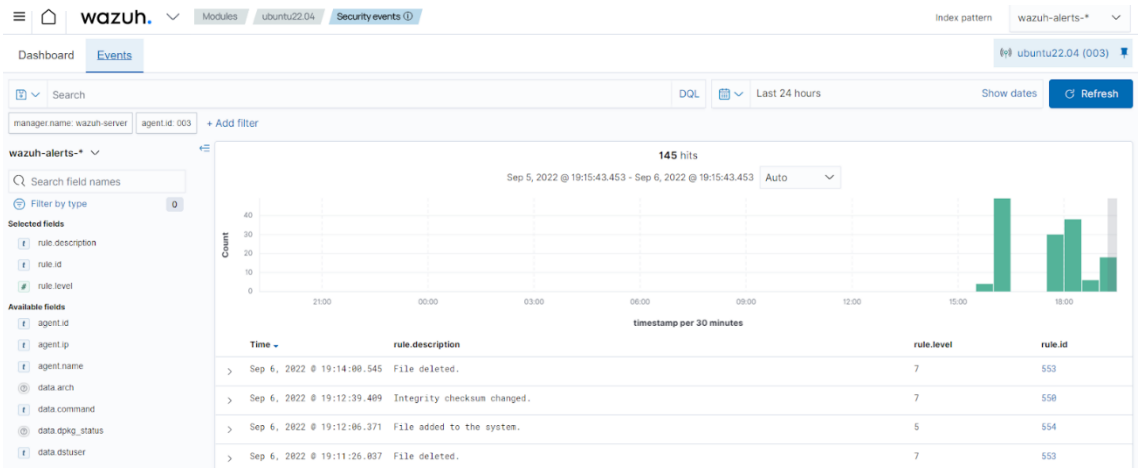

Figura 37 - Teste 5

Figura 38 - Teste 6

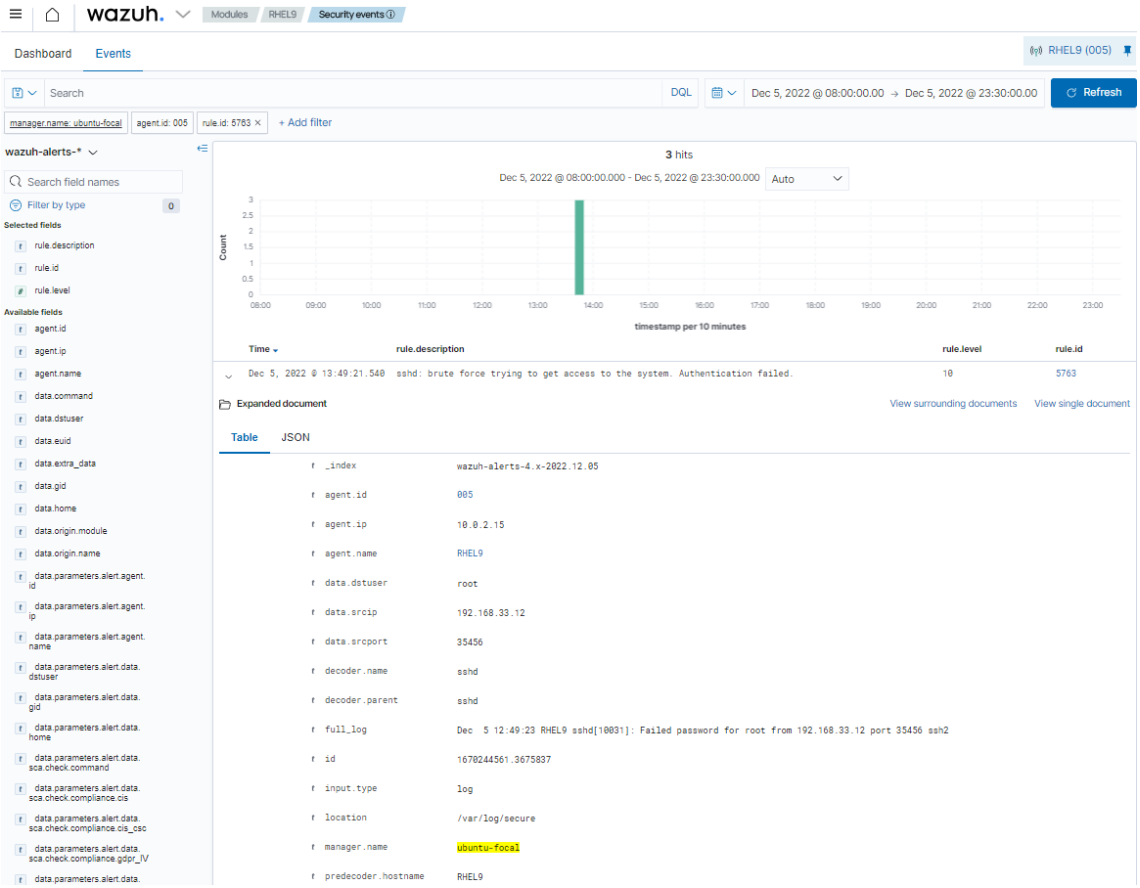

Figura 39 - Teste 7

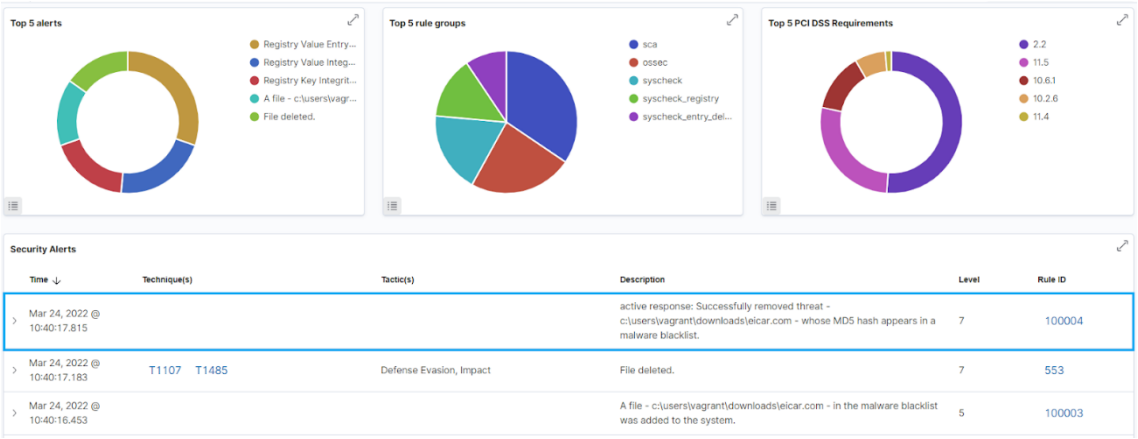

Figura 40 - Teste 8

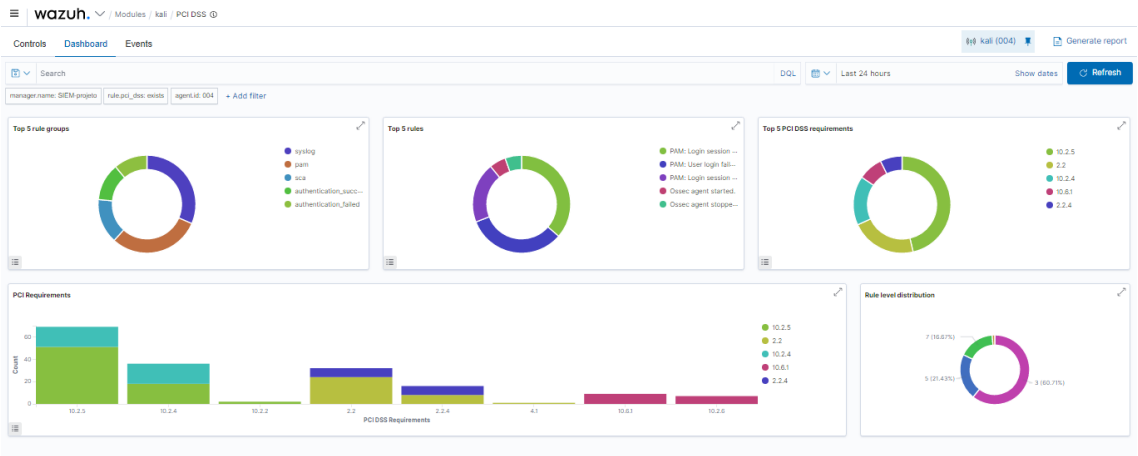

Figura 41 - Teste 9

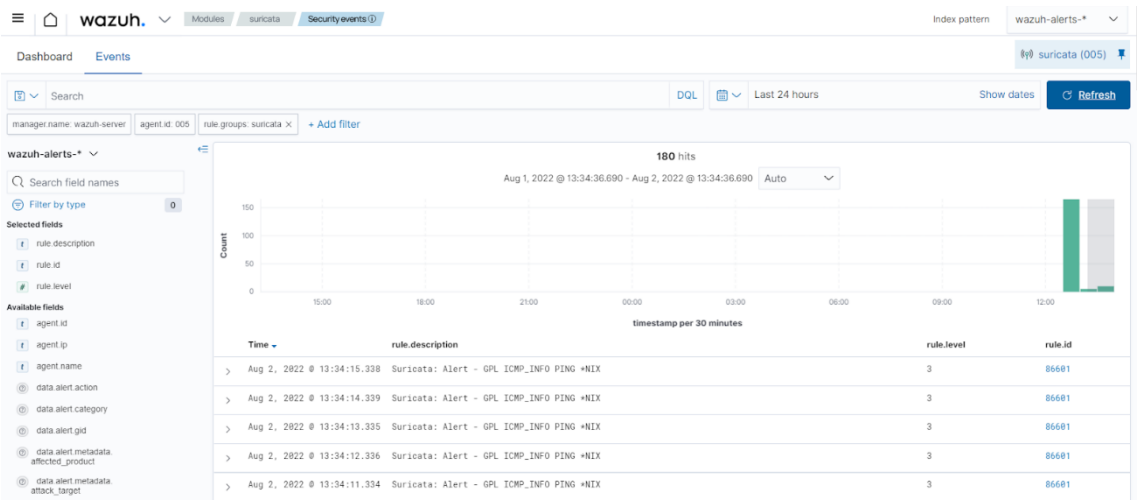

Figura 42 - Teste 10

7.2 Testes de Logs

Para além dos testes básicos no Wazuh, decidimos também, através da ferramenta de Log Testing, *"Ruleset Test"*. Podemos aceder a esta ferramenta através da consola do servidor local do nosso Wazuh, mas para efeitos de melhor visualização utilizámos a versão Web.

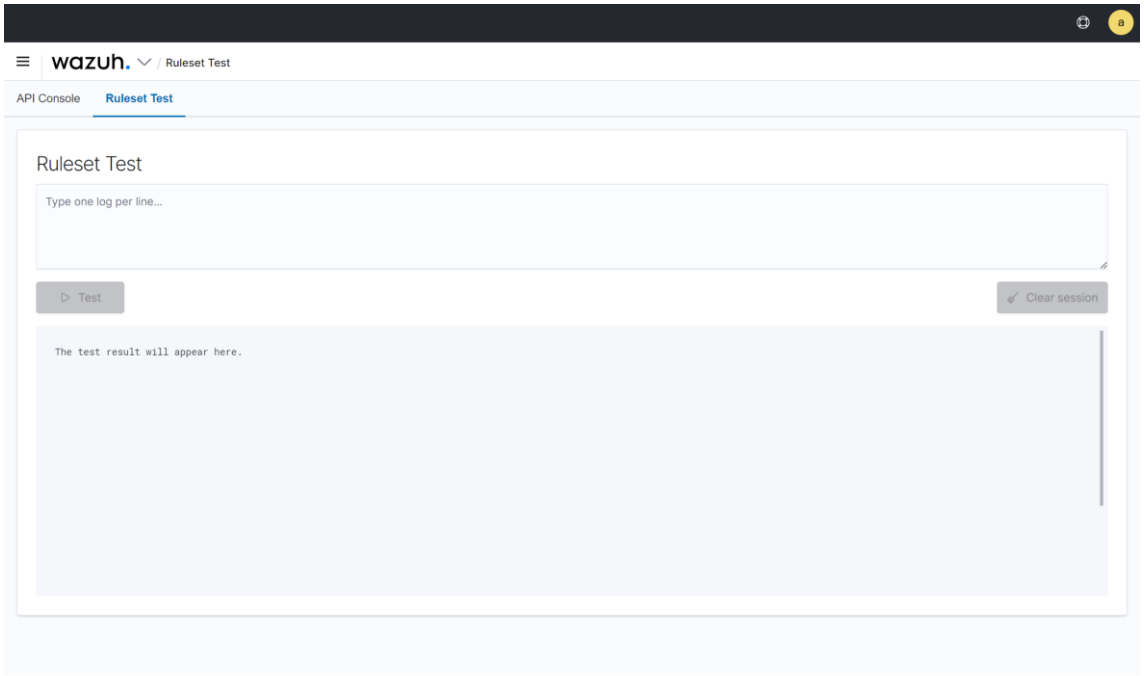

Figura 43 - Ecrã de Logtest

No nosso ficheiro de configuração do Wazuh Manager, temos uma configuração em que só são demonstrados alertas para eventos com uma importância igual ou superior a 5, de modo a evitar um spam por parte dos eventos, como é possível ver, na secção 5.4.1.4.

Estes testes não são possíveis de visualizar em nenhum diretório, pois são apenas testes, de certa forma "hipotéticos" e apenas podemos interpretar o output retornado. Para uma melhor organização dos logs, atribuímos, entre os dois participantes do grupo, números aos logs.

Os logs que testámos seguem geralmente (com exceção dos logs provenientes do pfSense) a seguinte composição:

<Timestamp> <Hostname> <Log Source>: <Message>

Onde, *"Timestamp"* se refere à data em que o log foi registado, *"Hostname"* o hostname do sistema em que o log foi registado, *"Logsource"* é a fonte, dentro do sistema, de onde provém o log e a *"Message"* diz respeito ao seu conteúdo.

