INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS DE LISBOA

A importância das plataformas SIEM, na deteção e mitigação de ciberameaças, em contexto *threat hunting* nas PME.

João Carlos Rito de Matos

Dissertação para obtenção do Grau de Mestre em

Informática

Orientador: Professora Doutora Isabel Surdinho Alvarez

Júri

Presidente: Professor Doutor Paulo André Reis Duarte Branco

Arguente: Professor Doutor Paulo Gonçalves Pinto

Orientador: Professora Doutora Isabel Surdinho Alvarez

Janeiro de 2024

Dissertação de Mestrado realizada sob a orientação de Professora Doutora Isabel Surdinho Alvarez, apresentada no ISTEC – Instituto Superior de Tecnologias Avançadas de Lisboa para obtenção de grau de Mestre em Informática.

Agradecimentos

Este trabalho não teria sido possível sem o apoio e a colaboração de várias pessoas que desempenharam papéis essenciais que culminam agora neste projeto. Em primeiro lugar, gostaria de agradecer à professora Isabel Alvarez, pela sua incansável e incondicional orientação. Ao professor Paulo Duarte e professora Andreia Vieira, pela boa disposição e valiosos conselhos ao longo deste meu percurso no ISTEC. À minha companheira, Patrícia Martins, um reconhecimento especial, em que nos momentos mais difíceis, esteve sempre ao meu lado, com um incentivo e apoio inabalável.

Um profundo agradecimento à minha mãe, Fátima Matos, cujo amor e educação moldaram a pessoa que sou hoje. Ao meu irmão, Pedro Matos, e ao meu tio, Adalberto Matos, grato pelo conhecimento e pelos valores que me transmitiram desde que me recordo.

Aos meus amigos José Pedro Aleixo e João Sacadura cuja amizade de décadas nos tornou família.

Ao Eng. João Reis Barata e ao Eng. Fernando Moreira, pela oportunidade, autonomia e confiança conferidas ao longo destes 19 anos na TECMIC, que formaram a pessoa que sou hoje. À minha equipa: João Sacadura, André Chumela, José Alves, Matheus Nunes e Leandro Dantas, pelo profissionalismo, compromisso e dedicação demonstrados diariamente, cujos resultados partilhamos.

Finalmente, um agradecimento muito especial à minha filha Aurora, nascida a meio deste projeto, cuja chegada trouxe uma nova dimensão à minha vida.

A todos vós, deixo o meu sincero obrigado.

Índice

Índice de Figuras

Índice de Tabelas

Abreviaturas e siglas

IOT - *Internet of Things*

PME – Pequenas e médias empresas

SIEM - *Security information and event management*

APT - *Advanced Persistent Threats*

WAF - *Web Applications Filters*

DoS – *Denial of Service*

DDoS - *Distributed Denial of Service*

CNCS – Centro Nacional de Cibersegurança

EDR - *Endpoint Detection and Response*

OSINT – Open Source Intelligence

IOC – *Indicators of compromise*

IOAs - *Indicators of attack*

VPN – *Virtual Private Network*

UEBA - *User and Entity Behavior Analytics*

TI – Tecnologias da Informação

SI – Segurança da Informação.

IP – *Internet Protocol*

DNS – *Domain Name System*

SOC – *Security Operation Center*

Resumo

Nos últimos anos, o número e complexidade das ameaças cibernéticas dirigidas às pequenas e médias empresas (PME) aumentaram de forma sistemática, tornando essencial uma abordagem e resposta cada vez mais proativas. Uma abordagem que tem sido cada vez mais evidenciada é a caça às ameaças (*Threat Hunting*), tendo como característica intrínseca a procura ativa e a identificação de potenciais perigos antes que possam causar danos aos sistemas ou dados de uma organização. A caça às ameaças exige que as organizações tenham acesso a ferramentas de segurança sofisticadas, como por exemplo plataformas de Gestão de Informação e Eventos de Segurança (SIEM), ajudando na identificação e investigação de potenciais ameaças, recolhendo e analisando dados de várias fontes, incluindo tráfego de rede, registos de sistema e dados de dispositivos, para identificar potenciais incidentes de segurança e fornecer alertas em tempo real. Nesta dissertação, iremos explorar a importância das plataformas SIEM na deteção e atenuação de ameaças cibernéticas, no contexto da caça às ameaças, abordando os conceitos-chave da caça à ameaça, incluindo indicadores de ataque e os tipos de perigos que as PME enfrentam, face ao panorama atual das ciberameaças, discutindo também a importância da inteligência da ameaça e o papel que desempenha na procura eficaz por este tipo de problema. Para realçar a importância das plataformas SIEM, será desenvolvido um protótipo, baseado no *Graylog*, uma plataforma SIEM de código aberto, que irá demonstrar se este tipo de tecnologia pode ser eficaz na identificação e investigação de potenciais ameaças, fornecendo alertas em tempo real, permitindo a tomada de medidas proactivas para mitigar os riscos cibernéticos. Esta dissertação tem como objetivo fornecer uma visão global da função que as plataformas SIEM desempenham na procura por ameaças, destacando a sua importância em ajudar as PME a protegerem-se contra as ameaças cibernéticas, num contexto prático real, recolhendo e correlacionando informação em tempo real relativamente às suas redes e sistemas informáticos, que servirão de base para sustentar e desencadear ações de mitigação, baseados em evidencias do seu contexto real.

Palavras-chave: *Threat Hunting, Cibersegurança, System Information and Event Management, PME, Correlação de Eventos, Ciberataques*

Abstract

In recent years, the number and complexity of cyber threats targeting small and medium-sized enterprises (SMEs) has increased systematically, making an increasingly proactive approach and response essential. One approach that is increasingly in evidence is Threat Hunting, an intrinsic characteristic of which is to actively seek out and identify potential threats before they can cause damage to an organization's systems or data. Threat Hunting requires organizations to have access to sophisticated security tools, such as Security Information and Event Management (SIEM) platforms, assisting in the identification and investigation of potential threats by collecting and analyzing data from various sources, including network traffic, system logs, and device data, to identify potential security incidents and provide real-time alerts. In this dissertation, we will explore the importance of SIEM platforms in detecting and mitigating cyber threats in the context of threat hunting, addressing the key concepts of threat hunting, including attack indicators and the types of threats that SMEs face, against the current cyber threat landscape, also discussing the importance of threat intelligence and the role it plays in effectively searching for threats. To highlight the importance of SIEM platforms in threat searching, a prototype will be developed, based on Graylog, an open source SIEM platform, which will demonstrate whether this type of technology can be effective in identifying and investigating potential threats, providing real-time alerts, enabling proactive measures to be taken to mitigate cyber risks. This dissertation aims to provide an overview of the role SIEM platforms play in threat search, highlighting their importance in helping SMEs protect themselves against cyber threats in a real-world practical context, seeking to collect and correlate information in real time about their networks and IT systems, which will serve as a basis for sustaining and triggering mitigation actions, based on evidence from their real context.

