Universidade Politécnica

A Politécnica

Instituto Superior de Gestão, Ciências e Tecnologias (**ISGCT**)

Departamento de Ciências de Engenharia

Licenciatura em Engenharia Informática e de Telecomunicações **(LEIT)**

SEGURANÇA DE REDES DE COMPUTADORES EM AMBIENTES CORPORATIVOS FACE AO TRABALHO REMOTO E HÍBRIDO: DESAFIOS E SOLUÇÕES EM MÉDIAS E GRANDES EMPRESAS DO RAMO DE CONSTRUÇÃO CIVIL

Caso de estudo - Mota-Engil África (Moçambique)

Crícias Carvalho Daúte

Maputo, Maio de 2024

Universidade Politécnica

A Politécnica

Instituto Superior de Gestão, Ciências e Tecnologia (**ISGCT**)

Departamento de Ciências de Engenharia

Licenciatura em Engenharia Informática e de Telecomunicações (**LEIT**)

SEGURANÇA DE REDES DE COMPUTADORES EM AMBIENTES CORPORATIVOS FACE AO TRABALHO REMOTO E HÍBRIDO: DESAFIOS E SOLUÇÕES EM MÉDIAS E GRANDES EMPRESAS DO RAMO DE CONSTRUÇÃO CIVIL

Caso de estudo - Mota-Engil África (Moçambique)

Crícias Carvalho Daúte

Supervisor:

MSc. Edvaldo da Glória Mahesh

Maputo, Maio de 2024

I. PARECER DO SUPERVISOR

Trabalho de Projecto apresentado a Universidade Politécnica – A Politécnica como parte dos requisitos de graduação e obtenção do grau de Licenciatura em Engenharia Informática e de Telecomunicações.

O candidato Crícias Carvalho Daúte, estudante do curso de Licenciatura em Engenharia Informática e de Telecomunicações, nesta Universidade, realizou seu trabalho final na área de Segurança de Redes de Computadores com o tema Segurança de Redes de Computadores em Ambientes Corporativos Face ao Trabalho Remoto e Híbrido: Desafios e Soluções em Médias e Grandes Empresas do Ramo de Construção Civil (Mota-Engil Moçambique), tendo aplicado os conhecimentos adquiridos ao longo da sua formação.

O trabalho desenvolvido cumpre com as normas de escrita e apresentação de trabalhos, desta Universidade, bem como o grau pelo qual se candidata, pelo que eu, Edvaldo Da Glória Mahesh, Supervisor, recomendo a submissão do trabalho para defesa pública conforme as normas da Universidade A Politécnica, abaixo, subscrevo.

_____

Tutor: MSc: Edvaldo Da Glória Mahesh

Maputo, Maio de 2024

II. DECLARAÇÃO DE HONRA

Eu, Crícias Carvalho Daúte declaro que este estudo é resultado da minha pesquisa pessoal e das orientações do meu tutor, feita segundo os critérios em vigor na Universidade Politécnica.

O seu conteúdo é original e este nunca foi submetido antes para a obtenção de nenhum grau ou como avaliação em nenhuma outra instituição de ensino.

_____

Crícias Carvalho Daúte

Maputo, Maio de 2024

III. DEDICATÓRIA

Dedico o presente trabalho a minha mãe, que foi meu maior apoio nos momentos de angústia. Também quero homenagear meu pai, que fez de tudo para a faculdade se tornar um sonho possível.

IV. AGRADECIMENTOS

Com a finalização deste trabalho não posso deixar de agradecer a algumas pessoas que, directa ou indirectamente, me ajudaram neste percurso tão importante da minha vida pessoal e profissional.

Em primeiro agradecer a Deus pela força que me deu, em segundo aos meus pais que nunca deixaram de me apoiar, em terceiro aos meus irmãos e amigos.

Gostaria de dirigir os meus sinceros agradecimentos a todos os elementos da empresa Mota-Engil Moçambique que me acolheram e por todos os conhecimentos que me transmitiram. Endereço os meus sinceros agradecimentos aos meus professores do curso de Licenciatura em Engenharia Informática e de Telecomunicações, pela disponibilidade e competência que demostraram ao longo do curso, disseminando conhecimento.

Agradecimento especial vai ao MSc. Edvaldo Mahesh pela colaboração e acompanhamento durante a realização deste trabalho.

V. RESUMO

A segurança de redes de computadores em ambientes corporativos é um tópico crucial nos dias de hoje. Uma vez que as organizações estão cada vez mais dependentes da tecnologia e enfrentam ameaças cada vez mais sofisticadas, neste estudo se faz a revisão dos estudos de Redes de computadores, Gestão de redes de computadores, onde menciona-se os assuntos de segurança de redes de computadores, *firewalls* e seu papel na protecção da rede, redes virtuais privadas para conexões seguras, autenticação e autorização de usuários, criptografia de dados e comunicações. Por último fala-se da Gestão de Vulnerabilidades e Avaliações de segurança, onde falou-se também das actualizações e *patches* de segurança.

Palavras-chaves: Segurança, Redes de Computadores, Trabalho Remoto, Engenharia Civil.

VI. ABSTRACT

The security of computer networks in corporate environment is a crucial topic these days. Since organizations are increasingly dependent on technology and face increasingly sophisticated threats, this study reviews the issues of Computer networks, Management networks, where it is mentioned the security issues of computer networks, firewalls and their role in protecting the network, virtual private networks for secure connections, authentication and authorization of users, data encryption and communications. Finally, we talk about the Vulnerability management and Security assessment, where security updates and patches were also discussed.

Keywords: Security, Computer Networks, Remote Work, Civil Engineering.

ÍNDICE

Lista de Abreviaturas

AD – Active Directory (Directório Activo)

API – Application Programming Interface (Interface De Programação De Aplicações)

AWS – Amazon Web Service

BYOD – Bring Your Own Device (Traga Seu Próprio Aparelho)

CRE – Custom Rules Engine (Mecanismo De Regras Personalizadas)

CVE – Common Vulnerabilities and Exposures (Vulnerabilidades E Exposições Comuns)

DNS – Domain Name System (Sistema De Nomes De Domínio)

2FA – Two-factor Authentication (Autenticação De Dois Factores)

FIM – File Integrity Monitoring (Monitoramento De Integridade De Arquivos)

HIDS – Host Based Intrusion Detection Systems (Sistemas De Detecção de Intrusão Baseados Em Host)

HTTPS – Hyper Text Transfer Protocol Secure (Protocolo De Transferência De Hipertexto Seguro)

IA – Artificial Intelligence (Inteligência Artificial)

IAM – Identity And Acess Management (Gerenciamento De Identidade E Acesso)

IDS – Intrusion Detection System (Sistema De Detecção De Intrusão)

IP – Internet Protocol (Protocolo De Internet)

IPS – Intrusion Prevention System (Sistema De Prevenção De Intrusão)

IT – Information Technology (Tecnologia de Informação)

MEMZ – Mota-Engil Mozambique

MFA – Multi-factor Authentication (Autenticação Multi-factor)

ML – Machine Learning (Aprendizado De Máquina)

NAC – Network Access Control (Controle De Acesso Á Rede)

OVA – Open Virtualization Alliance (Aliança Para Virtualização Aberta)

SAAS – Software As A Service (Software Como Serviço)

SIEM – System Information and Event Management (Informações Do Sistema e Gerenciamento De Eventos)

SO – Sistema Operativo

SSH – Secure Shell (Cápsula Segura)

TI – Tecnologia de Informação

URL – Uniform Resource Locator (Localizador Uniforme De Recursos)

VPN – Virtual Private Network (Rede Privada Virtual)

XDR – Extended Detection And Response (Detecção E Resposta Estendidas)

Lista de Figuras

CAPITULO I – INTRODUÇÃO

1.1. Contextualização

A mudança para um estilo de trabalho híbrido vem forçando as organizações a se adaptarem rapidamente. Os funcionários remotos estão fazendo o trabalho da maneira que puderem, usando dispositivos pessoais, colaborando por meio de serviços de nuvem e compartilhando dados fora do perímetro de rede corporativa. Os funcionários híbridos trabalham em redes corporativas e domésticas, alternando entre dispositivos corporativos e pessoais.

À medida que as redes domésticas dos funcionários ampliam o perímetro da rede corporativa, com diferentes dispositivos ingressando nessa rede, as ameaças de segurança estão se multiplicando e se tornando mais sofisticadas enquanto os vectores de ataque evoluem. Em médias e grandes empresas de construção civil isso é cada vez mais notável e vem progredindo de maneira mais rápida nos últimos anos no território nacional, principalmente por estas apresentarem necessidades de compartilhamento mais elevadas por terem sua constituição geográfica dispersa devido a projectos e obras em todo território e quase todas com sedes na capital do país devido a facilidade de acesso a infra-estruturas e tecnológicas.

1.2. Problema

Actualmente a rede de computadores na Mota-Engil Moçambique é composta por uma unidade central em Maputo e sub-redes em projectos e obras espalhadas em todo território nacional, fazendo-se uso de *firewalls* físicas para interconexão das mesmas e de aplicativo de *VPN* para acesso externo.

Toda a componente de segurança cibernética é gerida pelo departamento de *IT* central do grupo Mota-Engil em Portugal e com mínima intervenção dos representantes locais.

Porém, a organização não possui um sistema para monitoramento de eventos em tempo real de segurança da rede em relação aos acessos externos, eventos estes que podem em algum momento dar visibilidade aos administradores locais da infra-estrutura informática sobre eventuais anomalias que podem indicar ou não alguma tentativa de ataque cibernético.

Tendo em conta que a exploração da protecção de dados e informações sensíveis de uma empresa, incluindo a segurança de redes o presente estudo vem responder a seguinte questão:

> *"Como garantir a segurança de redes de computadores em ambientes corporativos face ao trabalho remoto e híbrido em médias e grandes empresas do ramo de construção civil nacionais?"*

1.3. Justificativa

O desenvolvimento da presente pesquisa deriva do interesse pela área de segurança cibernética para as organizações. Outro aspecto preponderante para a escolha deste tema é pelo facto de a organização não possuir mecanismos de monitoramento contínuo dos eventos de segurança na rede corporativa.

Uma das principais motivações para o desenvolvimento deste trabalho é o facto deste tema ser de extrema importância para o desenvolvimento da minha carreira profissional na área de TI.

A sociedade aproveitará este trabalho para melhor orientação sobre a segurança cibernética em uma organização e poderão estar mais a par do que realmente é uma ameaça cibernética. De forma especifica o grupo Meridian32, como o caso de estudo poderá aproveitar o facto de se estar a analisar e trabalhar com a sua realidade para melhorar a sua postura de segurança cibernética e implementar a solução.

A segurança digital tem sido um tema muito estudado actualmente e, mesmo assim, permanece como um aspecto preocupante no cotidiano das organizações.

Com base nisso, a realização desta pesquisa justifica-se, além do interesse do elaborador pelo tema, na necessidade de expor directrizes bases para implementação da segurança em redes de computadores organizacionais.

1.4. Objectivos

1.4.1. Objectivo Geral

- Analisar os desafios e soluções em segurança de redes de computadores em ambientes corporativos face ao trabalho remoto e híbrido em médias e grandes empresas do ramo de construção civil no território nacional.

1.4.2. Objectivos Específicos

- Identificar conceitos relacionados a segurança de redes de computadores em ambientes corporativos.
- Verificar os desafios e soluções adoptadas na Mota-Engil Moçambique.
- Identificar oportunidades de melhorias através do caso de estudo.

1.5. Organização do trabalho

O presente trabalho está dividido em quatros capítulos:

Capítulo I: Introdução – faz-se a referência aos assuntos de rede dando uma visão geral do que se trata o tema deste trabalho. Também justificando esta escolha, descrevendo os objectivos gerais e específicos e a metodologia utilizada.

Capítulo II: Revisão Bibliográfica – onde faz se a revisão das pesquisas e das discussões de outros autores sobre a segurança de redes de computadores que será abordado nessa pesquisa, ou seja, é a contribuição das teorias de outros autores para este caso de estudo.

Capítulo III: Metodologia – onde faz se a referência aos assuntos de Classificação da metodologia, onde se classifica quanto a abordagem, objectivos, e natureza, métodos de recolha de dados considerados, e o método de tratamento de dados.

Capítulo IV: Estudo De Caso **–** onde faz se o levantamento da situação actual da empresa Mota-Engil Moçambique e os seus constrangimentos.

Capítulo V: Apresentação Da Solução E Análise De Resultados – onde faz se a apresentação da solução, a arquitectura e a topologia proposta.

Capítulo VI: Análise E Discussão De Resultados – onde faz se a análise e discussão dos resultados que são abordados no trabalho.

Capítulo VII: Conclusões e Limitações – onde faz se a conclusão do que será abordado ao longo do trabalho e as suas limitações.

CAPÍTULO II – REVISÃO BIBLIOGRÁFICA

Este capítulo traz um referencial teórico no que diz respeito aos conceitos e ferramentas usadas para o desenvolvimento deste projecto.

2.1. Redes de computadores

Uma das maiores conquistas do século XX foi o início do desenvolvimento da aquisição, processamento e da distribuição de informações. Desde então essas áreas convergem, resultando no desenvolvimento de novas tecnologias que facilitem o processamento de informações.

A ideia inicial de um grande computador no qual os usuários concentram todas as informações substitui-se pelas chamadas rede de computadores, cujos trabalhos são realizados em vários computadores interligados entre si.

As redes de computadores são formadas por computadores autónomos que trocam informações entre si. Essa conexão pode ser feita de várias formas como fios de cobre, fibra óptica e ondas de rádio. Nestes sistemas são utilizados equipamentos concentradores denominados *switches*, para interligação dos computadores em uma rede e cliente-servidor que é uma estrutura que distribui as tarefas entre os fornecedores de um recurso (servidores) e os requerentes dos serviços (Clientes). Estas estruturas contam como uma estrutura lógica para se comunicar, denominado protocolo de comunicação (Tanebaum, 2011).

2.2. Segurança de redes de computadores

A segurança de redes consiste na provisão e políticas adoptadas por administradores de rede para prevenir e monitorar o acesso não autorizado, uso incorrecto, modificação ou negação da rede de computadores e dos seus recursos associados. Segurança de rede envolve a autorização de acesso aos dados de uma rede, os quais são controlados por administradores de rede. Usuários escolhem ou são atribuídos uma identificação e uma senha, ou outra informação de autenticação que permite que eles acedam as informações e programas dentro da sua autorização (Abdul Gany, 2023).

A segurança de rede cobre uma variedade de redes de computadores, tanto públicas quanto privadas, que são utilizadas diariamente conduzindo transacções e comunicações entre empresas, agências governamentais e indivíduos.

È possível garantir a segurança de redes de computadores através da adopção de diversas ferramentas como *firewalls, VPNs* e serviços de autenticação.

