INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

A importância de uma *Firewall* e um Sistema SIEM dentro de uma organização

Tiago Manuel Mina de Carvalho Rio Maior

Dissertação para obtenção do Grau de Mestre em

Informática

Júri

Presidente: Professora Doutora Maria Inês Vasconcellos Furtado

Orientador: Professor Doutor Pedro Ramos dos Santos Brandão

Arguente: Professora Doutora Carla Sofia Rocha da Silva

Maio, 2026

[Página intencionalmente deixada em branco]

Dissertação de Mestrado realizada sob a orientação do Professor Doutor Pedro Ramos dos Santos Brandão, apresentada no ISTEC – Instituto Superior de Tecnologias Avançadas de Lisboa para obtenção de grau de Mestre em Informática.

[Página intencionalmente deixada em branco]

Agradecimentos

A concretização desta dissertação não teria sido possível sem o apoio, orientação e incentivo de várias pessoas às quais expresso a minha mais profunda gratidão.

Em primeiro lugar, agradeço ao meu orientador, Dr. Pedro Brandão, pelo seu rigor académico e toda a formação ao longo do Mestrado que passou. O seu conhecimento e contributos foram fundamentais para a estruturação e concretização deste trabalho.

Agradeço também ao ISTEC, e ao professor Dr. Paulo Duarte, Professor Pedro Crispim pela oportunidade e pelos recursos disponibilizados.

Gostaria de expressar o meu reconhecimento à empresa onde trabalho, pelo acesso às ferramentas e pela partilha de experiências que enriqueceram este trabalho.

Aos meus colegas e amigos, que estiveram ao meu lado durante todo este percurso, agradeço todas as palavras de incentivo e apoio constante nos momentos de maior desafio.

Por fim, e com especial destaque, agradeço à minha família, pelo amor, compreensão e motivação incondicional que sempre me transmitiram, sendo o pilar principal que me permitiu superar cada obstáculo ao longo deste percurso.

A todos, o meu mais sincero obrigado por tudo.

Índice

Índice de Figuras

Índice de Tabelas

Abreviaturas

SIEM – Gestão de Informação e eventos de segurança

PME – Pequenas e Médias Empresas

VPN – Rede Privada Virtual

TCP/IP – Protocolo de Controlo de Transmissão / Protocolo de Internet

TIC — Tecnologias de Informação e Comunicação

IoT — Internet das Coisas

NIST — Instituto Nacional de Normas e Tecnologia

ISO — Organização Internacional de Normalização

IBM — Máquinas Internacionais de Negócios

DDoS — Negação de Serviço Distribuída

IOA — Indicador de Ataque

SMTP — Protocolo Simples de Transferência de Correio

IOC — Indicador de Comprometimento

SOC — Centros de Operações de Segurança

CNCS — Centro Nacional de Cibersegurança

RFC — Pedido de Comentários

HTTPS — Protocolo Seguro de Transferência de Hipertexto

SSH — Shell Seguro

HTTP — Protocolo de Transferência de Hipertexto

IP — Protocolo de Internet

MAC — Identificador físico único (Media Access Control)

TCP — Protocolo de Controlo de Transmissão

TLS — Segurança da Camada de Transporte

XSS — Script entre Sites

SQL — Linguagem de Consulta Estruturada

DoS — Negação de Serviço

CPU — Unidade Central de Processamento

ACL — Lista de Controlo de Acessos

IDS — Sistema de Deteção de Intrusões

PC — Computador Pessoal

APT — Ameaças Persistentes Avançadas

API — Interfaces de Programação de Aplicações

USB — Barramento Série Universal

HMM — Modelo de Maturidade de Hunting

ENISA — Agência da União Europeia para a Cibersegurança

CERT — Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

CNPD — Comissão Nacional de Proteção de Dados

UE — União Europeia

ATT&CK — Táticas, Técnicas e Conhecimento Comum de Adversários

TTPs — Táticas, Técnicas e Procedimentos

ICS — Sistemas de Controlo Industrial

OWASP — Projeto Aberto de Segurança em Aplicações Web

PaaS — Plataforma como Serviço

Syslog — Protocolo de Registo de Sistemas

LAN – Rede local

WAN – Rede de área alargada

HA – Alta Disponibilidade

MGMT — Porta de Gestão

PUA — Aplicação Potencialmente Indesejada

XDR – Deteção e Respostas Alargadas

MDR – Deteção e Resposta Geridas

Resumo

Nos dias de hoje, a realidade dos sistemas de informação das organizações, está cada vez mais complexa e com requisitos de segurança mais exigentes. Nos últimos anos, a *firewall* tornou-se uma ferramenta essencial para atingir o nível desejado de isolamento dentro das várias redes existentes que uma organização pode ter.

A abordagem que tem sido cada vez mais posta em prova é de *Threat Hunting*, exigindo abordagens de segurança mais proativas e eficazes. Este tipo de caça às ameaças (*Threat Hunting*), um processo caracterizado pela identificação ativa e antecipada de potenciais riscos que possam vir a comprometer sistemas ou dados das empresas, este tipo de método, requer o uso de ferramentas avançadas de segurança, tais como, plataformas de Gestão de Informação e Eventos de Segurança (*Security Information and Event Management – SIEM)*, onde desempenham um papel essencial na deteção e análise de potenciais ciberameaças.

As plataformas SIEM permitem detetar e analisar dados provenientes de diversas fontes, como o tráfego de rede, registo de sistemas e informação de dispositivos, desde que os mesmos estejam devidamente configurados. Este tipo de análise permite identificar possíveis ameaças e gerar alertas em tempo real, possibilitando um tipo de resposta mais ágil e eficiente.

Esta dissertação explora o papel crucial das plataformas SIEM em conjunto com uma *Firewall* no contexto da caça às ameaças, com o foco nos desafios que são enfrentados pelas PMEs no atual contexto de ciberameaças. Vai ser analisado diversos tipos de conceitos com enfoque à *Threat Hunting*, os principais tipos de riscos que afetam as organizações, o tipo de cultura, bem como a relevância da inteligência de ameaças para uma abordagem mais eficaz.

Como demonstração da aplicabilidade prática destas soluções, vai ser elaborado um caso prático baseado na plataforma SIEM *Wazuh*, uma plataforma SIEM de código aberto, em conjunto com a *firewall* da *Sophos*. Este caso prático vai ter como objetivo avaliar a eficácia destas tecnologias na identificação e análise de possíveis ameaças existentes e a importância que consegue trazer às PMEs em estar num estado de alerta em tempo real e de conseguir decidir diversas medidas proativas para mitigar riscos cibernéticos. Este estudo visa ainda evidenciar como as plataformas SIEM em conjunto com uma *firewall* podem apoiar as PMEs na proteção dos seus sistemas e redes, no qual proporciona uma visão integrada da segurança e facilitando ações de mitigação baseadas em evidências num contexto prático real.

Palavras-chaves: *Sophos, SIEM, Segurança informática, PME*

Abstract

Nowadays, the reality of organisations' information systems is becoming increasingly complex and security requirements more demanding. In recent years, the firewall has become an essential tool for achieving the desired level of isolation within the various existing networks that an organisation may have.

The approach that has been increasingly put to the test is Threat Hunting, requiring more proactive and effective security approaches. Threat hunting, a process characterised by the active and early identification of potential risks that could compromise company systems or data, requires the use of advanced security tools, such as Security Information and Event Management (SIEM) platforms, which play an essential role in detecting and analysing potential cyber threats.

SIEM platforms make it possible to detect and analyse data from various sources, such as network traffic, system logs and device information, as long as they are properly configured. This type of analysis makes it possible to identify possible threats and generate alerts in real time, enabling a more agile and efficient type of response.

This dissertation explores the crucial role of SIEM platforms in conjunction with a Firewall in the context of threat hunting, with a focus on the challenges faced by SMEs in the current context of cyber threats. It will analyse various types of concepts with a focus on Threat Hunting, the main types of risks affecting organisations, the type of culture, as well as the relevance of threat intelligence for a more effective approach.

As a demonstration of the practical applicability of these solutions, a practical case will be developed based on the Wazuh SIEM platform, an open source SIEM platform, in conjunction with the Sophos firewall. The aim of this case study will be to assess the effectiveness of these technologies in identifying and analysing possible threats and the importance they can bring to SMEs in being alert in real time and being able to decide on various proactive measures to mitigate cyber risks. This study also aims to show how SIEM platforms in conjunction with a firewall can support SMEs in protecting their systems and networks, providing an integrated view of security and facilitating evidence-based mitigation actions in a real practical context.

Keywords: *Sophos, SIEM, Information Security, PME*

[Página intencionalmente deixada em branco]

1. Introdução

1.1. Objetivo

O objetivo desta dissertação foca-se essencialmente em dar uma base de estratégia de Cibersegurança na necessidade de as empresas estarem protegidas de ciberataques e dar a conhecer umas das soluções que existe no mercado a nível empresarial e perceber o quão eficaz é a ferramenta.

Com base nisso, promover a aprendizagem de uma abordagem de Cibersegurança, onde é fomentado o interesse de simular alguns ataques contra essa Ferramenta, a Sophos XG, utilizando várias ferramentas e processos para resolver estas ameaças que existem diariamente nas empresas e as mesmas estarem em alerta.

1.2. Questões de Investigação

O presente estudo pretende validar a seguinte hipótese: A importância que uma *Firewall* tem dentro de uma empresa. Para tal é necessário responder à seguinte questão:

1. Em que medida poderão as plataformas SIEM ser eficazes em conjunto com uma *Firewall* para a deteção e mitigação de ciberameaças para as PME?

1.3. Estrutura da Dissertação

No primeiro capítulo, é efetuada uma pequena introdução através da explicação dos objetivos, contexto e estrutura desta dissertação.

Capítulo 1 (Introdução): Este presente capítulo, é composto pela introdução, objetivo, questões de investigação que caracterizam o trabalho efetuado nesta dissertação.

Capítulo 2 (Metodologia): Descreve qual a metodologia usada para o projeto, baseado na metodologia da gestão de mudança, e a sua aplicação em contexto da empresa.

Capítulo 3 (Revisão da Literatura): Descreve vários processos para enquadrar os temas abordados nesta dissertação, desde o processo de procura, descrição da informação, análise da mesma.

Capítulo 4 (Enquadramento do Projeto): Neste capítulo é descrito as fases de desenvolvimento do projeto, o tipo de ferramenta utilizado, configurações, etc.

Capítulo 5 (Resultados): Descreve todo o projeto de investigação, análise e respetivos resultados obtidos.

Em suma, termina com os capítulos de **Discussão, Conclusão, Referências Bibliográficas e Apêndices.**

2. Metodologia da Aplicação

O modelo escolhido para esta dissertação foi o modelo de gestão de alteração de Kurt Lewin, surgiu na década de 1940 como uma estrutura para compreender e gerir mudanças dentro das organizações (Cuofano, 2024).

O modelo de Lewin consiste em três estágios principais: descongelar, alterar e congelar, onde acaba por fornecer uma abordagem estruturada para a transição dentro de organizações de um estado para o outro (Cuofano, 2024), deste modo, vai ser feito uma breve explicação das três fases:

- A primeira fase implica a preparação para a mudança, é o exato momento em que se vai enfrentar um novo problema e ainda não existe compromisso com a ação (Chohan, 2024);
- Durante a segunda fase, a pessoa está ativamente preparada para fazer a mudança e enfrentar a incerteza, no qual, simboliza o receio de abandonar processos antigos e a resistência à mudança (Chohan, 2024);
- Por fim, na terceira fase, ocorre uma transformação e a pessoa está pronta para congelar o seu novo estado, assim que as três fases estiverem concluídas, considera-se que ocorreu uma transformação bem-sucedida (Chohan, 2024).

Antes da implementação da *Firewall*, foram identificadas várias fases críticas que potenciaram esta mudança, tais como:

- Alterar os processos, estruturas e sistemas de organização;
- Alteração do tipo de tecnologia;
- Mudança da cultura da organização;
- Avaliação dos resultados.

Na primeira fase, existiu a necessidade de recolher várias informações sobre a infraestrutura da empresa para obter o máximo de informação sobre as dificuldades existentes da operação e corrigir as mesmas, que são as seguintes:

- Inexistência de uma proteção da infraestrutura licenciada e com registo de *logs*;
- Análise de *logs* complexa e demorada;
- Pouca informação ou inexistência de identificação de um serviço na infraestrutura.

Após identificação da necessidade de mudança, deu-se início à segunda fase, designada como Mudança, envolvendo a implementação da *Firewall* para recolha, monitorização e mitigação de ciberameaças, através da correlação dos eventos que existe na rede e dos *logs* de sistema. Foi definido alguns índices de comprometimento a nível organizacional, que são os seguintes:

Indicador Chave de Risco	Risco	Probabilidade	Impacto
Sessões falhadas c/ credenciais de Administrador	Alto	Alto	Alto
Informações dos Access Point	Alto	Médio	Médio
Tráfego c/ origem/destino suspeito	Médio	Médio	Médio

Tabela 1 - Índice de comprometimento para a organização escolhida Fonte: Autor

Após definir os Índices de Comprometimento, optou-se pela implementação da *Sophos XG Firewall*, adveio por uma questão de aquisição de contratação pública com serviços alojados com a própria *Firewall*, com o objetivo inicial de centralizar os *logs* das aplicações utilizadas na organização, criação de *VPN's*, centralização, controlo e monitorização dos *access points* da *Sophos*, para posterior análise e correlação, reduzindo assim a probabilidade de qualquer impacto no desempenho.

Este capítulo pretende descrever a metodologia aplicada, cujo objetivo é demonstrar a implementação da *Firewall* num contexto real, interligando-a a uma tecnologia *SIEM*, dando origem a deteção de possíveis ameaças cibernéticas e mitigação das mesmas através de uma análise ao tráfego das comunicações *TCP/IP*.

3. Enquadramento Teórico

3.1. Cibersegurança

3.1.1. O que é?

A Internet é uma infraestrutura de comunicação que se interliga, a um nível global, entre vários computadores e utilizadores. O seu papel dinamizador no quotidiano das empresas tem alavancado a digitalização de vários negócios e potenciado o empreendedorismo tecnológico (Antunes & R., 2022). A evolução da Internet ao longo de mais de 50 anos de vida é apreciável. As Tecnologias de Informação e Comunicação (TIC) têm passado por uma evolução significativa desde o seu início, alcançando altas taxas de transmissão e uma ampla variedade de aplicações.

Tal está bem visível nas melhorias obtidas pelo uso das TIC e da Internet num vasto leque de atividades levadas a cabo no ciberespaço, nomeadamente o tratamento e o processamento de informação, o fortalecimento de relações comerciais e sociais, a aprendizagem, o entretenimento e, mais recentemente, a Internet das Coisas (IoT, do Inglês *Internet of Things*) e a Indústria 4.0 (Antunes & R., 2022). A presença digital na Internet, por parte das empresas, das organizações e dos cidadãos, é, por isso, uma necessidade inquestionável e uma obrigação em prol do desenvolvimento, da competitividade e da inovação.

A gestão e a regulação distribuída da Internet encetaram vários desafios e potenciaram o aparecimento de um vasto leque de ameaças no ciberespaço. São inúmeras as vulnerabilidades e as ameaças às empresas, aos cidadãos e às instituições reguladores do ciberespaço, de que se destacam a proliferação de ataques intrusivos aos dados dos cidadãos e das empresas (Antunes & R., 2022). Este resultado, realçou-se no aumento crescente da vigilância às atividades dos utilizadores realizadas na Internet, que se traduziu na correspondente perda de privacidade.

Hoje em dia, a informática está munida com um vasto conjunto de meios tecnológicos para identificar, reagir e mitigar ameaças e ataques em curso, exemplo disso são as tecnologias de *firewall*, os mecanismos de autenticação e controlo de acesso, bem como a diversidade de normas e procedimentos oriundos de várias entidades internacionais, como o *National Institute of Standards and Technology* (NIST) ou a *International Organization for Standardization* (ISO) (Antunes & R., 2022). No entanto, há um conjunto de medidas proativas que deverão ser tidas em conta no planeamento das estratégias de segurança, sendo que a formação contínua e

a consciencialização dos utilizadores são as que têm maior impacto na prevenção de potenciais ataques às ciberameaças.

A quase inexistente preocupação com a segurança no desenho da Internet, o número considerável de equipamentos ligados e a sua heterogeneidade, bem como o número igualmente elevado de utilizadores com acesso à Internet, têm-na tornado mais complexa e com necessidades permanentes de vigilância, monitorização e resiliência (Antunes & R., 2022). A Internet tem-se tornando um espaço menos seguro para a comunicação, a partilha de dados e o trabalho colaborativo (Antunes & R., 2022).

A Internet é o componente mais relevante do ciberespaço e aquele onde mais utilizadores e aplicações se encontram interligados. Além desta infraestrutura física de comunicação, o ciberespaço inclui outros componentes fundamentais no contexto da comunicação global, como os dados que são produzidos e armazenados de forma distribuída em várias localizações (Antunes & R., 2022).

A autora Rita (2019) baseando-se em (Fernandes, 2012), o conceito de ciberespaço pode ser explicado como sendo uma rede global de infraestruturas de tecnologias de informação interligadas entre si, onde existe uma troca constante de dados e informações, no qual é extremamente dinâmico (Craigen, Defining Cybersecurity, 2014). Estas fazem com que seja um espaço mais propício ao crime, quando comparado com os ambientes tradicionais, o que faz com que a criminalidade *online* registe um crescimento ao longo dos anos (Gonçalves, 2019).

Por outras palavras, a segurança é um termo muito abrangente e pode ser aplicado em várias áreas. De uma forma geral, a segurança é um conceito que refere a ausência de ameaças ou perigo (Craigen, Defining Cybersecurity, 2014).

Em suma, são várias as definições para Cibersegurança, pelo que, de uma forma generalizada, esta define-se como um conjunto de tecnologias, processos e procedimentos que foram desenhados para proteger o ciberespaço de potenciais ataques ou ameaças, designadamente as redes, os computadores e outros dispositivos eletrónicos interligados, programas, dados e a iteração das pessoas através da sua presença virtual nas redes sociais e noutros espaços virtuais (Antunes & R., 2022).

3.1.2. Qual a importância da Cibersegurança?

O autor Bay (2020), partilha a opinião de que a Cibersegurança é importante na medida em que diversas organizações governamentais, corporativas, militares, médicas e financeiras, armazenam uma grande quantidade de dados em computadores, visto que estes dados são maioritariamente confidenciais e com informação sensível, que se forem expostos podem ter altas consequências negativas.

Atualmente é essencial que todas as empresas se consciencializem sobre a temática da segurança digital, pois o número de ataques cibernéticos tem sido cada vez mais frequente nos dias que correm.

A importância da Cibersegurança é fundamental para garantir a proteção dos dados pessoais, comerciais e governamentais que estão armazenados na internet, para evitar dessa forma, possíveis fraudes e crimes cibernéticos. A falta de segurança nos sistemas pode levar a graves consequências, como prejuízos financeiros, danos à reputação, perda de informações sensíveis, além de colocar em risco a privacidade e a segurança de indivíduos e empresas (Bay, 2020).

Além disso, a Cibersegurança é importante para garantir a continuidade dos serviços essenciais, como sistemas de energia, transporte e saúde, no qual são cada vez mais dependentes dos sistemas computacionais.

3.1.3. Ciberameaças

Uma ciberameaça ou *Cyber Threat* é definido como um ato malicioso com a intenção de provocar danos ao danificar os dados ou prejudicar o sistema informático de um indivíduo ou de uma empresa (Roy, 2021).

De acordo com Roy (2021), as ameaças cibernéticas buscam transformar vulnerabilidades potenciais em ataques reais a sistemas e redes. As ameaças à segurança cibernética podem incluir de tudo, desde *trojans*, vírus, *hackers* até *backdoors.*

Na maioria das vezes, o termo "ameaça cibernética combinada" é o mais apropriado, de acordo com Roy (2021), uma única ameaça pode envolver múltiplas explorações, por exemplo, um *hacker* pode usar um ataque de *phishing* para obter informações e invadir a rede.

Ciberameaça também se referem a um potencial ataque cibernético que visa obter acesso não autorizado, interromper, roubar ou danificar um ativo de TI, propriedade intelectual, rede de computadores ou qualquer outra forma de dados sensíveis.

3.1.4. Atores de ameaça

O termo de ator de ameaça é amplo e relativamente abrangente, estendendo-se a qualquer pessoa ou grupo que represente uma ameaça à segurança cibernética (IBM, 2023). Os atores de ameaça são frequentemente categorizados em diferentes tipos com base na sua motivação e, em menor grau, o seu nível de sofisticação (IBM, 2023).

O que torna os agentes de ameaças únicos é a sua capacidade de usar uma variedade de técnicas e ferramentas para atingir os seus objetivos, elas podem variar de ataques de *phishing* a *malware* e *ransomware*, até aos métodos mais avançados, como ataques *DDoS* e exploração de vulnerabilidades dentro de sistemas (Maile, 2023).

À medida que a tecnologia continua a avançar, o cenário de ameaças para empresas e utilizadores individuais têm-se tornando cada vez mais complexo, existindo vários tipos diferentes de ameaça, dos quais as organizações devem estar cientes, tais como (Maile, 2023):

- **Cibercriminosos:** São indivíduos ou grupos que usam tecnologia para cometer crimes, no qual são motivados por ganho financeiro e frequentemente focam-se em roubar dados (Maile, 2023).
- **Atores Estado-Nação:** Estados-nação e governos são grupos que financiam frequentemente agentes de ameaças com o intuito de roubar dados sensíveis, recolher informações confidenciais ou interromper a infraestrutura crítica de outro governo, este tipo de atividades maliciosas, normalmente inclui a espionagem ou guerra cibernética e tendem a ser altamente financiadas, tornando as ameaças complexas e desafiadores de detetar (IBM, 2023).
- **Hacktivistas:** Estes atores de ameaças usam técnicas de *hacking* para promover agendas políticas ou sociais, como espalhar a liberdade de expressão ou descobrir violações de direitos humanos (IBM, 2023). Um exemplo do grupo de *Hacking* é o *Anonymous*, que usou *hacking* e violações de dados para chamar a atenção para questões como corrupção governamental ou brutalidade policial, embora os hacktivistas possam não ter motivações financeiras, os seus ataques podem ter impacto significativo nos alvos a atingir (Maile, 2023).

3.1.5. Indicadores de Ataque

Em Cibersegurança, um Indicador de Ataque (IOA), são ferramentas essenciais para identificação antecipada de ameaças, basicamente são sinais reveladores ou atividades que sinalizam que uma potencial ameaça à segurança cibernética ou de um ataque em andamento (Bergmans, 2024). As IOAs são proativas e são uma parte vital dos estágios iniciais da deteção de ameaças, elas visam identificar e mitigar uma ameaça antes que esta possa se materializar completamente (Bergmans, 2024). Alguns exemplos de ataques IOAs:

- Conexões por meio de portas não padronizadas em vez da porta 80 ou da porta 443 (Edward, 2024).
- *Hosts* internos a comunicar com países fora do alcance comercial (Edward, 2024).
- Tráfego *SMTP* excessivo, pode ser evidência de um sistema comprometido sendo usado para lançar ataques *DDoS* (Edward, 2024).
- Logins de vários utilizadores de diferentes regiões, isto pode ser indicativo de credencias de utilizador roubadas (Edward, 2024).

As IOAs desempenham um papel fundamental na deteção precoce das ameaças cibernéticas, isto é crucial no mundo digital que está com uma grande aceleração, onde cada segundo conta. Ao identificar IOAs como um ataque em andamento, as organizações podem responder rapidamente a ameaças potenciais, geralmente ataques que podem trazer danos reais (Bergmans, 2024).

3.1.6. Indicadores de comprometimento

Um Indicador de Comprometimento (IOC) é uma evidência digital de que um incidente cibernético ocorreu, essa inteligência é recolhida por equipas de segurança em resposta a especulações de uma violação de rede ou durante auditorias de segurança programadas (Edward, 2024).

Enquanto as IOAs focam em detetar os sinais de um ataque que esteja a iniciar-se, por outro lado, as IOCs focam-se em indicadores de um ataque cibernético que ocorreu, as IOCs são as evidências de um incidente de segurança que os analistas vão recolher dados (Bergmans, 2024).

Desta forma, a principal diferença entre os dois é a sua posição na linha do tempo do ataque cibernético, como os IOAs ocorrem antes de uma violação de dados, se as respostas aos incidentes forem ativadas em tempo hábil, o incidente de segurança pode ser intercetado e prevenido (Edward, 2024).

3.1.7. Como se caracterizam e quais os tipos de ameaças de Cibersegurança?

No ciberespaço, existem diversas vulnerabilidades, estas são habitualmente exploradas tanto nas aplicações como nos sistemas operativos e no *hardware* dos servidores, por pessoas mal-intencionadas que pretendem provocar danos no alvo ou obter indevidamente informação privilegiada (Antunes & R., 2022). Após o estudo e a identificação das vulnerabilidades, os atacantes desencadeiam um conjunto de procedimentos que, na maioria dos casos, infringem uma intrusão na rede ou equipamento-alvo, tornando-o, assim, vulnerável.

Os ataques podem ter várias formas, desde o acesso remoto indevido, através da instalação de programas maliciosos (*malware)*, à usurpação de credenciais de acesso (Antunes & R., 2022). Genericamente, os ataques podem ser classificados em dois grupos principais:

- Os que exploram vulnerabilidades já conhecidas e para as quais já foi disponibilizada uma medida corretiva;
- Os que não são conhecidos, também designados por *zero day attacks*, visto que ocorrem pela primeira vez e não se sabe muito sobre a sua ação e sobre os danos que poderão causar.

As tendências e padrões ligados à exploração de vulnerabilidades e falhas de segurança são periodicamente revelados em relatórios técnicos elaborados por grandes empresas do setor. Entre os relatórios disponíveis para consulta, destacam-se os produzidos pela Trustwave Global Security Report e pelo Microsoft Digital Defense Report. Estes documentos analisam e organizam um grande volume de dados coletados pelos Centros de Operações de Segurança (SOC) dessas empresas ao longo de um período, com o objetivo de identificar perfis de ameaças, estatísticas sobre ataques e boas práticas a adotar.

O Centro Nacional de Cibersegurança (CNCS), especificamente o seu Observatório de Cibersegurança, disponibiliza regularmente diversos relatórios e boletins com informações sobre os tipos de ataques mais comuns e as principais medidas a tomar para os mitigar.

São também publicados relatórios específicos, nomeadamente para empresas e entidades públicas, onde é possível identificar boas práticas e diretrizes para melhorar a segurança cibernética.

A insegurança fundamental da Internet tem alguns aspetos relacionados com a segurança, que não fizeram parte dos princípios que guiaram o seu desenvolvimento inicial. A sua natureza demonstra a intenção de implementar uma infraestrutura acessível e aberta a todos, onde a tecnologia utilizada deveria ser de domínio público e com poucas preocupações sobre a segurança dos equipamentos e das aplicações que se comunicam. Como exemplo disso, não foi implementado qualquer mecanismo criptográfico ponto-a-ponto que assegurasse, desde o início, a confidencialidade das comunicações entre duas aplicações.