Keywords: *Threat Hunting, Cybersecurity, System Information and Event Management, Threat intelligence, Cyber threat, PME, Event Correlation, Cyberattacks*

1. Introdução

Numa altura em que qualquer organização ou empresa depende fortemente das tecnologias de informação para o desempenho da sua atividade, certamente terão necessidade de vários equipamentos interligados em rede, desde impressoras, computadores, servidores, sistemas de videovigilância, equipamentos *Internet of things* (IOT), que estando permanentemente ligados à Internet, podem rapidamente tornar-se numa ameaça do ponto de vista da segurança informática, principalmente quando mal parametrizados. Segundo um estudo realizado pela SAGE (Sousa, 2022), 59% das PME consideram-se mais dependentes da tecnologia, sobretudo após a pandemia, em que praticamente metade, 49%, espera aumentar o seu investimento em tecnologia nos próximos 12 meses. Para além deste fator, existe outro, de não menos importância, que reflete os potenciais perigos na utilização da Internet de forma negligente, com displicência ou por falta de consciencialização dos seus possíveis danos advindos, quando não usada de forma consciente e com uma mentalidade de segurança digital, sendo por isso necessário apostar numa cultura de segurança nas PME (Medeiros, 2023), considerando assim o fator humano como o vetor mais importante nesta temática, desde o colaborador comum, os especialistas em cibersegurança e os seus respetivos executivos. Esta dissertação pretende descrever a forma como as organizações podem endereçar a temática da cibersegurança, adaptando-se e mudando a sua abordagem de atuação, começando com a própria consciencialização das ameaças, que frequentemente passa apenas pela comunicação, adoção de procedimentos e implementação de ferramentas para a deteção e mitigação das ciberameaças, desenvolvendo uma estratégia em cibersegurança, baseada numa análise de risco (Pires, 2023). Pese embora este projeto possa ser usado pelo público em geral, visa sobretudo dotar os departamentos das tecnologias da informação das PME, de métodos e ferramentas para a deteção e mitigação de ataques informáticos, onde os orçamentos são tipicamente limitados.

Com base nesta introdução, a dissertação pretende endereçar e dar resposta à seguinte questão:

- Em que medidas poderão ser as plataformas SIEM eficazes na deteção e mitigação de ciberameaças para as PME?

1.1 Motivação

Durante o ano de 2022, o termo cibersegurança tem sido amplamente difundido pelos inúmeros ataques que têm vindo a público, nomeadamente a empresas com alguma relevância no nosso quotidiano, desde órgãos de comunicação social a operadoras de comunicações, com impactos e repercussões significativos nos serviços que prestam, que colocaram não só os gestores de empresas, mas como a sociedade em geral mais atentos a esta realidade. Analisando alguns dados e estudos, como por exemplo a elevada percentagem de PME´s que compõem o nosso tecido empresarial, 99,9% em 2021, onde 48% afirmam já ter sofrido algum tipo de cibercrime ou até mesmo que tenham encerrado os seus serviços devido a ataques informáticos (Pontual, 2023), tornando-se assim interessante e relevante perceber como poderão estas desenvolver mecanismos para detetar e mitigar estes incidentes, sobretudo quando os orçamentos atribuídos a esta área são tipicamente reduzidos ou inexistentes.

1.2 Objetivos

O objetivo principal é disseminar a consciencialização generalizada para as ciberameaças e possíveis danos advindos, dotando principalmente as PME de metodologias e ferramentas de deteção e mitigação de ciberataques, com uma postura pró-ativa, alertando para a importância da existência de um sistema de agregação de ficheiros de *log*, que permita correlacionar eventos em tempo real e sobretudo com o passado, tipicamente após um ciberataque, imprescindível para o uso de diversas técnicas, como por exemplo, a "caça de ameaças" (doravante mencionado por *threat hunting*), para a análise forense e essencial para a obtenção de meio de prova criminal, caso se dê lugar. Este projeto visa analisar e discutir a eficácia das ferramentas SIEM na mitigação de ataques cibernéticos, com especial detalhe na componente de *threat hunting*, visando a deteção de ameaças numa fase ainda inicial, através de uma procura e análise pró-ativa de toda a informação recolhida dos equipamentos ativos que compõem tipicamente uma infraestrutura informática, comumente presente na maioria das organizações. Este projeto tem também como o objetivo intrínseco, a consciencialização dos departamentos de TI/SI para o panorama atual das ciberameaças, promovendo uma mudança de paradigma na área da segurança informática, tornando-a mais proativa e menos reativa, dando um exemplo de projeto em contexto real para a concretização deste objetivo, com casos práticos com elevada aplicabilidade real, com custos relativamente reduzidos e baseado em tecnologias *open source*. Este estudo investiga um modelo prático de implementação de um sistema SIEM, no contexto de *threat hunting*.

1.3 Organização do documento

Esta dissertação encontra-se organizada por capítulos, promovendo uma estrutura completa para melhor compreensão da dissertação, com a seguinte estrutura:

Capítulo 1 (Introdução): Integrado no presente capítulo, é composto pela introdução, motivação e objetivos, que caracterizam o alcance e contribuições do projeto.

Capítulo 2 (Revisão da Literatura): Descreve o processo de procura, análise e descrição da informação e conhecimento relevante para a matéria discutida, composto por cinco subcapítulos, Cibersegurança, *Threat Hunting*, Cibersegurança nas PME, *System Information and Event Management*, O papel da tecnologia SIEM no contexto *Threat Hunting,* onde é exposto o que os vários autores abordaram sobre as respetivas temáticas.