2.2.1. *Firewalls* e seu papel na protecção da rede

Firewalls são dispositivos ou programas de *software* que actuam como uma barreira de segurança entre uma rede privada e a internet pública. Seu principal papel é controlar o tráfego de rede, permitindo ou bloqueando o acesso com base em um conjunto de regras de segurança predefinidas. Eles são projectados para proteger a rede contra ameaças externas, como ataques cibernéticos, *malware*, intrusões e tentativas não autorizadas de acesso (Pedro Meirelles, Redes de computadores 1 – 2013/1). Além desta ferramenta de segurança, temos também as Redes Virtuais Privadas (*VPNs*) para conexões seguras.

2.2.2. Redes virtuais privadas *(VPNs*) para conexões seguras

VPNs são uma forma de estabelecer conexões seguras e criptografadas através de uma rede pública, como a Internet. Elas permitem que os usuários acedam uma rede privada remotamente de forma segura, como se estivessem fisicamente presentes na rede local. As *VPNs* são amplamente utilizadas para proteger a comunicação e o acesso a recursos em redes corporativas ou comerciais (Douglas Paula). Sendo que podemos associar o uso destas com a autenticação e autorização de usuários como uma forma de maximizar a segurança de redes de computadores em ambientes corporativos.

2.2.3. Autenticação e autorização de usuários

A autenticação e autorização de usuários são elementos essenciais da segurança de rede. A autenticação envolve a verificação da identidade do usuário, geralmente por meio de um nome de usuário e senha, *tokens* de autenticação, certificados digitais ou biometria. A autorização, por sua vez, determina os privilégios e permissões de um usuário autenticado, definindo quais recursos, dados ou funcionalidades ele pode aceder (Abdul Gany, 2023).

Em redes corporativas, sistemas de *gerenciamento* de identidade e acesso *(IAM)* são frequentemente utilizados para centralizar e controlar as políticas de autenticação e autorização. Além disso, técnicas como autenticação de dois factores *(2FA)* e autenticação multifactor *(MFA)* são cada vez mais utilizadas para aumentar a segurança, exigindo informações adicionais além de nome de usuário e senha. Ainda na segurança, também temos a criptografia de dados e comunicações.

2.2.4. Criptografia de dados e comunicações

A criptografia é uma técnica fundamental para garantir a confidencialidade e a integridade dos dados e comunicações em uma rede. Ela envolve a codificação das informações de forma que apenas os destinatários autorizados possam decifrá-las (Abdul Gany, 2023).

A criptografia é usada em vários aspectos da segurança da rede, incluindo a protecção de dados em repouso (armazenados em dispositivos de armazenamento), dados em trânsito (transmitidos através de redes) e autenticação de dados (verificação de integridade dos dados). Além disso, protocolos como o *HTTPS* utilizam criptografia para garantir a segurança das comunicações na *Web*, protegendo informações confidenciais durante a transmissão.

2.3. Soluções de segurança em redes corporativas

Em resumo, a segurança digital é cada vez mais importante em um mundo conectado, porque a tecnologia se tornou uma parte essencial de nossas vidas pessoais e profissionais, e a protecção contra ameaças cibernéticas é crucial para evitar prejuízos e garantir a privacidade e integridade dos dados (Emílio Nakamura, 2002). Uma das soluções de segurança é a detecção e prevenção de intrusões *(IDS/IPS).*

2.3.1. Detecção e prevenção de intrusões *(IDS/IPS)*

IDS (Sistema de Detecção de Intrusões) e *IPS* (Sistema de Prevenção de Intrusões) são mecanismos de segurança projectados para monitorar e analisar o tráfego de rede em busca de actividades suspeitas ou maliciosas. O *IDS* identifica e alerta sobre possíveis intrusões, enquanto o *IPS* não só detecta, mas também toma medidas activas para bloquear ou prevenir os ataques em tempo real (Carvalho, 2005). Além da detecção e prevenção de intrusões, os Antivírus e os *Antimalware* também são muito importantes nas soluções de segurança em redes corporativas.

2.3.2. Antivírus e *antimalware*

Essas são soluções de segurança projectadas para detectar, remover e prevenir a propagação de vírus, *malware, spyware* e outras ameaças digitais. Os antivírus são capazes de identificar e eliminar arquivos maliciosos em dispositivos, enquanto os *antimalware* são mais abrangentes e também abordam ameaças mais avançadas (Anderson Nascimento, 2014).

2.3.3. Filtragem de conteúdo da *web*

Essa medida de segurança envolve a filtragem e o controle do acesso a determinados conteúdos na *web*. Ela pode ser usada para bloquear sites maliciosos, conteúdo impróprio ou não autorizado, protegendo os usuários contra ameaças e ajudando a cumprir as políticas de uso da empresa (Abdul Gany, 2023). Não só, ainda nas soluções de segurança existe o controle de acesso a rede *(NAC).*

2.3.4. Controle de acesso à rede *(NAC)*

O controle de acesso à rede é um conjunto de tecnologias e políticas que garantem que apenas dispositivos autorizados e usuários legítimos tenham acesso à rede corporativa. Isso envolve a autenticação de usuários, verificação da conformidade dos dispositivos com políticas de segurança, segmentação de rede e imposição de restrições de acesso com base em perfis de usuário ou dispositivo (Abdul Gany, 2023). Por outro lado, é possível verificar a segurança sem fio e *BYOD (Bring Your Own Device)*.

2.3.5. Segurança sem fio e *BYOD (Bring Your Own Device)*

Com a proliferação de dispositivos móveis e a prática de *BYOD* (trazer seu próprio dispositivo), é essencial ter medidas de segurança adequadas para proteger as redes sem fio. Isso envolve o uso de autenticação robusta, criptografia de dados, segregação de rede e políticas de uso de dispositivos móveis para garantir a segurança dos dados corporativos (Ideir Coto IFRO, 2023).

2.4. Security Information and Event Management

O *SIEM* (*Security Information and Event Management*) é um sistema baseado em regras, ele é responsável em colectar *logs*, eventos e dados. O seu objectivo é detectar ocorrências suspeitas que possam, de alguma forma, comprometer a segurança dos dados da empresa.

De acordo com (Fruhlinger, 2022) o *SIEM* é a combinação de *SIM* e *SEM* sendo que *SIM* é uma ferramenta que providencia análise e relatórios de eventos de segurança que ocorreram no passado enquanto o *SEM* é uma ferramenta que tem como intuito lidar com eventos de segurança em tempo real.

Em um passado recente, tinha se a visão que o *SIEM* era usado apenas por grandes organizações, com recursos avançados para segurança dos seus dados. Porém, hoje ele é um componente de segurança extremamente importante para todas organizações. Empresas de pequeno, médio e grande porte, precisam para fins de compliance, gerar automaticamente relatórios que fornecem requisitos de conformidade.

Com isso, pode ser visto como uma ferramenta que permite a colecta de informações relativas a eventos de segurança para permitir o processamento, análise e armazenamento de eventos de segurança para detecção de anomalias em uma rede corporativa, eventos estes que podem ser passados ou em tempo real para auxiliar os administradores de TI na identificação e resposta a anomalias no que tange a eventos de segurança cibernética.

2.4.1. Arquitectura *SIEM*

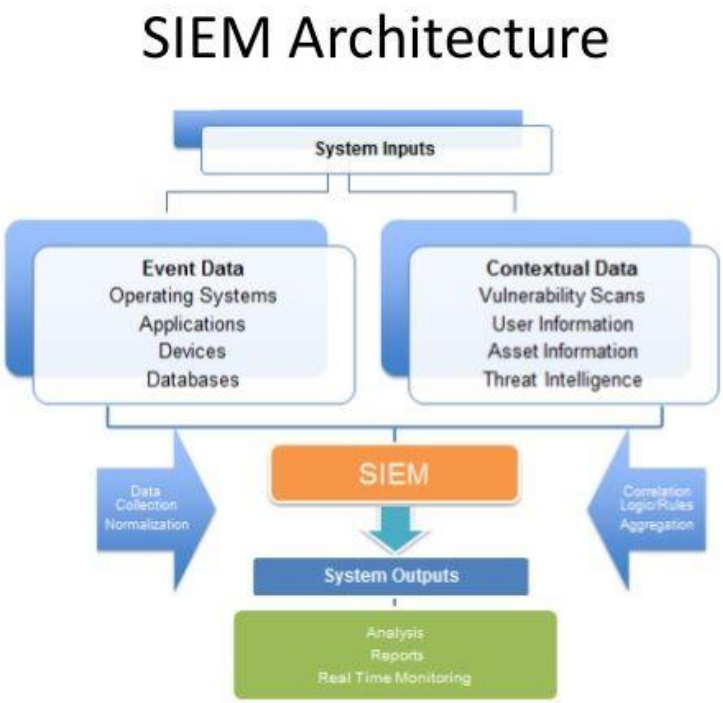

Figura 2.1 – Arquitectura do SIEM

A arquitectura *SIEM* fornece capacidades para apresentar, analisar e colectar informações de dispositivos de rede e de segurança.

Segundo (Vielberth, 2018) o *SIEM* é composto por:

- **Colecção:** a colecta de *logs* pode ser feita de duas formas: através da fonte dos *logs*, ou pelo carregamento dos *logs* através do *SIEM*.
- **Normalização:** a normalização consiste no processamento e uniformização dos dados colectados.
- **Enriquecimento:** nesta fase os dados de *log* colectados anteriormente são enriquecidos com dados de contexto de diversas fontes para facilitação no processo de detecção de ataques cibernéticos.
- **Correlação e análise:** nesta fase o *SIEM* faz a dedução do estado do ambiente corporativo em termos de segurança, e é feita com base nos eventos observados de várias origens para ajudar na detecção de ataques.
- **Alerta e resposta:** nesta fase são notificados todos os intervenientes relevantes com vista a informar sobre possíveis detecções de incidentes de segurança cibernética e as

medidas devem ser tomadas automaticamente ou manualmente para proteger a organização contra mais danos.

- **Relatórios e troca de ameaças:** nesta fase o *SIEM* permite a visualização de relatórios de incidentes de segurança cibernética que podem ser usados para fins de conformidade ou mesmo por obrigações legais.

Um aspecto muito importante na arquitectura do *SIEM* é como os dados de *log* são transferidos de cada sistema, que podem ser baseados em agente ou sem agente. Com o agente, é instalado um agente em cada máquina que gera os registos, e este agente é responsável por extrair, processar e transmitir dados para o servidor. Sem o agente, o sistema que gera os *logs,* pode transmitir directamente para o sistema. Em muitos casos, pode ter um servidor de registo intermediário.

2.4.2. Vantagens do uso de uma ferramenta *SIEM*

Eventos de segurança da informação estão cada vez mais comuns, e as soluções *SIEM* geralmente obedecem a combinação de algumas funcionalidades essenciais para a detecção de anomalias de segurança cibernética.

As principais vantagens da ferramenta *SIEM* são o armazenamento massivo dos dados, mecanismos de suporte que actuam para mitigar as ameaças automaticamente e o acesso em tempo real às informações, todas centralizadas para diminuir o seu tempo de resposta.

Outros benefícios do *SIEM* são:

- **Detectar incidentes**

Por estar com o monitoramento em tempo real, uma ferramenta eficiente vai emitir um alerta de invasão ou mesmo de brecha.
Isso vai permitir que a equipe de T.I aja rapidamente e actue em cima de onde está o problema, pois fica fácil ver onde se iniciou o ataque e para onde ele está indo dentro do seu sistema.

- **Melhora a eficiência**

A *SIEM* alerta para possíveis vulnerabilidades de sistemas e *softwares*, dentre elas estão as actualizações dessas aplicações, que muitas vezes deixam vulnerabilidades.
Manter os programas sempre actualizados, é uma forma de aumentar a segurança, mas também melhoram o desempenho das máquinas, pois permite que operem na sua máxima eficiência.

- **Agilizar a criação de relatórios**

O armazenamento de *logs* de segurança e o monitoramento em tempo real, permite que a ferramenta *SIEM* entregue relatórios completos de forma muito mais rápida que os tradicionais consolidados em Excel.

Fora que são visualmente muito mais directos ao ponto, para você ter em mãos as informações que realmente importam para sua estratégia.

Eles que vão direccionar as acções dos times de T.I e também servirão para fins de compliance dependendo das obrigações da empresa.

2.4.3. Soluções de plataformas *SIEM*

A solução *SIEM* actualmente é muito utilizada por diversas empresas, instituições e alguns centros académicos no âmbito de pesquisa, segundo (Tavares, 2005).

Para a escolha da solução *SIEM* que será analisada na pesquisa, foram considerados dois critérios, estes que nomeadamente são: Se a solução é *open-source* ou não, isto é, se é de código-fonte aberto ou não, e o preço, se a solução é grátis ou comercial.

Deste modo foram escolhidas 4 soluções, em que duas delas foram escolhidas segundo Gartner, que são o ***Splunk*** e o ***IBM QRadar***, e as outras duas soluções são o ***Wazuh*** e o ***Elastic Security***.

As soluções *Splunk* e o *IBM QRadar* são de código-fonte fechado e de preço comercial, enquanto a solução *Wazuh* é de código-fonte aberto e sem preço comercial, e a solução *Elastic Security* é de código-fonte aberto e de preço comercial.

De seguida irá se fazer uma descrição em torno das 4 soluções de modo a contextualizar a análise que será feita ao longo do trabalho.

1. ***Splunk***

   Segundo a (*Splunk*, 2003) o *Splunk* foi fundado em 2003 para resolver problemas em infraestruturas digitais complexas. Desde o início, ajuda as organizações a explorar as vastas profundezas de seus dados como espeleólogos em uma caverna (daí "*Splunk*").

   Splunk é uma empresa americana de *software* com sede em São Francisco, Califórnia, que produz *software* para pesquisar, monitorar e analisar dados gerados por máquina por meio de uma interface estilo *web.*

   Seu *software* ajuda a capturar, indexar e correlacionar dados em tempo real em um repositório pesquisável, a partir do qual pode gerar gráficos, relatórios, alertas,

dashboards e visualizações. O *Splunk* usa dados de máquina para identificar padrões de dados, fornecendo métricas, diagnosticando problemas e fornecendo inteligência para operações de negócios. *Splunk* é uma tecnologia horizontal usada para operações para *gerenciamento* de aplicativos, segurança e conformidade, bem como análises de negócios e da *web*.

O *Splunk* é um *software* de código-fonte fechado, e com um preço comercial.

Funcionalidades

As principais funções do *Splunk* são:

- Pesquisa e análise de dados;
- Visualização de dados em painéis personalizados;
- Acção com base nos dados;
- Recursos de Aprendizado de Máquina e *IA*;
- Colecta, processo e distribuição de dados em milissegundos com processamento de *stream* em tempo real;
- Espaço de trabalho analítico;
- Recursos de *IA* da *Splunk*.

Arquitectura do *Splunk*

Segundo a (*Splunk Enterprise*), usando um único componente de software que é fácil de entender em suas configurações, o *Splunk Enterprise* pode coexistir com a infra-estrutura existente ou pode ser implantado como uma plataforma universal para acessar dados de TI. A implementação mais simples é aquela obtida por padrão ao instalar o *Splunk Enterprise*: Indexando, pesquisando e exibindo dados no mesmo servidor.