Com o tempo e com a globalização da Internet e a sua utilização diversificada, tornou-se evidente a necessidade de introduzir mecanismos de segurança capazes de garantir a confidencialidade, a integridade e a autenticação dos dados. Diante dessa realidade, foram desenvolvidos e implementados diversos algoritmos criptográficos, posteriormente integrados nas aplicações que usamos. Tecnologias de deteção de software malicioso, implementação de controlo de acesso e autenticação segura também passaram a ser incorporadas nas redes das empresas e nos seus servidores.

Assim, na fase de planeamento e implementação de redes de computadores baseadas nas tecnologias da Internet, devem ser integrados todos os mecanismos de segurança disponíveis e que possam mitigar, ao máximo, a exploração de vulnerabilidades e a tentativa de intrusão ou acesso indevido.

A adoção de medidas preventivas e a definição de vários perímetros de segurança na infraestrutura de rede são uma necessidade absoluta e devem estar sempre presentes nas fases de planeamento, implementação e monitorização de uma solução tecnológica de redes de computadores, tendo em conta a premissa inicial de que a Internet, por definição, não é segura.

Infraestrutura Física – o acesso aos equipamentos que asseguram a interligação de uma rede empresarial à Internet deve ser condicionado e apenas permitido pontualmente. Estes equipamentos estão, normalmente, alojados em salas específicas (*datacenters*), onde a presença física deve ser igualmente condicionada e fortemente vigiada (Antunes & R., 2022). Alguns dos ataques físicos incluem o roubo ou a desativação de equipamentos, especialmente de armazenamento de dados, o acesso local e físico às consolas dos equipamentos e a instalação de dispositivos de recolha ilegítima de dados;

Protocolos – os protocolos da Internet são baseados em mensagens simples e em formato de texto. Ou seja, a utilização de programas de captura de pacotes de redes (por exemplo, o *Wireshark)* permite facilmente recolher o conteúdo integral das mensagens. Inicialmente, os protocolos não tiveram em linha de conta aspetos relacionados com a segurança, como a autenticação e a cifragem das mensagens. Neste sentido, tendo acesso ao formato das mensagens, disponível nas *Request For Comments* (RFC) dos protocolos, é possível interagir com um servidor aplicacional e executar ações maliciosas apenas com recurso ao conhecimento do funcionamento dos protocolos. Torna-se, assim, importante garantir que são usadas as versões seguras dos protocolos aplicacionais, pois estas asseguram a integridade e a confidencialidade dos dados através da adoção de algoritmos criptográficos, exemplo disso, é o *Hypertext Transfer Protocol Secure* (HTTPS) e o *Secure Shell* (SSH) devem ser utilizados em detrimento dos seus congéneres não seguros (*Hypertext Transnfer* Protocol (HTTP) e Telnet (Antunes & R., 2022);

Documentação Pública – no seguimento do item anterior, é importante realçar que toda a informação referente ao funcionamento dos serviços e dos protocolos da Internet que se encontra acessível de forma gratuita e simples (Antunes & R., 2022). Estando esta documentação disponível, é igualmente possível desenvolver programas que produzem pacotes IP com conteúdo malicioso, mas cujo formato não levante suspeitas nas diversas operações de controlo que são realizadas pelas equipas de gestão da rede. O desígnio da Internet de disponibilizar de forma acessível todos os detalhes sobre o seu funcionamento e os protocolos que dela fazem parte pode, assim, ser aproveitado para desenvolver aplicações maliciosas. Também por esta razão, os sistemas operativos e as aplicações de todos os equipamentos ativos devem estar sempre atualizados, mitigando, assim, a exploração de vulnerabilidades e ameaças que já são conhecidas e para as quais já foi desenvolvida a correspondente correção.

Man-in-the-middle – a recolha dos pacotes que circulam na Internet, por exemplo entre duas aplicações, e a possibilidade de os alterar maliciosamente e de os voltar a retransmitir designa-se por ataque de *Man-in-the-middle*. Novamente, tendo em conta que algumas mensagens circulam sem cifragem, a análise do seu conteúdo para fins ilícitos torna-se fácil e tecnicamente bastante acessível (Antunes & R., 2022);

MAC e IP *spoofing* – trata-se de uma técnica que envolve a modificação do endereço IP e/ou MAC de uma interface de rede com o objetivo de capturar mensagens que normalmente não são destinadas ao computador onde essa alteração foi realizada. Dessa maneira, torna-se possível ouvir comunicações que não estavam previamente destinadas a esse dispositivo;

TCP – na camada de transporte, a principal preocupação é a proteção dos dados trocados entre aplicações por meio de uma conexão TCP. A estratégia mais comum é o uso de conexões TLS para enviar os dados de forma segura, permitindo, por exemplo, uma comunicação web protegida via HTTP seguro (HTTPS). Uma das preocupações nesse contexto é o uso de certificados digitais criados com algoritmos criptográficos de baixa segurança.

Aplicações e serviços – Na camada de aplicação, as vulnerabilidades são significativas e estão diretamente ligadas ao desenvolvimento inadequado dos programas utilizados pelos clientes e servidores dos serviços da internet. Para cada aplicação existem diversas vulnerabilidades, que geralmente surgem de erros no desenvolvimento do software, e a maioria está associada ao serviço *web* (Antunes & R., 2022). Alguns exemplos são:

- ***Buffer overflow*** – permite que um programa aceda a uma área de memória não protegida, podendo, assim, obter os valores de variáveis aos quais não teria acesso (Antunes & R., 2022);
- ***Cross-Site Scripting*** **(XSS)** – Técnica utilizada em aplicações *web* para permitir que uma aplicação cliente execute *scripts* diretamente em páginas *web*, podendo, assim, mostrar informação não autorizada ou ultrapassar controlos de acesso estabelecidos (Antunes & R., 2022);
- ***SQL injection*** – técnica muito frequente que consiste em enviar uma mensagem HTTP, com comandos maliciosos de *Structured Query Language (*SQL), para aceder indevidamente ao conteúdo de uma base de dados (Antunes & R., 2022);
- ***Remote access*** – Vulnerabilidades das aplicações que permitem o acesso remoto aos equipamentos, normalmente como utilizador com acessos privilegiados (Antunes & R., 2022).

Denial Of Service (DoS) – um tipo de ataque muito comum que tem como principal objetivo desativar um serviço (por exemplo, o serviço *web*) através do aumento anormal do número de pedidos que é feito ao servidor. Cada pedido efetuado a um servidor origina o consumo de dois recursos fundamentais: *CPU* e memória. Se o número de pedidos simultâneos for muito superior ao número máximo suportado pelo servidor, este irá invariavelmente ficar indisponível logo que os recursos sejam totalmente esgotados (Antunes & R., 2022). Esta técnica pode ser efetuada de forma distribuída (*Distributed Denial of Service (DDoS))* e com recurso a uma rede de computadores configurada para o efeito (*botnet)*, em que o ataque a um

único servidor é iniciado a partir de vários pontos, com o objetivo de mais rapidamente o tornar indisponível (Antunes & R., 2022).

Serviço *web* – proliferam as mais diversas atividades no serviço *web.* Inicialmente usado para consulta e partilha de conteúdos, foi sendo progressivamente utilizado em muitas outras atividades (Antunes & R., 2022). Uma das que mais danos tem causado está relacionada com as transações comerciais e o pagamento eletrónico com cartão de crédito.

Existe uma vasta lista de medidas que pode tomar para mitigar totalmente ou parcialmente as vulnerabilidades que foram apresentadas anteriormente, no entanto, na maioria dos casos, bastará uma mudança de atitude e a instalação de aplicações específicas, tais como, *firewalls*, antivírus ou sistemas de deteção de intrusões. Noutros casos, as medidas poderão ser mais abrangentes e envolver mais setores da empresa (Antunes & R., 2022).

Os equipamentos de comutação, *routers* e *switches*, permitem definir listas de controlos de acesso, designadas como ACL, cujo objetivo consiste em definir políticas que permitam aceitar ou bloquear determinado tráfego proveniente de ou com destino a uma determinada rede ou computador.

As *firewalls* são programas que efetuam o filtro do tráfego de rede através de vários parâmetros, como os endereços *IP*, os endereços *MAC* ou os protocolos aplicacionais (Antunes & R., 2022).

Os sistemas de deteção de intrusões, designado como *IDS*, funcionam, normalmente, através de assinaturas das intrusões e vírus já existentes, não sendo, por isso, viáveis para situações de novos vírus que ainda não tenham aparecido (Antunes & R., 2022). Estes programas utilizam técnicas de deteção de padrões e analisam a existência de atividade maliciosa nos pacotes processados pela interface de rede e também nas operações desencadeadas pelo sistema operativo.

As aplicações apresentadas anteriormente atuam na filtragem de pacotes e posterior deteção de padrões anormais que poderão indiciar a existência de um ataque (Antunes & R., 2022). Trata-se por isso, de aplicações essencialmente reativas e que permitem aos técnicos de gestão da rede identificar os incidentes e tomar decisões sobre as ações a desenvolver com vista à reposição da normalidade (Antunes & R., 2022).

A nível da prevenção, é possível encontrar vários procedimentos de boas-práticas que poderão minimizar a ocorrência de anomalias:

- Instalar e configurar eficientemente os sistemas operativos e aplicações, recorrendo sempre às últimas versões estáveis. Evitar as instalações por predefinição e afinar cuidadosamente os parâmetros relacionados com a segurança (Antunes & R., 2022).
- Recolher, analisar e interpretar os registos de funcionamento dos servidores, tentando, assim, identificar situações anormais que requeiram intervenção. A análise eficiente de relatórios da atividade dos servidores, vulgarmente designados por ***logs*** é fundamental para identificar proactivamente a necessidade de intervenção (Antunes & R., 2022).
- Implementar vários níveis de segurança na rede, não recorrendo apenas a uma técnica em particular, exemplo disso, a existência de uma ou mais *firewalls* não deverá permitir que se abdique de um *IDS* ou de uma aplicação de antivírus nos servidores e nos PC da rede. São aplicações diferentes e com objetivos distintos, mas que contribuem para o objetivo global: a proteção da rede, dos servidores, dos PC e dos dados que estão armazenados (Antunes & R., 2022).
- Efetuar sempre o acesso remoto à rede empresarial através de uma *virtual private network* (VPN), assegurando, assim, a confidencialidade e a autenticação da ligação. Esta solução é particularmente relevante na adoção do teletrabalho, permitindo aos trabalhadores acederem aos serviços da empresa através de uma ligação segura e iniciada no PC. A utilização de uma VPN obriga a uma autenticação válida e garante a confidencialidade do tráfego gerado entre os extremos comunicantes (Antunes & R., 2022).

As soluções tecnológicas descritas anteriormente e outras que possam implementar-se para proteger a infraestrutura de rede e de servidores de uma empresa terão de ser acompanhadas de consciencialização e boas-práticas por parte dos colaboradores (Antunes & R., 2022). O fator humano é fundamental para a eficácia dos vários perímetros de segurança que são definidos. Do ponto de vista tecnológico, é sempre possível adicionar complexidade e eficácia à segurança da infraestrutura de rede. Contudo, a menor consciencialização dos utilizadores, a falta de conhecimento técnico para manter as soluções de segurança adotadas, a falta de formação contínua em segurança da *Internet* e Cibersegurança e a deficiente monitorização e acompanhamento dos eventos de segurança que possam ocorrer contribuirão ativamente para o aumento da exposição ao risco por parte da empresa (Antunes & R., 2022).

3.1.8. Cultura de Segurança nas empresas

Nos últimos anos, as organizações têm lutado pela competitividade do mercado. Ao mesmo tempo que estão a lutar pela competitividade, o impacto tecnológico tem forçado as organizações a realizar mudanças significativas na sua gestão estratégica quanto na gestão interna.

Durante o início do século XX, houve um significativo avanço teórico voltado para a compreensão e a descrição das mudanças contantes presentes nas organizações.

No contexto competitivo atual do mundo organizacional, a abordagem cultural é amplamente considerada como um paradigma analítico relevante (Caetano & Vala, 2007). A cultura organizacional é definida como um conjunto de valores, crenças, normas, tradições, entre outros, que são partilhadas por um grupo de pessoas dentro de uma organização (Schein, 1992).

A definição do conceito de estratégia está baseada no conceito de cultura, que permite uma compreensão dos processos dinâmicos das organizações, analisando-as numa perspetiva cultural e valorizando os aspetos humanos. Durante o século passado, foram desenvolvidas práticas e modelos inovadores de gestão de recursos humanos, que promoveram a interligação entre os objetivos organizacionais e individuais.

A cultura de uma organização deve ser vista como um conceito complexo e abrangente que complementa as abordagens tradicionais utilizadas pelas organizações (Morgan, 2007) (Lopes & Reto, 1990). A transversalidade da cultura organizacional no âmbito empresarial permite a aquisição de novos conhecimentos e aprimoramento das práticas organizacionais, o que contribui para o aumento da eficácia.

A análise cultural visa orientar e estruturar a interação dos colaboradores como integrantes da organização, em contraposição às perspetivas funcionalistas predominantes (Caetano & Vala, 2007). A cultura organizacional é um dos principais pilares de qualquer estrutura, mas é crucial que as lideranças e colaboradores compreendam a sua importância e o impacto nos resultados. No atual contexto tecnológico, é essencial ter uma abordagem estratégica na definição da cultura organizacional, visto que esta pode ser um fator de diferenciação para atrair e reter talentos, durante a concorrência e competitividade dos mercados atuais, bem como diante da escassez de profissionais qualificados.

3.1.9. A importância do comportamento organizacional nos processos de gestão da organização

A interação humana é um fator chave na eficácia de qualquer organização, visto que as pessoas são um recurso fundamental em todas as estruturas organizacionais. A psicologia, ensina que cada indivíduo é único, com a sua própria personalidade, perceções e estilo. O comportamento de uma organização é definido não apelas pelas características comportamentais individuais, mas também pela interação dos indivíduos em grupos.

A área de conhecimento denominada como comportamento organizacional, dedica-se a estudar o comportamento dos indivíduos no contexto das organizações, por meio de metodologias interdisciplinares que permitem compreender as suas perceções e valores. Através da análise da capacidade de executar atividades individuais e em grupo, contextualizadas nos objetivos e estratégias da organização, busca-se entender como esse comportamento pode impactar no desempenho da organização (Gibson, Ivancevich, Donnelly, & Konopaske, 2006).

A gestão eficaz de uma organização depende da interligação eficaz entre as suas estruturas, processos e cultura organizacional. A definição da cultura organizacional é fundamental para determinar e orientar o comportamento adequado dos colaboradores, de forma a motivá-los e a estabelecer a linha que guia a organização na definição de estratégias, valores e relações internas. O conceito multidisciplinar do comportamento organizacional opera em três níveis: grupo, individual e organizacional.

A gestão eficaz do comportamento organizacional é fundamental para o sucesso de uma organização. Ao gerir as atitudes dos colaboradores em contexto organizacional, é possível otimizar os processos e promover o desenvolvimento dos colaboradores, reconhecendo as suas necessidades individuais e como membros de um grupo (Gibson, Ivancevich, Donnelly, & Konopaske, 2006).

A evolução rápida das Tecnologias de Informação e Comunicação nos últimos anos tem levado muitas organizações em busca de uma maior eficiência na implementação de mecanismos de segurança. No entanto, esta necessidade surge num contexto em que as empresas estão cada vez mais expostas ao risco, no qual compromete a segurança do seu ativo principal: informação.

A importância da informação sempre foi relevante para a capacitação e desenvolvimento humano, mas tornou-se ainda mais crucial nas últimas décadas devido ao avanço das Tecnologias de Informação e Comunicação, que proporcionaram um grande contributo nesse sentido (Gaivéo, 2008).

A gestão eficaz da informação tornou-se uma necessidade imperativa para a sobrevivência e sucesso das organizações. Uma política estratégica bem estruturada pode garantir a proteção contra ciberataques, tornando a segurança da informação o principal objetivo. Essa segurança visa proteger os sistemas de informação de acesso não autorizado, modificação, divulgação ou destruição de dados, preservando assim três aspetos críticos (Gladden, 2017):

- Confidencialidade
- Integridade
- Disponibilidade

Os elementos que a segurança da informação procura garantir são os seguintes (Gomes, 2010):

- **Confidencialidade:** De acordo com Gomes (2010), a confidencialidade é um princípio fundamental que visa garantir que as informações de uma organização sejam acedidas por pessoas devidamente autenticadas.
- **Integridade:** o princípio de integridade tem como objetivo proteger a informação, garantindo que ela não será alterada sem a devida autorização dos responsáveis pela segurança, preservando assim a sua integridade.
- **Disponibilidade:** A disponibilidade é um princípio que pressupõe que as informações estejam disponíveis para uso pelos utilizadores autorizados, em qualquer momento que eles necessitem.

A Cultura da Segurança é uma extensão da Cultura Organizacional. Quando a segurança organizacional é valorizada como um elemento-chave na construção da cultura organizacional, é possível elaborar estratégias mais efetivas para os colaboradores, trazendo benefícios diretos para a organização.

3.1.10. A importância dos recursos humanos na gestão estratégica de segurança de uma organização

Embora as pessoas sejam frequentemente consideradas o elo mais fraco na segurança da informação, é inegável a sua importância como colaboradores de uma organização. O desempenho das pessoas está diretamente relacionado à eficácia dos processos organizacionais.

A utilização (correta ou não) da informação pelos colaboradores de uma organização condiciona o seu valor como ativo, especialmente quando se trata de assegurar os princípios de confidencialidade, disponibilidade e integridade (Caetano & Vala, 2007). As pessoas são o ativo mais importante na gestão estratégica de qualquer organização, pois a definição da estratégia exige a integração dos recursos humanos. As pessoas que fazem parte das organizações devem estar envolvidas na definição e planeamento da estratégia.

No mercado competitivo atual, o elemento diferenciador não se resume apenas à concorrência, mas também à motivação e envolvimento dos colaboradores, tornando o fator humano fundamental para uma nova gestão de pessoas. A gestão estratégica de recursos humanos deve atender às exigências das Tecnologias de Informação e Comunicação, visando fortalecer a conexão entre os colaboradores e as necessidades da organização. Isso requer que todos os colaboradores possuam um conjunto de competências e qualificações estratégicas para o futuro da organização (Bilhim, 2007). Quando a cultura organizacional é vista como um conjunto de ideias e significados, as organizações podem adotar novas abordagens e manifestos de consciência humana. Conforme as Tecnologias de Informação e Comunicação são usadas nas organizações, novos papéis devem ser desempenhados e alinhados com as necessidades emergentes (Caetano & Vala, 2007).

Nos últimos anos, uma série de ataques informáticos tem abalado o mundo, colocando em risco a segurança da informação de várias organizações nacionais e internacionais. Esses ataques em larga escala destacam a necessidade de as organizações estabelecerem uma cultura da Cibersegurança capaz de enfrentar possíveis ameaças, protegendo assim os seus ativos de informação. Apesar do termo “Cibersegurança” ser amplamente utilizado no contexto organizacional, as definições para este termo variam, podendo ser subjetivas e pouco informáticas.

A falta de uma definição concisa e aceite para compreender a multidimensionalidade do conceito de Cibersegurança muitas vezes dificulta a aplicação prática e científica do mesmo, especialmente em contexto organizacional (Craigen, Diakun-Thibault, & Purse, Defining Cybersecurity, 2014).

Cibersegurança pode ser definido como um conjunto de práticas digitais e métodos de defesa que são usados para detetar e prevenir possíveis *hackers* (Kemmerer, 2003) protegendo o ciberespaço, as organizações e os utilizadores (Von Solms & Van Niekerk, 2013) do aumento de risco de ciberataques (Amoroso, 2006). Para promover o uso seguro do ciberespaço, é fundamental estabelecer uma cultura de Cibersegurança que permeie toda a estrutura da organização (Gcaza, Von Solms, & Van Vuuren, 2015).

Capacitar os colaboradores da organização de acordo com os níveis de risco existentes é importante para a definição de uma política de segurança que caracterize toda a estrutura da organização.

É importante que os colaboradores da organização encarem as estratégias de Cibersegurança como parte integrante da cultura organizacional e não apenas como parte da transformação tecnológica. O objetivo principal de qualquer política de segurança deveria ser a interiorização de boas práticas pelos colaboradores nas suas rotinas diárias. A cultura da Cibersegurança não deve ser vista apenas como uma preocupação, mas também como um ativo de inovação pelos colaboradores.

3.1.11. Estratégia em Cibersegurança

Uma estratégia em Cibersegurança é um plano de ação projetado para maximizar a segurança e a resiliência de uma organização (Unni, 2022). Uma estratégia em Cibersegurança não deve ser perfeita, mas deve ser um palpite forte e devidamente fundamentado sobre o que se deve fazer, e a sua estratégia deve evoluir conforme a organização e o mundo ao seu redor evoluem (Scarfone, 2023).

O resultado pretendido do desenvolvimento e implementação de uma estratégia em Cibersegurança é que os seus ativos estejam devidamente protegidos, isto por norma, envolve uma mudança de uma abordagem de segurança reativa para uma proativa, onde se vai estar mais focado em prevenir ataques e incidentes cibernéticos do que a reagir a eles após o sucedido (Scarfone, 2023).

A estratégia em Cibersegurança deve ser adaptada às necessidades de segurança exclusivas de uma organização, independentemente de ser pequena, média ou grande empresa e o setor em que atue (CheckPoint, 2024).

De acordo com o Unni (2022), para a estratégia em Cibersegurança é necessário desenvolver e implementar uma estratégia eficaz de segurança cibernética, de seguida, é indicado sete etapas principais que podem ser usadas como base ao construir uma estratégia de Cibersegurança forte:

- **Realizar uma avaliação de risco de segurança**: Uma avaliação de risco de segurança cibernética é projetada para obter uma visão detalhada das possíveis ameaças cibernéticas do negócio e quais as capacidades de gerir os riscos associados (Unni, 2022).
- **Definir e estabelecer metas de segurança:** Um passo importante na construção de uma estratégia de Cibersegurança é garantir que ela seja congruente com os objetivos comerciais, a maneira como isso pode ser feito é definir objetivos de segurança que se alinhem e não comprometam os objetivos do negócio (Unni, 2022).
- **Avaliação do nível de tecnologia:** Uma parte essencial de uma estratégia de segurança cibernética é avaliar a tecnologia para ver se ela atende às melhores práticas atuais, com o rápido desenvolvimento das táticas, técnicas e procedimentos de agentes maliciosos, a tecnologia de uma organização necessita de estar atualizada com os últimos *patches* e atualizações de segurança (Unni, 2022).
- **Escolha de uma estrutura de Segurança Cibernética:** É essencialmente um sistema de padrões, diretrizes e melhores práticas para gerir riscos que surgem no mundo digital, existem várias estruturas de segurança cibernética que uma empresa pode escolher para orientar a sua estratégia geral de Cibersegurança (Unni, 2022)**.**
- **Rever as políticas de segurança existentes:** Uma política de segurança é um documento que declara por escrito como uma empresa planeia proteger os seus ativos físicos e de tecnologia da informação. Elas devem ser alteradas para refletir quaisquer mudanças em tecnologia, vulnerabilidades e requisitos de segurança (Unni, 2022)**.**
- **Gestão de Riscos:** Uma parte importante da criação de uma estratégia em Cibersegurança é a preparação para o pior cenário, por mais forte que sejam as medidas de segurança cibernética, ainda há uma chance de que a empresa seja vítima de um ataque cibernético ou violação de dados (Unni, 2022)**.**
- **Implementação e Avaliação:** Por fim, após definir a estratégia em Cibersegurança e as políticas terem sido criadas, é hora da implementação, é importante reconhecer a necessidade de suporte e avaliação contínuos, devido às vulnerabilidades continuarem a evoluir conforme os agentes de ameaças descobrem novos métodos de ataque (Unni, 2022).

3.1.12. Ciclo de vida de um incidente

O ciclo de vida de um incidente é uma série de procedimentos executados no caso de um incidente de Cibersegurança, essas etapas definem o fluxo de trabalho para o processo geral de resposta a incidentes, cada estágio envolve um conjunto específico de ações que uma organização deve concluir (Eccouncil, 2022).

Existem várias maneiras de definir o ciclo de vida de resposta a incidentes. O *National Institue Of Standards and Technology* (NIST; (Cichonski, 2022)) desenvolveu uma estrutura para tratamento de incidentes, que é o modelo mais usado, o processo descrito na estrutura do NIST inclui cinco fases:

- **1. Preparação:** Nesta fase, o negócio cria um plano de gestão de incidentes que pode detetar um incidente no ambiente da organização, a etapa de preparação envolve, por exemplo, identificar diferentes ataques de *malware* e determinar qual seria o seu impacto nos sistemas (Cichonski, 2022).
- **2. Deteção e Análise:** Um analista de resposta a incidentes é responsável por recolher e analisar dados para encontrar quaisquer pistas que ajudem a identificar a origem de um ataque (Cichonski, 2022).
- **3. Contenção, Erradicação e Recuperação:** Esta é a fase principal da resposta a incidentes de segurança, no qual são tomadas medidas para impedir qualquer dano adicional, esta fase abrange três etapas:
    - **Contenção:** Nesta etapa, todos os métodos possíveis são usados para evitar a disseminação de *malware* ou vírus (Cichonski, 2022).
    - **Erradicação:** Após conter o problema de segurança em questão, o código ou *software* malicioso precisa ser erradicado do ambiente (Cichonski, 2022).
    - **Recuperação:** Após eliminar o *malware*, restaurar todos os sistemas ao estado anterior ao incidente é essencial (Cichonski, 2022).

3.1.13. *Cibersecurity Kill Chain*

Uma *Cyber Kill Chain* é uma estrutura de segurança projetada para identificar e interromper ataques cibernéticos sofisticados ao dividir o ataque em vários estágios (Kidd, 2024). Este modelo ajuda as equipas de Cibersegurança a reconhecer, intercetar ou prevenir ataques antes que eles afetem uma organização.

O conceito de *Kill Chain* originou-se através das operações militares, onde um ataque inimigo é identificado, dividido em estágios e medidas preventivas são colocadas em prática. Essa estratégia militar inspirou a *Kill Chain*, que foi inicialmente criada por *Lockheed Martin* em 2011 (Kidd, 2024).

O propósito da cadeia de destruição cibernética é reforçar as defesas de uma organização contra ameaças persistentes avançadas (APTs), também conhecidas como ataques cibernéticos sofisticados (Kidd, 2024). No geral, as ameaças costumam ser as seguintes:

- *Malware;*
- *Ransomware;*
- Cavalo de Tróia;
- *Phishing;*
- Outras técnicas de engenharia social.

3.1.14. Superfícies de ataque

Uma superfície de ataque é o número total de todos os pontos de entrada possíveis para acesso não autorizado a qualquer sistema, as superfícies de ataque incluem todas as vulnerabilidades e *endpoints* que podem ser explorados para realizar um ataque de segurança (Gillis, 2021).