O output destes logs é composto por três fases:

1. **Pre-deconding:** Pode envolver tarefas como divisão do log, extração da data, identificação do host ou sistema que originou o log e determinar o programa ou o serviço responsável. O objetivo desta fase é extrair a informação necessária para uma análise posterior.

2. **Decoding:** Os atributos do log são extraídos para os campos necessários. Neste processo é feita uma nova divisão do log, de modo a obter, por exemplo, usernames, endereços IP, ports, o tipo do log, a descrição do evento, entre outras informações relevantes. Os campos resultantes são importantes para poder obter um contexto do log.
3. **Filtragem:** Nesta fase o log é processado através das regras definidas, de modo a determinar a sua importância. Estas regras podem variar bastante, dependendo do nível de segurança do log, descrições de eventos específicas ou outras regras personalizadas. Se o evento corresponder a alguma destas regras, é lhe atribuída uma importância.

Os logs provenientes da firewall pfSense têm a mesma composição com exceção da mensagem, que contém a seguinte formatação:

<numero da regra>,<id do evento>,<interface>,<match de uma regra>,<pacote bloqueado pela firewall>,<direção do tráfego>,<versão do IP>,<flags>,<valor TTL (Time to Live)>,<comprimento do pacote>,<valor checksum>,<nome da queue do evento>,<protocolo>,<detalhes do protocolo>,<tamanho do pacote>,<IP da fonte>,<IP destino>

7.2.1 LOG0

Input:

```
Jun 17 00:01:41 ip-10-0-1-175 sshd[21746]: Failed password for root from 61.177.172.13 port 61658 ssh2
```

Este log indica uma falha de password para o utilizador *"root"*, cujo IP é 10.0.1.175, utilizando a port 61658, através de um serviço SSH.

A log source *"sshd"* refere-se ao Secure Shell daemon, responsível por gerir conexões SSH. O número entre parênteses retos *"[21746]"* corresponde ao número do processo (PID) do SSH daemon.

No final da mensagem aparece *"ssh2"*, que corresponde à versão do protocolo SSH utilizado.

Este log pode significar um potencial acesso não autorizado ou até um ataque brute force a um sistema.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 00:01:41 ip-10-0-1-175 sshd[21746]: Failed password for root from 61.177.172.13 port 61658 ssh2'
        timestamp: 'Jun 17 00:01:41'
        hostname: 'ip-10-0-1-175'
        program_name: 'sshd'

**Phase 2: Completed decoding.
```

```
        name: 'sshd'
        parent: 'sshd'
        dstuser: 'root'
        srcip: '61.177.172.13'
        srcport: '61658'

**Phase 3: Completed filtering (rules).
        id: '5760'
        level: '5'
        description: 'sshd: authentication failed.'
        groups: '["syslog","sshd","authentication_failed"]'
        firedtimes: '1'
        gdpr: '["IV_35.7.d","IV_32.2"]'
        gpg13: '["7.1"]'
        hipaa: '["164.312.b"]'
        mail: 'false'
        mitre.id: '["T1110.001","T1021.004"]'
        mitre.tactic: '["Credential Access","Lateral Movement"]'
        mitre.technique: '["Password Guessing","SSH"]'
        nist_800_53: '["AU.14","AC.7"]'
        pci_dss: '["10.2.4","10.2.5"]'
        tsc: '["CC6.1","CC6.8","CC7.2","CC7.3"]'
**Alert to be generated.
```

Dado o nível de importância atribuído a este evento (5), será gerado um alerta, com o output "sshd: authentication failed."

7.2.2 LOG1

Input:

```
Jun 16 17:06:00 tfculht-VirtualBox sshd[29205]: Invalid user messi from 18.18.18.18 port 48928
```

Este log significa uma tentativa falhada de um nome de utilizador *"messi"*, proveniente do IP 18.18.18.18, utilizando a porta 48928, através de um serviço SSH.

Este log indica, geralmente, acesso não autorizado ou tentativas de scanning. Nestes casos, se necessário, podem ser implementados mecanismos de autenticação fortes ou bloquear IPs suspeitos.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 16 17:06:00 tfculht-VirtualBox sshd[29205]: Invalid user messi from 18.18.18.18 port 48928'
        timestamp: 'Jun 16 17:06:00'
        hostname: 'tfculht-VirtualBox'
        program_name: 'sshd'
```

```
**Phase 2: Completed decoding.
        name: 'sshd'
        parent: 'sshd'
        srcip: '18.18.18.18'
        srcport: '48928'
        srcuser: 'messi'

**Phase 3: Completed filtering (rules).
        id: '5710'
        level: '5'
        description: sshd: authentication failed.
        groups: '["syslog","sshd","authentication_failed","invalid_login"]'
        firedtimes: '1'
        gdpr: '["IV_35.7.d","IV_32.2"]'
        gpg13: '["7.1"]'
        hipaa: '["164.312.b"]'
        mail: 'false'
        mitre.id: '["T1110.001","T1021.004","T1078"]'
        mitre.tactic: '["Credential Access","Lateral Movement","Defense
Evasion","Persistence","Privilege Escalation","Initial Access"]'
        mitre.technique: '["Password Guessing","SSH","Valid Accounts"]'
        nist_800_53: '["AU.14","AC.7","AU.6"]'
        pci_dss: '["10.2.4","10.2.5","10.6.1"]'
        tsc: '["CC6.1","CC6.8","CC7.2","CC7.3"]'

**Alert to be generated.
```

Dado o nível de importância atribuído a este evento (5), será gerado um alerta com a mensagem "sshd: authentication failed."

7.2.3 Log2

Input:

```
Jun 17 10:32:45 server1 kernel: [12345.678] Out of memory: Kill process 1234 (myapp)
score=789 and restart
```

Este log indica que um sistema com nome *"server1"* enfrentou uma situação de *"Out of memory"* e terminou um determinado processo, cujo PID é 1234, nomeado de *"myapp"*.

A log source *"kernel"* corresponde à componente núcleo do sistema operativo.

De modo a aliviar a pressão na memória, o sistema decidiu terminar o processo referido acima. O termo *"score"* refere-se à métrica associada ao processo. No final deste log podemos observar que o sistema irá reiniciar, através do termo *"restart"*, de modo a recuperar da falta de memória.

Este tipo de logs são importantes de monitorizar, de modo a manter a estabilidade do sistema e evitar problemas.

Output:

```
**Phase 1: Completed pre-decoding.
```

```
        full event: 'Jun 17 10:32:45 server1 kernel: [12345.678] Out of memory: Kill process
1234 (myapp) score=789 and restart'
        timestamp: 'Jun 17 10:32:45'
        hostname: 'server1'
        program_name: 'kernel'

**Phase 2: Completed decoding.
        name: 'kernel'

**Phase 3: Completed filtering (rules).
        id: '5108'
        level: '12'
        description: 'System running out of memory. Availability of the system is in risk.'
        groups: '["syslog","linuxkernel","service_availability"]'
        firedtimes: '1'
        gdpr: '["IV_35.7.d"]'
        gpg13: '["4.12"]'
        hipaa: '["164.312.b"]'
        mail: 'true'
        mitre.id: '["T1499"]'
        mitre.tactic: '["Impact"]'
        mitre.technique: '["Endpoint Denial of Service"]'
        nist_800_53: '["AU.6"]'
        pci_dss: '["10.6.1"]'
        tsc: '["CC7.2","CC7.3"]'

**Alert to be generated.
```

Dado o nível de importância atribuído a este evento (12), será gerado um alerta com a mensagem "System running out of memory. Availability of the system is in risk."