A *Splunk* é constituída por 4 partes nomeadamente que são:

Indexador

Um Indexador de *Splunk* fornece processamento e armazenamento de dados locais e remotos, ou seja, é aquele que hospeda os dados que chegam à plataforma *Splunk* por diferentes métodos. Este componente é responsável por pegar os eventos ou dados gerados pelos dispositivos e/ou controles de segurança para indexá-los e disponibilizá-los dentro do *Splunk.* É responsável por armazenar dados por vários protocolos e portas de entrada. Ele é responsável por conectar remotamente via scripts a aplicativos, bancos de dados e *APIs* para consultar e indexar informações.

É responsável por filtrar informações seleccionadas para armazenamento.

É responsável por gerenciar os bancos onde a informação é inserida, comprimir as informações inseridas para reduzir os recursos de armazenamento, activar pesquisas distribuídas paralelas.

Permite estabelecer pesquisas remotas a partir de outros *search head*,

Cabeça de pesquisa ou *Search Head*

Um *Search Head* é uma instância do *Splunk Enterprise* que distribui pesquisas em indexadores (referidos como "*peer search*"). O *Search Head* pode ou não ser dedicado à função de gerenciamento de pesquisas, dependendo da arquitectura e topologia necessárias. Um *Search Head* dedicado não possui seus próprios índices ou índices internos. Em vez disso, os resultados originados de pares de pesquisa remotos (índices remotos) são consolidados e exibidos.

Este componente é responsável pelo processamento durante o processo de pesquisa. Ao incluir servidores como os *Search Heads*, liberamos o processamento em indexadores.

Encaminhador ou *Forwarder*

O Splunk *Forwarder* é uma instância do *Splunk* ou agente que encaminha dados para indexadores remotos para processamento e armazenamento de dados. Os *Forwarders Splunk* não indexam dados dentro deles.

É o mecanismo pelo qual os *logs* são enviados para o Indexador, considerando que o SO de origem está instalado e configurado, o uso de *gerenciamento* de encaminhamento é recomendado.

Servidor de Implementação

O servidor de implementação é uma ferramenta para distribuir configurações, aplicativos e actualizações de conteúdo para grupos de instâncias do *Splunk Enterprise Security*. Este servidor de implementação pode ser usado para distribuir actualizações dos componentes do *Splunk* que foram citados anteriormente.

2. IBM QRadar

Segundo a (*IBM QRadar Security Intelligence Platform*, 2023) a *IBM QRadar* é uma plataforma de gerenciamento de segurança de rede que fornece consciência situacional e suporte de conformidade. *QRadar* usa uma combinação de conhecimento de rede baseado em fluxo, correlação e avaliação de vulnerabilidades baseada em activos.

O *IBM QRadar* é um *software* de código-fonte fechado, e com um preço comercial.

Funcionalidades

As principais funções do *IBM QRadar* são:

- Investigação de ameaças;
- Entregue como *SaaS* na *AWS*;
- Procura federada;

- Colecta de dados;
- Centro de detecção e resposta;
- Experiência do usuário unificada;

Arquitectura do *IBM QRadar*

Segundo a (*IBM QRadar Security Intelligence Platform*, 2023) o *IBM QRadar SIEM (Security Information and Event Management)* é uma arquitectura modular que fornece visibilidade em tempo real de sua infraestrutura de TI, que se pode usar para detecção de ameaças e priorização.

O funcionamento da plataforma de inteligência de segurança *QRadar* consiste em três camadas, e se aplica a qualquer estrutura de implementação *QRadar*, independentemente de seu tamanho e complexidade.

As três camadas da arquitectura do *IBM QRadar* são:

Colecta de Dados

A colecta de dados é a primeira camada, na qual os dados, como eventos e fluxos, são colectados da rede. Os dados são analisados e normalizados antes de passar para a camada de processamento. Depois que os dados brutos são analisados, eles são normalizados para que sejam apresentados em um formato estruturado e utilizável.

A funcionalidade principal de *QRadar SIEM* é focada na colecta de dados do evento, e na colecta de fluxo.

Os dados de evento representam eventos que ocorrem em um determinado momento no ambiente do usuário, como logins de usuário, e-mail, conexões *VPN*, negações de *firewall*, conexões *proxy* e quaisquer outros eventos que se possa desejar registar nos *logs* do dispositivo.

Processamento de Dados

Após a colecta de dados, a segunda camada, ou camada de processamento de dados, é o local onde os dados de evento e de fluxo são executados por meio do *Custom Rules Engine (CRE*), que gera ofensas e alertas. Em seguida, os dados são gravados no armazenamento.

Os dados de evento e os dados de fluxo podem ser processados por um dispositivo *All-in-One* sem a necessidade de incluir Processadores de Eventos ou *Flow Processors*. Se a capacidade de processamento do dispositivo *All-in-One* for excedida, poderá ser necessário incluir Processadores de Eventos*, Flow Processors* ou qualquer outro dispositivo de processamento para manipular os requisitos adicionais. Também pode ser necessária mais capacidade de armazenamento, que pode ser manipulada incluindo *Data Nodes*.

Procuras de Dados

Na terceira ou na camada superior, dados que são colectados e processados por *QRadar* estão disponíveis para usuários para pesquisas, análise, relatórios e alertas ou investigação de ofensa. Os usuários podem pesquisar, e gerenciar as tarefas admin de segurança para sua rede a partir da interface do usuário no *QRadar Console*.

Em um sistema *all-in-one*, todos os dados são colectados, processados e armazenados no dispositivo *all-in-one*.

Em ambientes distribuídos, o *QRadar Console* não realiza processamento de eventos e de fluxo, ou armazenamento. Em vez disso, o *QRadar Console* é usado principalmente como a interface do usuário onde os usuários podem usá-lo para pesquisas, relatórios, alertas e investigações.

3. Wazuh

Segundo (*Wazuh*, 2024), ***Wazuh Security Information and Event Management (SIEM)*** é uma plataforma centralizada para agregar e analisar telemetria em tempo real para detecção e conformidade de ameaças. *Wazuh* colecta dados de eventos de várias fontes, como endpoints, dispositivos de rede, cargas de trabalho em nuvem e aplicativos para uma cobertura de segurança mais ampla.

O *Wazuh* é um *software* de código-fonte aberto, e grátis, isto é, sem preço comercial.

Funcionalidades

As principais funções do *Wazuh* são:

- Análise de *log*;
- Detecção de intrusão;
- Alertas em tempo real;
- Escalabilidade;
- Regras e decodificadores;
- Integrações;
- Painéis e visualização;
- Resposta a incidentes

Arquitectura do *Wazuh*

Segundo a (*Wazuh*, 2023), a arquitectura *Wazuh* é baseada em agentes, executados nos *endpoints* monitorados, que encaminham dados de segurança para um servidor central. Dispositivos sem agente, como *firewalls, switches*, roteadores e pontos de acesso, são suportados e podem enviar activamente dados de log via *Syslog*, *SSH* ou usando sua *API*. O servidor central decodifica e analisa as

informações recebidas e repassa os resultados ao indexador *Wazuh* para indexação e armazenamento.

Os componentes do *Wazuh* são:

- *Wazuh indexer*: é um componente central para indexação e armazenamento dos alertas gerados pelo *Wazuh server*.
- *Wazuh server*: recebe e analisa os dados recebidos pelos agentes distribuídos na rede. O *Wazuh server* pode ser formado por único servidor ou por um conjunto de servidores formando um *cluster*.
- *Wazuh dashboard*: é o componente responsável pela visualização e análise dos dados colectados.
- *Wazuh agents*: é instalado nos *endpoints* para realizar colecta de informações permitindo a prevenção e detecção de ameaças.

4. Elastic Security

Segundo (Rafael Medeiros, 2022), o *Elastic Security* pode ser descrito como a combinação dos recursos de detecção de ameaças *SIEM* com recursos de prevenção e resposta de *Endpoint* em uma única solução, a primeira solução *limetless XDR* gratuita e aberta de sector.

O *Elastic Security* é um *software* de código-fonte aberto e com um preço comercial.

Funcionalidades

As principais funcionalidades do *Elastic Security* são:

- Um mecanismo de detecção para identificar ataques e configurações incorrectas do sistema;
- Um espaço de trabalho para triagem e investigações de eventos;
- Visualizações interactivas para investigar relacionamentos de processos;
- Gerenciamento de casos integrado com acções automatizadas;
- Detecção de ataques com *machine learning (ML*) e regras de detecção.

Arquitectura do *Elastic Security*

A arquitectura do *Elastic Security* é baseada em quatro princípios:

- Computação e armazenamento dissociados;
- Camadas separadas de busca e indexação;
- Armazenamento de objectos económico como sistema de registo;
- Consulta de baixa latência.

Na **computação e armazenamento dissociados**, o *Elasticsearch* oferece várias camadas de dados para alinhar melhor os dados aos requisitos de hardware. A dissociação do armazenamento e da computação torna a classificação de dados em camadas obsoleta, levando a uma operação mais simples, e os índices da camada *frozen* podem armazenar grandes volumes de dados buscados com menos frequência, mas de forma semelhante a camada *hot*, em que esses dados podem ser actualizados e consultados rapidamente e qualquer momento.

Nas **camadas separadas de busca e indexação** em vez de depender de instâncias primárias e de réplica para gerenciar várias cargas de trabalho, a arquitectura *Serveless da Elastic* oferece suporte para camadas distintas de indexação e busca. Com essa separação, as cargas de trabalho podem ser redimensionadas de forma independente, e o *hardware* pode ser seleccionado e optimizado para cada caso de uso.

No **armazenamento de objectos económico como sistema de registo,** o *Elastic Security* conta com armazenamento de objectos económico para oferecer maior escala e, ao mesmo tempo, reduzir os custos de armazenamento.

Na **consulta de baixa latência** os armazenamentos de objectos podem acomodar grandes quantidades de dados, e mantém um óptimo desempenho de consultas feitas.

2.5. Gestão de vulnerabilidades e avaliações de segurança

A gestão de vulnerabilidades envolve a identificação, avaliação e mitigação das vulnerabilidades nos sistemas de uma organização. As vulnerabilidades podem ser falhas de segurança em *software*, configurações inadequadas de sistemas, problemas de rede ou qualquer outra fraqueza que possa ser explorada por invasores (Abdul Gany, 2023).

Para gerenciar as vulnerabilidades, as organizações podem usar várias técnicas, como:

- Varreduras de vulnerabilidade: Execução de ferramentas automatizadas que identificam vulnerabilidades conhecidas em sistemas, aplicativos e dispositivos de rede.
- Testes de penetração: Tentativas controladas de invadir sistemas para identificar vulnerabilidades desconhecidas ou explorar as já conhecidas.
- Monitoramento contínuo: Utilização de sistemas de detecção de intrusão e outras ferramentas para monitorar constantemente a infra-estrutura em busca de actividades suspeitas.

- Avaliações de segurança: As avaliações de segurança são processos sistemáticos para identificar, analisar e avaliar os riscos de segurança em uma organização. Essas avaliações ajudam a identificar pontos fracos e fornecem uma visão geral do estado da segurança, permitindo que as organizações tomem medidas adequadas para mitigar os riscos identificados. È possível garantir a gestão de vulnerabilidades e avaliações de segurança através das actualizações e *patches* de segurança.

2.5.1. Actualizações e *patches* de segurança

É essencial que as organizações implementem um processo eficiente para gerenciar as actualizações e *patches* de segurança, o que geralmente envolve as seguintes etapas:

- Monitoramento de notificações de segurança: Acompanhamento das informações fornecidas por provedores de *software* e sistemas operacionais sobre as actualizações e *patches* disponíveis.
- Avaliação de impacto: Avaliação do impacto potencial das actualizações e *patches* nos sistemas e aplicativos existentes antes de sua implantação. (Abdul Gany, 2023).

CAPÍTULO III – METODOLOGIA

Conforme Gil (2002), a metodologia descreve os passos a serem seguidos para a realização de uma pesquisa, em outras palavras, determinar o método que possibilitou chegar a esse conhecimento. Neste capítulo é apresentado à classificação da pesquisa quanto à abordagem, natureza, objectivos, método de recolha de dados, e o método de tratamento de dados.

3.1. Classificação da metodologia

3.1.1. Classificação quanto à abordagem

O estudo tem um princípio qualitativo envolvendo a colecta e análise de dados não numéricos, como narrativas, observações, entrevistas e análise de documentos para analisá-los como forma de identificar padrões e semelhanças de forma interpretativa, porém pode subsidiar-se de elementos quantitativos através de entrevistas não estruturadas esporádicas para sanar duvidas sobre elementos técnicos.

Segundo Denzin e Lincoln (2006), "a pesquisa qualitativa envolve uma abordagem interpretativa do mundo, o que significa que seus pesquisadores estudam as coisas em seus cenários naturais, tentando entender os fenómenos em termos dos significados que as pessoas a eles conferem".

Segundo Michel (2005), "a pesquisa quantitativa é um método de pesquisa social que utiliza a quantificação nas modalidades de colecta de informações e no seu tratamento, mediante técnicas estatísticas, tais como percentual, média, desvio-padrão, coeficiente de correlação, análise de regressão, entre outros. "

3.1.2. Classificação quanto à natureza

Quanto a sua natureza apresenta-se como uma pesquisa aplicada, uma vez que "o investigador é movido pela necessidade de contribuir para fins práticos mais ou menos imediatos, buscando soluções para problemas concretos (Cervo & Bervian, 1993)".

3.1.3. Classificação quanto aos objectivos

Esta pesquisa quanto aos seus objectivos é exploratória, segundo (Gil, 1991), "as pesquisas exploratórias têm como principal finalidade desenvolver, esclarecer e modificar conceito e ideias, tendo em vista a formulação de problemas mais precisos"

3.1.4. Métodos de recolha de dados considerados

Para esse estudo vai se considerar o uso dos seguintes métodos:

• A pesquisa bibliográfica, que é o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, Internet, isto é, material acessível ao público em geral (Davel & Vergana, 2008);

• Estudo de caso, este que foi realizado na Mota-Engil Moçambique, com a intenção de compreender os desafios e possíveis soluções trazidas pela adopção do trabalho remoto e híbrido em relação a segurança da rede de computadores.

Os métodos de colecta de dados utilizados foram o de observação não participante, entrevista não estruturada e análise documental.

- Observação não participante, o observador entra em contacto com o grupo, a comunidade ou a realidade estudada, porém, não se envolve, nem se integra a ela, permanece de fora. O observador presencia o fato, mas não participa dele (MARCONI & LAKATOS, 1996).
- Entrevista não estruturada, aquela em que é deixado ao entrevistado decidir-se pela forma de construir a resposta (Laville e Dione, 1999:188-190). Este tipo de entrevista não possui um roteiro, se assemelhando a um simples bate-papo, com perguntas abertas, e não estabelecidas anteriormente, mas que ainda podem ser planejadas de forma autónoma.
- Analise documental é o momento de reunir todas as partes – elementos da problemática ou do quadro teórico, contexto, autores, interesses, confiabilidade, natureza do texto, conceitos-chave (Cellard, 2008).

3.1.5. Método de tratamento de dados

Para atingir os objectivos pretendidos, em relação aos procedimentos técnicos vão se realizar as seguintes fases:

Fase 1 – Análise da situação actual

Compreensão da rede de computadores, assim como os serviços e recursos de rede, tipos de rede, conectividade com a internet, acesso remoto, acesso sem fio, implantação do computador cliente.