O tamanho de uma superfície de ataque pode mudar ao longo do tempo, conforme os novos sistemas e dispositivos são adicionados ou removidos, por exemplo, a superfície de ataque de uma aplicação pode incluir o seguinte (Gillis, 2021):

- Interfaces de administração;
- Interfaces de programação de aplicativos (*APIs*);
- Pontos de entrada de autenticação;
- Dados;
- Caminho de dados;
- Interfaces com outros aplicativos;
- Armazenamento local;
- Interfaces de utilizador.

Existem diferentes tipos de superfícies de ataque, sejam físicas, digitais ou sociais, como se pode observar com mais detalhe de seguida:

- **Superfície de ataque físico:** Compreendem todos os dispositivos de *endpoint*, como sistemas de *desktops*, *laptops*, dispositivos móveis, discos rígidos e portas *USB.* Este tipo de superfície de ataque inclui todos os dispositivos que um invasor pode aceder fisicamente (Gillis, 2021).
- **Superfície de ataque digital:** Abrangem aplicações, códigos, portas, servidores e sites, bem como pontos de acesso não autorizados ao sistema. Uma superfície de ataque digital é todo o *hardware* e *software* que se conectam à rede de uma organização (Gillis, 2021).
- **Superfície de ataque de Engenharia Social:** Envolvem o tópico de vulnerabilidades humanas em oposição às vulnerabilidades de *hardware* ou *software*. Engenharia social é o conceito de manipular uma pessoa com o objetivo de fazê-la compartilhar e comprometer dados pessoais ou da empresa (Gillis, 2021).

De certa forma, é necessário reduzir a superfície de ataque e monitorizar e auditar com regularidade, para um processo mais eficiente (Horenbeeck, 2023).

3.1.15. Vetores de ataque

Em Cibersegurança, um vetor de ataque é um método de obter acesso não autorizado à rede para lançar um ataque cibernético (Tyas, 2024). Os vetores de ataque permitem que os criminosos cibernéticos explorem vulnerabilidades do sistema para obter acesso a dados confidenciais e outras informações valiosas.

Os vetores de ataque mais comuns incluem *malware*, vírus, anexos de email, páginas da *web*, *pop-ups*, mensagens instantâneas, mensagens de texto e engenharia social, no entanto, o número de ameaças cibernéticas continua a crescer, pois os criminosos cibernéticos procuram explorar vulnerabilidades não corrigidas ou listas que sejam publicadas na *dark web*, isto porque não há uma solução única para prevenir todos os vetores de ataque (Tyas, 2024).

3.1.16. Estágios

Os ataques cibernéticos também podem ter vários tipos de estágios ou fases pelas quais passam, pode ser ainda chamado de "Ciclo de Vida do Ataque Cibernético" (Kidd, 2024), normalmente é composto por sete etapas, que são as seguintes:

1. **Reconhecimento:** Os invasores reúnem informações sobre o seu alvo para identificar vulnerabilidades e potenciais pontos de entrada (Kidd, 2024). Este estágio envolve:
    a. Recolha de dados públicos;
    b. Implementação de ferramentas de espionagem;
    c. Uso de *scanners* automatizados para detetar sistemas de segurança ou aplicações de terceiros.
2. **Intrusão**: Após coleta de informações, os invasores criam *malware* ou *payloads* maliciosos para explorar fraquezas identificadas (Kidd, 2024).
3. **Entrega:** Os invasores tentam infiltrar-se na rede do alvo, usando *malware* (Kidd, 2024).
4. **Exploração:** Uma vez que o *malware* esteja instalado, os invasores exploram as vulnerabilidades do alvo, infiltrando-se ainda mais na rede (Kidd, 2024).
5. **Instalação:** Nesta fase, os invasores adotam a estratégia de uso de cavalos de troia, manipulação de *token* de acesso para obter controlo adicional sobre a rede (Kidd, 2024).
6. **Comando e Controlo:** Os invasores estabelecem um canal de comando e controlo (C2) para monitorizar e guiar remotamente as suas armas cibernéticas implantadas.
7. **Ação:** A fase final envolve a execução do objetivo principal do ataque, como (Kidd, 2024):
    a. Extração de dados;
    b. Criptografia.

3.1.17. Inteligência sobre ameaças cibernéticas

A Inteligência sobre ameaças cibernéticas são informações detalhadas e acionáveis sobre ameaças para prevenir e combater ameaças de segurança cibernética direcionadas a uma organização (IBM, 2023).

Ao implementar esta tática, as empresas podem tomar medidas proativas para garantir que os seus sistemas estejam seguros, por meio de inteligência e análise de ameaças cibernéticas, violações de dados podem ser prevenidas completamente, economizando os custos financeiros de colocar em prática quaisquer planos de resposta a incidentes (Andrew, 2023).

O ciclo de vida da inteligência de ameaças é o processo iterativo e contínuo pelo qual as equipas de Cibersegurança produzem, disseminam e melhoram continuamente a sua inteligência de ameaças, embora os detalhes possam variar de organização para organização (IBM, 2023).

O ciclo de vida da inteligência de ameaças é um processo de seis etapas, que são as seguintes:

- Planeamento;
- Recolha de dados sobre ameaças;
- Processamento;
- Análise;
- Disseminação;
- Comentários.

3.1.17.1. Tipos de Cyber Threat Intelligence

O ciclo de vida da inteligência de ameaças produz diferentes tipos de inteligência dependendo das partes interessadas envolvidas, dos requisitos definidos e dos objetivos gerais de uma determinada instância de ciclo de vida (IBM, 2023). Existem três categorias amplas de inteligência de ameaças:

- **Estratégica:** É uma avaliação de alto nível de ameaças potenciais, identificando quem pode estar interessado em atacar a organização ou empresas no seu setor e as suas motivações (Andrew, 2023).
- **Táticas:** Relaciona-se como e onde a organização pode ser alvo e foca nas táticas, técnicas e procedimentos dos Cibercriminosos (Andrew, 2023).
- **Operacional:** É a informação recolhida de ataques ativos, *honeypots* cibernéticos (armadilhas para atrair *hackers* a revelar as suas táticas) e dados compartilhados por terceiros (Andrew, 2023).

Com informações e planeamento suficientes, é possível implementar as ferramentas certas para monitorizar determinados comportamentos e conduzir uma resposta eficiente a incidentes (IBM, 2023).

3.1.18. Threat hunting

3.1.18.1. Definição

A *Threat Hunting* também designada como caça de ameaças cibernéticas, é uma abordagem eficiente para identificação de ameaças previamente desconhecidas ou que já estejam dentro de uma rede da organização, mas em análise (IBM, 2023)**.**

Existem muitas técnicas diferentes que os caçadores podem usar para encontrar os *hackers*, e nenhuma delas está sempre "certa", a melhor delas geralmente depende do tipo de atividade que se procure (SQRRL, 2015). Um dos principais objetivos da *Threat Hunting* deve ser melhorar as capacidades de deteção automatizada, prototipando novas maneiras de detetar atividades maliciosas e transformando esses protótipos em capacidades de deteção de produção (SQRRL, 2015).

Infelizmente, a maioria das organizações ainda concentra muito dos seus recursos na prevenção do que na deteção, as principais ferramentas que eles implementam nos dias de hoje, incluem a *Firewall*, *Antispam, sandboxing*, IPS (prevenção de intrusão)*, feeds* de inteligência, filtragem de URL, entre outros (Mohit, 2018).

Existem três fatores a serem considerados ao julgar a capacidade de *Threat Hunting* de uma organização: a qualidade e a quantidade dos dados que são recolhidos para *Hunting*, as ferramentas que fornecem para aceder e analisar os dados e as habilidades dos analistas que realmente usam os dados e as ferramentas para encontrar incidentes de segurança (SQRRL, 2015).

Destes fatores, as habilidades dos analistas são provavelmente as mais importantes, pois são elas que permitem que eles transformem dados em deteções, a qualidade e a quantidade dos dados que uma organização recolhe rotineiramente no seu ambiente de trabalho, são um fator forte na determinação do nível *Hunting Maturity Model (HMM)* (SQRRL, 2015).

O *HMM,* desenvolvido pelo arquiteto de segurança e *hunter* da SQRRL, descreve cinco níveis de capacidade de *hunting* organizacional, variando de HMM0 (o menos capaz) a HMM4 (o mais capaz), conforme é discriminado de seguida (SQRRL, 2015)**:**

- **HMM0 (Inicial):** Neste nível, uma organização depende principalmente de ferramentas de alerta automatizadas, como IDS, SIEM ou antivírus para detetar atividades maliciosas em toda a organização.
- **HMM1 (Mínimo):** Uma organização na HMM1 ainda depende principalmente de alertas automatizados para conduzir o seu processo de resposta a incidentes, mas aspiram à deteção orientada por inteligência artificial.

- **HMM2 (Processual):** As organizações neste nível são capazes de aprender e aplicar procedimentos desenvolvidos por outros numa base relativamente regular e podem fazer pequenas alterações, mas ainda não são capazes de criar procedimentos totalmente novos por si mesmos.
- **HMM3 (Inovador):** Entendem uma variedade de diferentes tipos de técnicas de análise de dados e são capazes de aplicá-las para identificar atividades maliciosas.
- **HMM4 (Líder):** É essencialmente a mesma que uma na HMM3, com uma diferença importante: automação, ou seja, qualquer processo de caça bem-sucedido será operacionalizado e transformado em deteção automatizada.

3.1.18.2. Metodologias Threat Hunting

A linha de base é crítica antes de começar a criar os modelos de investigação para *Threat Hunting.* A linha de base refere-se ao estabelecimento de uma diferença clara entre um evento malicioso e um não malicioso para identificar anomalias, no entanto, vai-se demonstrar algumas metodologias comuns de *Threat Hunting* que são usadas (Sharma, 2024)**.**

3.1.18.2.1. Estruturado

A *Threat Hunting* estruturada é baseada em indicadores de comprometimento (IOCs) e táticas, técnicas e procedimentos. IOCs fornecem informações sobre potenciais adversários, como endereços IP, nomes de domínio, versões de sistemas operacionais, etc. Os procedimentos descrevem como os invasores operam e quais as ferramentas que eles usam, combinar IOCs e procedimentos torna possível construir uma imagem do adversário (Joe, 2022).

Este tipo de abordagem permite detetar ameaças mais cedo e prevenir ataques.

3.1.18.2.2. Não estruturado

O conceito de *Threat Hunting* não estruturado é relativamente novo, surgiu em 2013. Este é um método de encontrar *software* malicioso (*malware)*, como vírus, *trojans*, *worms,* etc., sem saber exatamente que tipo de *malware* se procura. Esta metodologia depende da análise comportamental para encontrar ameaças (Joe, 2022).

Em resumo, a metodologia não estruturada é um trabalho de investigação em que um analista de segurança observa o comportamento e procura por anomalias.

3.1.18.2.3. Situacional ou orientada por entidades

Esta metodologia é uma abordagem direcionada à caça de ameaças que se concentra em eventos, entidades ou situações específicas que podem representar um risco elevado à segurança de uma organização. Isso pode incluir eventos de alto perfil, como fusões e aquisições, lançamento de produtos ou incidentes de segurança, bem como entidades específicas (exabeam, 2023).

Neste tipo de abordagem situacional, os analistas usam inteligência de ameaças, juntamente com outros dados relevantes e informações contextuais sobre as entidades na rede, para identificar potenciais ameaças ou vulnerabilidades associadas à situação (exabeam, 2023).

3.1.19. Cibersegurança nas Pequenas e Médias Empresas

Portugal em matéria de segurança no ciberespaço, em 2018, ocupava o 42º lugar do *Global Cybersecurity Index*, em 2020, conseguiu saltar para 14ª posição, na Edição de 2021 (Francisca Andrade, 2021).

Em comunicado, Centro Nacional de Cibersegurança (CNCS) avançou que para a melhoria de Portugal no índice, contribuiu um conjunto de iniciativas legislativas, técnicas, organizacionais, de desenvolvimento de capacidades e de cooperação que têm vindo a ser definido e implementado com o objetivo de reforçar o quadro da Cibersegurança ao nível nacional (Francisca Andrade, 2021), no entanto, ainda existe muitas pequenas e médias empresas (PME) que não estão a investir em contexto de Cibersegurança.

Após um estudo efetuado, 90% das pequenas médias empresas (PME) não implementaram novas medidas de segurança para proteger as novas tecnologias que estão a adotar, resultado de uma transformação digital, segundo um estudo realizado pela Agência da União Europeia para a Cibersegurança (ENISA) (SECURITY, 2023).

Os estudos realizados, demonstram a real necessidade de implementar medidas de Cibersegurança em empresas de todos os setores e dimensões, os Cibercriminosos estão à procura da maior rentabilidade, mas também de quem seja alvo fácil para lançar os seus ataques (SECURITY, 2023).

Assim, a unidade de Cibersegurança da fibratel, identificou os ciberataques mais comuns entre as PME como sendo o *phishing*, de acordo com a ENISA, 41% das PME afirmam ter sido vítimas de um ataque de *phishing* (SECURITY, 2023).

3.1.20. Pequenas e Médias Empresas (PME)

De acordo com a Recomendação 2003/361/CE, da Comissão, uma micro, pequena ou média empresa define-se com base nos seguintes critérios (Portugal2020, 2021):

- Microempresa – contêm menos de 10 pessoas empregadas e o volume de negócios anual e/ou balanço total anual não pode exceder os 2 milhões de euros;
- Pequena empresa – contêm entre 11 a 50 pessoas empregadas e o volume de negócios anual e/ou balanço total anual não pode exceder os 10 milhões de euros;
- Média empresa – contêm entre 51 a 250 pessoas empregadas, o volume de negócios anual não pode exceder os 50 milhões de euros e/ou o balanço total anual não pode exceder os 43 milhões de euros.

3.1.21. Centro Nacional de Cibersegurança

A criação, instalação e operacionalização do Centro Nacional de Cibersegurança (CNCS) foi iniciada pela Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril (CNCS, 2023).

No dia 6 de outubro de 2014, foi criado o CNCSeg, dentro do Gabinete Nacional de Cibersegurança, através do Decreto-lei n.º 69/2014, de 9 de maio. Após esta publicação, o CNCS recebeu a sua atual designação pelo Decreto-lei n.º 136/2017, do dia 6 de novembro (CNCS, 2023).

A publicação efetuada da lei n.º 46/2018, de 13 de agosto, determina o Regime Jurídico da Segurança do Ciberespaço, em que o CNCS passou a ter competência de Autoridade Nacional de Cibersegurança, enquanto o CERT.PT foi atribuído a função de ponto de contato único internacional para a gestão de ciberincidentes (CNCS, 2023).

3.1.22. Roteiro para as Capacidades Mínimas em Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) definiu um modelo de capacitação em Cibersegurança, visando a melhoria de processos, pessoas e tecnologias nas organizações nacionais, com enfoque especial em PME (CNCS, 2023).

O documento, denominado por Roteiro para as Capacidades Mínimas em Cibersegurança, apresenta um conjunto de ações que se dividem em cinco fases, sendo que estas foram pensadas para uma adaptação gradual, a implementar em cada organização, quer seja por meios próprios internos, ou mesmo recorrendo a subcontratação ou externalização de soluções (CNCS, 2023), no entanto, esse documento apresenta uma das ações de destaque que vai ao encontro desta dissertação, a Ação 3.8 – "Instalação e Configuração de um Security Information and Event Managment (SIEM)", com o intuito de obter uma visão global da segurança de informação crítica que uma organização pode conter e permitir detetar e mitigar ciberameaças.

Assim, destaca-se que este conjunto de atividades, enquadradas no âmbito do Quadro Nacional de Referência para a Cibersegurança, representa a base para estabelecer a capacidade mínima em Cibersegurança, fornecendo assim às organizações os recursos necessários para que possam enfrentar as ameaças e os desafios do mundo digital (CNCS, 2023).

3.1.23. Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

O Centro de Estudos para Reposta e Tratamento de Incidentes em Computadores (CERT.PT), no qual está integrado no CNCS, é um serviço que tem a responsabilidade de coordenar a resposta a incidentes que envolvam entidades da Administração Pública, operadores de infraestruturas críticas, entre outros que envolva o ciberespaço nacional. Com isto, pode incluir qualquer dispositivo que seja conectado à rede ou bloco de endereçamento pertencentes a operadores de comunicações, instituições, pessoas coletivas ou singulares sediadas em território português, ou fisicamente localizados em território português (CNCS, 2023).

3.1.24. Comissão Nacional de Proteção de Dados (CNPD)

A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa independente, com personalidade jurídica de direito público, com autoridade própria e

autonomia administrativa e financeira, que atua junto da Assembleia da República (CNPD, 2023).

A CNPD ficou responsável por controlar e fiscalizar o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, e de outras normais legais e regulamentares relacionadas com a proteção de dados pessoais, com o intuito de defender os direitos, liberdades e garantias das pessoas singulares no domínio dos tratamentos dos seus dados pessoais (CNPD, 2023).

Desta forma, as entidades públicas e privadas devem auxiliar com a CNPD, concedendo todas as informações solicitadas, bem como o acesso ao sistema informático, a ficheiros de dados pessoais e a documentação relativa ao tratamento de dados pessoais (CNPD, 2023).

3.1.25. Agência Europeia para a Segurança das Redes e da Informação

A ENISA contribui para a política da UE em matéria de Cibersegurança, reforçando a confiança nos produtos, serviços e processos digitais graças à elaboração de sistemas de certificação da Cibersegurança, coopera com os países e organismos da UE e contribui para a preparação na perspetiva de futuros desafios cibernéticos (ENISA, 2021).

A ENISA foi criada em 2004 e trabalha com organizações e empresas para aumentar a confiança na economia digital, reforçar a resiliência das infraestruturas da UE e, em última análise, manter os cidadãos da UE seguros no plano digital, fá-lo através da partilha de conhecimentos (ENISA, 2021).

3.1.26. Frameworks

3.1.26.1. MITRE ATT&CK

MITRE ATT&CK é uma coleção documentada de informações sobre os comportamentos maliciosos dos grupos de ameaças persistentes avançadas (APT) usaram em vários estágios de ataques cibernéticos do mundo real (Debbie, 2021).

ATT&CK significa *Adversarial Tactics, Techniques, and Common Knowledge*, inclui descrições detalhadas das táticas observadas desses grupos (os objetivos técnicos que eles estão tentando atingir), técnicas (os métodos que eles usam) e procedimentos (implementações específicas de técnicas), comumente chamados de TTPs (Debbie, 2021).

MITRE ATT&CK é uma ferramenta gratuita que as organizações tanto do setor público e privado, independentemente da sua dimensão, adotaram amplamente, para utilização das equipas de segurança internas interessadas em construir sistemas, aplicações e serviços seguros, a riqueza de informações sobre ataques (e invasores) que ele contém pode ajudar as organizações a determinar se estão a recolher os dados certos para detetar ataques de forma eficaz e avaliar o quão bem estão as suas defesas atuais a funcionar (Debbie, 2021).

Antes de aprofundar-se na Matriz, é importante entender como o MITRE ATT&CK define táticas, técnicas e procedimentos, pois esses termos podem ter significados diferentes em outros contextos (Debbie, 2021), de seguida, vai-se definir então os termos:

- **Táticas:** Descreve os objetivos técnicos imediatos (o "o quê") que os invasores estão a tentar atingir, como obter acesso inicial, manter a persistência ou estabelecer comando e controlo (Debbie, 2021).
- **Técnicas:** Descreve o "como" – os métodos que os invasores usam para atingir uma tática, todas as táticas em cada matriz têm várias técnicas (Debbie, 2021).
- **Procedimentos:** Descreve as implementações específicas das técnicas e sub-técnicas que os APTs usaram (às vezes de maneiras inteligentes ou inovadores) ou pode se referir a *malwares* específicos ou outras ferramentas que os invasores usaram (Debbie, 2021).

O MITRE ATT&CK organiza táticas e técnicas adversárias (e sub-técnicas) em matrizes, cada matriz inclui táticas e técnicas correspondentes a ataques em domínios específicos:

- **Matriz Empresarial:** A *Enterprise Matrix* abrange todas as técnicas utilizadas por adversários em ataques contra infraestrutura empresarial (IBM, 2023).
- **Matriz Móvel:** A Matriz Móvel inclui técnicas usadas em ataques diretos a dispositivos móveis e em ataques móveis baseados em rede que não exigem acesso a um dispositivo móvel (IBM, 2023).
- **Matriz ICS:** A Matriz ICX inclui técnicas usadas em ataques a sistemas de controlo industrial, especificamente máquinas, dispositivos, sensores e redes usadas para controlar ou automatizar operações de fábricas, serviços públicos, sistemas de transporte, entre outros (IBM, 2023).

Cada tática MITRE ATT&CK representa um objetivo adversário específico – algo que o invasor deseja realizar em um determinado momento, por exemplo, as táticas ATT&CK cobertas pela *Enterprise Matrix* incluem (IBM, 2023):

- **Reconhecimento**: Recolhe informações para planear um ataque;
- **Desenvolvimento de recursos:** Estabelece recursos para dar suporte às operações de ataque;
- **Acesso inicial:** Comprometimento inicial de um sistema ou rede de destino;
- **Execução:** Realização de *malware* ou código malicioso no sistema comprometido;
- **Persistência:** Manter o acesso ao sistema comprometido;
- **Escalonamento de privilégios:** Aquisição de permissões ou acesso a níveis superiores dentro do sistema;
- **Evasão de defesa:** Técnicas utilizadas para evitar a deteção uma vez dentro de um sistema;
- **Acesso de credencial:** Obtenção de nomes de utilizadores, senhas e outras credenciais de *login*;
- **Descoberta:** Pesquisar o ambiente alvo para saber quais os recursos que podem ser acedidos ou controlados para dar suporte a um ataque planeado;
- **Movimento lateral:** Obtenção de acesso a recursos adicionais dentro do sistema;
- **Recolha:** Recolha de dados relacionados ao objetivo do ataque;
- **Comando e Controlo:** Estabelece as comunicações secretas/indetetáveis que permitem ao invasor controlar o sistema;
- **Exfiltração:** Roubo de dados do sistema;
- **Impacto:** Interromper, corromper, desabilitar ou destruir dados ou processos de negócios.

As táticas e técnicas variam de matriz (e submatriz), por exemplo, a Matriz Móvel não inclui táticas de Reconhecimento e Desenvolvimento de Recursos, mas inclui outras táticas – Efeitos de Rede e Efeitos de Serviço Remoto – onde não são encontradas na Matriz Empresarial (IBM, 2023).

3.1.26.2. OWASP

Open Web Application Security Project (OWASP) é uma organização sem fins lucrativos comprometida em melhorar a segurança de *software*. OWASP é baseado numa

abordagem de “comunidade aberta”, permitindo que qualquer um se envolva e contribua com projetos, eventos, conversas online, entre outras atividades (Pranav, 2022).

O conceito orientador da OWASP é que todos os recursos e informações no seu site sejam gratuitas e acessíveis livremente a qualquer pessoa. A OWASP oferece uma variedade de ferramentas, vídeos, fóruns, iniciativas e eventos, entre outras coisas. Em poucas palavras, a OWASP é um balcão único para tudo sobre segurança de aplicações *Web*, apoiado pela sabedoria coletiva e experiência de todos os utilizadores da comunidade aberta (Pranav, 2022).

O OWASP top 10 é um relatório atualizado regularmente, onde descreve as preocupações de segurança para segurança de aplicações *web*, com foco nos 10 riscos mais críticos. O relatório é elaborado por uma equipa de especialistas em segurança de todo o mundo. O OWASP refere-se ao top 10 como um “documento de conscientização” e recomenda que todas as empresas incorporem os relatórios nos seus processos para minimizar e/ou mitigar riscos de segurança (Cloudflare, 2024).

Adotar a conformidade com o OWASP como parte do processo de desenvolvimento de *software* e políticas de gestão de risco, aumenta a reputação de uma empresa. O OWASP estabelece um padrão da indústria para diretrizes e estruturas de revisão de código que fornecem aos desenvolvedores documentação para as melhores práticas de teste de penetração, o mesmo também facilita o trabalho dos desenvolvedores para criar as suas próprias diretrizes de teste de penetração e avaliar o risco nas suas próprias configurações (Pranav, 2022).

Ao aderir a estes princípios do OWASP e incentivar os desenvolvedores a serem mais conscientes sobre segurança, a empresa pode gerir melhor as vulnerabilidades e melhorar a qualidade geral das suas aplicações (Pranav, 2022).

3.1.27. *System Information and Event Management* (SIEM)

É uma Plataforma de gestão de informação e eventos de segurança, ou designado como SIEM, basicamente é uma solução de segurança que ajuda as organizações a reconhecer e lidar com potenciais ameaças e vulnerabilidades de segurança antes que elas tenham a chance de interromper as operações comerciais (IBM, 2023).

Inicialmente, as plataformas SIEM originais eram ferramentas de gestão de *logs*, combinavam funções de gestão de informações de segurança (SIM) e gestão de eventos de

segurança (SEM), estas plataformas permitiam o monitoramento e a análise em tempo real de eventos relacionados à segurança (IBM, 2023).

Ao longo dos anos, o SIEM evoluiu para incorporar análises de comportamento de utilizadores e entidade (UEBA), bem como outras análises avançadas de segurança, IA e recursos de aprendizagem de máquina para identificar comportamentos anómalos e indicadores de ameaças avançadas (IBM, 2023).

3.1.27.1.1. Características

No nível mais básico, todas as soluções SIEM realizam algum nível de agregação de dados, consolidação e funções de classificação para identificar ameaças e aderir aos requisitos de conformidade de dados (Ferrill, 2024). Algumas soluções diversificam em capacidade, a generalidade oferece o mesmo conjunto principal de funções:

- Recolha de dados e *logs* em tempo real;
- Alertas e notificações em tempo real;
- Priorização, análise, relatórios e IA;
- Integração com *firewalls*, entre outras ferramentas de segurança.

3.1.27.1.2. Arquitetura

A arquitetura SIEM é robusta e compreende uma série de componentes-chave que desempenham um papel muito importante no processo de garantir a monitorização total da segurança e resposta a incidentes (SentinelOne, 2024). De seguida, vai ser apresentado os componentes da arquitetura SIEM:

- **Recolha e agregação de dados:** A base de qualquer SIEM é a recolha e agregação de dados, obtendo informações de segurança de uma ampla variedade de fontes: dispositivos de rede, incluindo *firewalls,* servidores, entre outros.
- **Normalização e análise sintática:** O próximo passo importante no processo após a recolha de dados, é a normalização e a análise dos dados.
- **Motor de Correlação de dados:** O mecanismo de correlação é provavelmente a parte mais crítica de um SIEM, onde o núcleo analítico do sistema é realizado, este mecanismo processa os dados normalizados para identificar padrões e relacionamentos, que, de outra forma, apontariam para uma ameaça à segurança.