7.2.4 Log3

Input:

```
Jun 17 12:34:56 pfsense filterlog:
2,,,1000000103,igb0,match,block,in,4,0x0,,64,12678,0,none,1,icmp,56,192.168.1.10,8.8.8.8,
,
```

Evento proveniente da firewall pfSense.

A log source *"filterlog"* refere-se à funcionalidade de filtragem de pacotes da pfSense que recolhe informação sobre o tráfego na rede.

A mensagem pode ser repartida pelas suas componentes:

2: Número da regra ou identificador associado ao evento.

1000000103: Identificador único do evento ou número de referência.

igb0: Interface onde o evento ocorreu.

match: O pacote correspondeu a uma regra e ativou um evento.

block: O pacote foi bloqueado ou negado pela firewall.

in: Direção do tráfego, neste caso, *inbound*.

4: Versão do IP, neste caso IPv4.

0x0: Flags do pacote.

64: Valor TTL (Time to Live) do pacote.

12678: Comprimento do pacote.

0: Valor checksum.

none: Nome da fila associada ao evento.

1: Protocolo utilizador pelo pacote, neste caso ICMP.

icmp: Detalhes do protocol, ICMP neste exemplo.

56: Tamanho do pacote.

192.168.1.10: Endereço IP da fonte.

8.8.8.8: Endereço IP destino.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 12:34:56 pfsense filterlog:
2,,,1000000103,igb0,match,block,in,4,0x0,,64,12678,0,none,1,icmp,56,192.168.1.10,8.8.8.8,
,'
        timestamp: 'Jun 17 12:34:56'
        hostname: 'pfsense'
        program_name: 'filterlog'

**Phase 2: Completed decoding.
        name: 'pf'
        action: 'block'
        dstip: '8.8.8.8'
        id: '1000000103'
        protocol: 'icmp'
        srcip: '192.168.1.10'

**Phase 3: Completed filtering (rules).
        id: '87701'
        level: '5'
        description: 'pfSense firewall drop event.'
        groups: '["pfsense","firewall_block"]'
        firedtimes: '1'
        gpg13: '["4.12"]'
        hipaa: '["164.312.a.1"]'
        mail: 'false'
        nist_800_53: '["SC.7"]'
        pci_dss: '["1.4"]'
        tsc: '["CC6.7","CC6.8"]'
```

```
**Alert to be generated.
```

Alerta gerado associado com o bloqueamento da firewall. Nivel 5, então gera um alerta com a mensagem "pfSense firewall drop event."

7.2.5 LOG4

Input:

```
Jun 17 14:20:30 pfsense filterlog: 4,,,1000000101,igb1,match,pass,out,6,0x0,,116,0,0,DF,1,tcp,40,192.168.1.20,203.0.113.10,1234,80,0x0
```

Este log representa um pacote TCP originário do IP 192.168.1.20 na porta 1234 que foi permitido para um endereço IP de destino externo 203.0.113.10 na porta 80 (HTTP) através da interface exterior igb1. O pacote tem um IPv6, um TTL de 116 e flags do TCP 0x0.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 14:20:30 pfsense filterlog: 4,,,1000000101,igb1,match,pass,out,6,0x0,,116,0,0,DF,1,tcp,40,192.168.1.20,203.0.113.10,1234,80,0x0'
        timestamp: 'Jun 17 14:20:30'
        hostname: 'pfsense'
        program_name: 'filterlog'

**Phase 2: Completed decoding.
        name: 'pf'
        action: 'pass'
        dstip: '203.0.113.10'
        dstport: '80'
        id: '1000000101'
        length: '0'
        protocol: 'tcp'
        srcip: '192.168.1.20'
        srcport: '1234'

**Phase 3: Completed filtering (rules).
        id: '87700'
        level: '0'
        description: 'pfSense firewall rules grouped.'
        groups: '["pfsense"]'
        firedtimes: '1'
        mail: 'false'
```

Este evento não irá gerar nenhum alerta, dado o seu nível de importância (0).

7.2.6 LOG5

Input:

```
Jun 17 15:45:12 pfsense filterlog:
2,,,1000000104,igb0,match,block,in,4,0x0,,64,12345,0,none,17,udp,60,192.168.1.30,8.8.4.4,
5000,53,0x0
```

Log proveniente da firewall pfSense e indica que um pacote UDP, originário do endereço IP 192.168.1.30 na porta 5000 foi bloqueado, numa tentativa de comunicação com um IP de destino 8.8.4.4 na porta 53 (DNS) através da interface igb0. O pacote tem um IPv4, um TTL de 64 e flags de UDP 0x0.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 15:45:12 pfsense filterlog:
2,,,1000000104,igb0,match,block,in,4,0x0,,64,12345,0,none,17,udp,60,192.168.1.30,8.8.4.4,
5000,53,0x0'
        timestamp: 'Jun 17 15:45:12'
        hostname: 'pfsense'
        program_name: 'filterlog'

**Phase 2: Completed decoding.
        name: 'pf'
        action: 'block'
        dstip: '8.8.4.4'
        dstport: '53'
        id: '1000000104'
        length: '0'
        protocol: 'udp'
        srcip: '192.168.1.30'
        srcport: '5000'

**Phase 3: Completed filtering (rules).
        id: '87701'
        level: '5'
        description: 'pfSense firewall drop event.'
        groups: '["pfsense","firewall_block"]'
        firedtimes: '1'
        gpg13: '["4.12"]'
        hipaa: '["164.312.a.1"]'
        mail: 'false'
        nist_800_53: '["SC.7"]'
        pci_dss: '["1.4"]'
        tsc: '["CC6.7","CC6.8"]'
**Alert to be generated.
```

Dado o nível do evento (5), será gerado um alerta com a mensagem "pfSense firewall drop event".

7.2.7 LOG6

Input:

```
Jun 17 16:55:43 pfsense filterlog: 4,,,1000000102,igb2,match,pass,out,6,0x0,,150,0,0,DF,1,tcp,52,192.168.1.40,104.18.22.72,4321,443,0x0
```

Log proveniente da firewall pfSense, que indica um pacote TCP originário do endereço IP 192.168.1.40 na porta 4321 foi permitido para um endereço IP externo 104.18.22.72 na porta 443 (HTTPS) através da interface igb2. O pacote tem um IPv6, um TTL de 150 e flags TCP 0x0.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 16:55:43 pfsense filterlog: 4,,,1000000102,igb2,match,pass,out,6,0x0,,150,0,0,DF,1,tcp,52,192.168.1.40,104.18.22.72,4321,443,0x0'
        timestamp: 'Jun 17 16:55:43'
        hostname: 'pfsense'
        program_name: 'filterlog'

**Phase 2: Completed decoding.
        name: 'pf'
        action: 'pass'
        dstip: '104.18.22.72'
        dstport: '443'
        id: '1000000102'
        length: '0'
        protocol: 'tcp'
        srcip: '192.168.1.40'
        srcport: '4321'

**Phase 3: Completed filtering (rules).
        id: '87700'
        level: '0'
        description: 'pfSense firewall rules grouped.'
        groups: '["pfsense"]'
        firedtimes: '1'
        mail: 'false'
```

O evento não irá gerar nenhum alerta, dada a sua importância (0).