Capítulo 3 (Metodologia): Descreve a metodologia seguida para o referido projeto, baseada na metodologia da gestão da mudança, de *Kurt Lewin* e a sua aplicabilidade do contexto da empresa escolhida para a execução do projeto.

Capítulo 4 (Protótipo): Descreve todas as fases de desenvolvimento do protótipo, desde a especificação e planeamento, instalação, configuração, normalização da informação e teste, suportado pelas evidências nos respetivos apêndices.

Capítulo 5 (Resultados): Explica todo o projeto de investigação, a análise e os respetivos resultados.

Termina com os capítulos **Discussão, Conclusões e trabalho futuro**.

2. Revisão da literatura

Neste capítulo, pretende-se apresentar o contexto, abordando as terminologias mais usadas nesta temática, de modo a se poder compreender, nos capítulos seguintes, o funcionamento das plataformas SIEM e a sua possível mais valia no contexto das ciberameaças, onde atualmente, também devido à recente volatilidade internacional, nomeadamente da guerra entre a Rússia e a Ucrânia, se crê ser expectável a observação de cada vez mais operações cibernéticas no futuro próximo e a médio prazo, sob forma de ataques híbridos. A título de exemplo, em 2022, a Rússia aumentou em 300% os ataques aos utilizadores pertencentes a países da NATO, quando comparado com 2020 (Huntley, 2023). Neste capítulo, dissecaremos as terminologias tipicamente associadas à temática da cibersegurança e respetivos modelos de compreensão, que servirão de base para a construção de alertas e *dashboards* personalizados a cada realidade, em maior detalhe no capítulo 5, na apresentação do estudo de projeto.

2.1 Cibersegurança

No sentido lato, Cibersegurança é a prática de proteger sistemas informáticos, redes de comunicação e software de ataques digitais, com o objetivo de aceder, alterar ou destruir informações, sob forma de ameaça com o objetivo de extorquir financeiramente ou apenas de interromper os processos normais de negócio (Kovacs, 2021).

2.1.1 Ciberameaça

Cyber threat ou ciberameaça, é definido como algo com o potencial de causar consideráveis danos a um sistema informático ou outros ativos digitais de uma organização ou indivíduo (Roy, 2021). As ameaças cibernéticas procuram transformar potenciais vulnerabilidades em ataques a sistemas e redes, onde se incluem normalmente *trojans*, vírus e *backdoors*, sendo que na sua grande maioria perpetrados através do uso de várias técnicas de exploração, como por exemplo, um ataque de *phishing* para obter informações e simultaneamente invadir a rede informática. As ameaças cibernéticas também se referem a um possível ataque cibernético que visa obter acesso não autorizado, interromper, roubar ou danificar um ativo, propriedade intelectual, rede de computadores ou qualquer outra forma de dados confidenciais (Vankirk, 2022), podendo inclusive ter origem em utilizadores ou dispositivos confiáveis, a partir da rede interna de uma empresa e de locais remotos desconhecidos. Como nos evidencia o passado, as ameaças cibernéticas podem resultar em falhas em serviços críticos (Ingerslev, 2021), como por exemplo

numa rede de energia elétrica, falhas em equipamentos militares ou violação de segredos de segurança nacional, afetar redes de computadores, sistemas de comunicação, tornando indisponível o acesso à informação. Segundo o relatório *Threat Landscape 2022*, que analisa o panorama geral das ciberameaças e com especial foco nas ameaças, atores de ameaça e técnicas de ataque, identificou o *ransomware* como a maior ameaça em 2022. Verificou-se ainda, o aumento dos ataques de cibersegurança durante o segundo semestre de 2021 e 2022, não apenas em termos de quantidade e vetores de ataque, mas também em termos do seu impacto. A crise entre Rússia e a Ucrânia definiu uma nova era para a guerra cibernética, nomeadamente no seu papel e impacto nos conflitos, paradigma trazido pela guerra com fortes implicações para as normas internacionais no ciberespaço e, mais especificamente, para a patrocínio de ataques cibernéticos direcionados a infraestruturas civis críticas (Huntley, 2023).

2.1.2 Atores de ameaça

Em cibersegurança, um "ator da ameaça" é um termo utilizado para descrever qualquer indivíduo ou grupo que esteja envolvido num ataque ou ameaça cibernética (McCarthy, 2023). Os atores de ameaças são tipicamente classificados em diferentes categorias, com base nos seus motivos, aptidões e nível de sofisticação (Dimaggio, 2022), como por exemplo:

- Cibercriminosos: São indivíduos ou grupos que se envolvem em atividades ilegais, tais como roubar informação pessoal, conduzir fraude financeira, ou utilizar *malware* para fins lucrativos.

- Hacktivistas: Estes são indivíduos ou grupos que utilizam técnicas de *hacking* como meio para promover a sua agenda política ou social. Podem visar agências governamentais, corporações, ou outras organizações que considerem ser contra as suas crenças. Alguns grupos hacktivistas bem conhecidos incluem *Anonymous, LulzSec e AntiSec*. Estes grupos têm estado envolvidos em vários ataques de alto nível contra agências governamentais, corporações, e outras organizações (Stouffer, 2021). Os ataques perpetrados por hacktivistas podem ser politicamente motivados, como se viu no caso das revoltas da Primavera Árabe, ou socialmente motivados, como no caso do movimento *Occupy Wall Street*.

- Atores Estado-nação: Estes são grupos patrocinados pelo Estado que realizam espionagem cibernética ou ataques cibernéticos a outras nações, organizações, ou indivíduos para ganho político, militar ou económico. As motivações deste tipo de atores podem variar muito, mas muitas vezes envolvem roubar informação sensível, perturbar infraestruturas críticas, ou

promover a instabilidade política de outras nações ou regiões, podendo visar agências governamentais, organizações militares, instituições de investigação, ou corporações de uma série de indústrias. Alguns exemplos bem conhecidos de atores do Estado-nação incluem o grupo chinês de APT10, o grupo russo APT29 e o grupo norte-coreano *Lazarus*, grupos estes que têm estado ligados a uma série de ataques cibernéticos contra alvos nos Estados Unidos, Europa, e outras regiões (BrandDefense, 2022).