Fase 2 – Averiguação de soluções de segurança de rede de computadores

Aqui decorreu a avaliação de algumas ferramentas de segurança digital que poderiam suprir os desafios ainda existentes na instituição.

Fase 3 – Demonstração do funcionamento da solução

Por fim pretendeu-se demonstrar os resultas obtidos da realização de testes funcionais da solução proposta. Limitando-se à utilização de um ambiente simulado.

CAPÍTULO IV – ESTUDO DE CASO

Segundo Hartley (1994), o estudo de caso consiste em uma investigação detalhada de uma ou mais organizações, ou grupos dentro de uma organização, com vista a prover uma análise do contexto e dos processos envolvidos no fenómeno em estudo.

4.1. Situação actual

Segundo (Mota-Engil, 2024) a Mota-Engil Moçambique (MEMZ) é uma subsidiária da Mota-Engil, um grupo português de engenharia e construção que opera em vários países da Europa, África, América Latina e Ásia. Esta tem participado em vários projectos de grande escala no país, relacionados com edificação de infra-estruturas públicas e privadas, energia e mineração.

Assim como muitas organizações a MEMZ, no contexto da pandemia teve que implementar rapidamente modelos de trabalho remoto e híbrido. Porém, agora os desafios a longo prazo trazido por estes modelos devem ser mais uma vez retractados e solucionados, a infra-estrutura, seus serviços e fluxos de trabalho precisaram ser reavaliados, pois ataques cibernéticos têm vindo a crescer, já que as informações corporativas estão sendo acessadas e compartilhadas de diferentes lugares e dispositivos numa superfície de ataque expandida.

A princípio a MEMZ com a infra-estrutura tecnológica central (rede de computadores, *softwares* e *hardware* como serviços) na sua sede na cidade de Maputo e tratava os projectos (obras e estaleiros) como extensões directamente ligadas, como representada na figura 4.1, teve de implementar soluções para permitir acessos fora desta.

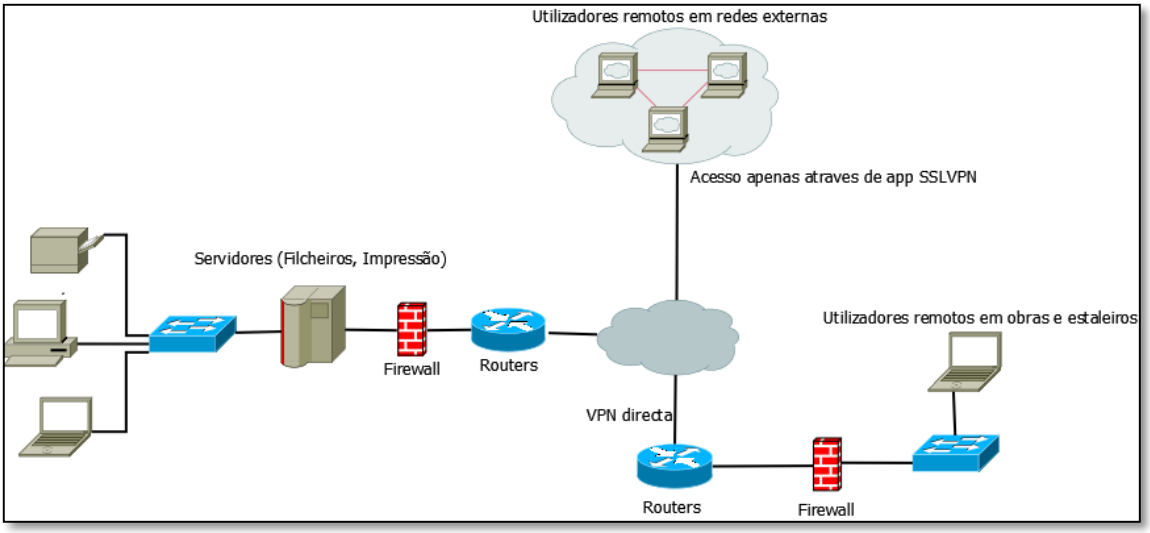

Figura 4.1 – Estrutura orgânica da Mota-Engil (Fonte: Mota-Engil, 2023).

Estas soluções basearam em suma no investimento para implementação de *VPNs* e segurança de *endpoints* através da adopção da *Fortinet* e soluções de segurança corporativas associadas a contas Microsoft corporativas como *defender XRD* e antivírus diversos. Contudo existe a necessidade de ter maior visibilidade sobre a rede e conseguir identificar e responder a ameaças vinculadas ao trabalho remoto e híbrido assim como manter o controlo e ter o registo actualizados de dispositivos utilizados.

Actualmente a MEMZ tem na sua infra-estrutura de rede corporativa como activo:

- Servidor de Impressora
- Servidor de Ficheiros
- Terminais Fixas e Móveis
- *Switches* e Roteadores
- *Firewall, Vpn,* entre outros.

Ainda na infra-estrutura de rede corporativa da MEMZ, em relação aos mecanismos de segurança temos: Uma máquina *Firewall* e um sistema de prevenção de intrusão (*IPS*) e o *CrowdStrike Falcon*.

O servidor de impressoras, é onde estão as impressoras que são utilizadas dentro da empresa, e o servidor de Ficheiros onde ficam guardados os arquivos da empresa. Com base a cada sector que existe na empresa, o colaborador tem acesso só a arquivos em que trabalha e faz parte do sector, isto é, se faz parte do sector de informática só terá acesso ao mapeamento dos arquivos em que trabalha nele, isto que são os arquivos de informática.

Sendo uma empresa com várias filiais, tem uma *Virtual Private Network (VPN),* para que se possa ter acesso a rede interna da empresa e para enviar dados com segurança pela internet. Esse serviço da *VPN* usa criptografia para proteger a conexão com a internet contra acesso não autorizado, cria um túnel de dados seguro entre a terminal local e o servidor *VPN,* este que se encontra na sede da MEMZ, podendo estar em um local a milhares de quilómetros de distância.

Tratando-se de uma empresa no ramo de construção civil e com muitas filiais, a atribuição da *VPN* foi feita por toda empresa. Os colaboradores que se encontram localmente na empresa tem o acesso a *VPN,* e os colaboradores que se encontram nas obras localmente e nas províncias também tem o acesso a *VPN* para que tenha o acesso a rede privada da empresa.

Os trabalhadores que se encontram localmente na empresa, foram atribuídos a *VPN* pela razão de se tratar de uma empresa do ramo de construção civil, pode haver a necessidade de algum

colaborador ter que se ausentar a uma obra e não pode ficar sem ter o acesso a rede privada da empresa, e pelo trabalho remoto, então a instalação e configuração da *VPN* foi feita a todos colaboradores da MEMZ.

A MEMZ tem várias terminais, estas que se dividem em terminais fixas e terminais móveis. Terminais fixas que são os computadores *Desktops* e as Terminais móveis que são os computadores laptops. Dependendo do trabalho de cada colaborador na empresa são feitas as atribuições dos terminais aos colaboradores. Geralmente aos trabalhadores que estão sempre a deslocar se de obras para obras, usam os terminais móveis para facilitar o trabalho, e alguns que estão localmente na empresa usam os terminais fixos. A MEMZ consta também com uma política de segurança.

Actualmente a MEMZ usa o mecanismo de segurança *Falcon CrowdStrike,* este que monitora as terminais dos colaboradores da empresa toda em geral. Os terminais da MEMZ tem o *endpoint*, e o *Falcon CrowdStrike* instalado no servidor, este que gerou uma chave para colocar em todos terminais da empresa para que se possa verificar o monitoramento de todos os terminais em geral da empresa.

O *CrowdStrike* na MEMZ consegue interromper violações através do conjunto unificado de tecnologias em nuvem, uma delas que é o Antivírus, que evitam todos os tipos de ataque, incluindo *malwares* e muito mais. Com o *Falcon* a empresa já não precisa de instalar um antivírus, o *Falcon* já vem com o antivírus para as ameaças.

Mas o *CrowdStrike* tem uma limitação, porque as terminais da empresa tem de estar registadas na *AD* (*Active Directory*) da empresa e tem que fazer login na *AD* para ser visto. Se a terminal ficar mais de 60 dias sem fazer login não será mais visto pela *AD*, ela sai do *AD*, e saindo do *AD* já não será mais monitorada pelo *CrowdStrike*. Por ser um software pago, visto que a terminal não faz mais login na *AD* a mais de 60 dias, automaticamente sai da *AD*, pois ira poupar recursos da empresa. A outra limitação é o gasto para a gestão de actualizações, as vezes a terminal não consegue fazer todas as actualizações necessárias. O monitoramento na MEMZ localmente é um pouco complicado, porque quem faz a gestão geral é uma central na Mota-Engil em Portugal, então colaboradores da informática localmente não tem uma visão ampla.

Para os colaboradores da MEMZ que trabalham nas obras, estaleiros, isto é, fora da sede, no trabalho remoto, é difícil ter um alerta rápido do *Crowdstrike*, por causa da rede, e o *proxy* do terminal.

4.2. Constrangimentos

Actualmente podem ser listados os seguintes:

- Inexistência de um mecanismo capaz de realizar o monitoramento de terminais que não estejam na *AD* da MEMZ (as terminais que por terem ficado mais de 60 dias sem fazer o login no *AD* foram apagadas automaticamente da *AD*);
- Capacidade de correlação de *logs* de segurança gerados pelos activos que não estejam localmente na sede da MEMZ, é praticamente inexistente para identificar ameaças em tempo útil;
- Não é feita a gestão centralizada e automatizada de *logs* na infra-estrutura de rede corporativa.
- Não é feito o controle de terminais (fixas e moveis), o controle de servidores de arquivos e de servidores de impressoras.

CAPÍTULO V – APRESENTAÇÃO DA SOLUÇÃO E ANÁLISE DOS RESULTADOS

5.1. Apresentação da solução

Para a realização da presente análise comparativa, foram consideradas as soluções *Splunk*, *IBM QRadar*, *Wazuh e Elastic Security,* e de seguida foram definidos critérios que foram escolhidos de acordo com os seguintes aspectos em torno das plataformas *SIEM*:

- ✓ O preço/Licença: Grátis ou Comercial;
- ✓ *Open-source*: Código Fonte aberto ou fechado;
- ✓ Principais funcionalidades e as características a observar na implementação.

5.1.1. Atendimento remoto e controle da infra-estrutura por *VPNs*

Para auxiliar as equipas e gestores no desenho de planos de contingência para segurança de infra-estrutura durante o trabalho remoto uma boa prática recomendada é o desenvolvimento do Plano de Controle.

Este plano garante a possibilidade de as equipes obterem acesso aos equipamentos (sejam eles roteadores, *switches* ou servidores, por exemplo) para diagnosticar, verificar e promover a recuperação de falhas na infra-estrutura. Além desta solução temos a segregação física de *firewalls*.

5.1.2. Segregação física de *firewalls*

Firewall pode ser um hardware, um software ou a combinação de ambos, que confere e filtra o fluxo dos dados dos computadores. Os resultados dos sistemas *firewall* são excelentes, oferecendo segurança, comunicação optimizada, flexibilidade e disponibilidade. Trata-se de uma solução para ambiente virtual que mantém a confidencialidade dos dados e protege a integridade das informações.

Eles bloqueiam sites utilizando filtros de *URL*, fazem actualização dos protocolos de protecção e dos antivírus automaticamente e garantem conectividade ininterrupta. Além do mais, ajudam a reduzir os custos, já que dispensam a necessidade de técnicos por disponibilizar um serviço de *gerenciamento* próprio. Outro factor que merece destaque é a possibilidade de controlar a entrada dos colaboradores às informações corporativas. Ainda na apresentação da solução existe o *SIEM* que também é muito importante.

5.1.3. Monitoramento unificado de eventos de segurança e *endpoint* (*SIEM*)

Ter visibilidade sobre a rede e conseguir identificar e responder a ameaças é um desafio tanto no trabalho remoto quanto no presencial. Uma ferramenta que ajuda nessa tarefa é o *SIEM* (*Security Information and Event Management),* que faz o *gerenciamento* de eventos de segurança.

O *SIEM* colecta dados do maior número de fontes possíveis, como diferentes ferramentas de segurança (*firewall, secure web gateway*, antivírus etc.) e dispositivos, incluindo os equipamentos utilizados em *home office*. Esses dados são então centralizados e correlacionados para identificar ameaças, emitir alertas e automatizar respostas sempre que possível.

5.2. Descrição da solução

5.2.1. *Open-Source Security information Management - Wazuh*

A solução ***Wazuh Security Information and Event Management (SIEM)*** segundo (*Wazuh*, 2024) é uma plataforma centralizada para agregar e analisar telemetria em tempo real para detecção e conformidade de ameaças. *Wazuh* colecta dados de eventos de várias fontes, como *endpoints*, dispositivos de rede, cargas de trabalho em nuvem e aplicativos para uma cobertura de segurança mais ampla.

O *Wazuh* é uma solução de segurança defensiva com muitas habilidades encontradas em outros *softwares* de segurança de ponta. Ele é um *open-source* que possui funcionalidades de *HIDS (host-based intrusion detection system*) e *SIEM (Security information and event Management*). Essa solução foi lançada por volta de 2015 e originalmente é baseada no *OSSEC*.

O *Wazuh* fornece aos analistas uma correlação e contexto dos eventos em tempo real através do seu *dashboard*.

A funcionalidade *HIDS* analisa *logs* em tempo real, integridade de arquivos entre outras actividades no *host* onde ele está instalado, enquanto o *SIEM* faz o gerenciamento de eventos de segurança, colecta dados do maior número de fontes possíveis, com diferentes ferramentas de segurança.

O *Ossec* tem a capacidade de gerar alertas, enviá-las por e-mail e de até executar algum *script* ou programa para agir activamente diante de um incidente. Por exemplo, ao detectar um ataque ele poderá executar um *script* que criará uma regra de *firewall* bloqueando o *IP* do atacante, inclusive essa criação de regra poderá ser feita em todos os *hosts* onde houver um agente, ampliando a protecção da infra-estrutura em todas as pontas.

Actualmente o *Wazuh* possui quatro componentes que são:

- *Wazuh indexer*
- *Wazuh server*
- *Wazuh dashboard*
- *Wazuh agents*.

A figura a seguir ilustra o diagrama geral dos componentes do *Wazuh*.