- **Alertas e relatórios:** É que aqui os alertas gerados pelo SIEM se tornam muito importantes, porque quando o mecanismo de correlação identifica uma potencial ameaça de segurança, o processo para mitigar uma ameaça rapidamente está dependente destes alertas.
- **Gestão e retenção de *logs*:** O SIEM envolve gestão e retenção de *logs* em relação à conformidade e investigações forenses.

3.1.27.1.3. Modelos de Serviço

Um SIEM também consegue oferecer um serviço através de diferentes modelos (SentinelOne, 2024), como os seguintes:

- **On-Premise:** São hospedados em *datacenters* locais e mantidos pela equipa de IT interna da empresa (Katie, 2023);
- **SIEM com gestão:** Neste caso, as ferramentas SIEM são implementadas no local e executadas de forma remota.
- **PaaS:** Fornece recursos por meio de modelos baseados em nuvem.

3.1.27.2. Integrações com outras ferramentas de Segurança

A eficácia das plataformas SIEM, muitas das vezes, são limitadas devido ao seu isolamento de outras ferramentas de segurança, muitas organizações operam uma coleção díspar de ferramentas de segurança, cada uma com o seu formato de dados, protocolos de comunicação e interface de gestão (Deshetty, 2022).

As integrações SIEM com outras ferramentas de segurança pode melhorar significativamente a postura de segurança cibernética de uma organização (Deshetty, 2022):

- **Melhorar a deteção de ameaças:** Ao combinar dados de várias fontes de segurança, o SIEM pode fornecer uma visão mais abrangente do cenário de segurança, permitindo a deteção de padrões e anomalias que podem indicar uma ameaça (Deshetty, 2022).
- **Simplificação de investigação de incidentes:** Quando o SIEM é integrado com outras ferramentas, os analistas podem aceder e correlacionar rapidamente dados relevantes de diferentes fontes, reduzindo o tempo necessário para investigar e entender o escopo de um incidente (Deshetty, 2022).

- **Automatização da resposta a ameaças:** O SIEM pode automatizar tarefas como bloquear endereços IP maliciosos, colocar em quarentena sistemas infetados e emitir alertas para os analistas de segurança, permitindo uma resposta mais rápida e eficaz às ameaças (Deshetty, 2022).

Neste projeto, a plataforma de SIEM vai-se integrar com duas ferramentas adquiridas pela empresa, que são as seguintes:

- ***Firewall*:** O SIEM vai ser integrado com a *Firewall* da *Sophos XG* para fornecer uma monitorização em tempo real do tráfego da rede e fazer identificação de potenciais ameaças;
- **Deteção e resposta de pontos finais (EDR):** Integração com uma solução EDR da *Sophos,* designada como *Endpoint Sophos*, serve para monitorizar em tempo real a atividade da rede, detetar e mitigar ameaças que surjam em diversos dispositivos.

3.1.27.3. Os papéis da tecnologia SIEM no contexto *Threat Hunting*

As soluções SIEM são criadas para executar correspondência de regras em dados de *log* de muitas fontes, com a integração de inteligência de ameaças, as soluções SIEM podem ficar um passo à frente de ameaças e alertas emergentes (Wang, 2023). De seguida, vai ser explorado alguns benefícios de incorporar inteligência de ameaças numa plataforma SIEM:

- **Defesa proativa:** A caça às ameaças é essencial para uma segurança cibernética eficaz. Em vez de reagir às ameaças depois delas causarem estragos, as organizações podem usar uma solução SIEM e *Threat Hunting* para identificar agentes de ameaças que já podem estar à espreita num ambiente e impedir ataques antes que eles continuem (Wang, 2023).
- **Deteção de ameaças em tempo real:** Integrar *feeds* de *Threat Hunting* numa solução SIEM aprimora as suas capacidades, ao fazer referência cruzada de dados internos com a inteligência de ameaças externas, as organizações podem identificar padrões e anomalias que, de outra forma, poderiam passar despercebidos (Wang, 2023).
- **Resposta a incidentes aprimorada**: Ocorre um incidente de segurança, o poder combinado do SIEM e da inteligência de ameaças é inestimável. As soluções SIEM fornecem uma linha do tempo de eventos que levam à violação, enquanto a inteligência de ameaças fornece *inshights* sobre os TTPs do invasor e os IOCs associados que podem acelerar a investigação (Wang, 2023).

Num cenário digital caracterizado por ameaças em constante evolução, as organizações devem permanecer vigilantes e adaptáveis nas suas estratégias de segurança cibernética. Soluções SIEM e *Threat Hunting/Intelligence* são ferramentas vitais que fornecem os *insights* necessários para ficar atento. Ao utilizar deteção de ameaças em tempo real, recursos de defesa proativos e resposta aprimorada a incidentes, em que esteja habilitado para estes sistemas, as empresas podem fortalecer as suas próprias defesas e proteger os seus dados confidenciais dos perigos sempre presentes no mundo cibernético. Adotar SIEM e *Threat Hunting* não é uma opção, mas sim uma necessidade para qualquer organização séria em que contenha algo sobre segurança cibernética (Wang, 2023).

4. Protótipo

4.1. Configuração da Plataforma SIEM

Neste subcapítulo, o seu objetivo é demonstrar uma visão geral da configuração da plataforma SIEM, onde é detalhado os *logs* recolhidos e os alertas que foram configurados.

4.1.1. Especificação e Planeamento

Após vários estudos e pesquisas das diferentes plataformas SIEM existentes, e definido os objetivos principais, foi selecionado a aplicação *Wazuh*.

Numa primeira fase, é necessário proceder a uma correta validação do inventário de ativos, de forma a garantir a maior abrangência possível, e de certa forma, distinguir os vários tipos de ativos existentes. No caso do inventário de ativos, é um procedimento que já existe dentro da empresa e que é levado a cabo todos os anos, de forma a manter o mais atualizado possível o ficheiro do inventário de ativos, este ficheiro é efetuado através de uma folha de excel, com várias análises da rede e em conjunto com o *endpoint* existente da *firewall*.

4.1.2. Instalação da plataforma SIEM

A implementação do SIEM, neste caso escolhido, foi o *Wazuh*, envolve uma série de passos de forma a garantir a sua instalação e configuração adequada em ambientes virtuais, desta forma, o *Wazuh* foi implementado numa máquina virtual no *VMWare Vsphere*, sendo descrito abaixo o processo em detalhe.

O primeiro passo a efetuar, consiste na criação de uma máquina virtual na plataforma *VMWare Vsphere*, este processo inicia-se com a definição das especificações de *hardware* e *software* necessárias para suportar o *Wazuh* de forma eficiente, de seguida, apresenta-se a Tabela 2, onde contém as configurações de *hardware* necessárias para o *Wazuh*.

Recursos *Hardware*	
Processador	4 vCPUs
Memória RAM	8GB (recomendando)
Armazenamento	50GB
Sistema Operativo	Ubuntu Server 22.04

Tabela 2 - Recursos de Hardware para Wazuh Fonte: Autor

Na Figura 1 demonstra-se a configuração dos recursos em concordância com a Tabela 2.

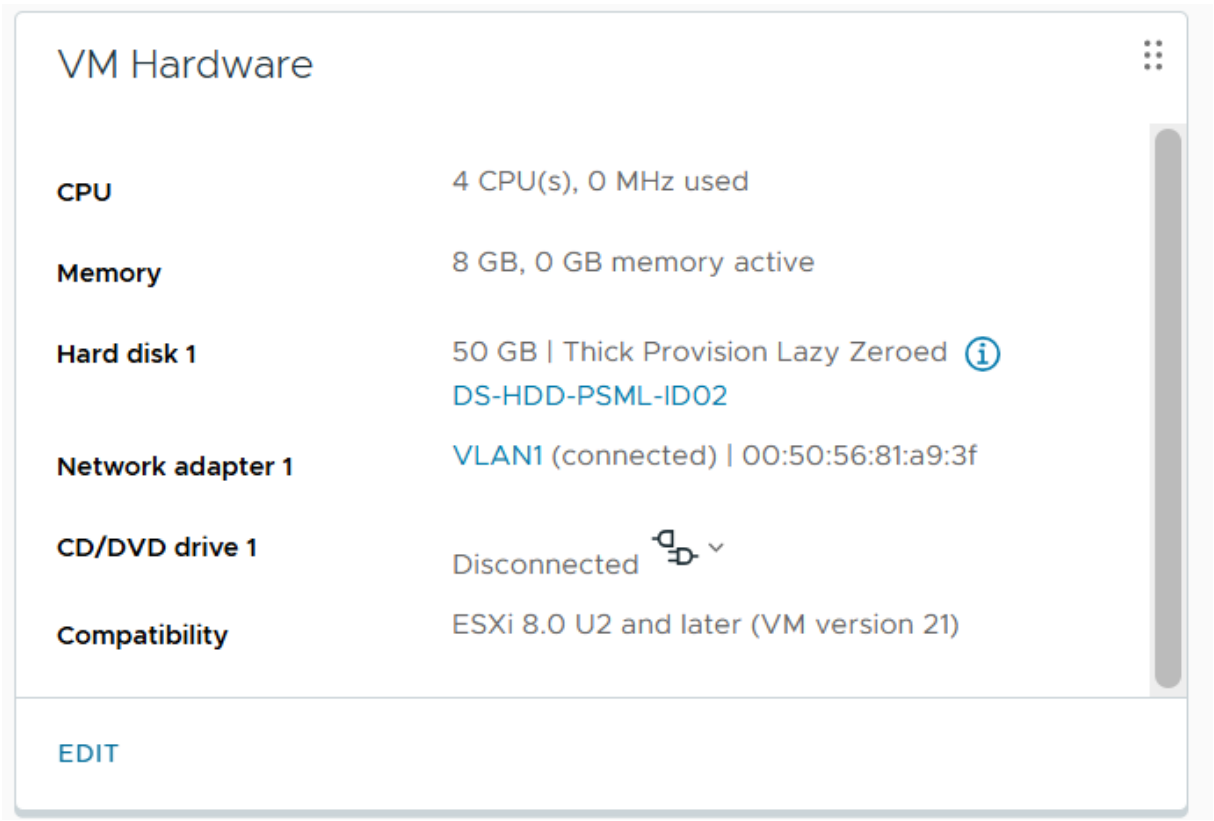

Figura 1 - Recursos atribuídos à VM Wazuh Fonte: Autor

Após efetuarmos a atribuição dos recursos à máquina virtual (VM), faz-se a associação da imagem ISO, neste caso, o *Ubuntu Server 22.04* à VM, que vai ser utilizado para o processo de instalação.

Assim que se acaba os passos anteriores, procede-se à instalação do sistema operativo, onde se configura os parâmetros básicos, como o fuso horário, a rede (neste caso em específico, configurou-se um IP Fixo), isto para não interferir com as restantes máquinas que estão criadas dentro da empresa, e faz-se a criação das credenciais do utilizador de administrador.

Com a VM devidamente preparada, avança-se para a instalação do Wazuh, para instalar o Wazuh existe diversas maneiras, podemos recorrer diretamente a uma máquina virtual já pronta, ou usar os comandos Linux para aceder às bibliotecas e fazer a instalação e configuração localmente, por questões preferenciais, instalou-se o Wazuh de forma manual.

De forma a garantir uma instalação do Wazuh limpa, é necessário garantir que todos os pacotes do sistema operativo usado, estão com uma versão recente e estável, para garantir este passo, usou-se o seguinte comando dentro do *Linux*:

```
psmladmin@srvpsmlwazuh:~$  sudo apt update && sudo apt upgrade -y
[sudo] password for psmladmin:
```

Figura 2 - Comando usado para garantir software atualizado no Linux Fonte: Autor

Depois de termos garantido que está tudo atualizado com o nosso sistema operativo, passamos então à fase de instalação oficial do Wazuh, todos os comandos e scripts usados, são informações disponibilizados pelo fabricante: (*https://documentation.wazuh.com/current/quickstart.html).*

Para instalarmos o Wazuh dentro do *Linux*, usou-se o seguinte comando:

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

Figura 3 - Comando usado para instalar o Wazuh Fonte: (Wazuh,2024)

Após a instalação ter sido efetuado, verifica-se o estado dos serviços principais do *Wazuh*, isto serve para validar se os mesmos foram iniciados corretamente, usou-se os seguintes comandos:

```
systemctl status wazuh-manager
systemctl status filebeat
```

Figura 4 - Comandos para reiniciar os serviços Wazuh Fonte: (Wazuh,2024)

Finalizado a instalação, é necessário proceder à configuração de rede e definições de acesso ao *Wazuh*, dentro deste processo, inclui configurar as regras de *firewall* para permitir a comunicação do servidor *Wazuh* com os restantes dispositivos na rede, sendo necessário abrir a seguinte porta da *firewall*:

- **514**: esta porta serve para a receção de *logs* via *syslog*.

Podemos confirmar a acessibilidade do painel de gestão do Wazuh através de um *browser*, utilizando o endereço IP definido para a máquina virtual ou, em caso de não se saber, podemos usar o seguinte URL:

- https://wazuh-dashboard-ip/

Por fim, realiza-se testes para validarmos a instalação, estes incluem validar/configurar os dispositivos de rede ou aplicações (como *firewalls)* para enviar *logs* ao *Wazuh* e verificar se os *logs* recebidos são processados e apresentados de forma correta no painel de análise.

4.1.3. Configuração dos logs

No *Wazuh* é fundamental assegurar a configuração de *logs*, para assegurar a recolha, análise e correlação de eventos provenientes de diferentes fontes na infraestrutura da organização. O *Wazuh* utiliza o *Filebeat*, este é um agente de recolha de *logs*, serve para captar dados de sistemas e dispositivo e enviá-los para o gestor de eventos.

Para configurar os *logs* é necessário identificar os dispositivos e sistemas cujos eventos deverão ser monitorizados, o mais comum, é *firewalls*, servidores, aplicações e os dispositivos atribuídos aos colaboradores.

Dentro do servidor *Wazuh*, existe um ficheiro de configuração do *Filebeat*, está localizado em ***/etc/filebeat/filebeat.yml***, dentro desse ficheiro, adiciona-se as definições para que o agente receba *logs* das fontes identificadas, utilizando protocolos como *syslog*

Para interpretar os dados recebidos, deve-se configurar regras específicas localizadas no seguinte diretório ***/var/ossec/rules/*,** estas regras permitem classificar e associar eventos a potenciais incidentes de segurança.

4.1.4. Criação de Regras

Uma vez configurado os *logs*, devemos fazer a criação das regras para permitir a classificação e associação do tipo de evento, as regras, conforme descrito no capítulo anterior, estão localizadas no diretório ***/var/ossec/rules/*,** cada regra é composta por elementos que especificam os padrões a ser detetados, quais as ações a tomar e qual o tipo de gravidade associada ao evento. De seguida, é apresentado uma estrutura básica do que inclui uma regra:

- **ID da Regra:** campo identificador único que permite distinguir a regra.
- **Descrição:** Um campo que descreve o tipo de evento ou comportamento que a regra procura identificar.
- **Padrões de Correspondência:** Campo baseado em critérios de expressões regulares ou outros tipos de atributos que os eventos devem cumprir para serem processados pela regra.
- **Ações e Gravidade:** Definições que determinam como o evento será tratado, incluindo o nível de alerta e qualquer ação subsequente.

Para criação de uma regra personalizada, dentro do *Wazuh*, vai-se criar um ficheiro XML com a definição da nova regra, por exemplo:

```
<rule id="100001" level="7">
  <decoded_as>syslog</decoded_as>
  <description>Autenticação falhada detectada</description>
  <match>authentication failure</match>
  <group>authentication_failed</group>
</rule>
```

Figura 5 - Criação de Regra Wazuh de Autenticação Falhada

Neste exemplo, a regra que foi criada, procura eventos de autenticação falhada nos *logs* recebidos via *syslog.*

De forma a garantir que a regra fica implementada, é necessário guardar o ficheiro no diretório ***/var/ossec/rules/*** e certificar-se de que o ficheiro tem as devidas permissões. Após guardar o ficheiro, deve-se reiniciar o serviço do *Wazuh* para aplicar as alterações, através do seguinte comando:

```
systemctl restart wazuh-manager
```

Figura 6 - Comando para reiniciar os serviços Wazuh

Depois de reiniciar os serviços, pode-se testar a regra, simulando eventos que correspondam ao padrão definidor e verificar se são detetados corretamente.

4.2. Implementação da Firewall Sophos XG

A organização em que foi implementado a solução de segurança da *Sophos XG*, atua no setor público, como prática comum no âmbito da função pública, qualquer aquisição de bens ou serviços deve obedecer às regras definidas no Código dos Contratos Públicos, sendo necessário a realização de um concurso público.

No concurso em questão, após avaliação das propostas submetidas, foi selecionado um fornecedor que demonstrou cumprir os requisitos do caderno de encargos, no qual, este fornecedor é especializado na implementação de solução da *Sophos*, razão pela qual a *Firewall* escolhida é da *Sophos.*

Este subcapítulo pretende descrever um pouco da visão geral da *Firewall* da *Sophos*, de como foi configurada, que tipo de *logs* recolhe, que alertas estão configuradas e que *feeds* de inteligência de ameaças foram integrados com esta solução.

4.2.1. Especificação e Planeamento

Inicialmente, foi necessário realizar uma análise detalhada da infraestrutura existente para identificar as necessidades específicas da organização, este processo incluiu o seguinte:

- Levantamento das redes existentes e serviços críticos;
- Identificação de ameaças e vulnerabilidades pré-existentes.

Depois de ter sido especificado e definido os requisitos necessários a implementar na *Firewall Sophos*, foi iniciado a aplicação da *appliance* da *Sophos*.

4.2.1.1. Modelo aplicado

O modelo aplicado na infraestrutura da organização, foi o modelo XGS 4300 conforme é demonstrado na Figura 7.

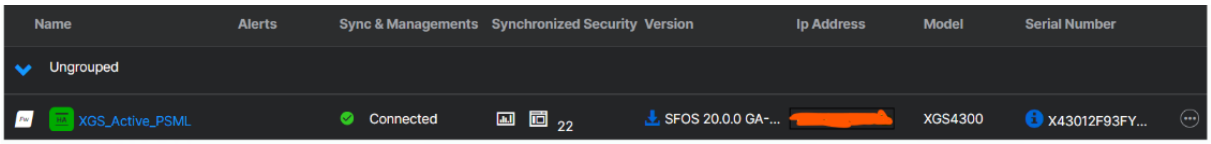

Figura 7 - Validação Modelo Firewall Fonte: Autor

4.2.1.2. Ligações de Interfaces de Rede

Após ligar a *appliance Sophos XGS* 4300, é necessário proceder às configurações das interfaces *Ethernet* às seguintes portas:

- **Porta WAN:** Onde vai ligar-se ao router da operadora;
- **Portas LAN:** Conexão aos *switches* da rede interna;
- **Portas MGMT:** Gestão da *Appliance da Sophos;*
- **Porta HA:** Porta de alta disponibilidade.

Na Figura 2, demonstra-se o painel frontal da *appliance Sophos XGS* 4300*:*

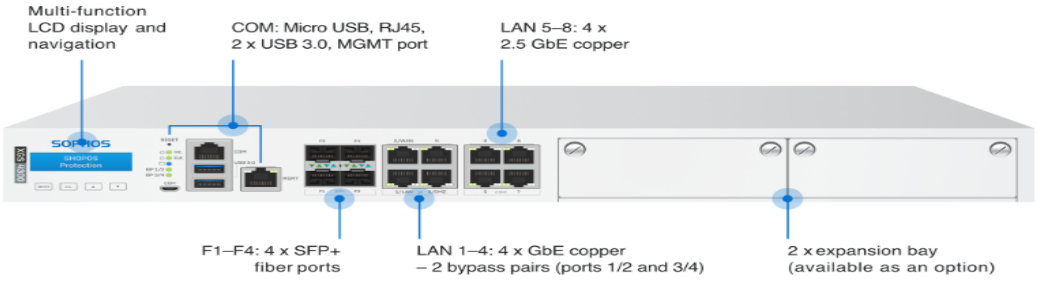

Figura 8 - Applicance Sophos XGS 4300 *Fonte: (Avanet, 2021)*

As configurações podem ser efetuadas de duas formas através de interface gráfica ou por consola, neste caso, procedeu-se à configuração através da interface gráfica, e seguiu-se o seguinte padrão de configuração das portas de acordo com a Tabela 3:

Interface	Zona	Endereço IP	Máscara	Estado
Port1	LAN	192.168.1.12	255.255.255.0	Ativa
Port2	WAN	62.28.132.235	255.255.255.0	Ativa
Port3	HA	203.0.113.2	255.255.255.252	Ativa
Port6	LAN	172.16.17.1	255.255.255.0	Ativa
PortMGMT	MGMT	172.16.16.16	255.255.255.0	Ativa

Tabela 3 - Configuração de interfaces Appliance Sophos Fonte: Autor

Através da interface gráfica, configurou-se as portas, em concordância com a Tabela 3:

Port1 – LAN (Rede Interna):

A Port1 foi configurada para a rede interna, servindo como ponto de conexão para dispositivos e sistemas locais, desta forma, garanta-se que o tráfego originado pelos utilizadores, servidores e dispositivos seja devidamente filtrado e protegido.

Atribuiu-se um endereço IP fixo para facilitar a comunicação e evitar conflitos de IP, de acordo com a Figura 9.

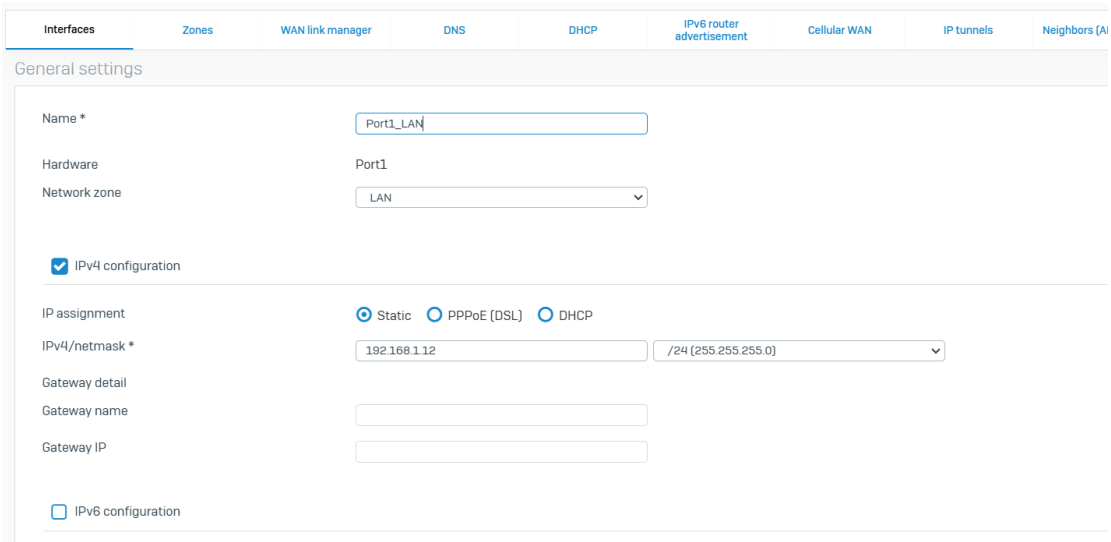

Figura 9 - Configuração Porta LAN Fonte: Autor

Port2 – WAN (Rede Externa):

A Port2 foi configura para ligar a *firewall* à rede externa, onde estabelece a conetividade com a operadora que nos fornece o serviço de Internet. Esta porta é essencial para garantir o acesso à Internet e serviços externos. Atribuiu-se o IP público para facilitar a comunicação entre a *Firewall* e o router da operadora, de acordo com a Figura 10.

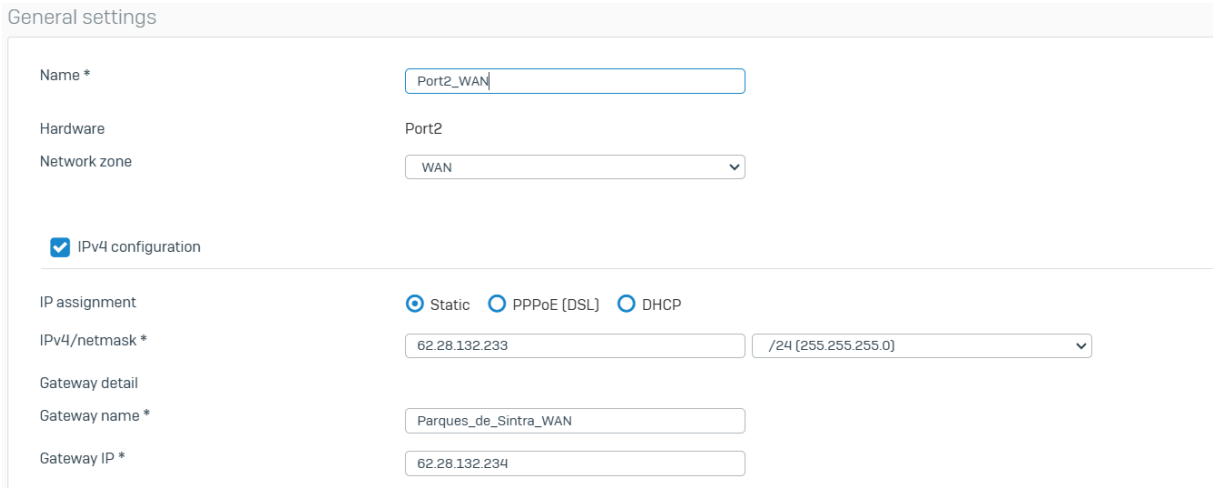

Figura 10 - Configuração Porta WAN Fonte: Autor

Port3 – HA (*High Availability)*:

Esta porta é utilizada para configurar a funcionalidade alta disponibilidade (HA) entre duas *appliances Sophos*, permitindo a redundância do sistema. A Configuração HA assegura a continuidade do serviço em caso de falha da *Firewall* principal.