- *Insiders*: Indivíduos que têm acesso autorizado aos sistemas e dados de uma empresa, mas utilizam esse acesso para se envolverem em atividades maliciosas, tais como roubar informação confidencial ou sabotar sistemas.

- *Script kiddies*: Indivíduos que não possuem as competências técnicas necessárias para criar as suas próprias explorações ou *malwares*, utilizando por isso ferramentas e guiões pré-fabricados para lançar ataques.

2.1.3 Indicadores de ataque

Os indicadores de ataque (IOA) são provas ou sinais de que um ator de ameaça está a tentar ou já obteve acesso não autorizado a um sistema ou rede (Kost, 2022). Os IoA estão centrados no comportamento ou atividade do ator de ameaça, em vez de artefactos ou indicadores específicos deixados para trás após um ataque. Alguns exemplos comuns de IoA incluem:

- Padrões de tráfego de rede: Padrões de tráfego de rede pouco normais ou suspeitos, tais como um número excessivo de tentativas de login falhadas, que pode ser um indicador de que um ator de ameaça está a tentar obter acesso não autorizado a um sistema ou rede.

- Atividade de ficheiros: Atividade de ficheiro inusitada ou suspeita, tal como tentativas de apagar ou modificar ficheiros críticos do sistema, pode ser um indicador de que um ator de ameaça obteve acesso não autorizado a um sistema e está a tentar cobrir as evidencias registadas.

- Comportamento do utilizador: Comportamento não habitual ou suspeito do utilizador, tais como tentativas de aumentar os privilégios ou de acesso a recursos que normalmente não teriam permissões, pode ser um indicador de que um ator de ameaça obteve acesso não autorizado a um sistema ou rede.

- Carga útil maliciosa: As cargas úteis maliciosas, tais como vírus ou *malware*, podem ser um indicador de que um ator de ameaça obteve acesso não autorizado a um sistema e está a tentar levar a cabo um objetivo específico.

- Portas de rede incomuns: Ligações realizadas via portas de comunicação não padrão, ao invés das comuns (portas 80 ou 443).

Estes indicadores são frequentemente utilizados em conjunto com outras ferramentas e técnicas de segurança, tais como sistemas de deteção de intrusão (IDS) e sistemas de gestão de informação e eventos de segurança (SIEM), para detetar e responder a potenciais ameaças à segurança (Nazarov, 2022), identificando os IOA, no sentido de tomar medidas imediatas para as mitigar, minimizando o impacto de ataques bem-sucedidos e prevenindo possíveis danos advindos.

2.1.4 Indicadores de comprometimento

Indicadores de comprometimento são sinais de que um ator de ameaça já obteve acesso à rede, fornecendo provas de que ocorreu uma violação, pelo que tipicamente a equipa das tecnologias de informação (TI) ou a equipa da segurança da Informação (SI) são forçadas a agir reativas, implementando medidas para mitigar a ameaça e reparar os possíveis danos advindos (Roberts, 2022). Isto torna os IOC uma forma de deteção de ameaças reativa, porque ajudam a reagir a um ataque que já aconteceu, através da análise de atividade maliciosa, fornecendo informações relevantes sobre as características de um ataque, conhecidos como assinaturas de ameaça e ajudando as equipas de TI/SI a detetar e prevenir ataques semelhantes no futuro. Neste tipo de indicadores incluem-se:

- Tráfego de rede anormal: O tráfego de saída anormal pode ser um sinal de exfiltração de dados, enquanto os pedidos internos sobre portos pouco usados poderiam apontar para a utilização de ferramentas comuns de *hacking*.

- Pedidos anómalos de DNS: Pedidos de DNS suspeitos, tais como nomes de domínio mal soletrados, podem ser uma prova de que o *malware* na rede estava a tentar comunicar com um servidor externo de Comando e Controlo (C&C).

- Ataques DDoS: Os ataques de Negação de Serviço Distribuída (DDoS) são frequentemente utilizados para disfarçar as atividades e intenções dos atores de ameaça na rede.

- Atividade de conta privilegiada anormal: Se uma conta privilegiada apresentar um comportamento anormal, como a elevação aleatória de outras contas de utilizadores ou o acesso a dados sensíveis fora da sua função normal de trabalho, pode ser um sinal de que a conta foi comprometida.

- Picos no volume de leitura em base de dados: Picos invulgares no volume lido na base de dados, especialmente em momentos ímpares, indicam que um ator de ameaça poderá estar a aceder ou a exfiltrar dados.

- Alterações suspeitas: Alterações suspeitas nos registos ou ficheiros do sistema indicam frequentemente que o sistema foi infetado por *malware*, que poderia ter sido utilizado para criar uma porta traseira para a exfiltração de dados.

- Engenharia social: Uma tentativa bem-sucedida de engenharia social, tal como o *phishing* por correio eletrónico, resultando em credenciais roubadas.

- Reinfeção de *malware*: A rápida reinfeção após a remoção de um vírus ou outro *malware* pode ser prova de um *rootkit* ou uma ameaça persistente avançada (APT).

No sentido classificar uma ameaça cibernética, a matriz do Indicador de Compromisso, avalia as ameaça utilizando três critérios, tais como localizar, identificar e resposta, descritos em maior detalhe na secção – 2.2.4 *Frameworks* e Matrizes.

2.1.5 Tipos de *Cyber Threats*

Embora exista uma panóplia de ameaças detetadas, este estudo incidiu sobre as técnicas mais usadas em 2022 (Stone, 2022), relativamente às quatro maiores categorias:

2.1.5.1 *Ransomware*

O *ransomware* é um tipo de *software* malicioso (*malware*) que encripta determinados ficheiros ou todo o sistema operativo e exige o pagamento em troca da chave de desencriptação (Palmer, 2022). Os ataques de *ransomware* envolvem normalmente o uso de táticas de engenharia social para levar as vítimas a descarregar ou abrir um anexo malicioso, clicar num *link* malicioso ou a visitar uma página de *Internet* comprometida. Assim que o *software* de resgate infecta o

sistema de uma vítima, começa a encriptar os ficheiros, tornando-os inacessíveis. A vítima recebe então um pedido de resgate do ator de ameaça, geralmente sob a forma de uma mensagem *pop-up* ou ficheiro de texto, exigindo o pagamento em troca da chave de desencriptação.