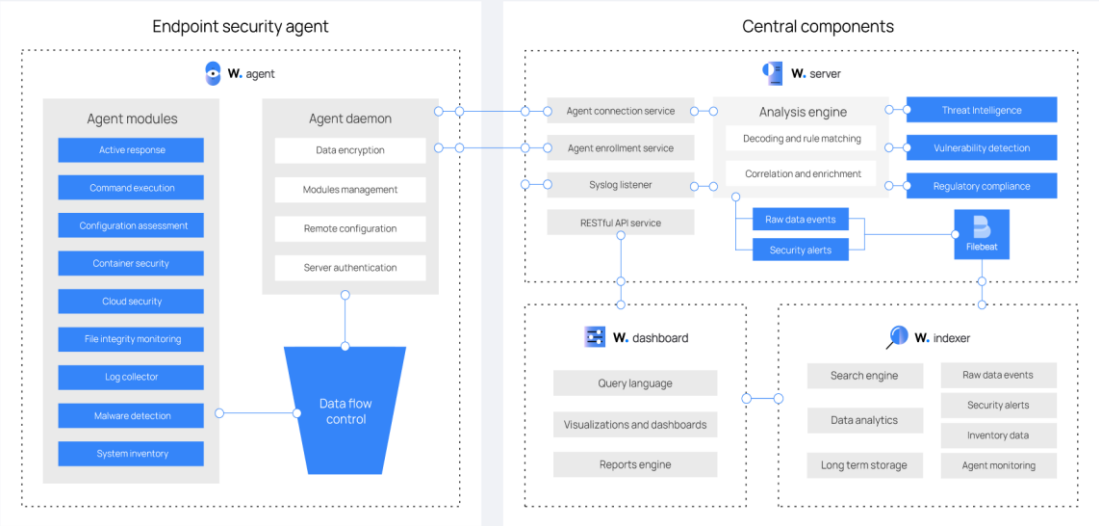

Figura 5.1 – Visão geral do diagrama geral dos componentes do Wazuh (Fonte: Wazuh, 2024).

Onde cada componente tem a função de:

- *Wazuh indexer*: é um componente central para indexação e armazenamento dos alertas gerados pelo *Wazuh server*.
- *Wazuh server*: recebe e analisa os dados recebidos pelos agentes distribuídos na rede. O *Wazuh server* pode ser formado por único servidor ou por um conjunto de servidores formando um *cluster*.
- *Wazuh dashboard*: é o componente responsável pela visualização e análise dos dados colectados.
- *Wazuh agents*: é instalado nos endpoints para realizar colecta de informações permitindo a prevenção e detecção de ameaças.

Na prática, funciona assim: a plataforma indexa os dados gerados pelo servidor, que é responsável por gerenciar e analisar os agentes. O painel permite a visualização e análise desses dados em tempo real e, juntos, estes três componentes formam a solução *Wazuh*.

O *Wazuh* possui as seguintes capacidades:

- Análise dos eventos de segurança colectados pelo *Wazuh agents*.

- Detecção de arquivos maliciosos nos endpoints monitorados pelo *Wazuh Agent* por meio de buscas por *malwares*, *rootkits* e comportamentos suspeitos.
- Monitoramento de *logs* de aplicação, de sistema e de integridade de arquivos.
- Detecção de vulnerabilidades com base em *CVE*.
- *Gerenciamento* de configuração de arquivos.

5.2.2. Detecção de intrusão

Os recursos de *IDS* do *Wazuh* permitem que ele monitore o tráfego de rede e os *logs* do sistema em busca de sinais de acesso não autorizado, *malware* e outras ameaças potenciais. Este é o módulo que realiza o monitoramento em tempo real de detecção de ameaças de tipos variados como infecção por *malware*, *rootkits*, ferramentas de acesso remoto, execução de comandos suspeitos, arquivos maliciosos escondidos, integração com assinaturas de *IDS*.

5.2.3. *Logs* de dados

È o módulo do *Wazuh* que regista eventos do sistema operacional e aplicações do *host,* monitorando por exemplo, versão do sistema. actividades de login, etc. Esse registo pode ser utilizado para restabelecer o estado original do sistema operacional ou para que o administrador conheça o seu comportamento no passado.

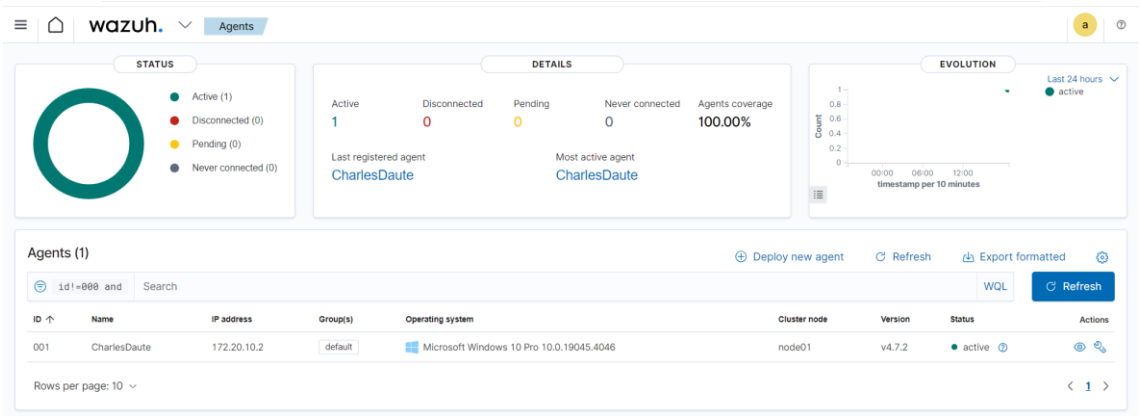

Figura 5.2 – Log de dados (Fonte: Autor, 2024).

5.2.4. Monitoramento de Integridade de Arquivos

O sistema de monitoramento de integridade de arquivos *(FIM)* observa os arquivos seleccionados e acciona alertas quando esses arquivos são modificados. O componente responsável por esta tarefa é chamado *syscheck*. O *syscheck* é a ferramenta que fornece feedback de aprovação ou reprovação em todas as verificações. Essa solução geralmente é

utilizada geralmente quando é preciso ter controle sobre acesso ou mudança de dados ou arquivos sensíveis.

5.2.5. Gestão de Vulnerabilidades

A gestão de vulnerabilidades fornece relatórios detalhados sobre as vulnerabilidades encontradas, incluindo informações sobre como corrigi-las. Isso permite que a empresa mantenha o sistema protegido contra ameaças de segurança.

Com a solução, você pode identificar, por exemplo, se as senhas usadas são fortes, se serviços desnecessários estão sendo executados ou se a *firewall* está configurada de forma adequada.

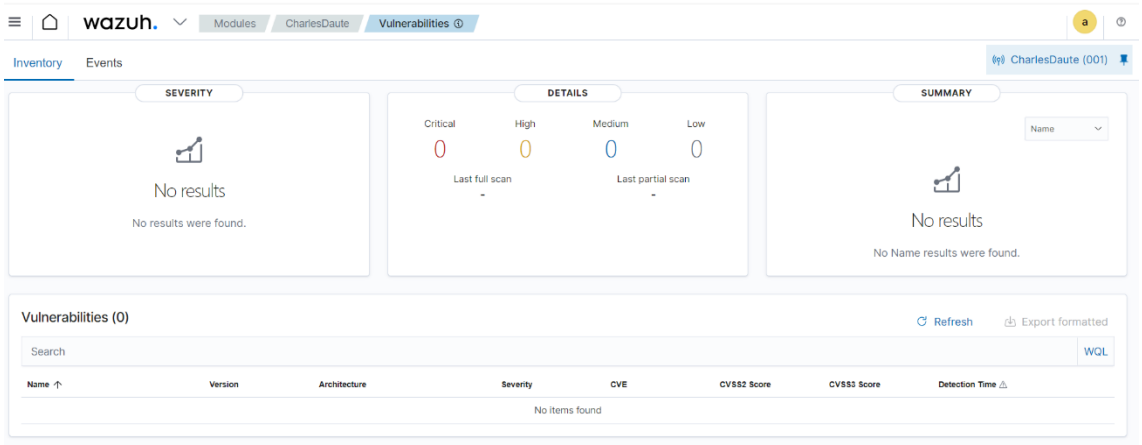

Figura 5.3 – Gerenciamento de vulnerabilidades (Fonte: Autor, 2024).

5.2.6. Compliance Regulatório

Essa função é utilizada quando se deseja estar em conformidade com aspectos técnicos de padrões regulatórios. Como empresa, é importante estar em conformidade com as regulamentações de segurança de dados aplicáveis no seu território. O *Wazuh* ajuda a atender a esses requisitos de conformidade, fornecendo recursos para monitorar e garantir o cumprimento das políticas de segurança de dados.

O *Wazuh* permite, por exemplo, a criação de regras específicas para monitorar o acesso a dados sensíveis e garantir que as políticas de segurança de dados sejam seguidas. O *Wazuh* também fornece relatórios regulares e personalizáveis para ajudar a verificar o cumprimento da conformidade e identificar rapidamente quaisquer problemas ou desvios.

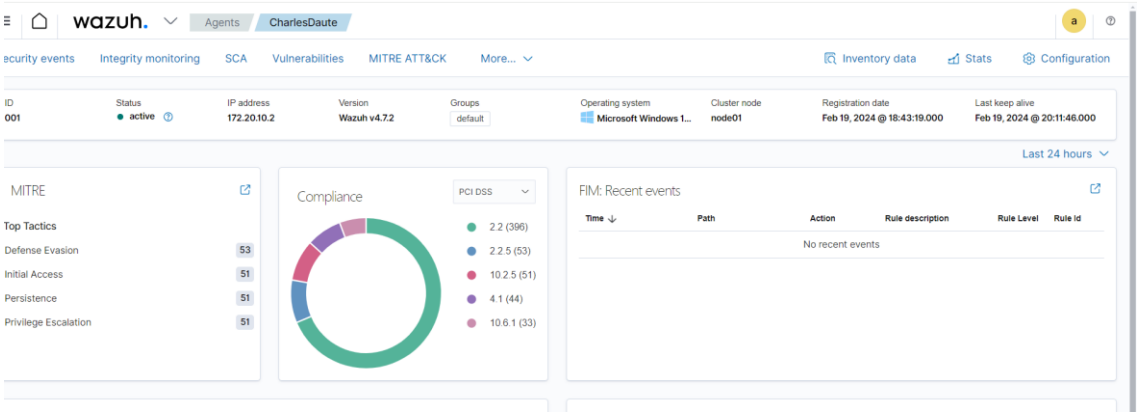

Figura 5.4 – Compliance regulatório (Fonte: Autor, 2024).

5.2.7. Segurança na Nuvem

Com a popularização da nuvem, a segurança de dados e infraestrutura tornou-se um desafio crescente para empresas e organizações. A solução *Wazuh* também foi projectada para atender a essa demanda, fornecendo monitoramento e segurança em ambientes de nuvem.

O *Wazuh* pode monitorar e detectar actividades suspeitas em instâncias da nuvem, como acessos não autorizados a dados confidenciais, modificações não autorizadas de configurações de segurança e ataques de força bruta. A solução oferece integração com provedores de nuvem populares, como *Amazon Web Services* (AWS) e *Microsoft Azure*.

5.3. Arquitectura e topologia proposta

Nesta secção, será apresentada a proposta de solução para o caso de estudo que é uma componente importante para este trabalho. Pelo cenário actual da organização, percebe-se a incapacidade no concemente a detecção de eventos de segurança na rede corporativa, assim sendo, a seguir será demonstrado a topologia e o cenário pretendido.

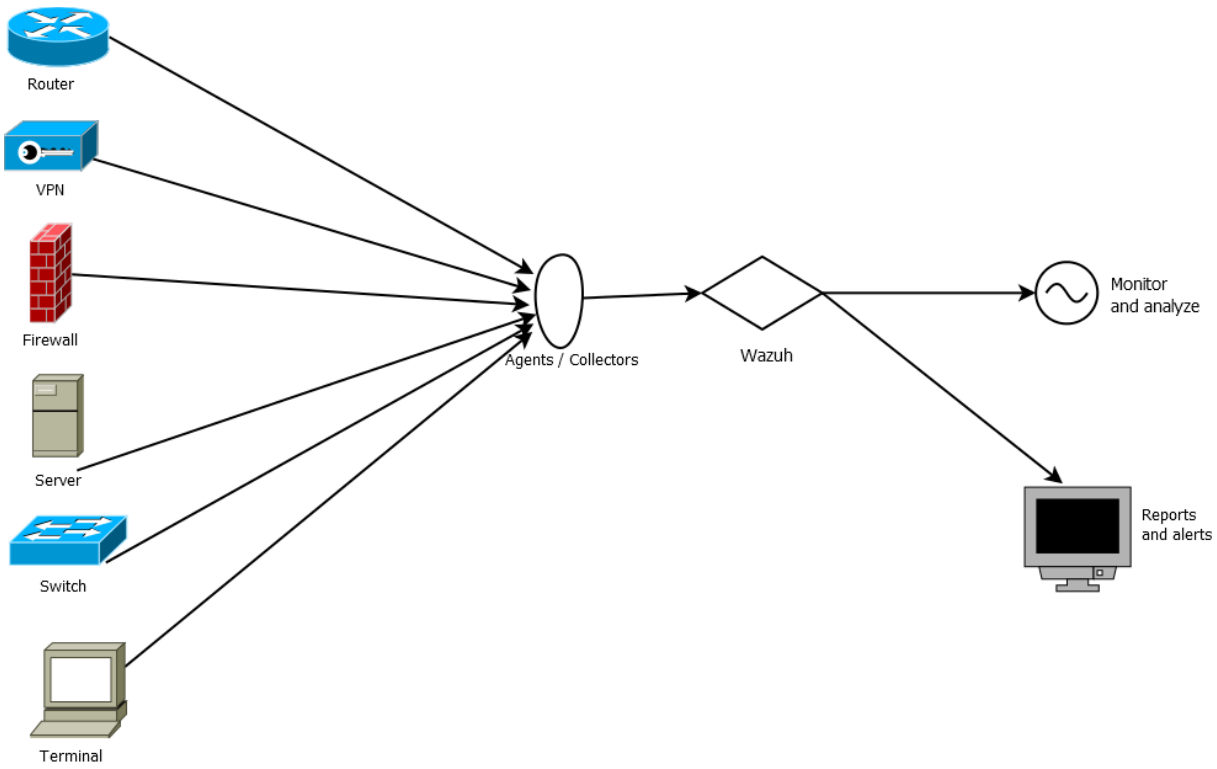

Figura 5.5 – Cenário com implementação de um SIEM (Wazuh) (Fonte: Autor, 2024).

5.3.1. Configuração do *Wazuh Server*

Como forma de proposta foi configurado um ambiente virtual simulado composto por uma máquina virtual servidor *Wazuh* pré-configurada (OVA) pelo fornecedor do *software* e uma máquina virtual cliente Windows.

O servidor *Wazuh* é o responsável por colectar e analisar dados dos agentes, desencadear alertas para anomalias detectadas e monitorar os status dos agentes.

Primeiramente foi feito o download do *Wazuh* pré-configurado OVA fornecido pelo fornecedor, e a seguir configuramos o ambiente, onde configuramos duas máquinas virtuais, onde uma é a máquina virtual servidor, e a outra é uma máquina virtual do agente *Wazuh*, a máquina que será monitorada.