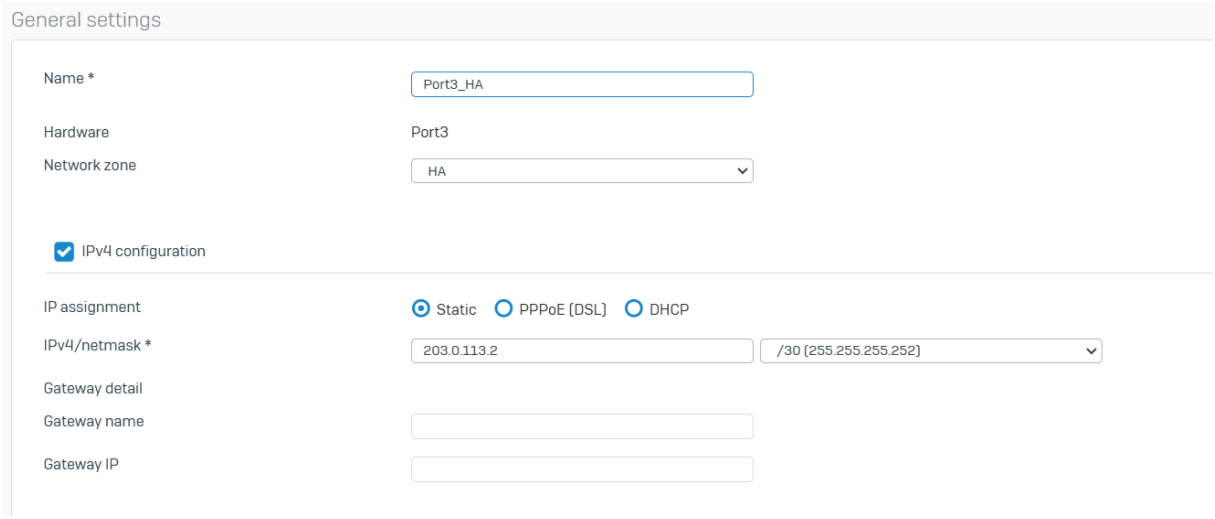

Figura 11 - Configuração Porta HA Fonte: Autor

Port6 – LAN2 (Segmentação Adicional):

Esta porta foi configurada como uma extensão da rede interna, para suportar outro segmento de dispositivos e serviços existentes dentro da organização, basicamente é útil para separar fisicamente os diferentes tipos de departamentos e dispositivos existentes dentro da organização, permitindo aumentar a segurança e facilitar a aplicação de políticas distintas.

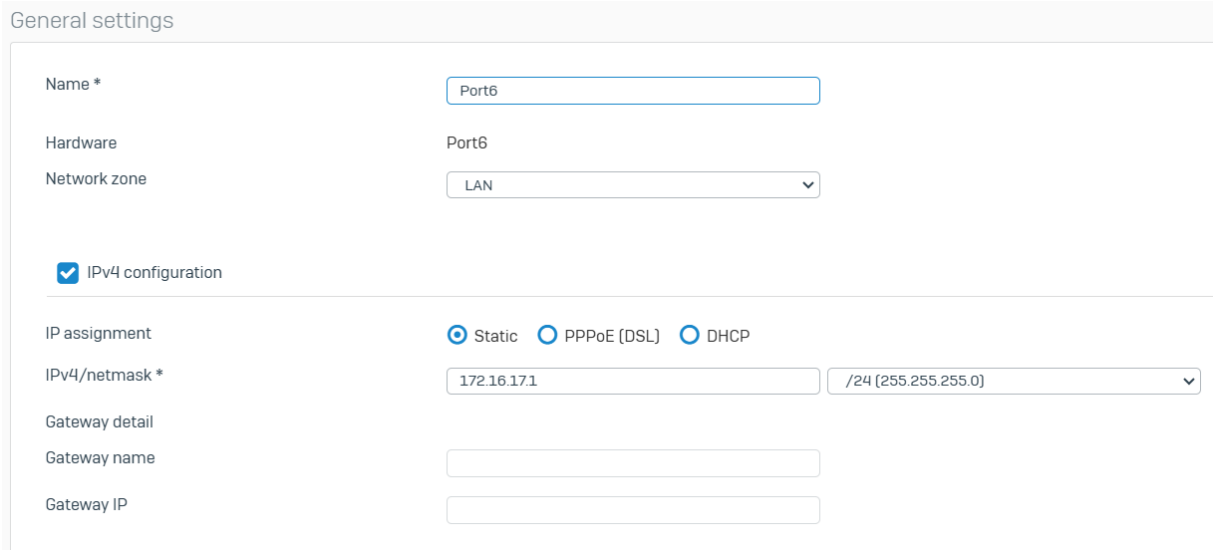

Figura 12 - Configuração Porta LAN2 Fonte: Autor

PortMGMT – Gestão:

A porta MGMT está reservada para funções de gestão (MGMT) da *firewall*, permite o acesso direto ao interface administrativo da *Sophos*, esta porta é dedicada à gestão e oferece uma maior segurança e controlo da *appliance.*

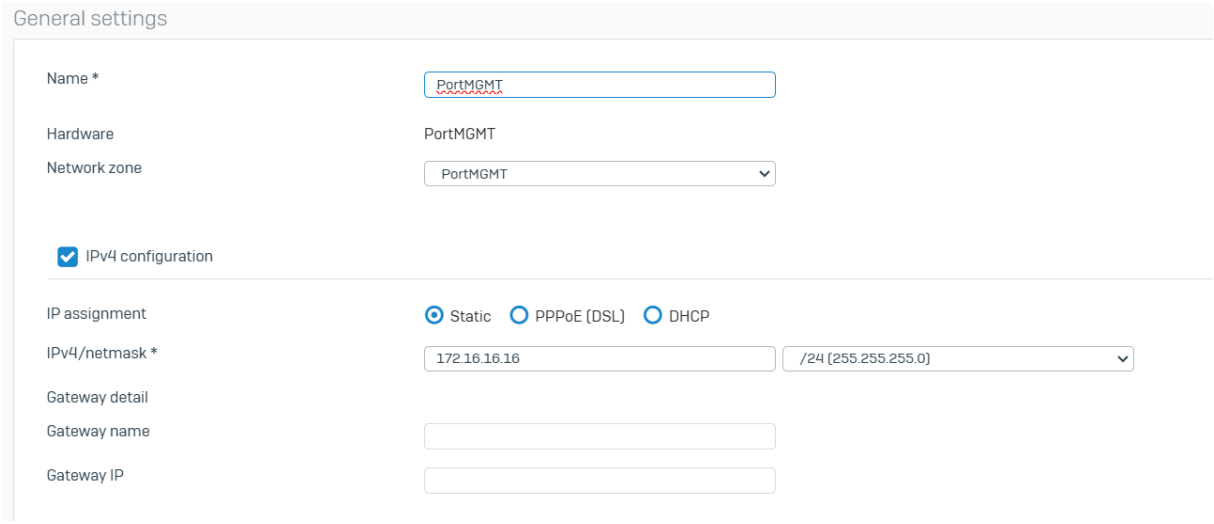

Figura 13 - Configuração Porta MGMT Fonte: Autor

Em conclusão, esta atribuição efetuada às portas específicas da *appliance Sophos XGS 4300*, segue as boas práticas de segmentação e segurança de rede.

4.2.2. *Sophos Endpoint Protection*

O *Sophos Endpoint Protection* é uma solução de segurança avançada com o objetivo de proteger os dispositivos finais, tais como computadores e servidores, contra os ataques cibernéticos. Esta solução combina tecnologias como deteção baseada em assinatura, inteligência artificial e análise comportamental para prevenir *malware*, *ransomware*, *exploits*, entre outros tipos de ataques.

Para implementar este agente, é necessário instalar nos vários dispositivos existentes que se pretende proteger, a instalação é efetuada através de um *setup* existente, tanto para Windows como para MAC OS.

Este *Endpoint* vai servir para proteger os dispositivos finais contra uma vasta gama de ameaças, incluindo o *malware, ransomware*, explorações de vulnerabilidade, acesso não autorizado a atividades maliciosas. A integração com a *firewall Sophos XGS 4300*, funciona através da funcionalidade *Synchronized Security,* onde conseguimos ter acesso em tempo real sobre o estado de segurança do dispositivo, caso o dispositivo esteja comprometido, a *firewall* pode isolar automaticamente o mesmo dispositivo da rede para evitar a propagação de ameaças, permite também, efetuar o reforço de políticas de rede, através das definições do *Endpoint.*

No dispositivo final, o *Sophos Endpoint Agent* é o componente instalado, responsável por implementar as políticas de segurança definidas e monitorização de atividades relacionadas com a proteção contra ameaças. Este agente, disponibiliza três categorias principais de informações no *Sophos Central: Status, Events* e *Detections*, cada uma desempenha um papel distinto na monitorização e gestão de segurança.

O *Status* apresenta uma visão geral do estado atual do dispositivo e da proteção fornecida pelo *endpoint*, conforme se pode visualizar na Figura 14.

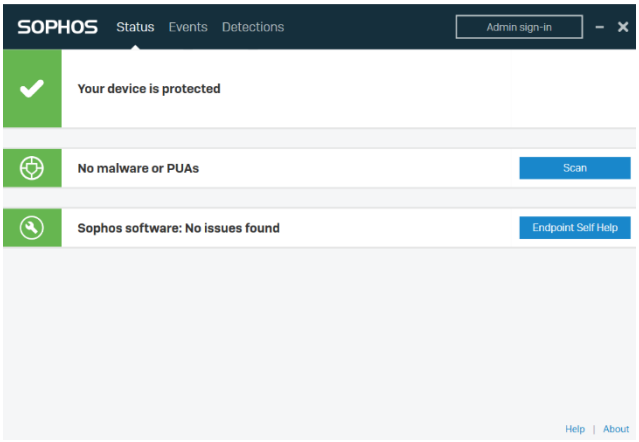

Figura 14 - Endpoint Sophos - Separador Status Fonte: Autor

No caso do *Events*, este regista todas as atividades relacionadas com o *endpoint*, o dispositivo e a interação com o sistema, ou seja, a informação que apresenta é as atividades gerais, tais como atualizações do agente ou reinícios de serviços, alterações nas configurações ou nas políticas. A finalidade é oferecer uma visão holística das interações do sistema, permitindo auditorias detalhadas e identificação de alterações ou ações específicas que possam ter impactado o estado de segurança do dispositivo, conforme demonstra a Figura 15.

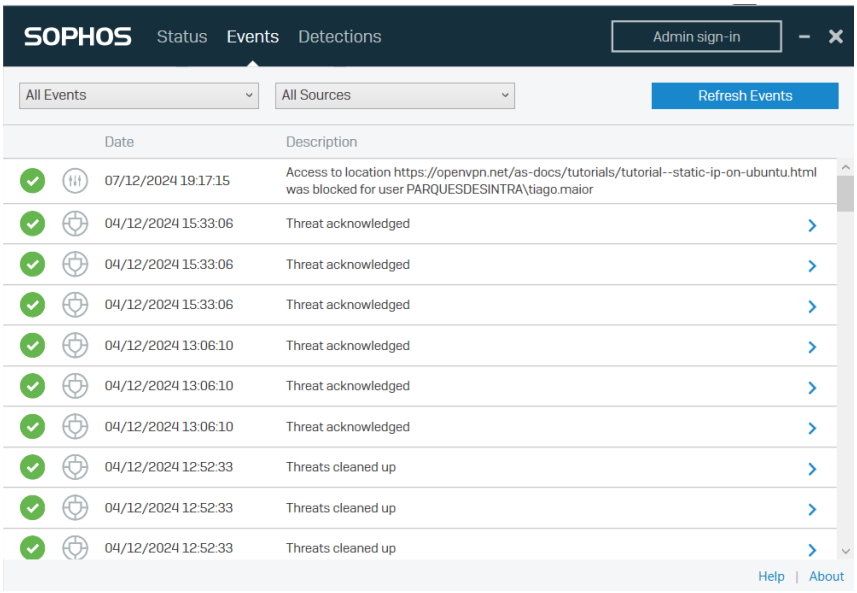

Figura 15 - Endpoint Sophos - Separador Events Fonte: Autor

No separador *Detections*, este apresenta todas as ameaças identificadas pelo agente no dispositivo, tais como a descrição detalhada das ameaças (em *Malware and PUA Event History)*, indicadores de comprometimento, como ficheiros maliciosos, endereços IP ou processos envolvidos e qual o tipo de ação tomada automaticamente pelo *endpoint,* conforme é possível observar na Figura 16.

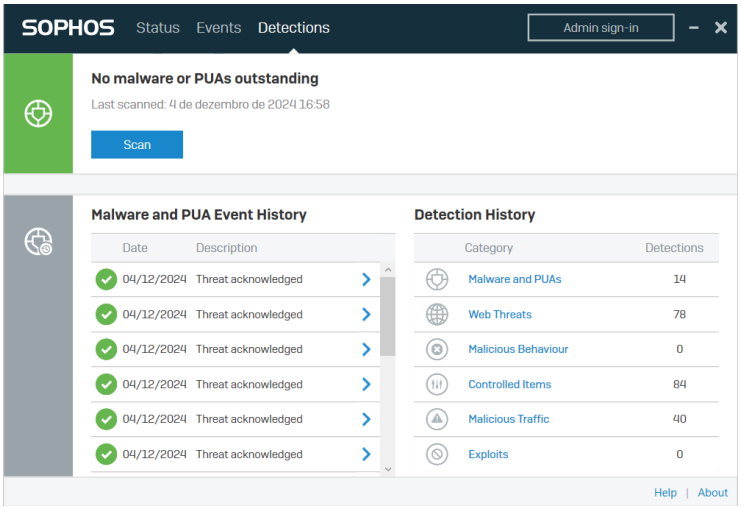

Figura 16 - Endpoint Sophos - Separador Detections Fonte: Autor

Este tipo de informação disponibilizada pelo *Endpoint da Sophos*, também é possível ser acessível através da central da *Sophos*.

A finalidade destes separadores é de permitir que os administradores de sistemas possam verificar rapidamente a saúde geral do dispositivo, identificar problemas de configuração ou falhas de proteção, e atuar de forma preventiva, de forma a garantir que todos os dispositivos estejam devidamente protegidos.

4.2.3. Sophos Central

A *Sophos Central* é uma plataforma de gestão unificada baseada na *cloud*, em que foi configurado para administrar, monitorizar e proteger os diferentes tipos de componentes da infraestrutura de segurança de uma organização. Dentro deste portal centralizado, é permitido a configuração de políticas, monitorizar o estado dos dispositivos e serviços, responder a incidentes de segurança e gerar relatórios de conformidade.

Existe diversas funcionalidades principais da *Sophos Central*, no qual vai ser demonstrado exemplos disso:

1. **Gestão Centralizada:**
    a. Aqui permite configurar e aplicar políticas de segurança em dispositivos finais (*endpoints*), *firewalls*, e outros serviços que estejam integrados com a *Sophos*. Na Figura 17, é possível observar as informações de *dashboard* que aparece ao iniciarmos sessão na *Sophos Central.*

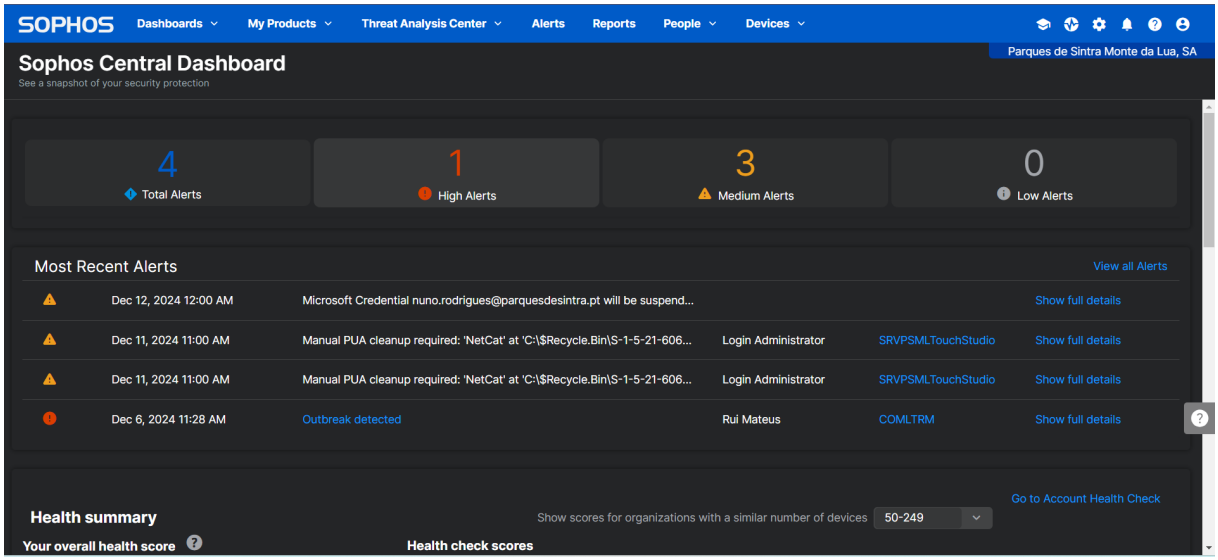

Figura 17 - Sophos Central Fonte: Autor

2. **Monitorização em Tempo Real:**
    a. Demonstra informações detalhadas sobre o estado de saúde e as atividades de segurança dos *endpoints*, incluindo os eventos que decorreram, deteções e ações corretivas que tenham ocorrido. Na Figura 18, observamos um exemplo de um *endpoint* com monitorização em tempo real.

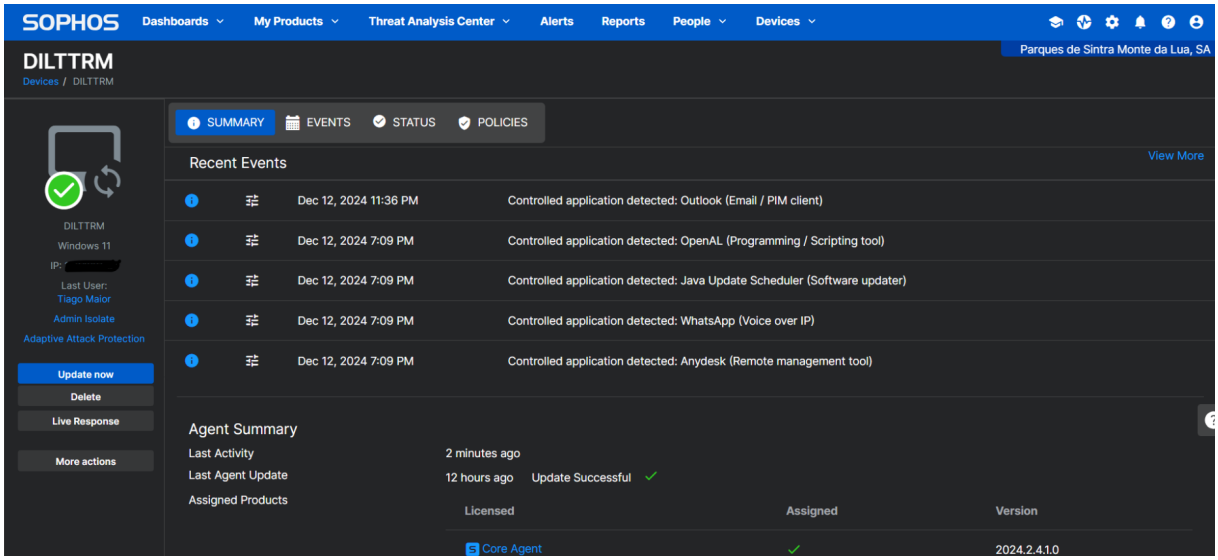

Figura 18 - Monitorização em Tempo Real de um Endpoint Fonte: Autor

3. **Resposta a incidentes:**
    a. Facilita o tipo de resposta a ameaças detetadas, incluindo o isolamento a efetuar aos dispositivos, eliminação de ficheiros maliciosos e ajustes nas políticas de segurança.

4. **Relatórios e Auditorias:**
    a. A *Sophos Central* oferece ferramentas para gerar relatórios personalizados sobre incidentes, comportamentos dos *endpoints*, entre outros registos que

seja necessário para uma auditória ou relatórios anuais a entregar ao CNCS. Na Figura 19, é possível observar os vários tipos de *dashboards* que existem.

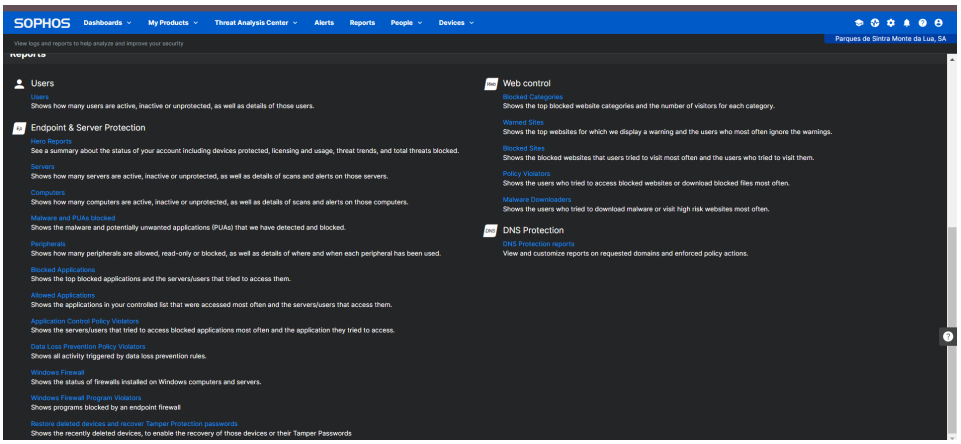

Figura 19 - Vários tipos de Dashboards Fonte: Autor

4.2.4. Threat Analysis Center Sophos

O *Threat Analysis Center* da *Sophos* é um módulo que está na *Sophos Central* que agrega, relaciona e apresenta dados sobre eventos de segurança provenientes de diferentes soluções da *Sophos*, como o *Endpoint Protection, Firewall Sophos XGS* e *XDR (Extended Detection and response)*, este centro de análise, acaba por atuar como um *hub* de inteligência de ameaças, auxiliando na deteção precoce e na resposta coordenada a incidentes. Na Figura 20, é demonstrado os casos que vão acontecendo e os alertas que envia.

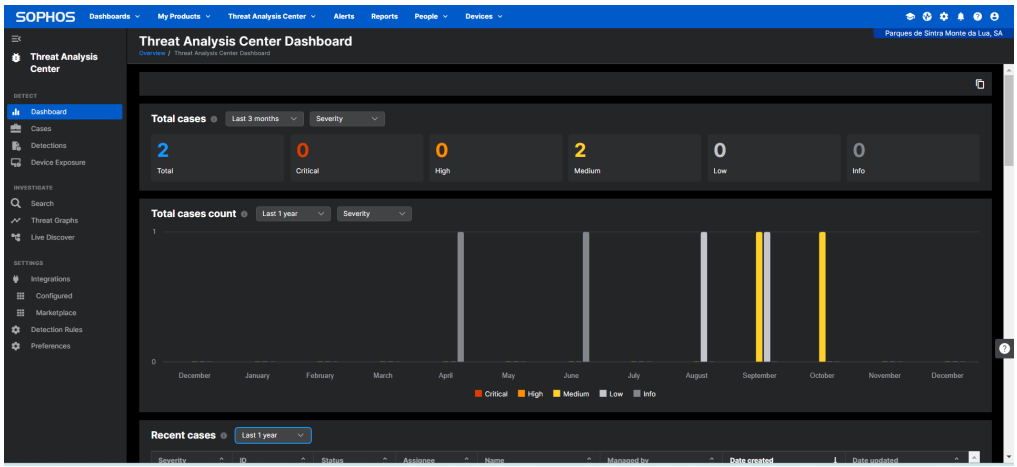

Figura 20 - Threat Analysis Center Fonte: Autor

O *Threat Analysis Center* centraliza uma série de funcionalidades essenciais, desde a deteção de ameaças, identificando atividades maliciosas, como *malware*, tentativas de acesso não autorizado e comportamentos anómalos. Utilizando inteligência artificial e *machine learning*, a *Sophos* Central consegue relacionar eventos e destacar incidentes críticos.

Além disso, oferece uma monitorização centralizada, agregando todos os tipos de dados, provenientes de *endpoints*, *firewalls*, entre outros, desde que estejam devidamente configurados

para serem detetados, é possível também, efetuar uma análise forense, onde permite investigar com detalhe os incidentes, apresentando a origem, o vetor de ataque os impactos potenciais que essa ameaça possa vir a trazer, permite também aceder a indicadores de comprometimento (IOCs), tais como IPs maliciosos, ficheiros suspeitos ou processos comprometedores.

Estas capacidades permitem uma resposta a incidentes de forma rápida e eficaz, devido a proporcionar ferramentas para mitigar as ameaças de forma célere, incluindo o isolamento dos dispositivos, bloqueio de acessos e eliminação de ficheiros maliciosos.

Os benefícios deste tipo de serviço, proporciona uma visão ampliada de todas as ameaças existentes, facilitando os administradores de sistemas a compreenderem a postura de segurança global da organização, uma deteção mais eficaz e rápida, existir uma mitigação proativa e a redução da complexidade a identificar e gerir incidentes.

4.2.5. Inputs

A *Sophos Central* permite, através de políticas configuráveis, a injeção de *logs* das aplicações, servidores, *routers*, *endpoints* finais utilizando múltiplas fontes de entrada. Para viabilizar este tipo de integração, foi necessário proceder-se à definição e configuração de várias políticas que vão ser exemplificadas de seguida.

Existem diversos tipos de políticas dentro da *Sophos Central*, cada uma com a sua finalidade, de seguida, segue alguns exemplos do tipo de políticas possíveis de aplicar:

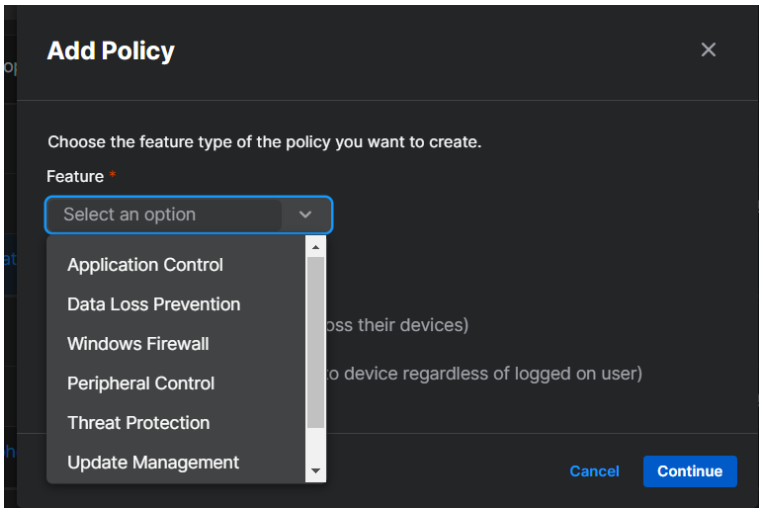

Figura 21 - Exemplos de tipos de políticas Fonte: Autor

No caso desta organização, aplicou-se quase na totalidade, para todos os *endpoints* finais, a mesma política, conforme exemplos a serem demonstrados de seguida:

1- Threat Protection:

Esta política é responsável por ativar e configurar várias funcionalidades de deteção, prevenção e mitigação de ameaças, onde permite implementar uma abordagem robusta e eficiente para proteger todos os dispositivos e dados contra um cenário de ameaças em constante evolução.

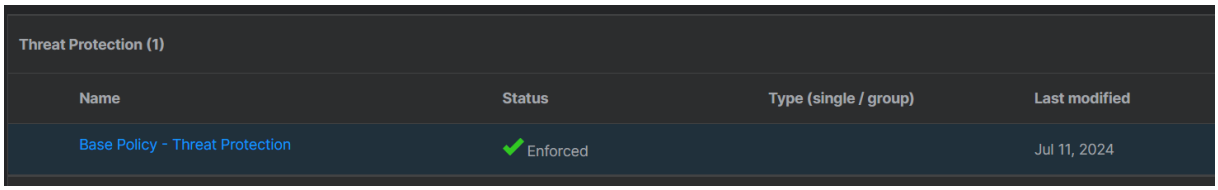

Figura 22 - Exemplo de Política aplicada Fonte: Autor

2- Peripheral Control:

Esta política serve para permitir e gerir o acesso e uso de dispositivos periféricos nos *endpoints*, tais como pen USB, impressora, entre outros. Esta política desempenha um papel fundamental na proteção contra a perda de dados, introdução de ameaças e utilização indevida de dispositivos não autorizados.