Os ataques de resgate podem ter consequências significativas para as organizações, nomeadamente a perda de dados críticos, interrupção de negócios, e inclusive perdas financeiras. Os ataques de resgate podem também resultar em danos de reputação, uma vez que as vítimas podem hesitar em admitir que foram alvo de um resgate. Nos últimos anos, os ataques de resgate tornaram-se cada vez mais comuns e sofisticados (Kerner, 2023), com os atores de ameaça a utilizarem táticas e técnicas avançadas para escapar à deteção e atingir os seus objetivos. Neste tipo de ataque, as organizações são aconselhadas a tomar várias medidas, incluindo o *backup* regular dos seus dados, mantendo o seu software e sistemas de segurança atualizados, como por exemplos *anti-malware*, com também formar os seus colaboradores sobre como reconhecer e evitar ataques de *phishing* ou outros tipos de ataques de engenharia social (Irwin, 2021). Além disso, as organizações devem ter um plano de resposta em caso de ataque de resgate, incluindo políticas e procedimentos, diferentes *softwares* para detetar ataques de resgate, tais como AV, deteção e resposta de pontos finais (EDR) e soluções SIEM. No caso específico de um ataque de resgate, as plataformas SIEM podem ajudar em várias fases da infeção para responder a pedidos de resgate, podendo recuperar de uma infeção por resgate de *software,* quando detetado precocemente (Clarke, 2023).

2.1.5.2 *Phishing*

Phishing é um tipo de ataque cibernético em que um ator de ameaça envia um *e-mail* ou mensagem fraudulenta que aparenta ter origem numa fonte legítima (Palmer, 2023), tal como um banco, plataforma de meios de comunicação social, ou outra organização de confiança, numa tentativa de enganar o destinatário para que este revele informação sensível ou clique numa ligação maliciosa. Os ataques de *phishing* são tipicamente realizados através de correio eletrónico (Palmer 2023), mas podem também assumir a forma de mensagens de texto, publicações em meios de comunicação social ou outros tipos de comunicações digitais e podem ter consequências graves para as organizações, incluindo o roubo de informações sensíveis, tais como palavras-passe, números de cartões de crédito ou outros dados pessoais. Os ataques de *phishing* podem também levar à instalação de *malware* no dispositivo de uma vítima, o que pode resultar em mais roubos de dados ou outros tipos de atividade maliciosa, especialmente se contiverem pedidos de informação sensível ou pedirem ao destinatário para clicar num *link* (Brooke, 2022).

2.1.5.3 *Supply Chain Attacks*

Os ataques na cadeia de fornecimento são um tipo de ataque cibernético em que um ator de ameaça visa a cadeia de fornecimento de *software* ou *hardware* de um determinado produto, com o objetivo de comprometer a integridade do produto e potencialmente ganhar acesso a informação sensível (Korolov, 2021).

Num ataque à cadeia de fornecimento, um ator de ameaça pode comprometer um fornecedor, fornecedor terciário de componentes de *software* ou *hardware* utilizados num produto, usando posteriormente esse acesso para injetar código malicioso ou *malware* no produto, podendo também comprometer o processo de produção ou distribuição do produto para introduzir vulnerabilidades ou *backdoors* no produto final (Liu, 2022). Este tipo de ataque pode ter consequências graves nas organizações e governos, podendo potencialmente comprometer a segurança de redes ou sistemas. Os ataques à cadeia de abastecimento têm sido utilizados em vários ciberataques de grande visibilidade nos últimos anos, incluindo o ataque *NotPetya* de 2017, que causou milhares de milhões de dólares em prejuízos às organizações em todo o mundo (Wolff, 2021). Para garantir proteção contra ataques da cadeia de fornecimento, as organizações são aconselhadas a examinar cuidadosamente os fornecedores e fornecedores terceiros, e realizar avaliações de segurança exaustivas de qualquer componente de *software* ou *hardware* utilizado nos seus produtos, sendo que as organizações devem também implementar fortes controlos de segurança, tais como *firewalls*, sistemas de deteção e prevenção de intrusão, controlos de acesso e plataformas SIEM, para ajudar a detetar e prevenir ataques à cadeia de fornecimento (Martin, 2021).

2.1.5.4 Ataques a equipamentos *IoT*

Os ataques cibernéticos visando os dispositivos da *Internet of Things* (IoT) têm-se tornado uma ameaça cada vez mais significativa nos últimos anos (Mcbride, 2023). Os dispositivos IoT são dispositivos ligados à *Internet,* tais como aparelhos domésticos inteligentes, tecnologia *wearable*, dispositivos médicos, e sistemas de controlo industrial. Estes dispositivos têm frequentemente medidas de segurança fracas em vigor, tornando-os vulneráveis a ataques cibernéticos. Os atores de ameaça podem explorar as vulnerabilidades dos dispositivos de *Internet* de alta velocidade para obterem acesso não autorizado a redes ou roubarem informação sensível e também utilizá-los para lançar ataques a outros sistemas, tais como ataques de negação de serviço distribuída (Gupta, 2021). Uma vez que os dispositivos IoT são frequentemente utilizados em infraestruturas críticas e sistemas de controlo industrial, um ataque cibernético bem-sucedido

a um dispositivo IoT poderia ter sérias consequências para a segurança pública e a segurança nacional. Para além das vulnerabilidades inerentes aos próprios dispositivos da IoT, os atores de ameaça podem também explorar fraquezas nas redes e sistemas que ligam estes dispositivos, como por exemplo, visar equipamentos de rede, tais como *routers* ou *switchs,* que não tenham sido atualizados com as últimas correções de segurança ou que tenham medidas de autenticação fracas. Outro desafio na segurança de dispositivos IoT, é que muitos deles são concebidos para serem de baixo custo e baixa potência, com capacidades limitadas de processamento e memória e que pode tornar difícil a implementação de medidas de segurança fortes, tais como encriptação e autenticação, nestes dispositivos. Uma solução potencial para este problema é utilizar medidas de segurança especializadas, tais como a integração em sistemas SIEM, por exemplo, para a deteção e mitigação da rede IoT-*botnet* e ataques DDoS (Al-Duwairi, 2019).