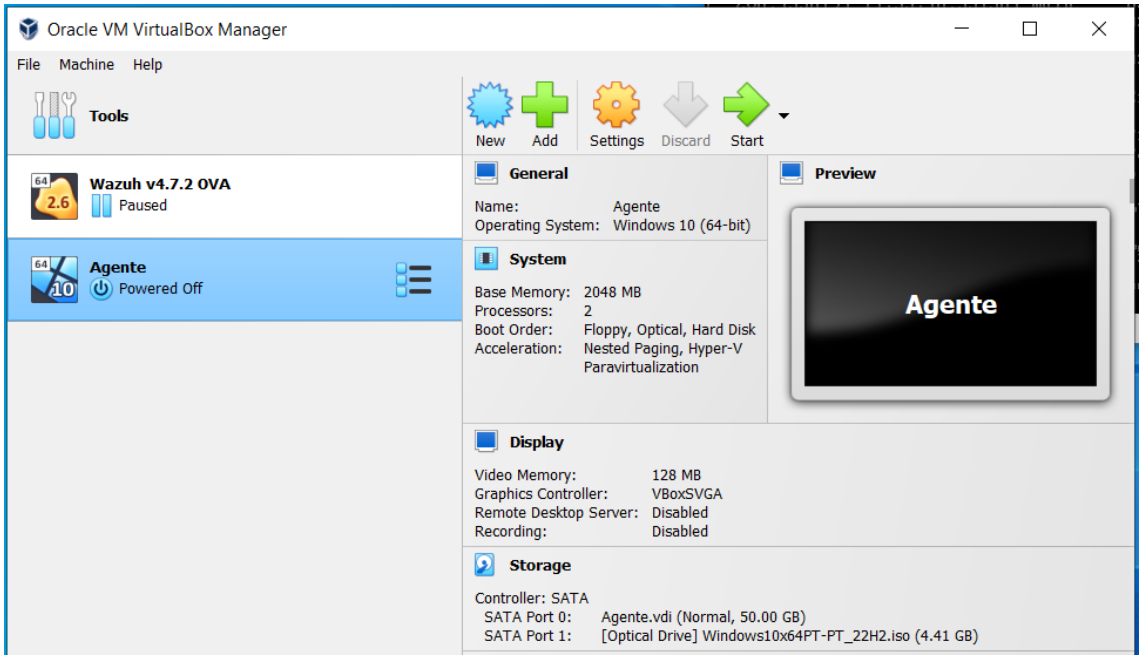

Figura 5.6 – Configuração do ambiente Wazuh Server e Wazuh Agent (Fonte: Autor, 2024).

De seguida importou-se o ficheiro *Wazuh* pré-configurado OVA para a máquina virtual servidor.

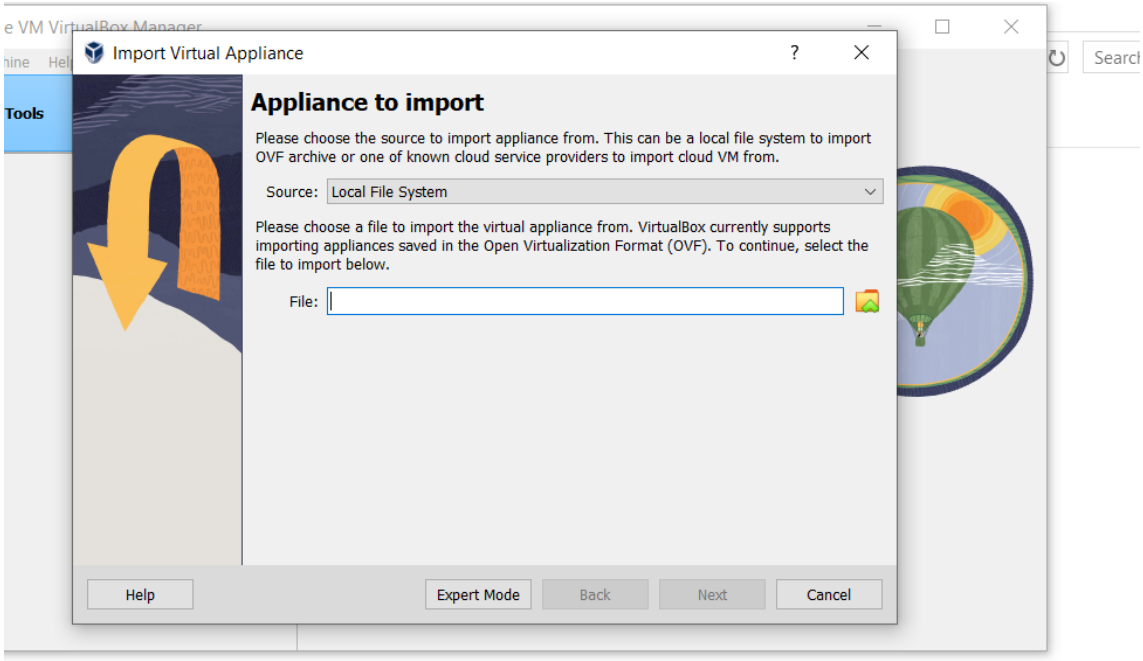

Figura 5.7 – Importação do ficheiro Wazuh pré configurado OVA (Fonte: Autor, 2024).

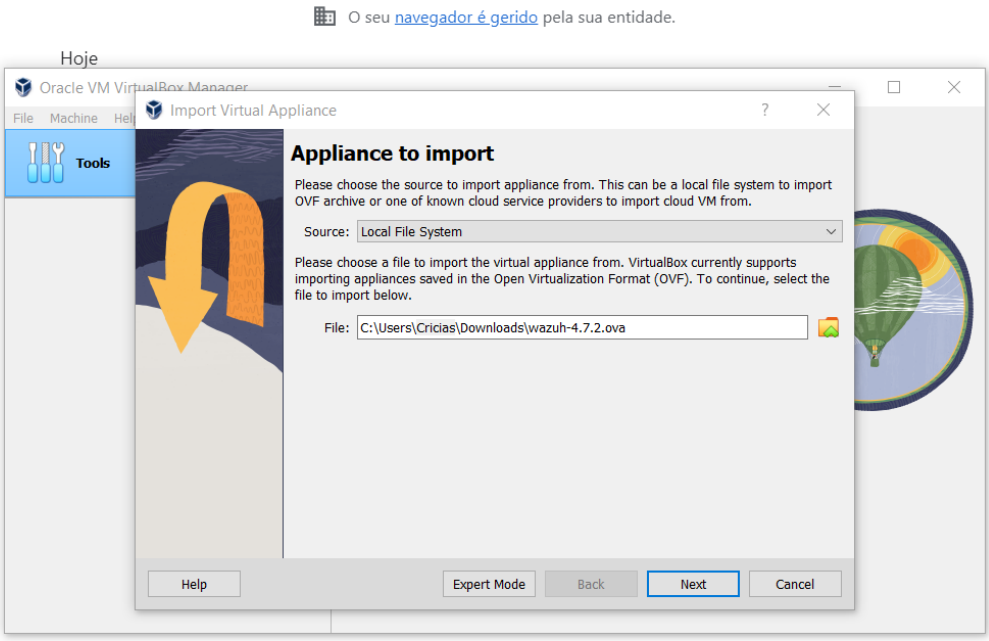

Figura 5.8 – Importação do ficheiro Wazuh pré configurado OVA (Fonte: Autor, 2024).

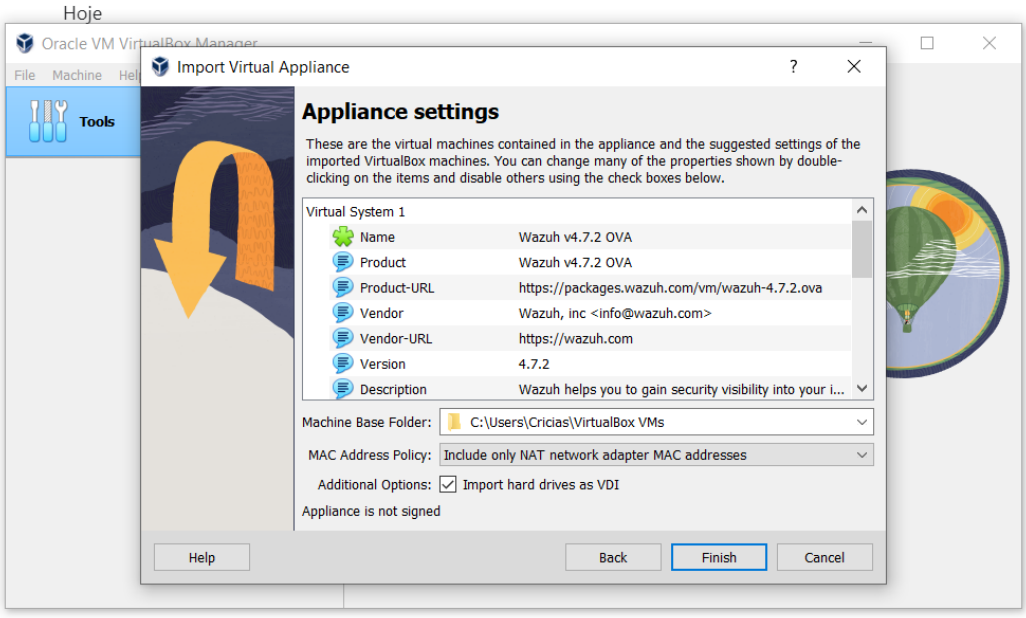

Figura 5.9 – Importação do ficheiro Wazuh pré configurado OVA para instalação (Fonte: Autor, 2024).

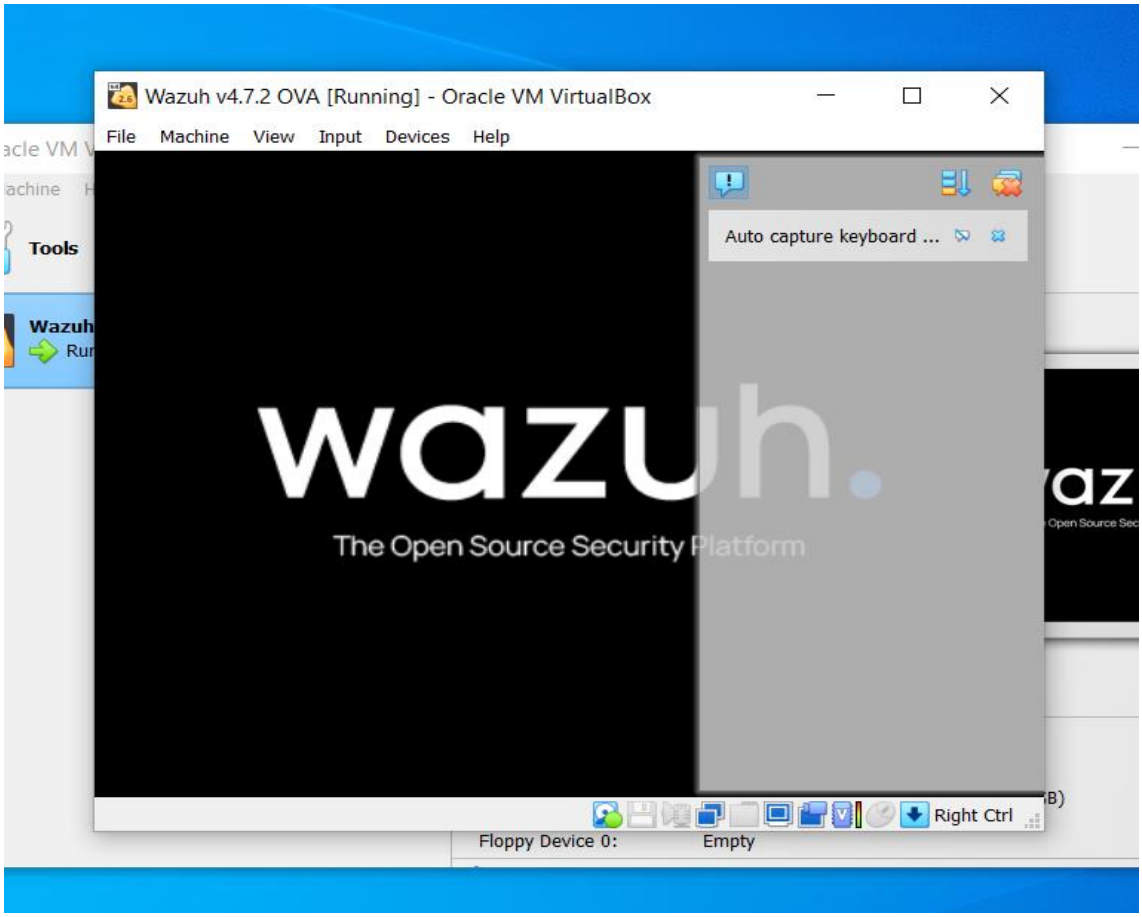

Figura 5.10 – Wazuh Server OVA instalado (Fonte: Autor, 2024).

Apos a realização de todos os passos, iniciamos a máquina virtual, onde iremos colocar as credencias do *Wazuh*, e identificar o *IP* gerado pelo servidor para poder ter acesso a interface do *Wazuh*, a *URL* de acesso (https://172.20.10.3, nome do usuário e senha).

Figura 5.11 – Tela inicial do Wazuh Server (Fonte: Autor, 2024).

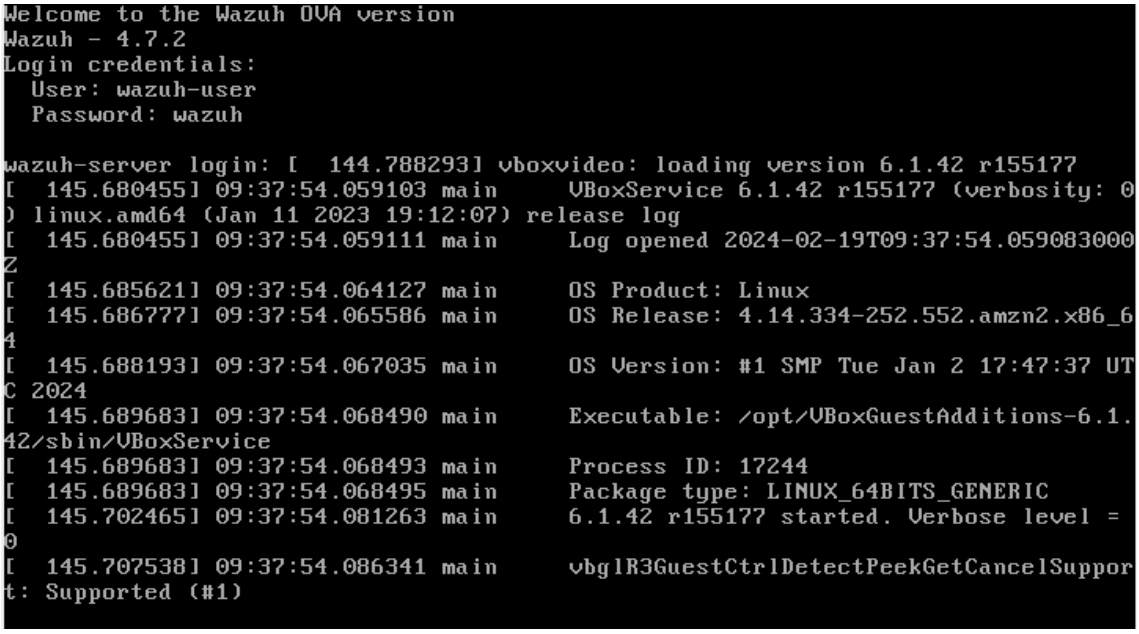

Figura 5.12 – Logando o Wazuh Server com as credenciais fornecidas pelo fornecedor (Fonte: Autor, 2024).