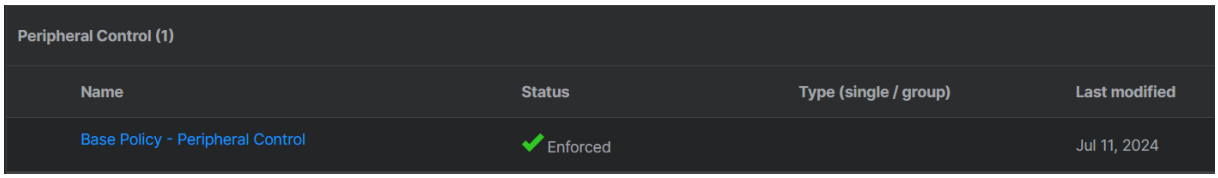

Figura 23 - Exemplo de Política 2 aplicada Fonte: Autor

3- Application Control:

Esta política foi projetada para gerir e controlar o uso de aplicações em *endpoints* e servidores, onde permite restringir ou bloquear a execução de aplicações não autorizadas, reduzindo o risco de segurança e garante o cumprimento das normas e políticas internas.

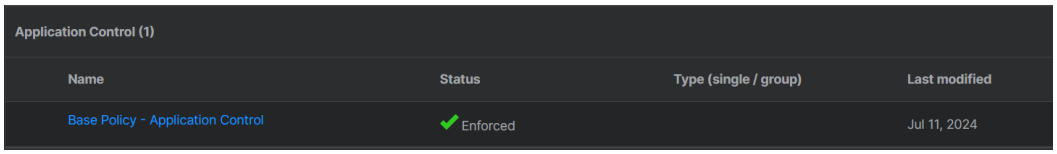

Figura 24 - Exemplo de Política 3 aplicada Fonte: Autor

4- Data Loss Prevention:

A política *Data Loss Prevention* é uma funcionalidade concebida para prevenir a perda, fuga ou partilha não autorizada de informações sensíveis, esta política, acaba por ajuda as organizações a proteger dados críticos, como informações financeiras, propriedade intelectual, dados pessoais e outras informações que sejam confidenciais.

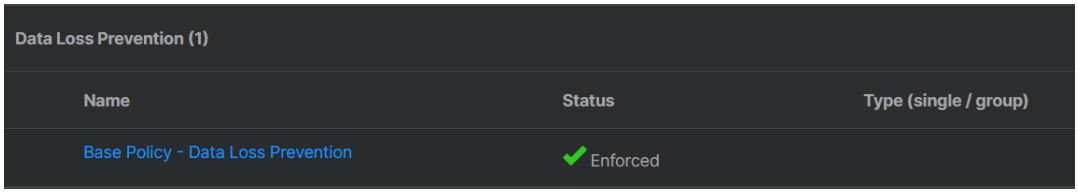

Figura 25 - Exemplo de Política 4 aplicada Fonte: Autor

5- Web Control:

A política *Web Control* é uma ferramenta que vai permitir gerir e monitorizar o acesso a websites através dos *endpoints* finais, onde consegue proporcionar uma proteção contra ameaças baseadas na *web* e promove o uso adequado da internet num ambiente corporativo.

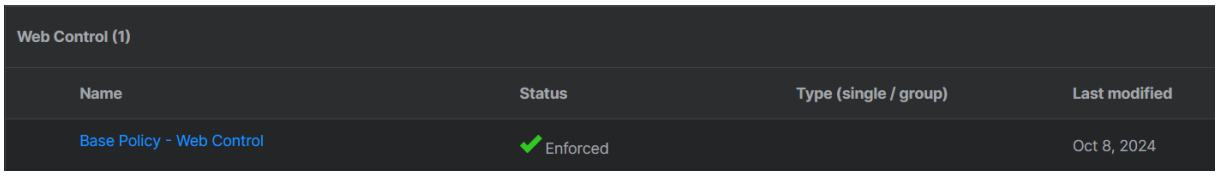

Figura 26 - Exemplo de Política 5 aplicada Fonte: Autor

6- Update Management:

Esta política é fundamental para gerir e instalar atualizações e *patches* nos *endpoints* protegidos, esta política vai garantir que os sistemas utilizam as versões mais recentes dos componentes de proteção da *Sophos*, reduzindo as vulnerabilidades e assegura o desempenho ideal das soluções de segurança existentes.

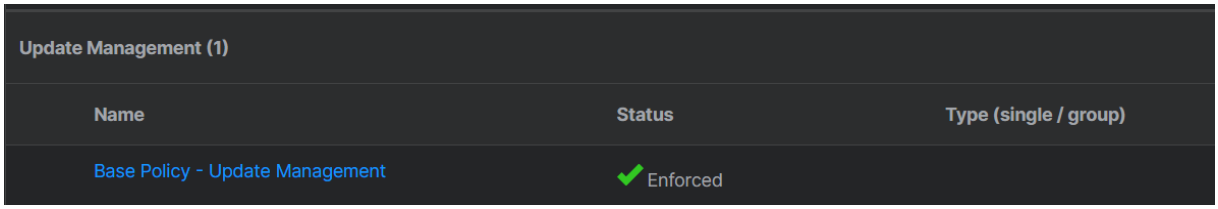

Figura 27 - Exemplo de Política 6 aplicada - Fonte: Autor

7- Windows Firewall:

Esta política oferece uma camada adicional de controlo e proteção ao permitir uma gestão centralizada das definições da *Firewall* nativa do *Windows*, esta funcionalidade complementa as defesas da *Sophos*, utilizando as capacidades integradas do sistema operativo para restringir o tráfego de rede não autorizado e proteger os *endpoints* contra ameaças externas e internas.

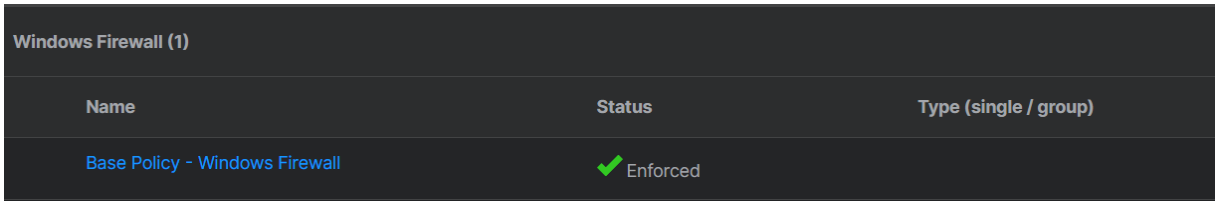

Figura 28 - Exemplo de Política 7 aplicada Fonte: Autor

Foi configurado várias funcionalidades dependendo do tipo de equipamento e protocolo na política, em que vai estar em maior detalhe no APÊNDICE I – Configuração Pormenorizada das Políticas *Endpoints*.

4.2.6. Dashboards

A construção de *dashboards* permite disponibilizar as informações de acordo com o que é pretendido, é uma ferramenta fundamental para a gestão centralizada e monitorização de segurança de uma organização, no caso da *Sophos*, ao ter uma gestão centralizada, permite que se visualize em tempo real, o estado geral da proteção, identificação de ameaças e que sejam tomadas decisões baseado em dados concretos e reais.

Dentro da *Sophos Central*, é possível criar um *dashboard* adaptado às necessidades da organização, de seguida, vai ser demonstrado alguns exemplos de dashboards montados.

O primeiro *dashboard*, Figura 29, demonstra as atividades dos *endpoints* finais em que foi configurado para obter este tipo de informação.

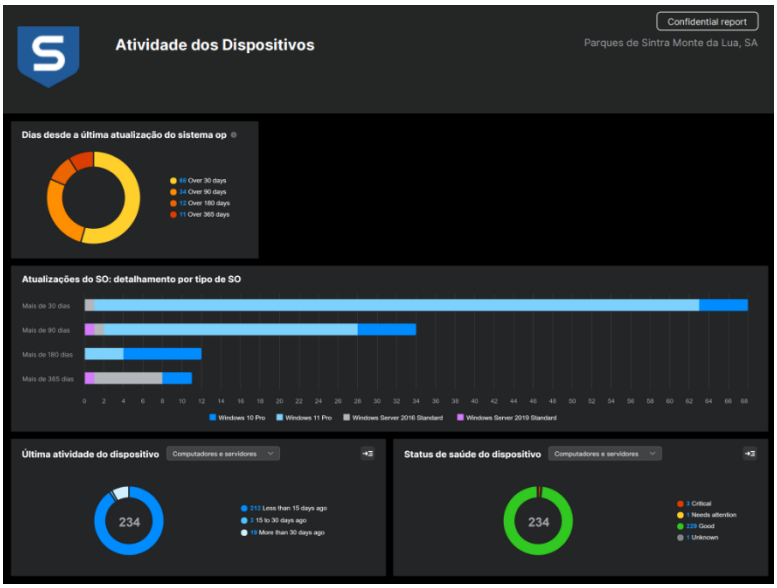

Figura 29 - Dashboard Atividade dos Dispositivos Fonte: Autor

O *Dashboard* da Figura 30, demonstra a atividade das análises avançadas e detetadas pelo XDR.

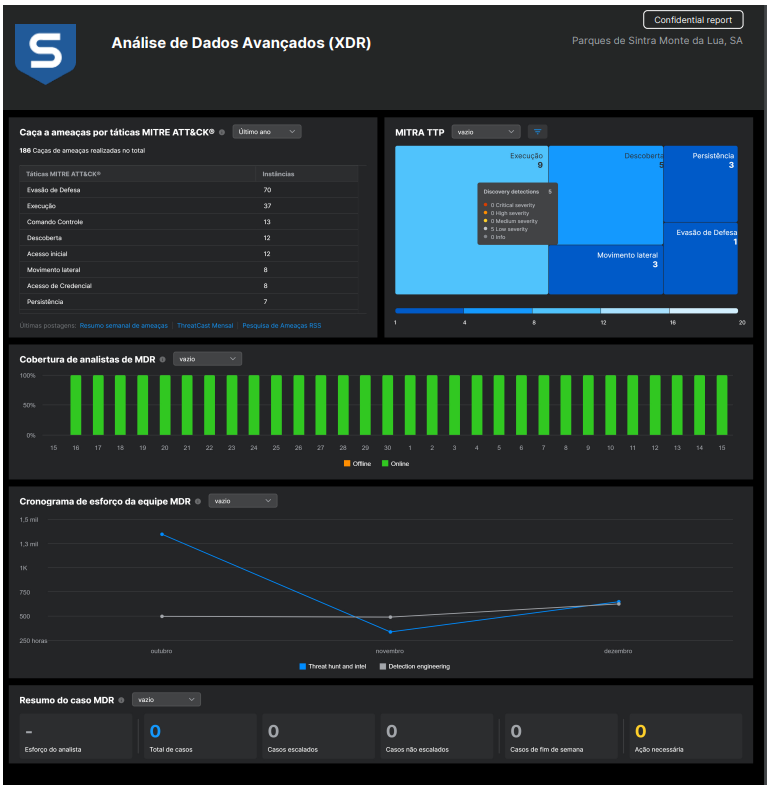

Figura 30 - Dashboard Análise de Dados Avançados (XDR) Fonte: Autor

4.2.7. Cenário Prático – Exemplo de deteção de ameaça

Ao analisar-se aleatoriamente o tráfego recebido, a plataforma SIEM e a *Sophos Central*, estão parametrizadas para emitir de imediato o seu alerta na deteção de ameaças.

Na Figura 31, é possível observamos a *Sophos Central*, no seu imediato a detetar uma ameaça e a notificar a mesma via email (Figura 32).

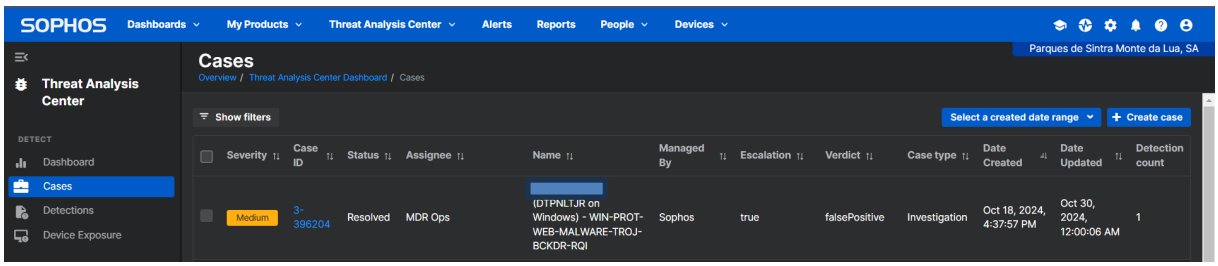

Figura 31 - Deteção de uma Ameaça Sophos Central Fonte: Autor

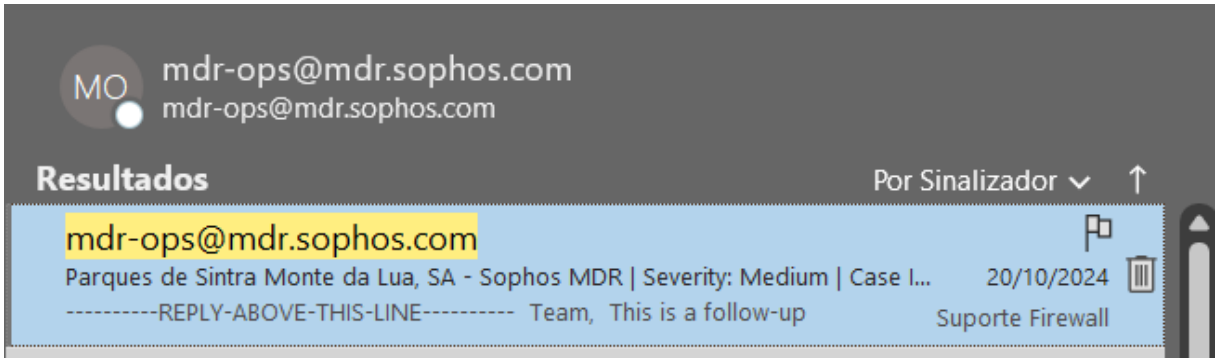

Figura 32 - Email alerta de deteção de Ameaça Fonte: Autor

Dentro da *Sophos Central,* é possível analisar com maior detalhe a ameaça detetada, onde faz uma breve descrição do caso, Severidade de ameaça, tipo de ameaça, fonte da ameaça e uma cronologia do caso em si, conforme a Figura 33 demonstra.

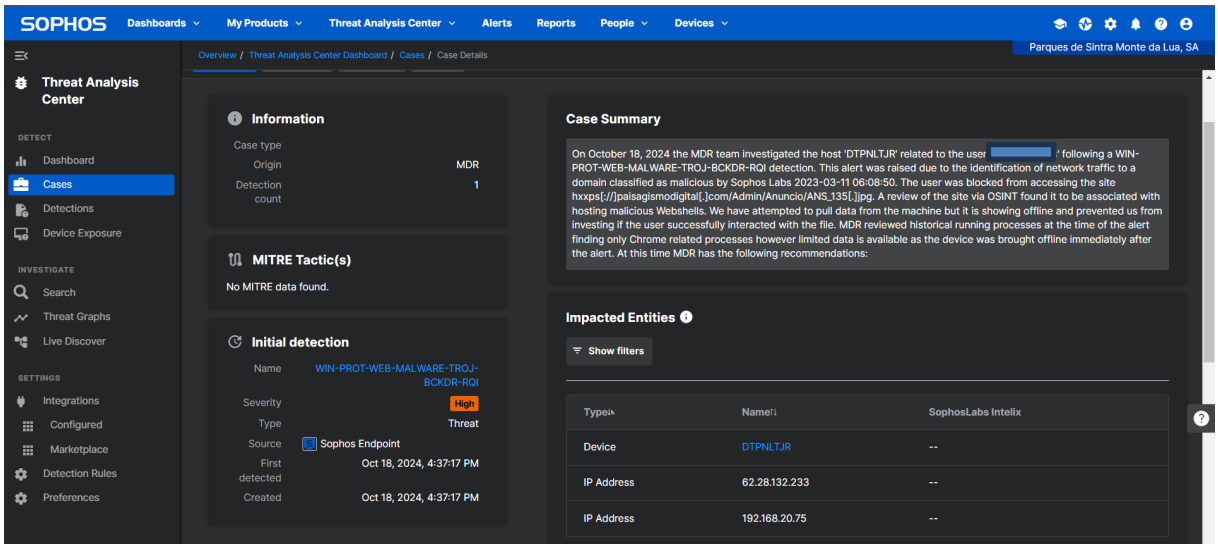

Figura 33 - Detalhe da Ameaça Detetada Fonte: Autor

Na Figura 34, observamos o tipo de deteção que foi efetuada, quando ocorreu e se foi detetada pelo *Endpoint* da *Sophos*.

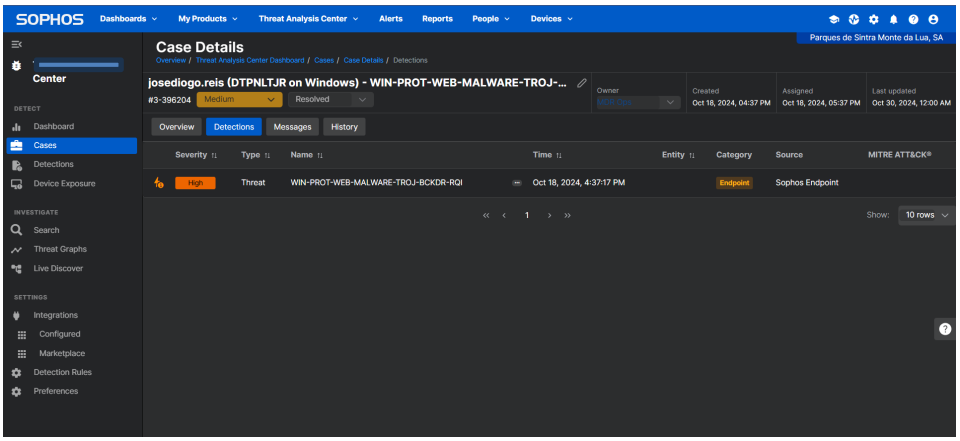

Figura 34 - Detalhes do Caso da Ameaça Deteada Fonte: Autor

Na Figura 35 ilustra as mensagens de alerta geradas por email, e serve como espaço para registo de mensagens, facilitando a continuidade do acompanhamento do caso em situações de escalonamento entre diferentes intervenientes.

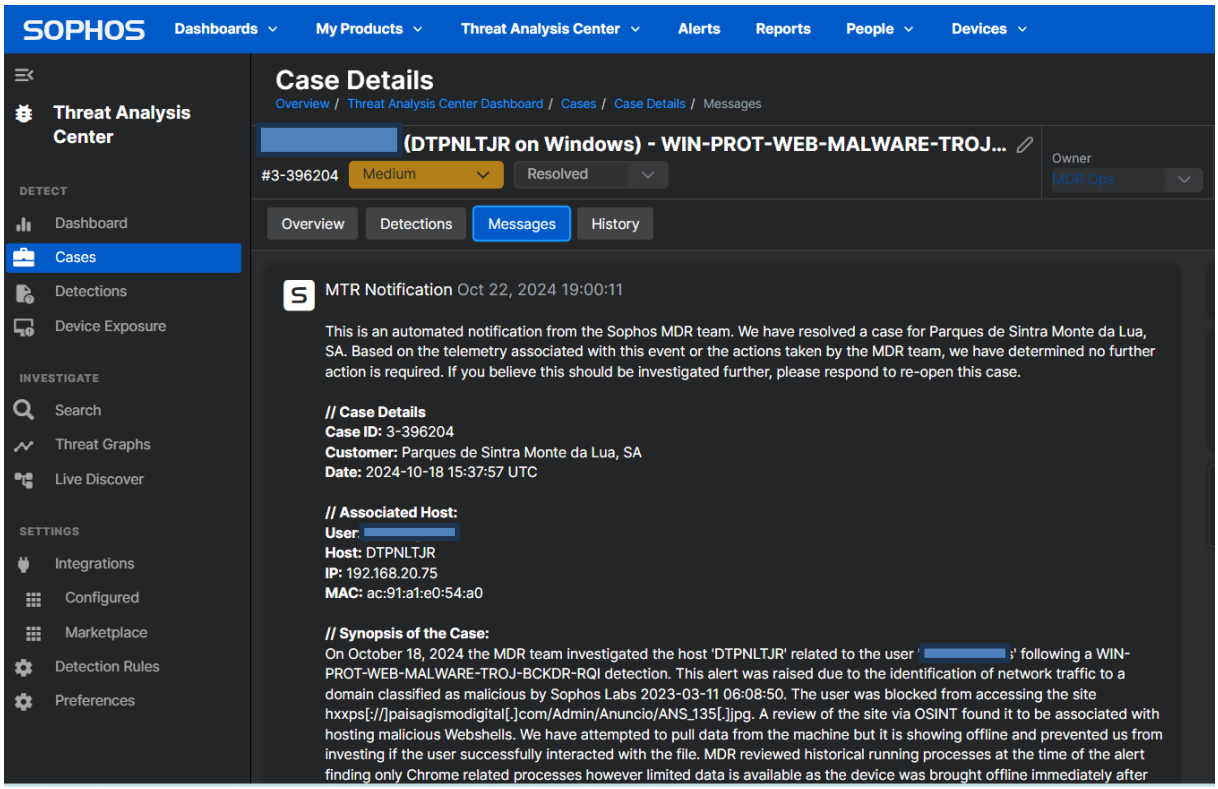

Figura 35 - Detalhes das Mensagens da Ameaça Detetada Fonte: Autor

Na Figura 36 é ilustrado o detalhe todo da ameaça que foi detetada, dados de onde foi encontrado a ameaça e se já existiu deteções similares ou não.

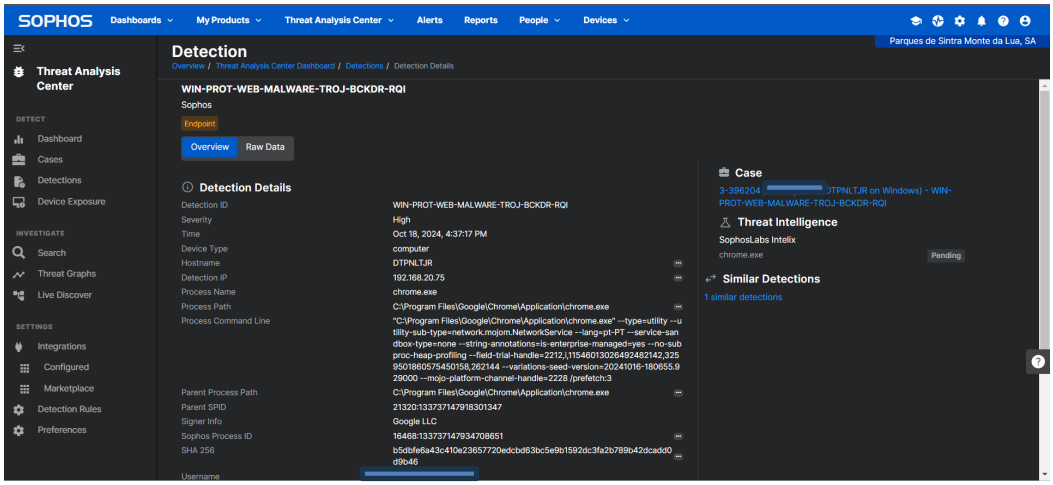

Figura 36 - Detalhe todo do caso de Ameaça Detetada Fonte: Autor

Na Figura 37, foi efetuado um exemplo de um agente instalado, neste exemplo específico, foi-se buscar o nome do meu computador de serviço, onde é possível visualizar que está ativo e regista os dados necessários.

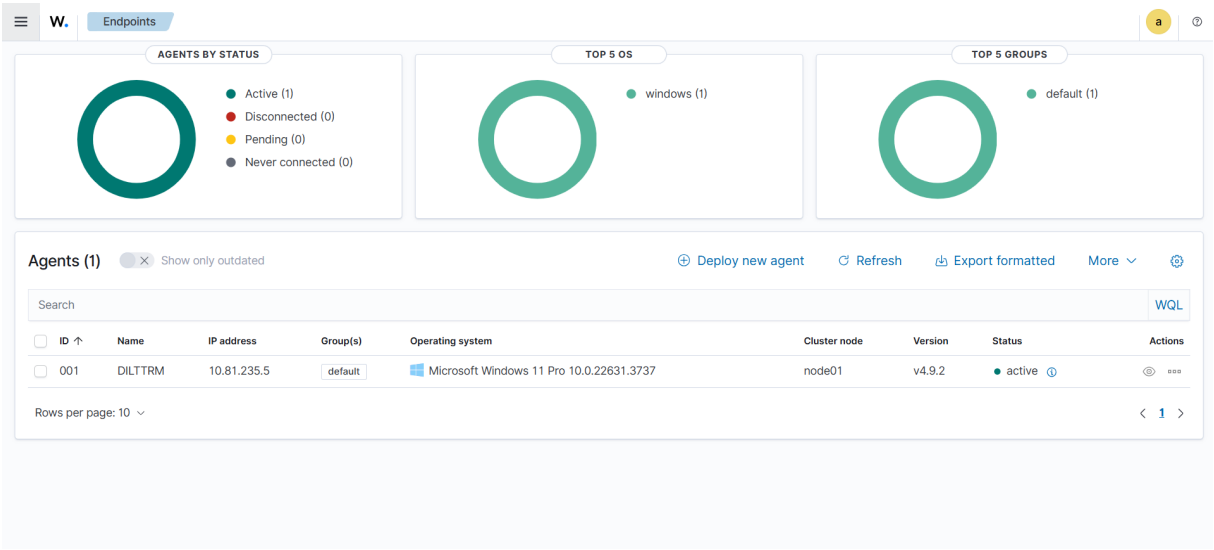

Figura 37 - Agente instalado com o Wazuh Fonte: Autor

5. Resultados

Após implementarmos o protótipo em produção, foi possível recolher e analisar os dados que vão ser apresentados nas alíneas seguintes, os quais são fundamentais para o estabelecimento de padrões em que possam indicar potenciais suspeitas, eventos de erro ou alertas das ciberameaças. Esta análise, baseia-se em dois fatores principais: a identificação de padrões relativos aos eventos e às respetivas comunicações, por outro lado, a validação da relevância da informação no contexto de ameaças cibernéticas, especialmente no que diz respeito à deteção e mitigação da ciberameaças.

a) Número de eventos reportados

Durante 90 dias, contabilizou-se um total de 238949 Eventos relativos a deteções de *malware* nos dispositivos finais.