2.1.6 Estratégia em cibersegurança

Uma estratégia no contexto de cibersegurança é tipicamente referida como uma forma de documentar os vários aspetos do ciberespaço, endereçando as necessidades da segurança no ciberespaço de uma entidade ou organização, descrevendo como a informação, rede de dados, sistemas informáticos e pessoas serão protegidas, com o objetivo de detalhar e prever todas as possíveis superfícies de ataque (Unni, 2022). Tendo em conta o crescente aumento dos ataques cibernéticos, tem sido aconselhado o desenvolvimento deste tipo de estratégia, de modo a assegurar a proteção das infraestruturas informáticas de diferentes riscos e ameaças através da criação de uma estratégia que procura entender o cenário de ameaças cibernéticas em que a organização se enquadra, avaliar a maturidade da organização na segurança cibernética, determinar como melhorar programa de cibersegurança para a organização e documentar a estratégia de cibersegurança (Scarfone, 2022).

Uma estratégia de cibersegurança é crucial na implementação da Gestão de Informação e Eventos de Segurança (SIEM) porque ajuda a assegurar que a solução SIEM está alinhada com as metas e objetivos globais de segurança da organização (Eley, 2023). As soluções SIEM são concebidas para recolher e analisar dados relacionados com a segurança de várias fontes para detetar e responder a incidentes de segurança, que, sem uma estratégia cibersegurança bem definida, a plataforma não pode ser configurada para recolher os dados corretos ou priorizar alertas e eventos, de forma a alinhar-se com as prioridades de segurança da organização, pelas seguintes razões:

- Definição dos objetivos de segurança: Estabelece os objetivos de segurança, prioridades e apetite de risco da organização. Garante que a solução é configurada para recolher dados alinhados com os objetivos de segurança da organização, podendo detetar e responder a incidentes de segurança que são mais críticos para a organização.

- Assegurar o seu cumprimento: Assegura que as soluções SIEM são configuradas para cumprir os requisitos regulamentares relevantes, as normas da indústria ou do negócio em específico. Os requisitos de conformidade podem ditar que tipos de dados o SIEM deve recolher, como deve ser analisado e comunicado.

- Alinhamento com os objetivos: Assegura que a solução SIEM está alinhada com os objetivos empresariais globais da organização e garante que as soluções SIEM são configuradas para apoiar as operações da organização e proteger ativos críticos, tais como dados de clientes, propriedade intelectual e informação financeira.

- Fornece uma estrutura de resposta a incidentes: Fornece um enquadramento para a resposta a incidentes e define os processos e procedimentos que devem ser seguidos em caso de incidente de segurança, incluindo a forma como solução SIEM deve ser utilizada para detetar, investigar e responder a incidentes de segurança.

2.1.7 Ciclo de vida de um incidente

O ciclo de vida do incidente é um quadro bem estabelecido que desempenha um papel crítico na cibersegurança, que descreve as várias fases envolvidas na deteção, resposta e recuperação de um incidente de segurança, consistindo tipicamente em quatro fases: identificação, contenção, erradicação e recuperação (Cynet, 2022).

Figura 1 - Ciclo de vida de um incidente. Adaptado de Kreisa (2023)

A primeira fase do ciclo de vida do incidente é a identificação e envolve a deteção de um incidente de segurança ou de um potencial incidente de segurança. A deteção pode ocorrer através de vários meios, tais como sistemas de deteção de intrusão, ferramentas de informação de segurança e gestão de eventos (SIEM), *firewalls* de rede e *host-based*, *software* antivírus, e outras ferramentas de segurança (Kreisa, 2023).

Uma vez identificado um incidente, a próxima etapa é a contenção, que envolve o isolamento dos sistemas ou segmentos de rede afetados para evitar que o incidente se propague, com o objetivo de limitar os danos causados pelo incidente, prevenindo a perda de mais dados ou recursos.

A terceira fase do ciclo de vida do incidente é a erradicação, onde implica identificar e remover a causa raiz do incidente, tal como *malware*, acesso não autorizado, ou sistemas mal configurados. A erradicação pode ser um processo desafiante, pois os atores de ameaça podem por vezes esconder a sua atividade ou criar acessos do tipo *backdoors*.

A fase final do ciclo de vida do incidente é a recuperação e implica restaurar os sistemas e recursos afetados ao seu estado normal de funcionamento. A recuperação pode envolver várias

atividades, tais como *backup* e restauro de dados, reconfiguração do sistema, correção de *software* ou ativação de planos de *disaster recover*.

O ciclo de vida do incidente é uma estrutura essencial em cibersegurança, uma vez que proporciona uma abordagem estruturada e sistemática à gestão de incidentes de segurança, podendo reduzir o impacto dos incidentes de segurança, minimizar o tempo de inatividade, no sentido de manter a continuidade do negócio.

Além disso, o ciclo de vida do incidente proporciona uma estrutura para o planeamento e teste da resposta a incidentes, onde as organizações podem utilizar o ciclo de vida do incidente para desenvolver planos de resposta a incidentes, que descrevem papéis e responsabilidades, assim como procedimentos e protocolos de comunicação. Podem também utilizar o ciclo de vida do incidente para conduzir exercícios de resposta a incidentes e simulações para testar a eficácia dos seus planos de resposta a incidentes (Kreisa, 2023).

2.1.8 *Cibersecurity Kill Chain*

A cadeia *Cyber Kill*, desenvolvido por *Lockheed Martin*, descreve as etapas de um ataque cibernético e tornou-se num dos modelos atualmente mais usado pelas organizações, no sentido de compreender, detetar, prevenir e controlar os vários estágios das intrusões cibernéticas, estudando assim os diversos perfis e metodologias das ameaças (Tunggal, 2022). O objetivo do modelo é compreender melhor as fases necessárias para executar um ataque e ajudar as equipas de TI/SI a mitigar um ataque em cada uma das suas fases.

2.1.9 Superfícies de ataque

Uma superfície de ataque consiste em enumerar todos os pontos de entrada possíveis, ou vetores de ataque, que podem potencialmente permitir que agentes de ameaças invadam um sistema, aplicação, dispositivo ou uma rede interna (Hanna, 2021). Uma superfície de ataque maior é mais difícil de proteger, porque significa que um sistema ou organização está exposta a mais ameaças, sendo geralmente categorizada em dois tipos: uma superfície de ataque digital e uma superfície de ataque físico (Magnusson, 2023), onde superfície de ataque digital consiste em *software* e *hardware* vulneráveis, enquanto uma superfície de ataque física consiste em instalações físicas, *datacenters* e equipamentos físicos. Neste sentido, podemos organizá-los nas seguintes categorias:

- Superfície de ataque física: Relacionado com a localização física de uma organização, refere-se a edifícios, *datacenters*, áreas de receção e inclusive os endereços das residências dos colaboradores, que nos permite perceber, a quem é permitida a entrada nas localizações físicas, como são identificados os visitantes, por exemplo, se a rede *Wi-Fi* é acessível fora das instalações. (Magnusson, 2023).