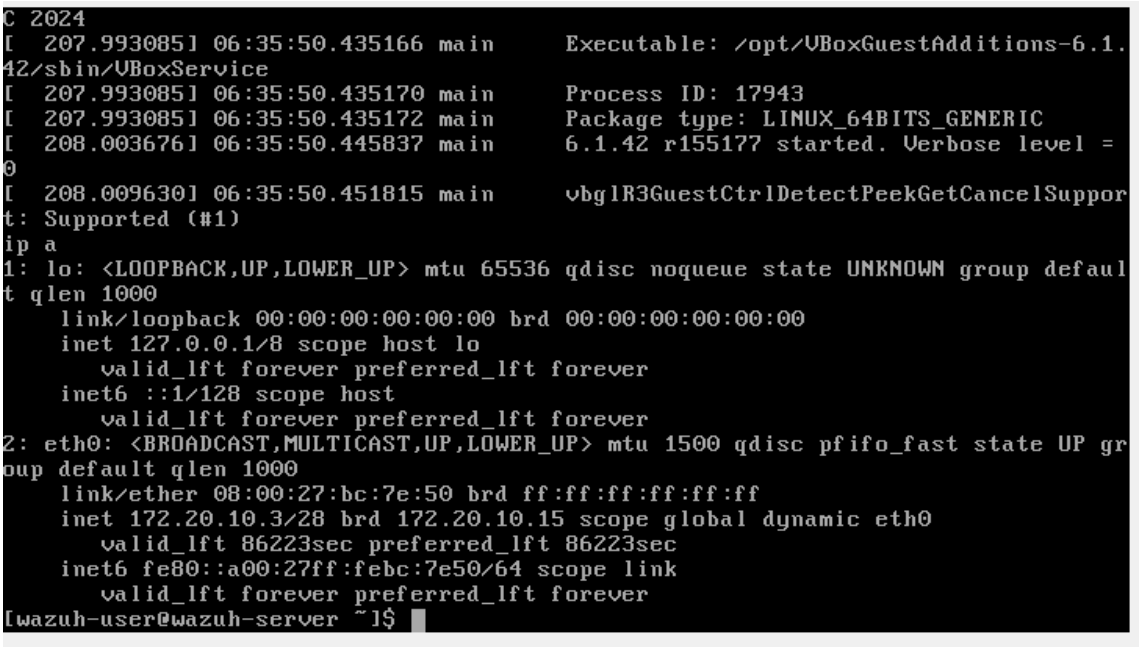

Figura 5.13 – Consulta do IP do Wazuh Server (Fonte: Autor, 2024).

Podemos verificar que a instalação funcionou e está operacional acessando o serviço através do *DNS* público associado ao servidor *Wazuh*, representado na figura 5.14.

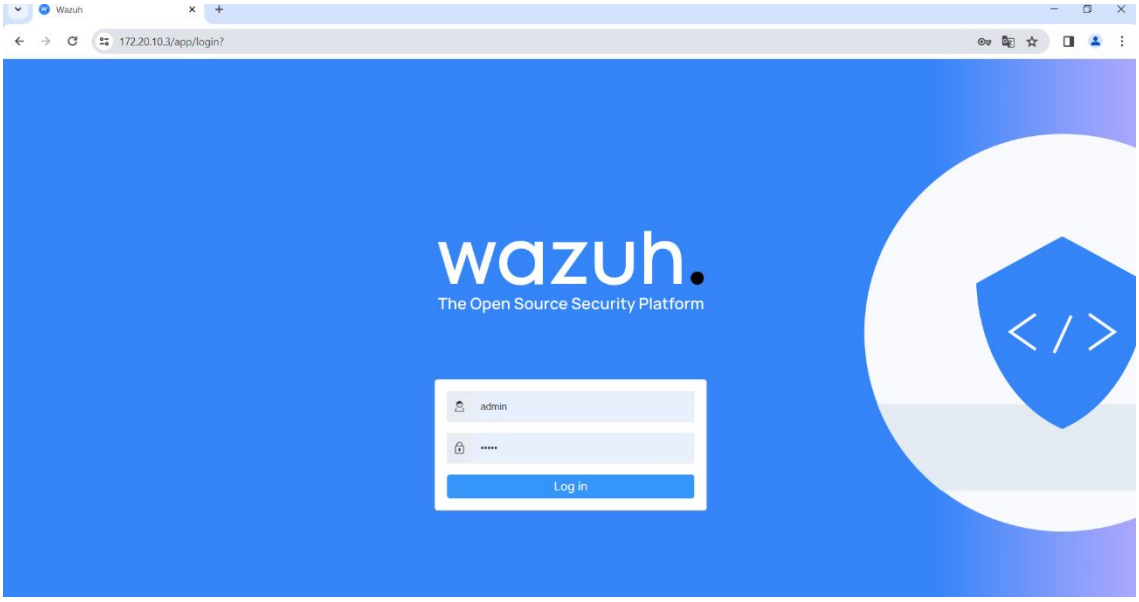

Figura 5.14 – Servidor Wazuh completamente operacional após instalação (Fonte: Autor, 2024).

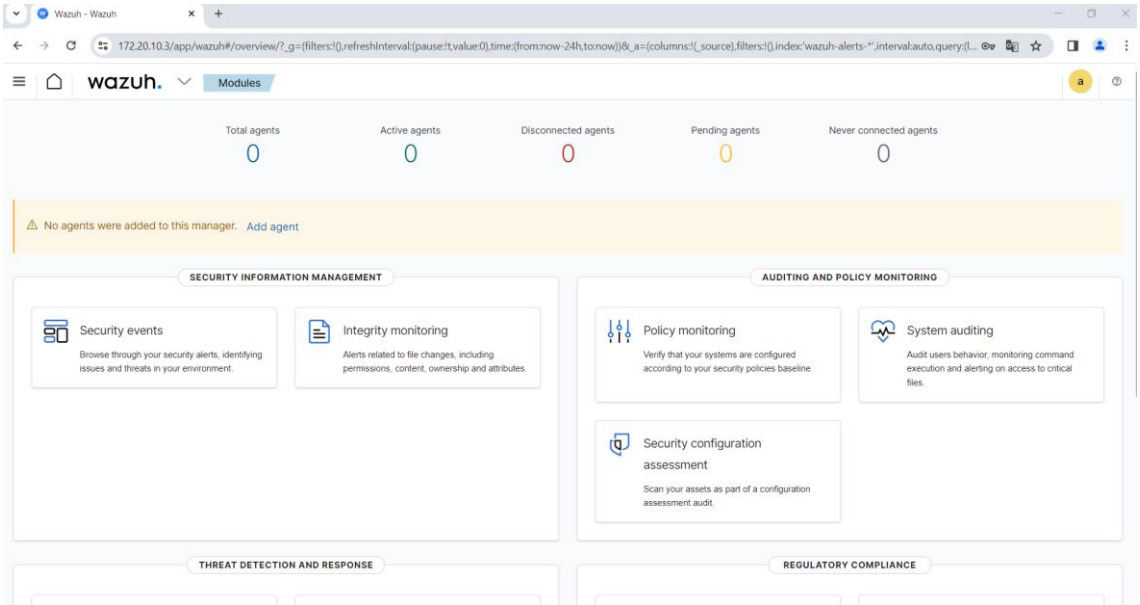

Figura 5.15 – Servidor Wazuh completamente operacional após a instalação (Fonte: Autor, 2024).

5.3.2. Configuração de Agente do *Wazuh*

Apos a configuração do *Wazuh Server*, vai se configurar o Agente. O Agente precisa ser registado com o servidor *Wazuh*, onde o registo é o processo de adicionar o agente à lista de agentes autorizados no servidor *Wazuh*.

Primeiramente criamos o grupo Windows, como ilustra a figura 5.16, para que quando formos a criar o agente ele vá para o grupo certo em termos de organização, e fazer uma divisão para criar configurações especificas para um determinado servidor.

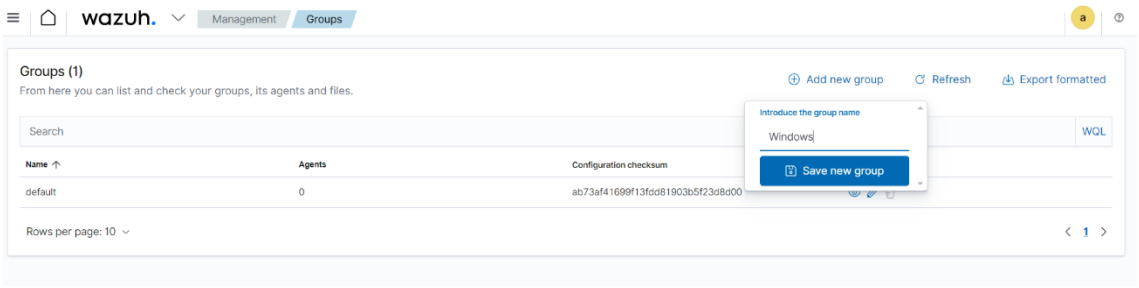

Figura 5.16 – Criando o grupo Windows (Fonte: Autor, 2024).

Criado o grupo Windows, vai se registar o Agente no servidor através do *IP* do servidor, no grupo em que foi criado na figura 5.16.

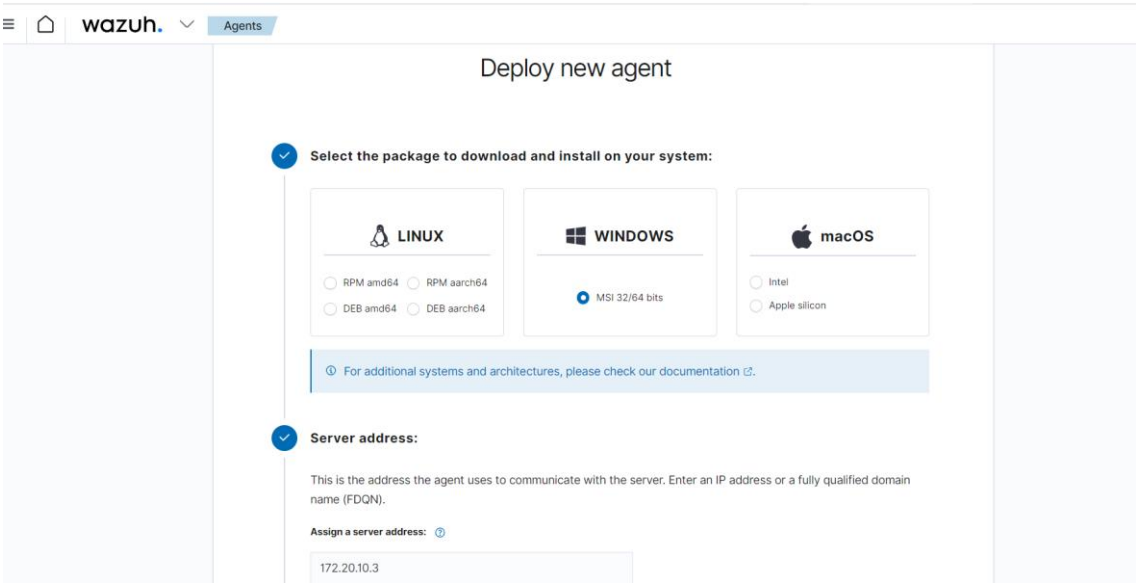

Figura 5.17 – Criando o Agente no servidor (Fonte: Autor, 2024).

De seguida, executa-se os comandos como ilustra a figura 5.18. Mas para executar os comandos, tem de se ter todos os privilégios como
administrador, e ter o *PowerShell* 3.0 ou mais recente onde se irá executar.

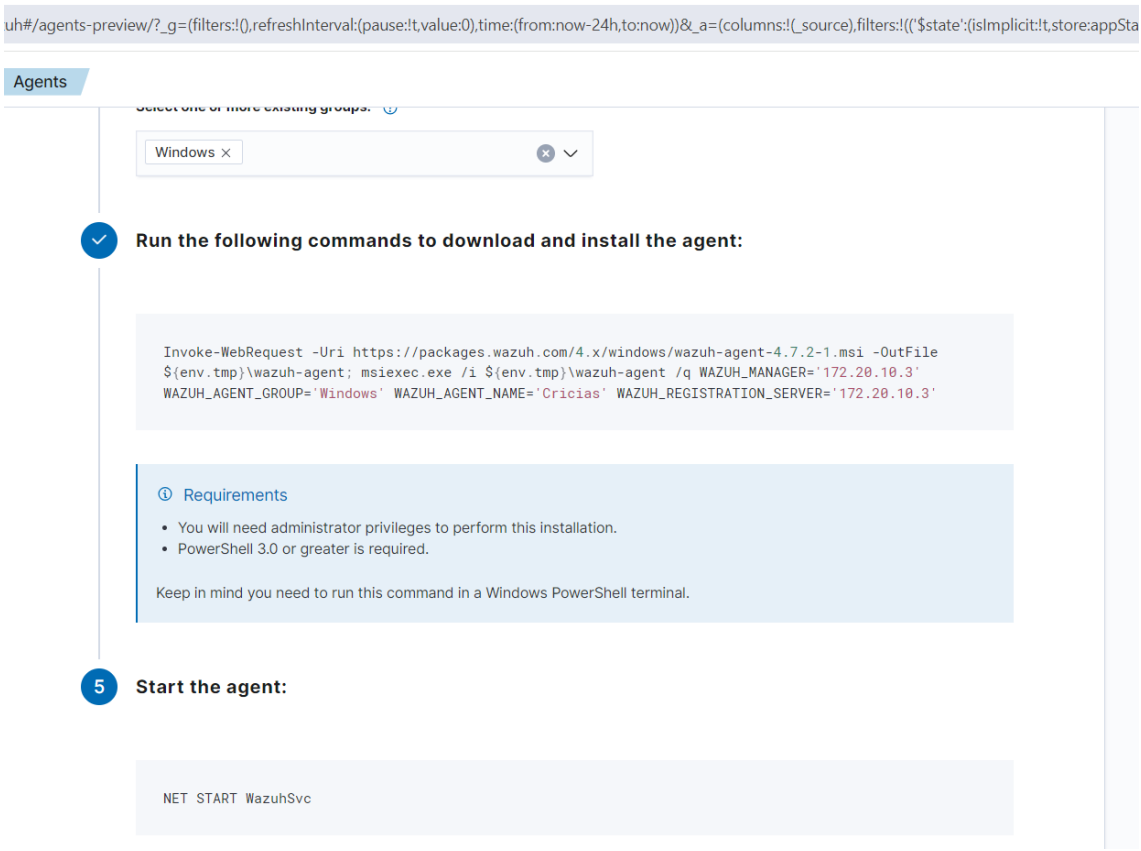

Figura 5.18 – Ilustrando os comandos (Fonte: Autor, 2024).