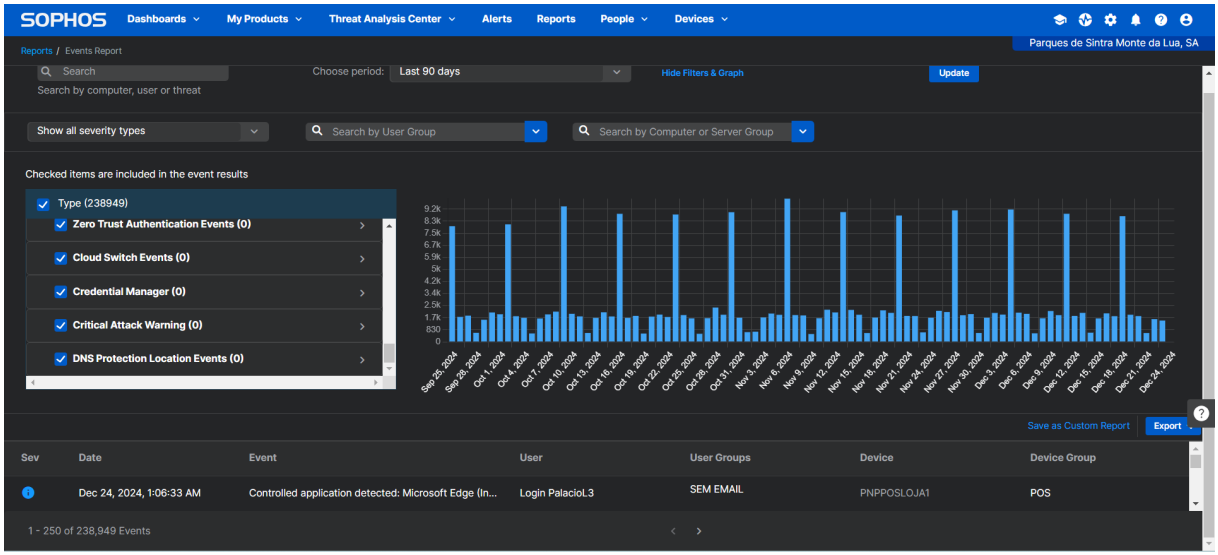

Figura 38 - Registo de eventos onde mostra todos os eventos de segurança, como deteções de malware Fonte: Autor

b) Auditoria de Logs

Registo de todas as atividades e alterações efetuadas no sistema, neste exemplo em concreto da Figura 38, foi escolhido a data de 17/12/2024 a 24/12/2024.

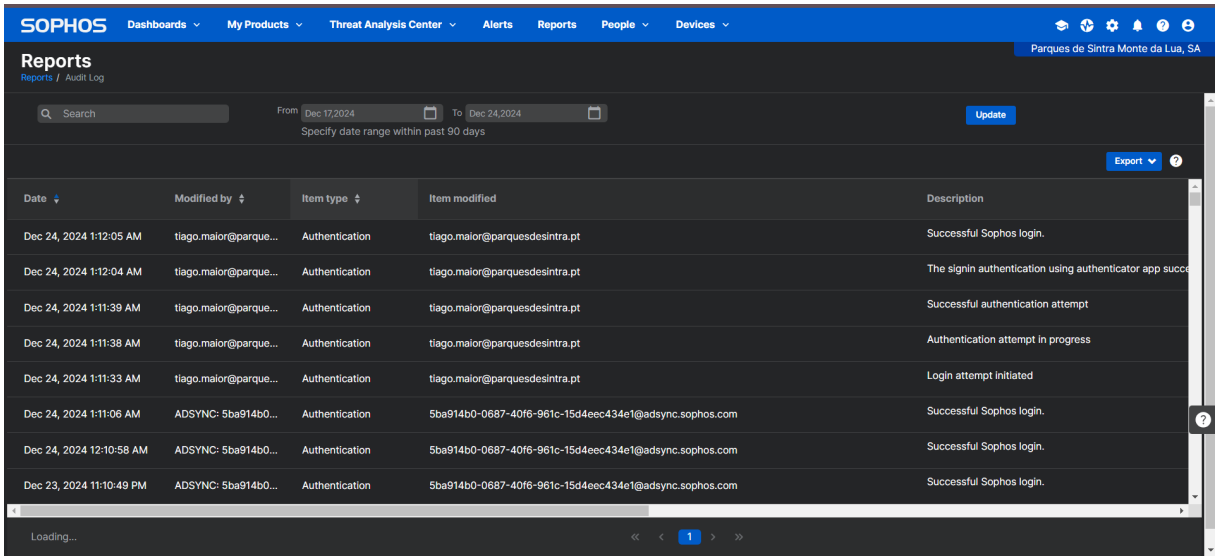

Figura 39 - Registo de Auditoria de Logs Fonte: Autor

c) Proteção dos *Endpoints Sophos*

Resumo do número de dispositivos protegidos e aplicações bloqueadas com um período de 1 mês.

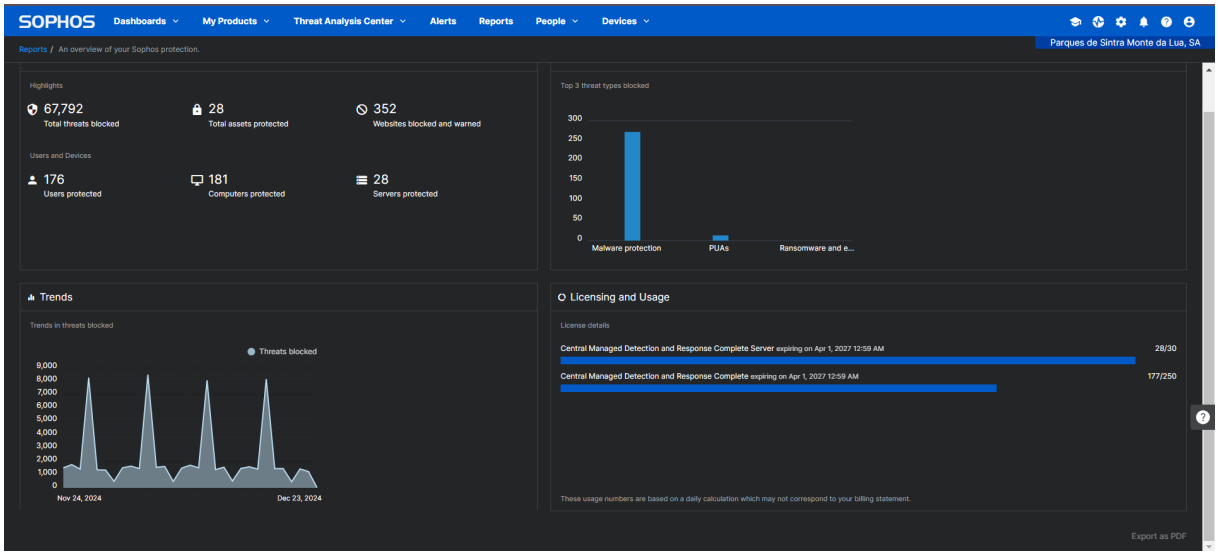

Figura 40 - Registo da Proteção dos Endpoints Sophos Fonte: Autor

d) *Malware* ou Aplicação Potencialmente Indesejada (PUA) bloqueado

Durante um período de 30 dias, é possível observar a quantidade de *Malware* e PUAs bloqueados nos *endpoints*.

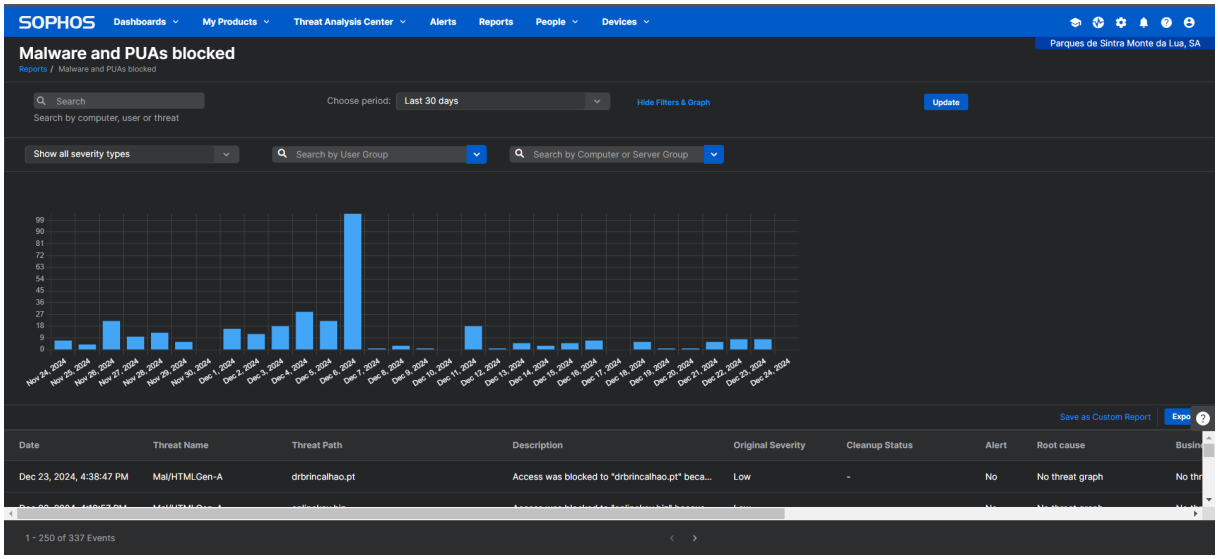

Figura 41 - Malware e PUAs bloqueados Fonte: Autor

e) *Windows Firewalls Report*

Número de dispositivos com a *Firewall do Windows Habilitada e Desabilitada.*

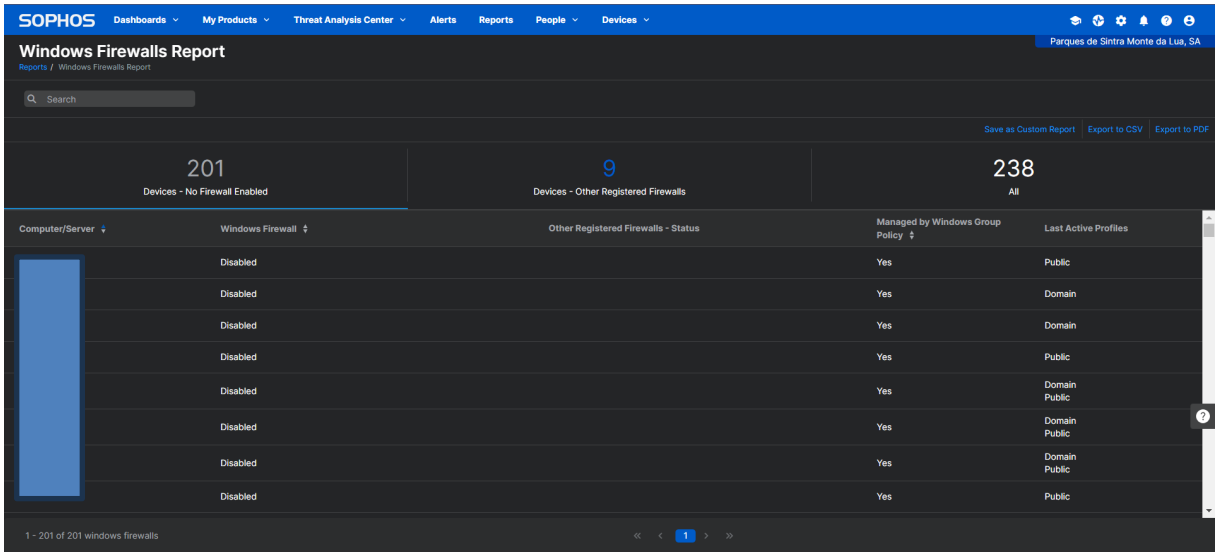

Figura 42 - Número de Dispositivos com Firewall Windows Fonte: Autor

f) *Dashboard* de Eventos no *Wazuh*

Dashboard dos eventos registados pelo Wazuh.

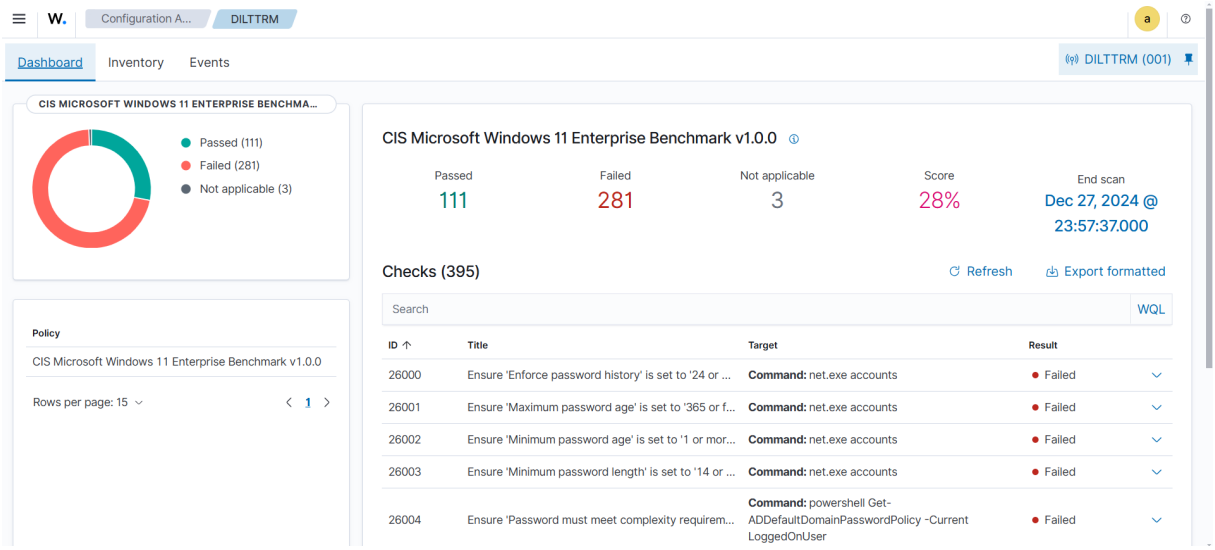

Figura 43 - Dashboard de eventos registados em Wazuh Fonte: Autor

6. Discussão

A implementação da plataforma SIEM em conjunto com uma *Firewall* na organização que serviu para este estudo de caso, ofereceu informações importantes sobre a eficácia destas tecnologias na Cibersegurança e qual a postura geral que as empresas enfrentam a nível de segurança. Neste capítulo, analisa-se as principais conclusões de eficiência, e limitações com base na análise deste caso de estudo.

6.1. Eficácia da Implementação da Plataforma e *Firewall*

A análise do presente estudo revela que a implementação do SIEM e da *Firewall* abordou de forma abrangente diversos aspetos críticos relacionados com a postura de Cibersegurança da organização em questão. Os principais objetivos deste projeto, nomeadamente a deteção e resposta a ameaças, introdução das políticas de segurança e melhoria na gestão de risco de incidentes, no qual foi alcançado com sucesso. A plataforma SIEM em conjunto com a *Firewall*, analisou eficientemente os dados de eventos de segurança de diversas fontes, proporcionando à organização uma visão abrangente e consolidada do seu panorama de segurança. Este avanço contribuiu para uma deteção e mitigação mais ágil e eficaz de ciberataques.

6.2. Limitações

Reconhecendo os desafios enfrentados pela organização, o processo de implementação do SIEM e da *Firewall* revelou-se moroso, primeiramente devido à natureza da entidade, que, apesar de ser uma sociedade anónima, rege-se pela contratação pública, o que acabou por prolongar significativamente o processo de aquisição da *Firewall*. Além disso, a implementação da *Firewall* em si, é algo com uma complexidade técnica elevada, relacionado com a integração de dados e normalização dos mesmos. Adicionalmente, registou-se alguma resistência com a implementação dos alertas lançados pelo SIEM e *Firewall.* Estes desafios evidenciam a importância de um planeamento bem elaborado, devidamente comunicado a todas as partes interessadas, bem como da alocação de recursos adequados para assegurar o sucesso deste tipo de projetos.

7. Conclusão

Ao longo desta dissertação procurei analisar, de forma estruturada e sustentada, o papel que as soluções de segurança e de monitorização centralizada desempenham no contexto atual da cibersegurança organizacional, com particular enfoque nas PMEs. Partindo da questão de investigação definida, tornou-se evidente que a utilização conjunta de uma firewall e de uma plataforma SIEM não só responde aos desafios atuais, como representa uma mudança necessária do paradigma e na forma como as organizações encaram a sua postura de segurança.

Com base no enquadramento teórico desenvolvido, foi possível compreender que o aumento exponencial da complexidade das infraestruturas tecnológicas e a evolução constante das ciberameaças exigem uma abordagem integrada, proativa e orientada à antecipação. Neste contexto, a articulação entre mecanismos tradicionais de defesa, como as firewalls, e soluções mais avançadas de análise e correlação de eventos, como as plataformas SIEM, assume um papel central na capacidade de as organizações detetarem, analisarem e responderem a incidentes de forma eficaz.

A componente prática deste trabalho, baseada na implementação de uma solução real, permitiu validar empiricamente os conceitos abordados. As integrações da plataforma SIEM Wazuh com a Firewall Sophos XGS 4300 demonstrou que é possível obter uma visão consolidada e centralizada sobre os eventos de segurança da organização, permitindo não apenas a deteção de ameaças, mas também a correlação de comportamentos anómalos e a resposta em tempo útil. Esta capacidade revelou-se essencial para transformar dados dispersos em informação acionável, contribuindo para uma gestão mais eficiente dos riscos e de forma centralizada.

Os resultados obtidos evidenciam que a monitorização contínua, aliada à análise de *logs* e à definição de regras de deteção, potencia significativamente a capacidade de identificação de padrões suspeitos e incidentes de segurança. A existência de alertas em tempo real e a possibilidade de intervenção imediata reforçam uma abordagem de defesa ativa, alinhada com os princípios de *Threat Hunting* explorados ao longo do estudo.

Contudo, importa reconhecer que a adoção destas soluções não está isenta de desafios. Tal como evidenciado no caso de estudo, fatores como a complexidade técnica da implementação, a necessidade de integração entre diferentes sistemas, e as condicionantes associadas a processos de aquisição, especialmente em contextos públicos, podem atrasar ou dificultar a concretização dos projetos. Para além disso, a resistência organizacional à mudança

e a necessidade de capacitação dos recursos humanos continuam a ser fatores críticos que influenciam diretamente o sucesso destas iniciativas.

Não obstante estas limitações, considero que o contributo desta dissertação é relevante ao demonstrar que a adoção de soluções integradas de segurança, independentemente do fabricante ou do modelo implementado, constitui um fator diferenciador na proteção das organizações. A capacidade de centralizar informação, correlacionar eventos e atuar de forma preventiva traduz-se numa melhoria efetiva da postura de segurança e numa maior resiliência face a incidentes cibernéticos.

Em termos futuros, torna-se pertinente aprofundar a automatização dos processos de deteção e resposta, através da integração com tecnologias emergentes como a inteligência artificial, bem como explorar modelos de segurança adaptativos capazes de responder dinamicamente às ameaças. Adicionalmente, considero fundamental reforçar a componente organizacional da cibersegurança, promovendo não apenas a adoção de tecnologia, mas também a criação de uma cultura de segurança transversal a toda a organização.

Em suma, concluo que a implementação conjunta de uma firewall e de uma plataforma SIEM não deve ser encarada apenas como uma opção tecnológica, mas como um requisito estratégico para qualquer organização, em especial para as PME, que pretenda proteger os seus ativos de informação num cenário digital cada vez mais exigente. Este trabalho permitiu-me não só consolidar conhecimentos teóricos, mas também validar, em contexto real, a importância crítica destas soluções na construção de um modelo de cibersegurança sólido, proativo e orientado à mitigação contínua do risco.

8. Referências Bibliográficas

Amoroso, E. (2006). Cyber Security. *New Jersey: Silicon Press*.

Andrew. (20 de Outubro de 2023). *What Is Cyberthreat Intelligence, and Why Do You Need It?* Obtido de https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html

Antunes, M., & R., B. (2022). *Introdução à Cibersegurança.* FCA.

Avanet. (2021). Obtido de https://www.avanet.com/en/shop/sophos-xgs-4300-security-appliance/

Bay, P. (2020). *Crispus.* Obtido de https://cyber-security.pt/blog/o-que-e-a-ciberseguranca/

Bergmans, B. L. (27 de Março de 2024). Obtido de https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-attack-ioa/

Bilhim, J. (2007). Gestão Estratégica de Recursos Humanos. Lisboa: Instituto Superior de Ciências Sociais e Políticas.

Caetano, A., & Vala, J. (2007). Gestão de recursos humanos. Contextos, processos e técnicas. Lisboa: Editora RH.

CheckPoint. (21 de Fevereiro de 2024). Obtido de https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/how-to-develop-a-cyber-security-strategy/

Chohan, S. (30 de 10 de 2024). *lemonlearning.com.* Obtido de https://lemonlearning.com/pt/blog/7-melhores-modelos-de-gestao-da-mudanca-para-2024

Cichonski, P. (2022). Obtido de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Cloudflare. (21 de Agosto de 2024). Obtido de https://www.cloudflare.com/learning/security/threats/owasp-top-10/

CNCS. (08 de Março de 2023). Obtido de https://www.cncs.gov.pt/pt/sobre-nos/

CNPD. (22 de Março de 2023). Obtido de https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

Craigen, D. (2014). *Defining Cybersecurity*. Obtido de https://www.researchgate.net/publication/267631801_Defining_Cybersecurity

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining Cybersecurity*. Obtido de vol 4, no. 10, pp.13-21: https://bit.ly/3yNI6XA

Cuofano, G. (21 de 03 de 2024). *https://fourweekmba.com/pt/modelo-de-gerenciamento-de-mudan%C3%A7as-lewins/.*

Debbie. (10 de Junho de 2021). Obtido de https://www.f5.com/labs/learning-center/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why

Deshetty, A. (2022). *Integrating SIEM with Other Security Tools.*

Eccouncil. (30 de Março de 2022). Obtido de https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

Edward, K. (16 de Setembro de 2024). Obtido de https://www.upguard.com/blog/what-are-indicators-of-attack

ENISA. (7 de Janeiro de 2021). Obtido de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pt

exabeam. (12 de Dezembro de 2023). Obtido de https://www.exabeam.com/explainers/information-security/threat-hunting-tips-and-tools/

Ferrill, T. (13 de Março de 2024). Obtido de https://www.csoonline.com/article/524286/what-is-siem-security-information-and-event-management-explained.html

Francisca Andrade. (02 de Julho de 2021). Obtido de https://tek.sapo.pt/noticias/internet/artigos/ciberseguranca-portugal-regista-melhorias-no-desempenho-e-sobe-para-o-14o-lugar-do-ranking-global

Gaivéo, J. (2008). *As pessoas nos Sistemas de Gestão da Segurança da Informação.* Obtido de Ph.D. Dissertation: https://bit.ly/3AVrpfK

Gcaza, N., Von Solms, R., & Van Vuuren, J. (2015). *An Ontology for a National Cyber-Security Culture Environment*. Obtido de Ninth International Symposium on Human Aspects of Information Security & Assurance: https://bit.ly/3uPJjfN

Gibson, J., Ivancevich, J., Donnelly, J., & Konopaske, R. (2006). Organizações: comportamento, estrutura e processos. São Paulo, Brasil: Mc Graw Hill.

Gillis, A. (2021). Obtido de https://www.techtarget.com/whatis/definition/attack-surface

Gladden, M. (2017). *An Introduction to Information Security in the Context of Advanced Neurprosthetics.* Obtido de The Handbook of Information Security for Advanced Neuroprosthetics: https://bit.ly/3IG2QFr

Gomes, R. (2010). *Uma abordagem relacional e planeada para a aplicação de modelos de gestão da segurança na saúde.* Obtido de https://bit.ly/3oarPqM

Gonçalves, R. (Outubro de 2019). O Fator Humano da Cibersegurança nas Organizações.

IBM. (2023). *IBM.* Obtido de https://www.ibm.com/topics/threat-actor

Joe, A. (20 de Outubro de 2022). Obtido de https://www.anomali.com/blog/threat-hunting-eight-tactics-to-a-better-cybersecurity-strategy

Katie. (11 de Novembro de 2023). Obtido de https://armorpoint.com/2019/04/04/the-it-leaders-guide-to-choosing-the-right-siem-deployment-method/

Kemmerer, A. R. (pp. 705-715 de 2003). *Cybersecurity.* Obtido de 25th International Conference on Software Engineering.

Kidd, C. (26 de Agosto de 2024). Obtido de https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Lopes, A., & Reto, L. (1990). Identidade da empresa e gestão pela cultura. Lisboa: Sílabo.

Maile, M. (5 de Maio de 2023). Obtido de https://www.strongdm.com/what-is/threat-actor

Mohit. (11 de Junho de 2018). Obtido de https://thehackernews.com/2018/06/cyber-threat-hunting.html

Morgan, G. (2007). Images of organizations. London: Sage.

Portugal2020. (2 de Novembro de 2021). Obtido de https://portugal2020.pt/glossario/pme-pequenas-e-medias-empresas/

Pranav. (19 de Julho de 2022). Obtido de https://www.tutorialspoint.com/what-is-open-web-application-security-project-owasp

Roy, R. (23 de 08 de 2021). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples.

Scarfone, K. (28 de Setembro de 2023). Obtido de https://www.techtarget.com/searchsecurity/tip/How-to-develop-a-cybersecurity-strategy-Step-by-step-guide

Schein, E. (1992). Organizational Culture and Leadership. San Francisco: Jossey-Bass Publisher.