- Superfície de ataque tecnológica: Relaciona toda e qualquer tecnologia que pertence ou é usada por uma organização, incluindo, servidores, rede, terminais, dispositivos móveis, incluindo qualquer serviço que aloje informação e que esteja inclusive exposto para a *Internet*, como por exemplo, um portal de suporte, que estão suscetíveis a mapeamento e recolha de dados através do uso de *scanners* de rede e vulnerabilidades. Este processo corresponde à fase de enumeração (Hanna, 2021).

Neste sentido, torna-se importante não só reduzir a superfície de ataque, como também geri-la de uma forma eficaz, sendo considerada boa prática a monitorização de todas a atividade do ambiente informático, fazendo uso nomeadamente de técnicas avançadas de auditoria e recolha de eventos, para posterior correlação, sendo considerado um SIEM a forma mais eficaz e simples de realizar este processo (Horenbeeck, 2023).

2.1.10 Vetores de ataque

Os vetores de ataque são os métodos ou caminhos utilizados pelos atores de ameaça para obter acesso não autorizado a um sistema ou rede alvo (Tunggal, 2023). Os vetores de ataque podem ser considerados como pontos de entrada ou fraquezas que um ator de ameaça pode explorar e comumente incluem:

- Ataques de *phishing*: quando um ator de ameaça envia um e-mail fraudulento, mensagem de texto, ou mensagem de meios de comunicação social para enganar uma vítima a clicar numa ligação maliciosa ou a descarregar um anexo infetado por *malware*.

- *Malware*: *software* malicioso concebido para se infiltrar num sistema e causar danos ou roubar dados.

- Explorações: vulnerabilidades de segurança (ex: vulnerabilidade *zero-Day*) em *software* ou *hardware* que podem ser exploradas por ator de ameaça para obter acesso a um sistema.

- Ataques com *passwords*: ataques de força bruta, ataques de dicionários, ou ataques de pulverização de senhas em que os atores de ameaça tentam adivinhar ou decifrar senhas para obter acesso a sistemas ou contas.

- Ataques físicos: onde um ator de ameaça obtém acesso a um dispositivo físico ou infraestrutura de rede e realiza atividades maliciosas.

Os vetores de ataque podem, contudo, variar em complexidade e sofisticação, e podem evoluir com o tempo à medida que novas vulnerabilidades são descobertas e exploradas.

2.1.11 Estágios

Além dos vetores de ataque, os ataques cibernéticos também podem ser descritos em termos dos estágios ou fases pelos quais passam. Esses estágios são comumente chamados de Ciclo de vida do ataque cibernético (Kidd, 2022) ou Cadeia de morte cibernética (*The Ciber Kill Chain*) e incluem:

- Reconhecimento: Onde o ator de ameaça procura descobrir tudo o que pode sobre o seu alvo através das superfícies de ataque, físicas, tecnológicas e humanas.

- Intrusão: Onde as informações recolhidas no estágio de reconhecimento são armadas. O vetor de ataque é encontrado e usado para obter acesso ao alvo.

- Exploração: Esta fase é onde é preconizada a introdução de *software* e/ou código malicioso no sistema.

- Escalonamento de privilégios (*privilege escalation*): Relacionada com a fase em que o ator de ameaça altera os seus direitos de acesso ao sistema, muitas vezes a um administrador de sistema para obter acesso a dados e permissões seguras.

- Movimento lateral (*lateral movement*): Processo em que o ator de ameaça necessita muitas vezes de se deslocar entre sistemas e contas no sentido de obter acesso a mais sistemas.

- Ofuscação (*Obfuscation*): É nesta fase que os atores da ameaça apagam todos os vestígios relacionados com os seus acessos, através da limpeza de ficheiros, substituindo dados por falsos, carimbos temporais e colocando inclusive vestígios adulterados.

- Negação de serviço (DoS): fase em que o serviço para utilizadores normais é interrompido ou afetado, com o intuito de impedir que os atores da ameaça sejam localizados monitorizados ou bloqueados.

- Exfiltração (*Exfiltration*): Este é todo o objetivo do ataque, ou seja, retirar dados do sistema comprometido.

2.1.12 Inteligência sobre ameaças cibernéticas

A inteligência relativa a ameaças cibernéticas é uma área da cibersegurança que se centra na recolha e análise de informações sobre as tendências relativas a ataques cibernéticos correntes, bem com os potenciais ataques que poderão afetar a segurança de uma organização ou dos seus ativos informáticos (Martins, 2023). São 5 as fases do ciclo de vida da informação sobre ameaças, que após o planeamento e a definição de objetivos, a informação é posteriormente analisada, correlacionada e organizada, envolvendo a recolha e análise de dados de várias fontes, tais como bases de dados públicas e privadas, inteligência de fonte aberta (OSINT), informação de vendedores e investigadores de segurança, no sentido de minimizar e mitigar os riscos de possíveis exposições a ameaças cibernéticas.

Figura 2 - As cinco fases do ciclo de vida da informação sobre ameaças. Adaptado de Baker (2023)

O objetivo das informações sobre ameaças cibernéticas é fornecer às organizações os conhecimentos de que necessitam para identificar, avaliar e responder a potenciais ameaças, de uma forma atempada e eficaz, através de informações atualizadas sobre as últimas tendências e desenvolvimentos no panorama das ameaças cibernéticas, permitindo-lhes antecipar e preparar-se para novas ameaças antes que estas ocorram.

2.1.12.1 Tipos de *Cyber Threat Intelligence*

- Estratégica – Analisa ciberataques hipotéticos e os seus potenciais efeitos nas partes interessadas, audiências não técnicas e decisores, baseando-se em análises aprofundadas de novos riscos e tendências e destinando-se a fornecer uma perspetiva ampla do cenário de ameaças que um determinado sector ou empresa enfrenta (Baker, 2023).