7.2.8 LOG7

Input:

```
Jun 17 16:38:27 server4 audit: USER_LOGIN_SUCCESS, username: goncalo, source_ip: 192.168.0.200
```

Log de um audit log (registo de eventos de segurança) que regista um login com sucesso de um utilizador *"goncalo"*, a partir de um endereço IP 192.168.0.200.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 16:38:27 server4 audit: USER_LOGIN_SUCCESS, username:
goncalo, source_ip: 192.168.0.200'
        timestamp: 'Jun 17 16:38:27'
        hostname: 'server4'
        program_name: 'audit'

**Phase 2: Completed decoding.
        name: 'solaris_bsm'

**Phase 3: Completed filtering (rules).
        id: '6100'
        level: '0'
        description: 'Solaris BSM Auditing messages grouped.'
        groups: '["syslog","solaris_bsm"]'
        firedtimes: '1'
        mail: 'false'
```

Evento com importância 0, que não irá gerar nenhum alerta.

7.2.9 LOG8

Input:

```
Jun 17 12:34:56 server1 apache: [error] [client 192.168.0.100] File does not exist:
/var/www/html/page-not-found
```

Este log indica que um cliente com um endereço IP 192.168.0.100 efetuou um pedido para o servidor web Apache, hospedado em *"server1"*, para um ficheiro *"page-not-found"* localizado em *"/var/www/html/"*. O servidor não conseguiu encontrar o ficheiro pedido e retornou um erro que indica que não existe.

O termo *[error]* especifica o nível de importância do log, que neste caso é um erro.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 12:34:56 server1 apache: [error] [client 192.168.0.100] File does
not exist: /var/www/html/page-not-found'
        timestamp: 'Jun 17 12:34:56'
        hostname: 'server1'
        program_name: 'apache'

**Phase 2: Completed decoding.
        name: 'web-accesslog'

**Phase 3: Completed filtering (rules).
```

```
        id: '31100'
        level: '0'
        description: 'Access log messages grouped.'
        groups: '["web","accesslog"]'
        firedtimes: '1'
        mail: 'false'
```

Não será gerado nenhum alerta, pois o nível de importância é 0.

7.2.10 LOG9

Input:

```
Jun 17 14:15:22 server2 sshd[1234]: Failed password for user suspeito from 192.168.0.150 port 54321 ssh2
```

Log que indica uma tentativa de password falhada durante uma sessão de login SSH no *server2*. O utilizador *"impostor"* tentou efetuar um login a partir do endereço IP 192.162.0.150 na porta 54321, utilizando SSH versão 2, mas a password inserida estava incorreta.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 14:15:22 server2 sshd[1234]: Failed password for user impostor from 192.168.0.150 port 54321 ssh2'
        timestamp: 'Jun 17 14:15:22'
        hostname: 'server2'
        program_name: 'sshd'

**Phase 2: Completed decoding.
        name: 'sshd'
        parent: 'sshd'

**Phase 3: Completed filtering (rules).
        id: '5760'
        level: '5'
        description: 'sshd: authentication failed.'
        groups: '["syslog","sshd","authentication_failed"]'
        firedtimes: '1'
        gdpr: '["IV_35.7.d","IV_32.2"]'
        gpg13: '["7.1"]'
        hipaa: '["164.312.b"]'
        mail: 'false'
        mitre.id: '["T1110.001","T1021.004"]'
        mitre.tactic: '["Credential Access","Lateral Movement"]'
        mitre.technique: '["Password Guessing","SSH"]'
        nist_800_53: '["AU.14","AC.7"]'
        pci_dss: '["10.2.4","10.2.5"]'
        tsc: '["CC6.1","CC6.8","CC7.2","CC7.3"]'

**Alert to be generated.
```

Dado o nível de importância (5), será gerado um alerta, com a mensagem "sshd: authentication failed."

7.2.11 LOG10

Input:

```
Jun 17 16:30:45 dns-server named[5678]: client 192.168.0.100#1234: query 'example.com' denied
```

Log que indica que um cliente com um endereço IP 192.168.0.100 na porta 1234 efetuou uma query DNS para o domínio *"exemple.com"* para o servidor DNS nomeado. O servidor DNS negou esta query, indicando que não preenche o pedido ou contém as políticas configuradas para essa query específica.

O termo *"named[5678]"* indica que esta log entry é proveniente de um servidor DNS nomeado especificamente para este processo com um PID 5678.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 17 16:30:45 dns-server named[5678]: client 192.168.0.100#1234: query 'example.com' denied'
        timestamp: 'Jun 17 16:30:45'
        hostname: 'dns-server'
        program_name: 'named'

**Phase 2: Completed decoding.
        name: 'named'
        parent: 'named'
        srcip: '192.168.0.100'

**Phase 3: Completed filtering (rules).
        id: '12100'
        level: '0'
        description: 'Grouping of the named rules'
        groups: '["syslog","named"]'
        firedtimes: '1'
        mail: 'false'
```

Não será gerado nenhum alerta, dado o nível de importância 0.

7.2.12 LOG11

Input:

```
Jun 22 10:12:45 ronaldo-virtual-machine login: pam_unix(login:session): session opened for user ronaldo by (uid=0)
```

Este log indica uma tentativa de login bem sucedida num sistema nomeado *"ronaldo-virtual-machine"*. O utilizador *"ronaldo"* abriu a sessão e o evento foi iniciado pelo utilizador root (UID 0).

O termo *"pam_unix(login:session)"* especifica o módulo PAM (Pluggable Authentication Modules) responsável pelo processo de autenticação.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 10:12:45 ronaldo-virtual-machine login: pam_unix(login:session):
session opened for user ronaldo by (uid=0)'
        timestamp: 'Jun 22 10:12:45'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'login'

**Phase 2: Completed decoding.
        name: 'pam'
        parent: 'pam'
        dstuser: 'ronaldo'
        uid: '0'

**Phase 3: Completed filtering (rules).
        id: '5501'
        level: '3'
        description: 'PAM: Login session opened.'
        groups: '["pam","syslog","authentication_success"]'
        firedtimes: '1'
        gdpr: '["IV_32.2"]'
        gpg13: '["7.8","7.9"]'
        hipaa: '["164.312.b"]'
        mail: 'false'
        mitre.id: '["T1078"]'
        mitre.tactic: '["Defense Evasion","Persistence","Privilege Escalation","Initial
Access"]'
        mitre.technique: '["Valid Accounts"]'
        nist_800_53: '["AU.14","AC.7"]'
        pci_dss: '["10.2.5"]'
        tsc: '["CC6.8","CC7.2","CC7.3"]'
```

Não será gerado nenhum alerta, pois o nível de importância deste evento é 3, e apenas são gerados alertas para valores maiores ou iguais a 5.

7.2.13 LOG12

Input:

```
Jun 22 10:30:45 ronaldo-virtual-machine sshd[1234]: Accepted publickey for ronaldo from
192.168.0.100 port 1234 ssh2
```

Este log indica uma conexão SSH aceite no sistema *"ronaldo-virtual-machine"*. O utilizador *"ronaldo"* efetuou uma autenticação com sucesso com recurso à chave pública originada pelo endereço IP 192.168.0.100 na porta 1234 utilizando um protocolo SSH de versão 2 (SSH2).

O termo *"Accepted public key for ronaldo"* indica que a método de autenticação da chave pública foi utilizado com sucesso para o utilizador *"ronaldo"*.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 10:30:45 ronaldo-virtual-machine sshd[1234]: Accepted publickey
for ronaldo from 192.168.0.100 port 1234 ssh2'
        timestamp: 'Jun 22 10:30:45'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'sshd'

**Phase 2: Completed decoding.
        name: 'sshd'
        parent: 'sshd'
        dstuser: 'ronaldo'
        srcip: '192.168.0.100'
        srcport: '1234'

**Phase 3: Completed filtering (rules).
        id: '5715'
        level: '3'
        description: 'sshd: authentication success.'
        groups: '["syslog","sshd","authentication_success"]'
        firedtimes: '1'
        gdpr: '["IV_32.2"]'
        gpg13: '["7.1","7.2"]'
        hipaa: '["164.312.b"]'
        mail: 'false'
        mitre.id: '["T1078","T1021"]'
        mitre.tactic: '["Defense Evasion","Persistence","Privilege Escalation","Initial
Access","Lateral Movement"]'
        mitre.technique: '["Valid Accounts","Remote Services"]'
        nist_800_53: '["AU.14","AC.7"]'
        pci_dss: '["10.2.5"]'
        tsc: '["CC6.8","CC7.2","CC7.3"]'
```

Não será gerado nenhum alerta, pois o nível de importância deste evento é 3, e apenas são gerados alertas para valores maiores ou iguais a 5.

7.2.14 LOG13

Input:

```
Jun 22 11:30:15 ronaldo-virtual-machine kernel: [12345.67890] Example log message from
the kernel.
```

Log proveniente do kernel de uma máquina virtual nomeada *"ronaldo-virtual-machine"*. Este log contém apenas uma mensagem de exemplo vinda do kernel.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 11:30:15 ronaldo-virtual-machine kernel: [12345.67890] Example log message from the kernel.'
        timestamp: 'Jun 22 11:30:15'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'kernel'

**Phase 2: Completed decoding.
        name: 'kernel'
```

Não será gerado nenhum alerta.

7.2.15 LOG14

Input:

```
Jun 22 12:00:15 ronaldo-virtual-machine audit: User 'messi' executed command 'rm -rf /' with elevated privileges.
```

Este log representa um audit event, que indica que um utilizador com nome *"messi"* executou o comando *"rm -rf/"* com privilégios.

Este comando é potencialmente perigoso, utilizado para eliminar ficheiros e diretórios da root de um sistema.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 12:00:15 ronaldo-virtual-machine audit: User 'messi' executed command 'rm -rf /' with elevated privileges.'
        timestamp: 'Jun 22 12:00:15'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'audit'

**Phase 2: Completed decoding.
        name: 'solaris_bsm'

**Phase 3: Completed filtering (rules).
        id: '6100'
        level: '0'
        description: 'Solaris BSM Auditing messages grouped.'
        groups: '["syslog","solaris_bsm"]'
        firedtimes: '1'
        mail: 'false'
```

Este evento não irá gerar nenhum evento dado o seu nível de importância 0, mas deveria apresentar um alerta com o texto "Solaris BSM Auditing messaged grouped."

7.2.16 LOG15

Input:

```
Jun 22 12:30:45 ronaldo-virtual-machine audit: USER_AUTH pid=1234 uid=1000 auid=1000 ses=1 msg='op=login id=ronaldo exe=/usr/bin/login success=yes'
```

Este log representa um evento de autenticação captado por um sistema de audit logs.

O termo *"USER_AUTH"* indica o tipo de evento de autenticação que está a fazer login. Sugere que está a ocorrer uma autenticação de um utilizador.

O termo *"uid=1000"* corresponde ao ID do utilizador autenticado (UID) e *"auid=1000"* ao audit ID (AUID) do mesmo.

"ses=1" corresponde ao ID da sessão associada com o evento de autenticação.

"msg='op=login id=ronaldo exe=/usr/bin/login success=yes'" é uma mensagem adicional que contém detalhes sobre este evento de autenticação. Indica que a operação efetuada foi um login, o ID do utilizador é *"ronaldo"* e o executável utilizado para o login é *"/usr/bin/login"* e o login foi efetuado com sucesso.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 12:30:45 ronaldo-virtual-machine audit: USER_AUTH pid=1234 uid=1000 auid=1000 ses=1 msg='op=login id=ronaldo exe=/usr/bin/login success=yes''
        timestamp: 'Jun 22 12:30:45'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'audit'

**Phase 2: Completed decoding.
        name: 'solaris_bsm'

**Phase 3: Completed filtering (rules).
        id: '6100'
        level: '0'
        description: 'Solaris BSM Auditing messages grouped.'
        groups: '["syslog","solaris_bsm"]'
        firedtimes: '1'
        mail: 'false'
```

Não será gerado nenhum alerta, dado o nível de importância 0.

7.2.17 LOG16

Input:

```
Jun 22 12:45:30 ronaldo-virtual-machine ossec: Alert Level: 7; Rule: File integrity checksum changed; Location: /var/log/system.log; Current checksum: abcdefg; Previous checksum: xyz12345
```

Este log relata um evento de integridade de ficheiros capturado por um sistema de deteção, como o Wazuh. O checksum do ficheiro está localizado em *"var/log/system.log"* e foi alterado de "*xyz12345"* para *"abcdefg"*.

Output:

```
**Phase 1: Completed pre-decoding.
        full event: 'Jun 22 12:45:30 ronaldo-virtual-machine ossec: Alert Level: 7; Rule: File integrity checksum changed; Location: /var/log/system.log; Current checksum: abcdefg; Previous checksum: xyz12345'
        timestamp: 'Jun 22 12:45:30'
        hostname: 'ronaldo-virtual-machine'
        program_name: 'ossec'