SECURITY, I. (07 de Agosto de 2023). Obtido de https://www.itsecurity.pt/news/analysis/maioria-dos-ciberataques-visam-pme

SentinelOne. (04 de Setembro de 2024). Obtido de https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/

Sharma, V. (17 de Janeiro de 2024). Obtido de https://www.knowledgehut.com/blog/security/cyber-threat-hunting

SQRRL. (21 de Outubro de 2015). Obtido de https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5

Tyas, A. (16 de Setembro de 2024). *UpGuard.* Obtido de UpGuard: https://www.upguard.com/blog/attack-vector

Unni, A. (28 de Março de 2022). Obtido de https://www.stickmancyber.com/cybersecurity-blog/how-to-develop-a-strong-cybersecurity-strategy

Von Solms, R., & Van Niekerk, J. (2013). *From information security to cyber security*. Obtido de Computers and Security, no. 38, pp. 97-102: https://bit.ly/3c823AL

Wang, J. (28 de Agosto de 2023). Obtido de https://www.ibm.com/think/insights/siem-and-threat-intelligence-stay-current-on-trending-threats

Wazuh. (08 de 2025). Obtido de https://wazuh.com/

9. Apêndices

9.1. APÊNDICE I - Configuração Pormenorizada das Políticas *Endpoints*.

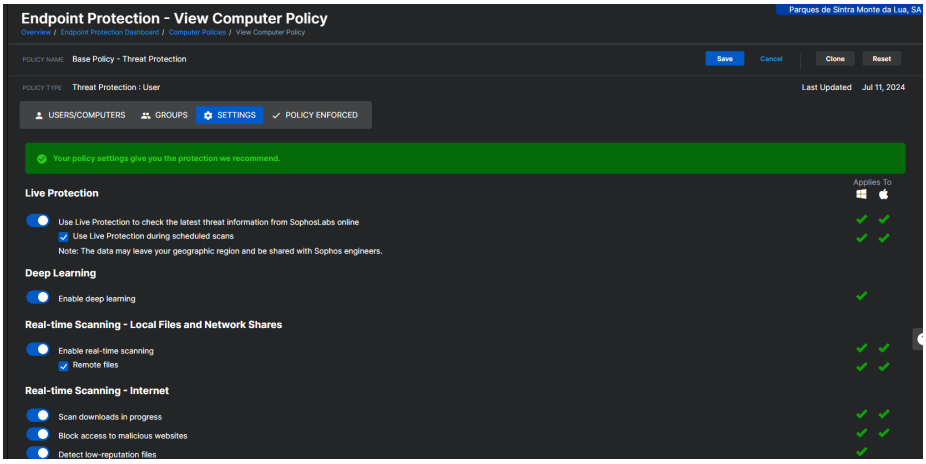

Figura 44 - Configuração Threat Protection Fonte: Autor

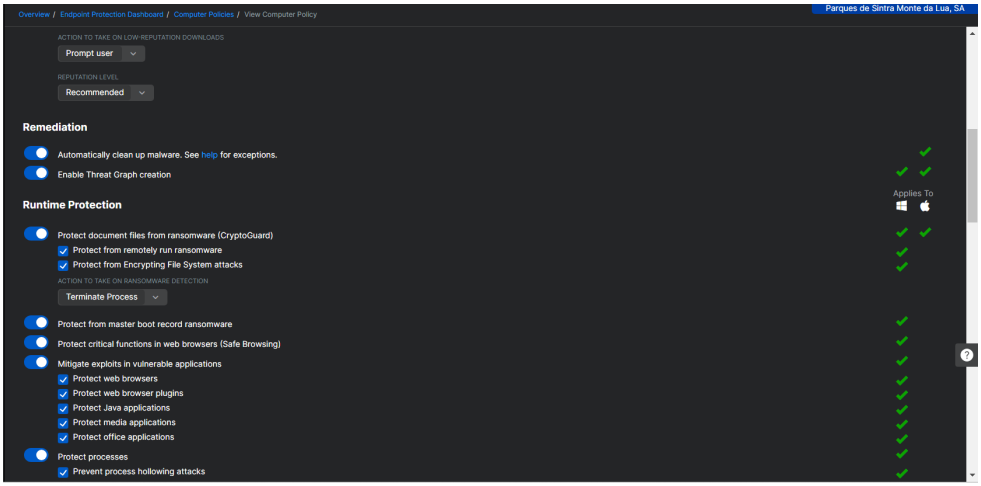

Figura 45 - Continuação Configuração Threat Protection Fonte: Autor

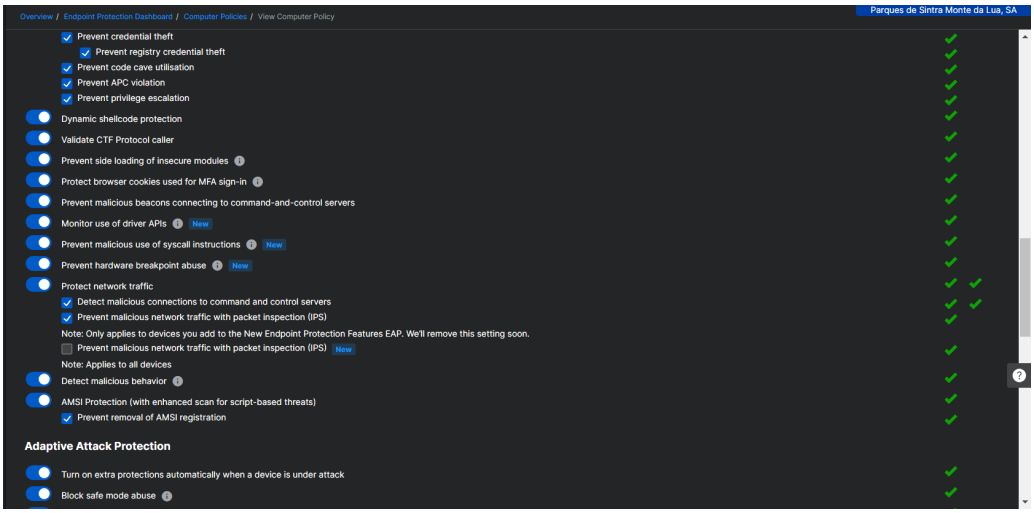

Figura 46 - Continuação Configuração Threat Protection Fonte: Autor

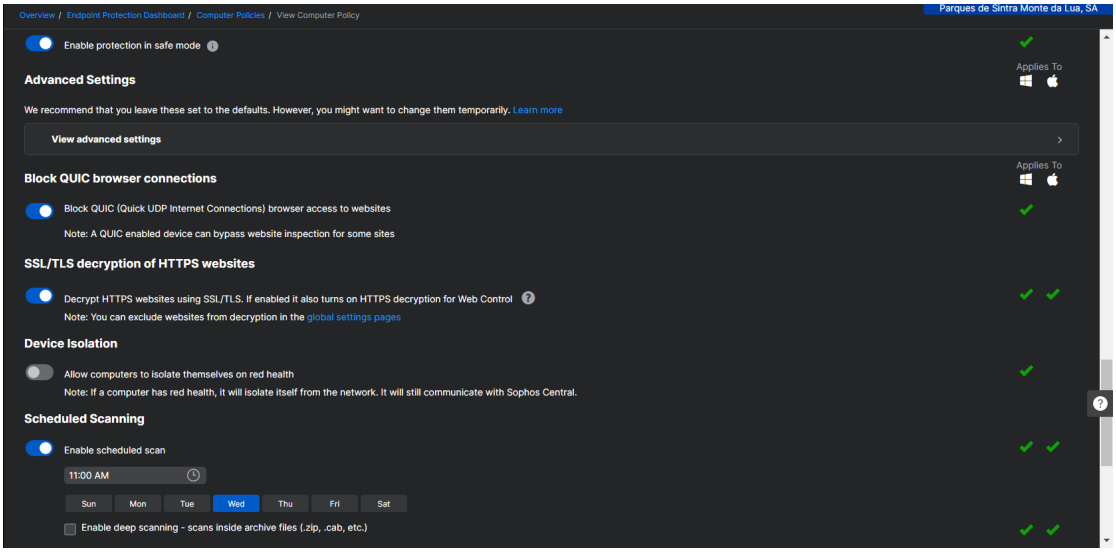

Figura 47 - Continuação Configuração Threat Protection Fonte: Autor

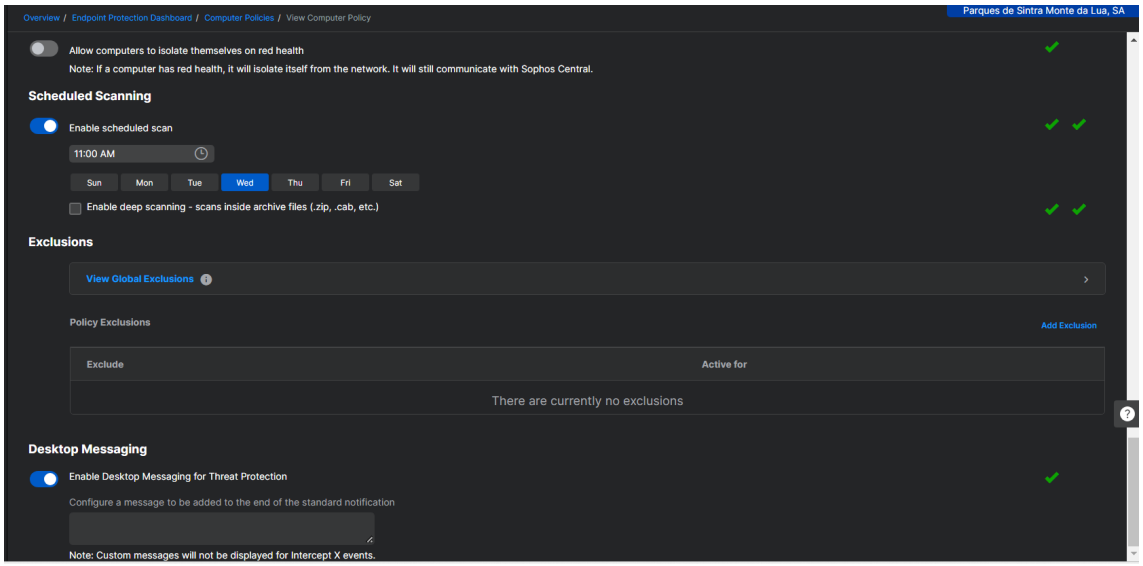

Figura 48 - Continuação Configuração Threat Protection Fonte: Autor

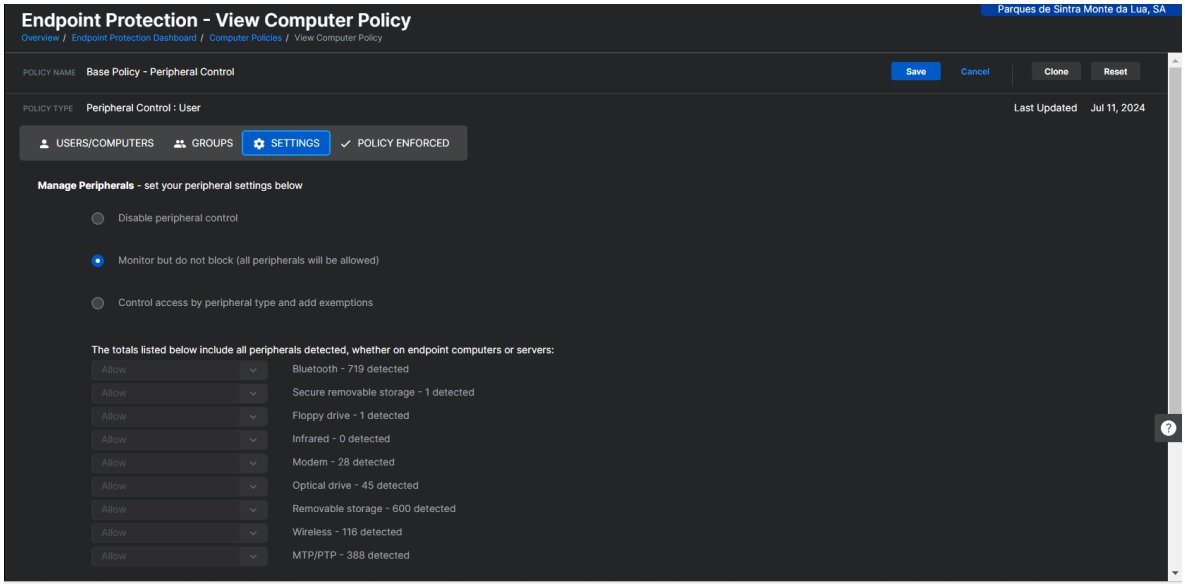

Figura 49 - Configuração Peripheral Control Fonte: Autor

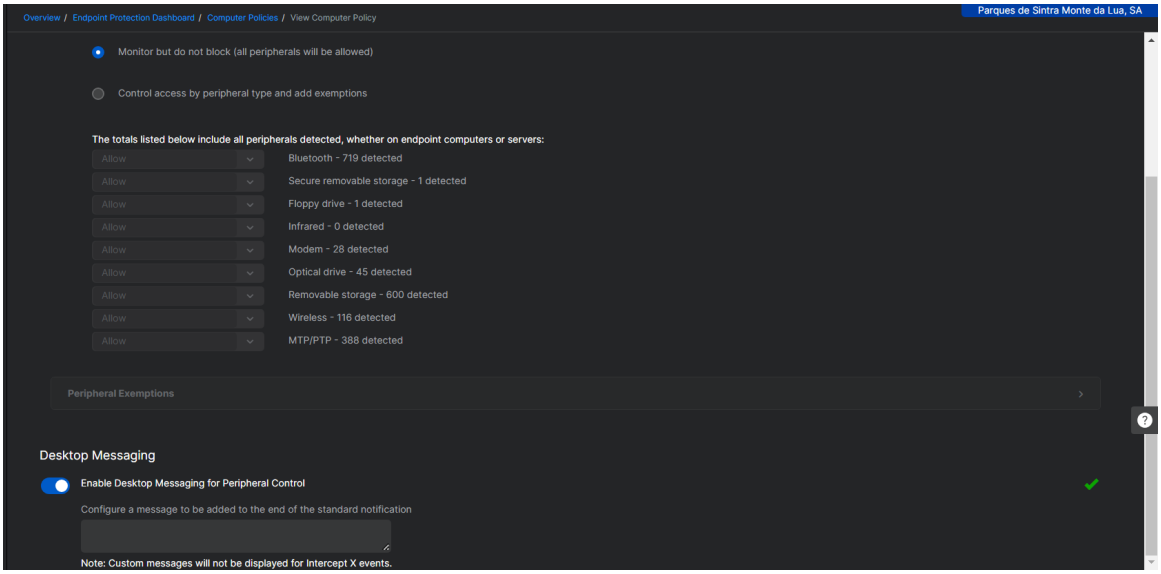

Figura 50 - Continuação Configuração Peripheral Control Fonte: Autor

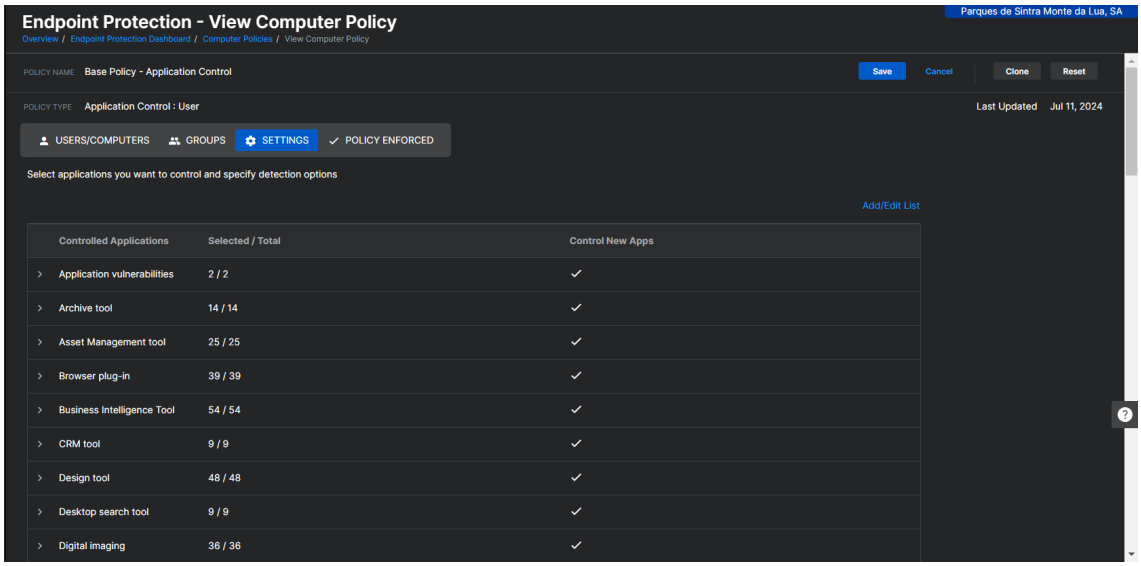

Figura 51 - Configuração Application Control Fonte: Autor

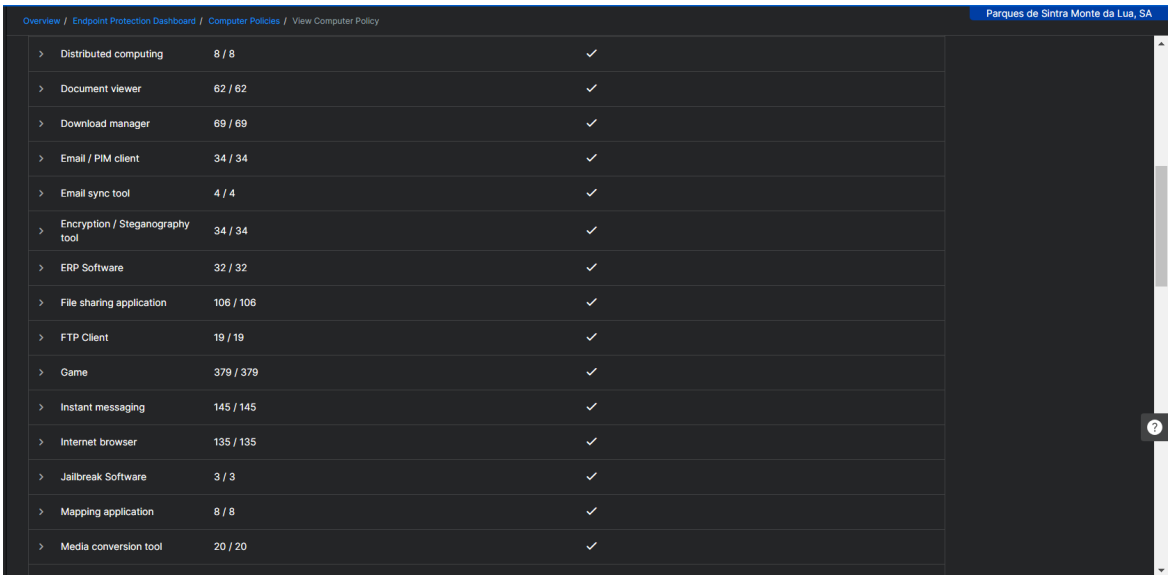

Figura 52 - Continuação Configuração Application Control Fonte: Autor

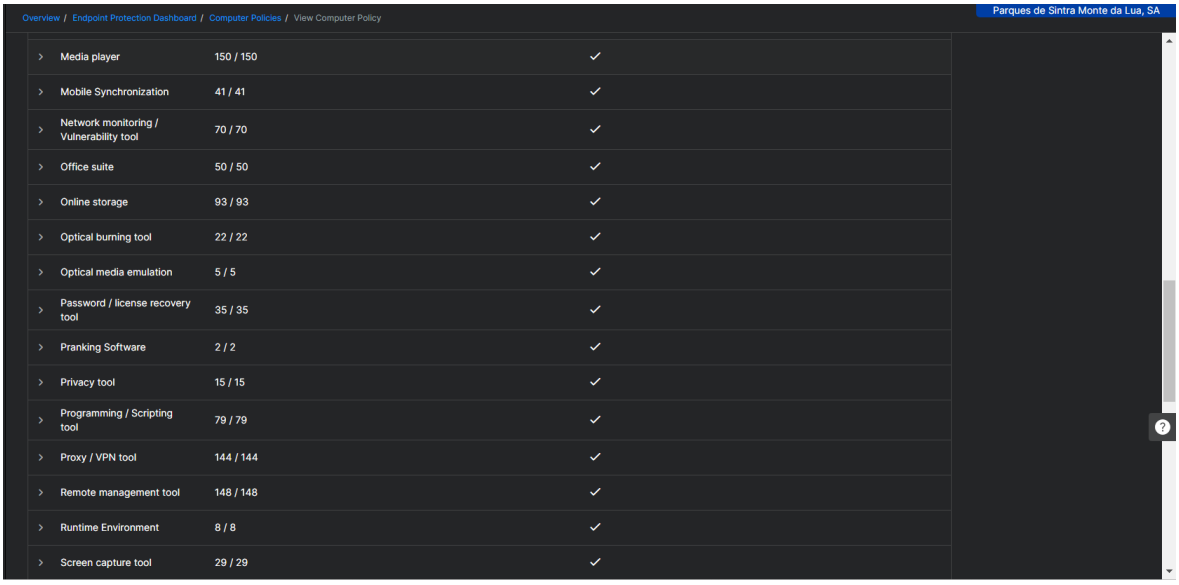

Figura 53 - Continuação Configuração Application Control Fonte: Autor

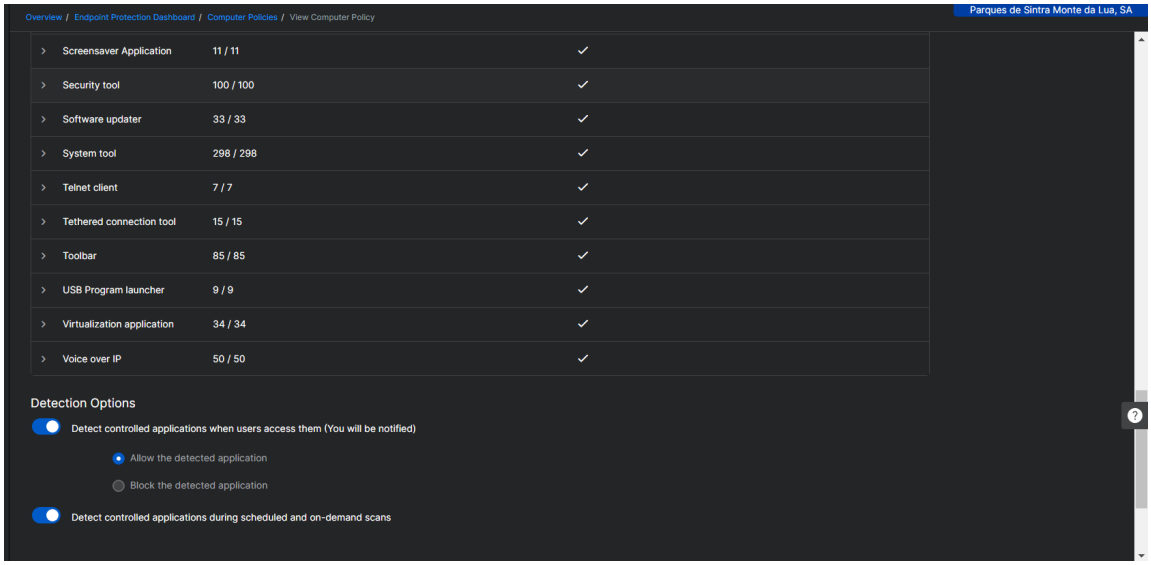

Figura 54 - Continuação Configuração Application Control Fonte: Autor

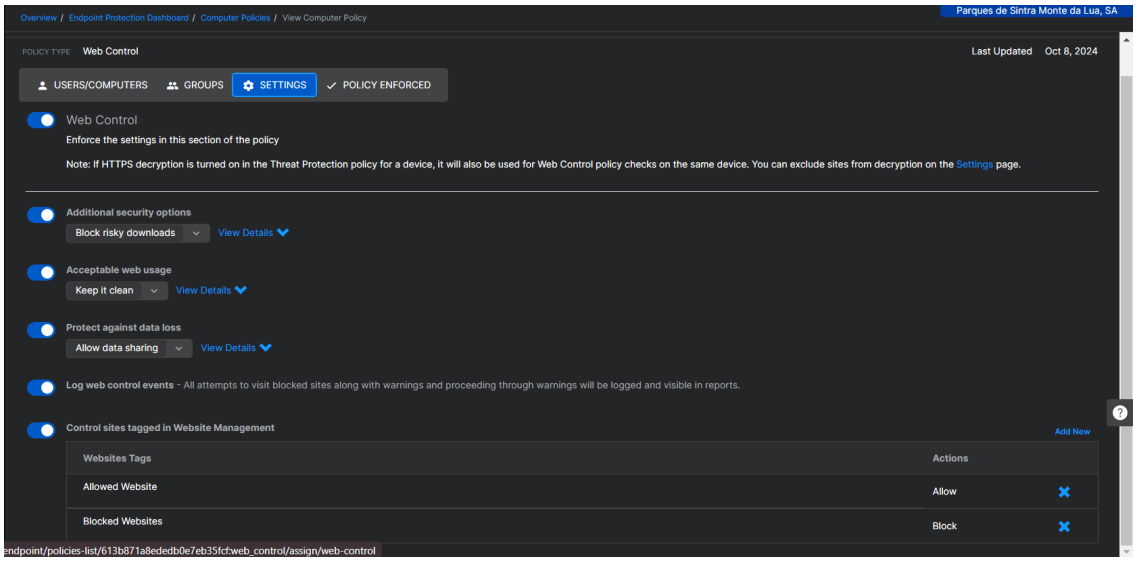

Figura 55 - Configuração Web Control Fonte: Autor

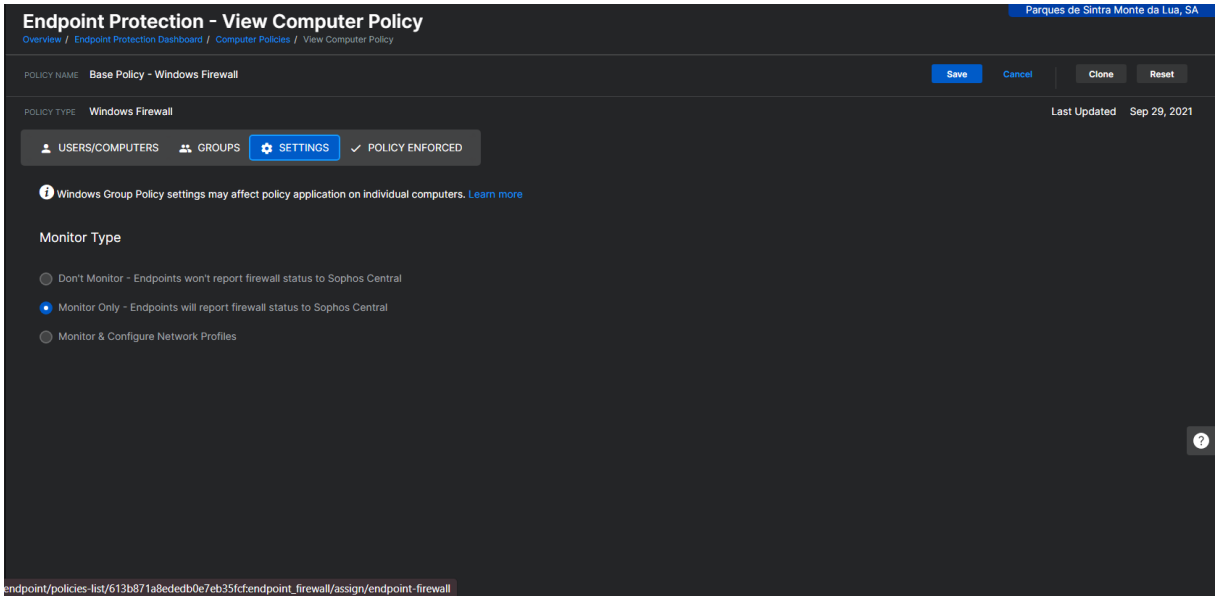

Figura 56 - Configuração Windows Firewall Fonte: Autor