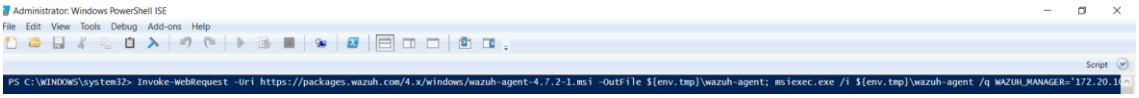

Figura 5.19 – Executando os comandos no PowerShell (Fonte: Autor, 2024).

E por último, fazemos o *Start The Agent* através do comando fornecido pelo fornecedor no *Wazuh Server* como ilustra a figura 18 no *powershell*.

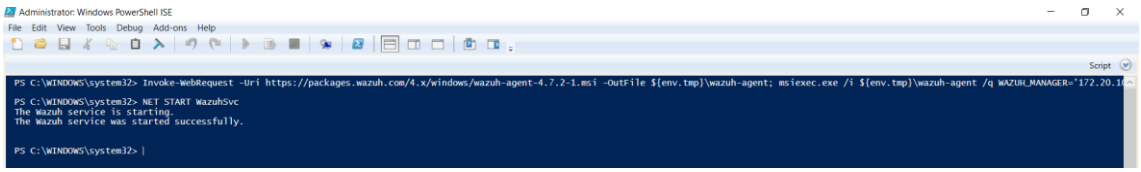

Figura 5.20 – Executando o comando para fazer o Start The Agent (Fonte: Autor, 2024).

Sendo assim, podemos ver no Servidor *Wazuh* que o Agente *Wazuh* foi registado com sucesso na figura 5.21.

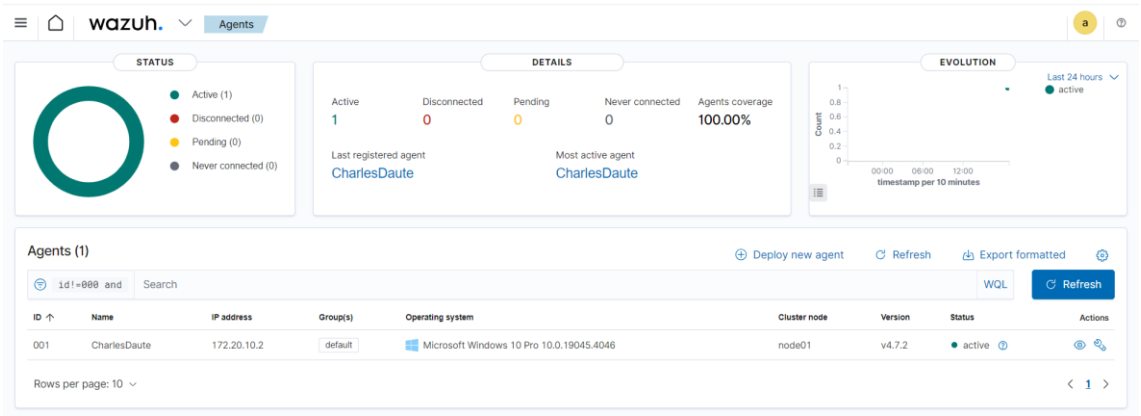

Figura 5.21 – Agente Wazuh registado (Fonte: Autor, 2024).

CAPÍTULO VI – ANÁLISE E DISCUSSÃO DOS RESULTADOS

A revisão da literatura visou em primeiro lugar, descrever a segurança cibernética em infra-estruturas de redes corporativas com destaque para mecanismos de segurança nomeadamente: *Firewalls*, *IPS* e *IDS*. Descreveu-se profundamente sobre o princípio de funcionamento destes e foram apresentadas algumas vantagens dos mesmos.

Aos sistemas de *firewall* são atribuídas responsabilidades, como a implementação da política de segurança da empresa no interior da rede protegida, entre outros, contudo eles apresentam alguns riscos como o de não protegerem contra-ataques de *malware*, como vírus, apesar do tráfego destes passar pela *firewall.*

A *firewall* não consegue impedir um ataque cuja origem e destino seja a rede interna, pois os dados não passaram por ele, tornando-o ineficaz nesse tipo de ataque.

As *firewalls* não aumentam força de senhas e nem previnem o uso inadequado das mesmas. Da mesma forma, eles são ineficazes em ataque não técnicos como Engenharia Social.

As *firewalls* não conseguem impedir que usuários acessem sites com códigos maliciosos, tornando necessária a conscientização dos usuários neste sentido.

A política de segurança da *firewall* deve ser revista periodicamente, de modo a garantir o bom funcionamento do mesmo. Além disso, é importante fiscalizar o funcionamento do mesmo com certa periodicidade para garantir que nenhum *Malware* ou *Cracker* tenha descoberto e esteja explorando alguma falha do mesmo.

As *Firewalls* não são capazes de interceptar conexões que não passam por ele, como por exemplo um usuário que acesse a internet usando um modem 3G.

No geral, esses mecanismos de segurança são cruciais e importantes para garantir a segurança de informações em meios digitais de empresas e instituições, entretanto, devemos ter consciência de que eles não são a pedra filosofal para os problemas de segurança em infra-estruturas de rede corporativa, desta forma, é crucial investir na segurança em camadas.

De seguida, estudaram-se os eventos (*logs*) e incidentes de segurança com o objectivo de se compreender o processo de registo de actividades de elementos que compõem uma infra-estrutura de rede corporativa. Feito isso, percebeu-se que os tais registos de actividade por si só não significam nada, porém, se forem devidamente recolhidos e investigados pode se descobrir um potencial incidente de segurança.

Finalmente, debruçou-se em torno das plataformas *SIEMs*, o *Wazuh*. O *Wazuh* que é um *opensource* que une a habilidade analítica de um *SIEM* com o poder de um *XDR*.

CAPÍTULO VII – CONCLUSÕES E LIMITAÇÕES

7.1. Conclusões

As soluções *SIEM* emergem da necessidade de adicionar mais um nível de segurança em infra-estruturas de redes corporativas de empresas ou instituições, principalmente para aquelas que lidam com o uso de *VPN* para o seu acesso remoto por ser uma empresa ou instituição dispersa, com suas filiais, e pelo seu transporte de informações seguras e sensíveis.

Com isso, por esses motivos e entre outros, as plataformas *SIEMs* devem ser vistas como uma obrigação.

O desenvolvimento do trabalho de pesquisa teve como objectivo geral analisar os desafios e soluções em segurança de redes de computadores em ambientes corporativos face ao trabalho remoto e híbrido em médias e grandes empresas do ramo de construção civil no território nacional (Mota-Engil Moçambique), e para se alcançar esse objectivo geral foram definidos três objectivos específicos nomeadamente:

- O primeiro, constituiu em identificar conceitos relacionados a segurança de redes de computadores em ambientes corporativos. Este objectivo foi cumprido, visto que ao longo do trabalho foi possível identificar os conceitos relacionados a segurança de redes de computadores em ambientes corporativos, tais como o conceito de *firewall*, *VPNs, IDS, IPS, SIEM,* entre outros.
- O segundo, constituiu em verificar os desafios e soluções adoptadas na Mota-Engil Moçambique. Este objectivo foi cumprido, visto ao longo do trabalho, através de princípios qualitativos e o estudo de caso da Mota-Engil Moçambique, foi possível verificar os fragilidades e desafios que a empresa enfrenta, descrevendo uma solução capaz de melhorar a sua segurança tecnológica.
- O terceiro e último objectivo consistia em identificar oportunidades de melhorias através do caso de estudo. Este objectivo também foi cumprido, pois ao longo do trabalho, debruçando-se através da descrição da solução, foi possível ver que com a plataforma *SIEM (Wazuh)* haveram melhorias, além da segurança em si da empresa, já não será preciso estar na *AD* e não terá nenhum custo, isto é, será grátis.

  Em suma pode-se afirmar que foi possível alcançar o principal objectivo do presente trabalho de pesquisa.

7.2. Limitações

Em fase de termino desta investigação, pretendemos delinear algumas limitações encontradas ao longo deste estudo.

Uma das limitações iniciais desta investigação foi a interacção com usuários remotos, por se tratar de uma empresa com filiais em algumas províncias de Moçambique, os usuários remotos não se encontravam na sede da Mota-Engil Moçambique.

Outra limitação encontrada, foi o facto de não poder mexer com a produção da empresa, o ambiente para realização do estudo teve de ser apenas simulado.

CAPÍTULO VIII – REFERÊNCIAS BIBLIOGRÁFICAS

- Abdul Gany (2021). Implementação de uma base de dados distribuída para monitoria de entrega de encomendas internacionais. Tete: Instituto Superior Politécnico de Tete.
- Anderson Nascimento (2014). Canaltech, Conceito de Antivírus: https://canaltech.com.br/amp/antivirus/o-que-e-antivirus/; Visitado em 16/08/2023.
- Arquitectura do IBM QRadar https://www.ibm.com/docs/pt-br/qsip/7.5?topic=deployment-qradar-architecture-overview; Visitado em 10/03/2024.
- Arquitectura do Elastic Security https://www.elastic.co/pt/blog/elastic-serveless-architecture; Visitado em 08/04/2024.
- Arquitectura do Splunk: https://medium.com/@gabrielaentringe/componentes-b%C3%A1sicos-de-uma-arquitetura-splunk-5b7145b0f778; Visitado em 4/03/2024.
- Conceito de Compliance Regulatório: https://www.diazerosecurity.com.br/pt/blog/wazuh-a-solucao-completa-para-protecao-de-dados-na-sua-empresa; Visitado em 18/02/2024.
- Conceito de Criptografia de dados e comunicações: https://www.hostinger.com.br/tutoriais/o-que-e-criptografia; Visitado em 6/12/2023.
- Conceito de Controle de acesso à rede (NAC): https://www.cisco.com/c/pt_br/products/security/what-is-network-access-control-nac.html; Visitado em 6/12/2023.
- Conceito de Metodologia: https://www.fm2s.com.br/blog/metodologia/amp; Visitado em 20/11/2023.
- Conceito de Redes Privadas Virtuais: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/seguranca/conteudo/redes-privadas-virtuais-VPN/Arquitetura-VPN.html; Visitado em 16/08/2023.
- Conceito de Referência bibliográfica: https://blogs.ua.pt/bibliotecainforma/?p=2309; Visitado em 20/11/2023.
- Conceito de IDS: https://www.gta.ufrj.br/grad/16_2_v1/2016IDS/conceituacao.html; Visitado em 6/12/2023.
- Conceito de Redes de Computadores: https://aws.amazon.com/pt/what-is/computer-networking/; Visitado em 6/21/2023.
- Conceito de Wazuh:

https://medium.com/@diegolopes962/uma-breve-descri%C3%A7%C3%A3o-do-wazuh-87eefa983150; Visitado em 28/01/2024.

- Conceito de Wazuh: https://wazuh.com/platform/siem/; Visitado em 28/01/2024.
- Conceito de Log de Dados: https://pt.wikipedia.org/wiki/Log_de_dados; Visitado em 18/02/2024.
- Conceito de Detecção de Intrusão: https://pt.linkedin.com/pulse/wazuh-sabe-o-que-%C3%A9-para-serve-funcionalidade-se-liga-felipe-amaral; Visitado em 18/01/2024.
- Conceito de Syscheck: https://support.lenovo.com/us/pt/solutions/ht509897; Visitado em 18/02/2024.
- Conceito de Gerenciamento de Vulnerabilidades: https://www.diazerosecurity.com.br/pt/blog/wazuh-a-solucao-completa-para-protecao-de-dados-na-sua-empresa; Visitado em 18/02/2024.
- Conceito de Wazuh: https://medium.com/@diegolopes962/uma-breve-descri%C3%A7%C3%A3o-do-wazuh-87eefa983150; Visitado em 18/02/2024.
- Conceito do Elastic Security: https://medium.com/@rafael.mmedeiros/o-que-%C3%A9-elastic-security-overview-3569ec4502fe; Visitado em 08/04/2024.
- Conceito de Análise Documental: https://revistas.fucamp.edu.br/index.php/cadernos/article/download/2356/1451; Visitado em 09/04/2024.
- Editora Conceitos.com (dez, 2013). Conceito de Antivírus.
- Entrevista Não Estruturada: https://www.redalyc.org/pdf/2410/241021497001.pdf: Visitado em 15/04/2024.
- Forte Security (2023). Boas práticas para manter sua rede corporativa segura.
- Fruhlinger, J (2022, março 16) Security Information and Event Management: https://www.csoonline.com/article/2124604/what-is-siem-security-information-and-event-management-explained.html; Visitado em 4/03/2024.
- Funcionalidades do Splunk:

https://www.remessaonline.com.br/blog/conheca-o-splunk-e-saiba-como-pagar-menos/ ; Visitado em 4/03/2024.

- Funcionalidades do IBM QRadar: https://www.ibm.com/br-pt/qradar; Visitado em 10/03/2024.
- Funcionalidades do Wazuh https://pt.linkedin.com/pulse/wazuh-sabe-o-que-%C3%A9-para-serve-funcionalidade-se-liga-felipe-amaral; Visitado em 10/03/2024.
- Funcionalidades do Elastic Security https://medium.com/@rafael.mmedeiros/o-que-%C3%A9-elastic-security-overview-3569ec4502fe; Visitado em 08/04/2024.
- IBM QRadar: https://www.ibm.com/docs/pt-br/qsip/7.5?topic=started-gradar-overview; Visitado em 10/03/2024.
- Limitações de *Firewall*: https://www.gta.ufrj.br/grad/15_1/firewall//limitacoesdofirewall.html; Visitado em 20/02/2024.
- Marconi, M. (2010). Metodologia científica. São Paulo: Atlas.
- Marconi, M. A; Lakatos, E. M. Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração e interpretação de dados. 3.ed. São Paulo: Atlas, 1996.
- Mota-Engil: https://www.mota-engil.com/areas-de-negocio/engenharia-e-construcao/; Visitado em 20/02/2024.
- Pedro Meirelles (2013/1). Redes de Computadores 1, Conceito de Firewall. Rio de Janeiro: Universidade Federal do Rio de Janeiro.
- ResearchGate, Conceito de Segurança de Redes em Ambientes Cooperativos: https://www.researchgate.net/publication/266124601_Seguranca_de_Redes_em_Ambientes_Cooperativos; Visitado em 16/08/2023.
- Splunk: https://www.splunk.com/en_us/about-splunk.htm; Visitado em 4/03/2024.
- Tanenbaum, A. (2011). Redes de Computadores (5 ed.). Sao Paulo: Pearson Universidades.

- Vielberth, (2018) Security Information and Event Management: https://www.researchgate.net/profile/Manfred-Vielberth-2/publication/349807309_Security_Information_and_Event_Management_SIEM/links/6041ebbd4585154e8c780a61/Security-Information-and-Event-Management-SIEM.pdf; Visitado em 4/03/2024;
- Vantagens do SIEM: https://vantix.com.br/blog/ciberseguranca/siem/; Visitado em 4/03/2024.
- Wikipédia, Conceito de Segurança de Redes: Https://pt.m.wikipedia.org/wiki/Segurança_de_rede; Visitado em 16/08/2023.