**Phase 2: Completed decoding.
        name: 'ossec-alert'
```

Não será gerado nenhum alerta.

8 Conclusões e Projetos Futuros

Combinando as capacidades, que só por si o Wazuh possui, com as capacidades de Firewalls do pfSense, foi possível termos uma melhor compreensão de como ajudar empresas a monitorizar e analisar uma rede, respondendo a potenciais incidentes de segurança em tempo-real.

A ferramenta Wazuh teve um papel de monitor central de segurança e gestor de Logs, coletando e analisando os logs dos diferentes agentes pertencentes à rede, bem como de si mesmo. Utilizando as suas capacidades de correlação e análise, é então possível analisar anomalias num sistemas que possam indicar ataques, permitindo assim uma equipa de segurança agir perante estas informações, minimizando o risco de ataques serem bem sucedidos e reduzindo o impacto que possa ter numa infraestrutura de rede.

A integração da firewall pfSense permitiu a inclusão de capacidades como filtragem de pacotes e suporte VPN na nossa infraestrutura, controlando o tráfego da rede e mitigando riscos. Felizmente, para esta firewall específica, o Wazuh já reconhece o seu formato de logs, não sendo necessário criarmos um decoder para traduzir os logs para o Wazuh.

Em suma, a combinação do Wazuh com o pfSense provou ser uma poderosa solução para melhorar a segurança de uma rede, a deteção de ameaças e a resposta às mesmas. Utilizando as capacidades de ambas as ferramentas, foi possível estabelecer uma estrutura de segurança que poderia permitir a PMEs a segurança necessária para se poderem proteger.

Este projeto permitiu-nos mostrar o valor das ferramentas open-source , neste caso na área da cibersegurança. Utilizando estas duas ferramentas, PMEs não necessitam de adquirir licenças de outros produtos, e obtendo uma solução robusta para a proteção da sua rede.

Bibliografia

Nesta bibliografia deixamos algumas referências de vídeos e artigos que consultámos para a concretização deste relatório.

Tabela 5 - Bibliografia

[LOGSTSH]	Vídeo no YouTube que faz um resumo do que é o Logstash, https://www.youtube.com/watch?v=gUJvP2OZENk&ab_channel=SundogEducationwithFrankKane, acedido em out. 2022
[ELASTSC]	Vídeo no YouTube que explica o que é o ElasticSearch, https://www.youtube.com/watch?v=-WF2fQFZ-Uk&ab_channel=EduonixLearningSolutions, acedido em out. 2022
[IBMSIEM]	Secção no site da empresa IBM que explica o que é um sistema SIEM, https://www.ibm.com/topics/siem, acedido em out. 2022
[SIEMCSO]	Artigo do website CSO que resume o que é um sistema SIEM, https://www.csoonline.com/article/2124604/what-is-siem-security-information-and-event-management-explained.html, acedido em out. 2022
[LOGSIEM]	Artigo da LogRhythm que resume o que é um sistema SIEM, https://logrhythm.com/blog/what-is-siem/, acedido em out. 2022
[GARTNER]	Website da Gartner – analistas de mercado de tecnologias de informação, https://www.gartner.com/reviews/market/security-information-event-management, acedido em out. 2022
[FORTSIEM]	Vídeo no YouTube que resume o qué o FortiSIEM, https://www.youtube.com/watch?v=GL6bcOBCbsI&ab_channel=TechnologyAdvice, acedido em out. 2022
[LOGPNT]	Vídeo no YouTube que resume o que é o LogPoint, https://www.youtube.com/watch?v=WKWGyFb1ugM&ab_channel=Logpoint, acedido em out. 2022
[ARCH01]	Artigo do site Exabeam que enumera as componentes de um sistema SIEM, https://www.exabeam.com/explainers/siem/siem-architecture/, acedido em nov. 2022
[ARCH02]	Artigo do site ManageEngine que enumera as componentes de um sistema SIEM, https://www.manageengine.com/log-management/siem/siem-components.html, acedido em nov. 2022
[VELELS]	Artigo do site Velox Softech, com vantagens da utilização do ElasticSearch, https://veloxsoftech.com/blog/benefits-of-using-elasticsearch/, acedido a jan. 2023
[ELSDOC]	Documentação do ElasticSearch, https://www.elastic.co/guide/en/elasticsearch/reference/current/documents-indices.html, acedido a jan. 2023

[REQS]	Artigo com indicações de como realizar o levantamento de requisitos, https://www.cedrotech.com/blog/levantamento-de-requisitos-e-desenvolvimento-de-softwares/, acedido a jan. 2023
[SIEMREQ]	Artigo com requisitos de uma solução SIEM, https://www.frankcardinale.com/2018/10/18/ssiss-a-siem-requirements-gathering-case-study/, acedido a jan. 2023
[WAZUHMIN]	Artigo sobre a ferramenta Wazuh, https://minutodaseguranca.blog.br/wazuh-pode-melhorar-a-seguranca-digital-para-empresas/, acedido a jan. 2023
[CYBERS3C]	Website da empresa de cibersegurança CyberS3c, https://www.cybers3c.pt/
[WAZARQ]	Documentação da arquitetura do Wazuh, https://documentation.wazuh.com/current/getting-started/architecture.html, acedido a jan. 2023
[WAZUSEC]	Documentação dos use cases do Wazuh, https://documentation.wazuh.com/current/getting-started/use-cases/index.html, acedido a jan. 2023
[OSSEC]	Secção "Sobre" no website oficial do OSSEC, https://www.ossec.net/about/, acedido a jan. 2023
[OPENSCAP]	Website oficial das funcionalidades do OpenSCAP, https://www.open-scap.org/features/, acedido a jan. 2023
[SIEMLEVRQ]	Artigo sobre o processo de levantamento de requisitos de uma plataforma SIEM, https://www.scirp.org/html/3-7800617_97094.htm, acedido a jan. 2023
[WAZUHPLAT]	Website oficial da ferramenta Wazuh, com informação sobre a arquitetura e o modelo da plataforma, https://wazuh.com/platform/, acedido a jan. 2023
[GGWAZ]	Google Groups com utilizadores da ferramenta Wazuh, https://groups.google.com/g/wazuh, acedido a jun. 2023.
[CVEWAZ]	Documentação do Wazuh referente aos CVEs, https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/how-it-works.html#:~:text=The%20Wazuh%20server%20automatically%20creates,Hat%20and%20CentOS%20Linux%20distributions, acedido a maio 2023

[WAZLOG]	Documentação do Wazuh referente a Logtest, https://documentation.wazuh.com/current/development/wazuh-logtest.html?highlight=logtest, acedido a jun. 2023
[WAZTEST]	Documentação do Wazuh referente a teste de decoders, https://documentation.wazuh.com/current/user-manual/ruleset/testing.html?highlight=logtest, acedido a jun. 2023

Glossário

1. **Log Data:** Data Logging é o processo de coletar e armazenar dados durante um período de diferentes sistemas e ambientes. Envolve rastreamento de uma variedade de eventos. Coleta de dados sobre um ou vários tópicos específicos e mensuráveis, independentemente do método utilizado
2. **IOC:** Indicator of Compromise é um termo que se refere à evidência num dispositivo que aponta para uma falha de segurança.
3. **Mean Time to Detect:** Medida de tempo que um problema existe num IT deployment antes das entidades apropriadas estarem cientes da sua existência.
4. **Mean Time to Response:** O tempo médio que demora a resvolver completamente uma falha.
5. **Big Data:** Gigante quantidade, velocidade e variedade de dados que precisam ser coletadas.
6. **NoSQL Database:** Bases de dados sem tabelas e armazenam dados diferentemente de tabelas relacionais. Bases de Dados NoSQL vêm com uma variedade de tipos baseadas no seu modelo. Fornecem esquemas flexíveis e são facilmente escaláveis com grandes quantidades de dados.
7. **Dock Containers:** Modo de embalagem e implementação das várias componentes da plataforma Wazuh, de uma forma leve e portátil. Permite correr software num ambiente isolado, separado do sistema hospedeiro.
8. **Active Directory:** Serviço de diretórios da Microsoft geralmente utilizado para armazenar informação sobre utilizadores, dispositivos e outras fontes numa determinada rede. No Wazuh, é utilizado para autenticar a autorizar utilizadores na interface web de utilizadores do Wazuh.
9. **RESTful API:** tipo de arquitetura e conjunto de regras da web que são utilizados quando se cria um determinado web servisse. É baseado num protocolo HTTP eé desenhado para trabalhar com infraestruturas já existentes.
10. **PCI-DSS:** Conjunto de padrões de segurança desenhados para assegurar quetodas as organizações aceitam, processam e armazenam informações de cartões de crédito num ambiente seguro.
11. **Signature-based Detection:** Método de identificação de atividade maliciosanuma rede ou num dispositivo através de padrões específicos de sinais de comportamentos maliciosos conhecidos.
12. **Protocol Anomaly Detection:** Método de identificação de atividade maliciosanuma rede ou num dispositivo através de desvios dos padrões normais da atividade no tráfego de uma rede.
13. **Mensagens de registos:** Registos de eventos que ocorrem num sistema ou numa aplicação. Geralmente incluem informação como o tempo em que o evento ocorreu, a fonte do evento e uma descrição.
14. **Fortinet:** A Fortinet protege grandes empresas e organizações governamentais mundialmente. Capacita os seus clientes com informação, proteção contínua. A arquitetura Fortinet Security fabric pode fornecer segurança sem compromisso para enfrentar os desafios de segurança mais altos, quer na rede, aplicação, cloud ou ambientes móveis. A Fortinet ocupa o primeiro lugar entre os dispositivos de segurança mais vendidos em todo o mundo com mais de 500.000 que confiam na Fortinet para proteger os seus negócios.
15. **SOC:** Um Security Operations Center (Centro de Operações de Segurança) tem a função de monitorizar, prever, detetar, investigar e responder a ciberataques a qualquer hora.

Equipas SOC são encarregues de monitorizar e proteger os ativos de uma organização, incluindo propriedade intelectual, dados pessoais e a integridade da marca.

16. **Amazon Web Services:** AWS é uma plataforma de serviços de computação em nuvem, que formam uma plataforma oferecida pela Amazon. Os serviços são oferecidos em várias áreas geográficas espalhadas pelo mundo.
17. **Real-Time Event Correlation Engine:** permite uma gestão proativa de ameaças instantâneas. O Correlation Engine processa todos os log data à volta da tua rede e correlaciona milhões de eventos simultaneamente e deteta automaticamente e alerta-te acerca da anomalia.
18. **Machine Learning:** Ramo da inteligência artificial que faz uso de modelos estatísticos para desenvolver previsões. É geralmente descrito como a forma de modelagem preditiva ou análise preditiva e tradicional, tem sido definida como a habilidade de um computador aprender sem ser explicitamente programado para o fazer.
19. **SOAR:** Tecnologia Security Orchestration, Automation and Response ajuda na coordenação, execução e automação de tarefas entre várias pessoas e ferramentas, todas numa única plataforma. Isto permite as organizações de não só responder rapidamente a ciberataques mas também observar, compreender e prever futuros incidentes, também melhorando a sua segurança geral.
20. **Threat Intelligence Cloud:** reúne uma abundância de dados à volta de cada ameaça identificada. Estes dados são então conectados a outras ameaças e vetores que partilham similaridades, contextualizando ataques na rede individual da empresa.
21. **CMDB:** Configuration Management Database é uma base de dados cujo propósito principal é de fornecer uma única fonte de verdade ao Serviço de Gestão de IT de uma organização, guardando informação de infraestruturas. Um CMDB contém informação acerca de cada asset, incluindo a sua histórica, localização, dono, função e relação com outros assets.
22. **Threat Intelligence:** Informação de ameaças que foram agregadas, transformadas, analisadas, interpretadas e enriquecidas para fornecer o contexto necessário para processos de decision-making.
23. **Hunting Playbook:** Projeto open-source conduzido pela comunidade, com o objetivo de partilhar lógica de deteção, ofício adversário e recursos para tornar o desenvolvimento de deteções mais eficiente.
24. **SAP:** Segurança Systems Applications and Products é um meio de proteger os dados de uma empresa e os sistemas, monitorizando e controlando o acesso interna e externamente. Sistemas SAP são o tipo de software ERP[25] utilizado largamente por todos os tipos de negócios através de uma variedade de indústrias.
25. **ERP:** Enterprise Resource Planning é um tipo de software que ajuda organizações a automatizar e a gerir processos principais de negócios para otimizar a performance.
26. **Cavalos de Tróia:** Programa malicioso que finge ser inofensivo para fazer com que as pessoas o baixem.
27. **Rootkit:** Coleção de software de computador, projetada para permitir o acesso privilegiado a um computador, ou a uma área do software que não é permitida (por exemplo, a um usuário não autorizado).
28. **Ransomware:** Tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate (ransom) para restabelecer o acesso a estes arquivos.
29. **Zero-Day Attacks:** Termo que descreve vulnerabilidades recentemente descobertas que os hackers utilizam para atacar sistemas. O termo “zero dias” refere-se ao facto de o fornecedor ou o developer acabou de aprender a falha – o que significa que tem “zero dias” para a tratar.

30. **SaaS:** Oferta de software como serviço. Empresas que disponibilizam aplicações pela Internet para a realização de várias tarefas, de forma remota.
31. **Endpoints:** Definição pontos de comunicação de acesso a uma aplicação ou como parte de uma estrutura de segurança de rede.
32. **Watson:** A QRadar Advisor with Watson app utiliza a Inteligência Artificial Cognitiva da IBM para assistir utilizadores com análise de incidentes e riscos, triagem e resposta, e permite equipas de operações de segurança prestarem mais serviços, com maior precisão.
33. **Modelo de Cibersegurança Zero Trust:** Framework de cibersegurança que necessita de todos os utilizadores, dentro ou fora da rede de uma organização, estejam autorizados e validados antes de serem admitidos a acessarem aos dados ou aplicações.
34. **X-Force Exchange:** Os experts em segurança da IBM X-Force utilizam uma série de data centres internos para coletar dezenas de milhares de amostras de malware, analisar páginas web e URLs e correr análises para categorizar potenciais endereços IP maliciosos. A IBM X-Force Exchange é plataforma onde estes dados são partilhados, que pode ser utilizada no IBM QRadar.
35. **Post incident analysis:** Guia para identificação de melhorias da resposta a incidentes, incluindo o tempo de deteção e mitigação.
36. **Unparsed Logging:** Extrair dados de um log longo para que os valores parsed possam ser utilizados como input para outro processo de logging.
37. **Autenticação centralizada:** Sistema em que a autenticação é concentrada num único local. Em vez de cada sistema ter o seu próprio mecanismo de autenticação e armazenamento das credenciais, na autenticação centralizada todos os sistemas compartilham um único ponto de autenticação.