- Tática - As informações relativas às táticas, métodos e procedimentos (TTPs) dos atores de ameaças são fornecidas através da informação tática, concebida para os colaboradores diretamente responsáveis pela proteção dos recursos informáticos e de dados, fornecendo informações sobre as estratégias mais eficazes de proteção contra ou redução de ataques, bem como informações sobre a forma como uma organização pode ser atacada utilizando as técnicas mais recentes (Baker, 2023).

- Técnica - Informação técnica sobre ameaças é a informação que as equipas de segurança obtêm normalmente dos seus *feeds* de informação de fonte aberta. As equipas de segurança utilizam a informação técnica sobre ameaças para monitorizar novas ameaças ou investigar um incidente de segurança. Alguns exemplos adicionais de informações técnicas sobre ameaças incluem: Vetor de ataque que os agentes maliciosos utilizam, Domínios de comando e controlo (C&C), Vulnerabilidades exploradas, Registos de *Infostealer* Dados de vulnerabilidade e exposição comuns (CVE) (Yadav, 2023).

- Operacional - Este método reúne dados de vários locais, como salas de conversação, redes sociais, registos de antivírus e ocorrências históricas, sendo utilizado para prever o tipo e a hora dos próximos ataques. O processamento automatizado de milhões de pontos de dados em muitas línguas e é frequentemente realizado utilizando a extração de dados e a aprendizagem automática. A inteligência operacional é utilizada pelas equipas de segurança e de resposta a incidentes para modificar as definições de alguns controlos, incluindo regras de *firewall*, regras de deteção de eventos e controlos de acesso, podendo também melhorar os tempos de resposta, uma vez que a informação fornece uma ideia mais clara do que procurar (Baker, 2023).

2.1.12.2 *Open-Source Intelligence*

Inteligência *open-source*, frequentemente referenciada como OSINT, é definido como qualquer inteligência produzida por informação publicamente disponível que é recolhida, explorada e disseminada sob forma atempada a um público adequado, para o efeito de abordar um requisito específico de inteligência. Como exemplo de algumas fontes *open source*, incluem-se os meios de comunicação social, *blogs*, notícias, e a *dark web* (Bazzel, 2022).

Para este projeto em específico serão usadas algumas respetivamente integradas na plataforma SIEM.

- ***Greynoise***

A *GreyNoise* é uma empresa de inteligência cibernética de segurança que recolhe, analisa e fornece contexto a dados de telemetria de varrimento e ataque em toda a *Internet* e focam-se no que chamam o ruído da *Internet* (Donnan, 2022). Foi fundada em 2017 por Andrew Morris, um antigo analista de cibersegurança da *Endgame* e tem como objetivo ajudar as organizações a detetar e responder à atividade de varrimento e ataque em toda a *Internet*. Recolhe dados de várias fontes, através de *honeypots* públicos e privados instalados em diversas localizações, telescópios de rede e outros sensores, para identificar a atividade de varrimento e de ataque em toda a *Internet*, analisando a informação através do comportamento, do método e a intenção e classificando posteriormente como benigno, maligno ou desconhecido, representado na figura 3. A empresa analisa estes dados e fornece contexto e perspetivas para ajudar as organizações a compreender o panorama de ameaças e a dar prioridade à sua resposta a potenciais ameaças, fornecendo posteriormente acesso à sua API, figura 4. Uma das características é a sua capacidade de distinguir entre varrimento e atividade de ataque à escala da *Internet* e ataques direcionados (APT). Ao concentrar-se na atividade ao nível da *Internet*, proporcionando uma compreensão mais ampla do cenário de ameaças, ajuda a identificar ameaças que possam ser ignoradas por outras fontes de informação sobre ameaças.

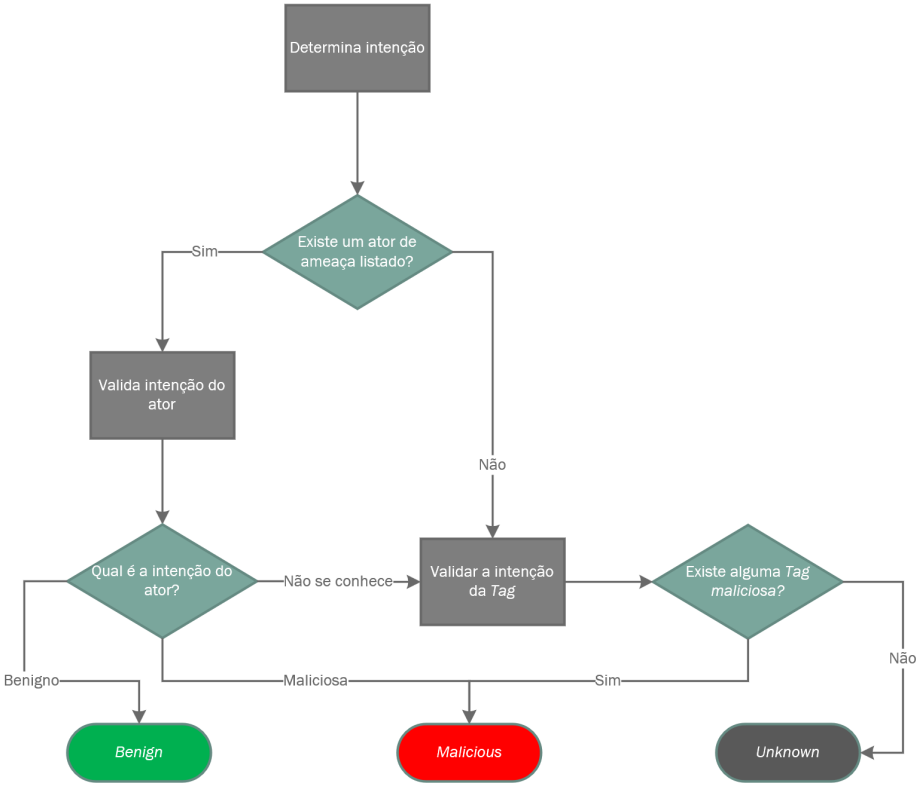

Figura 3 - Critério de classificação do Greynoise. Adaptado de Greynoise (2021)

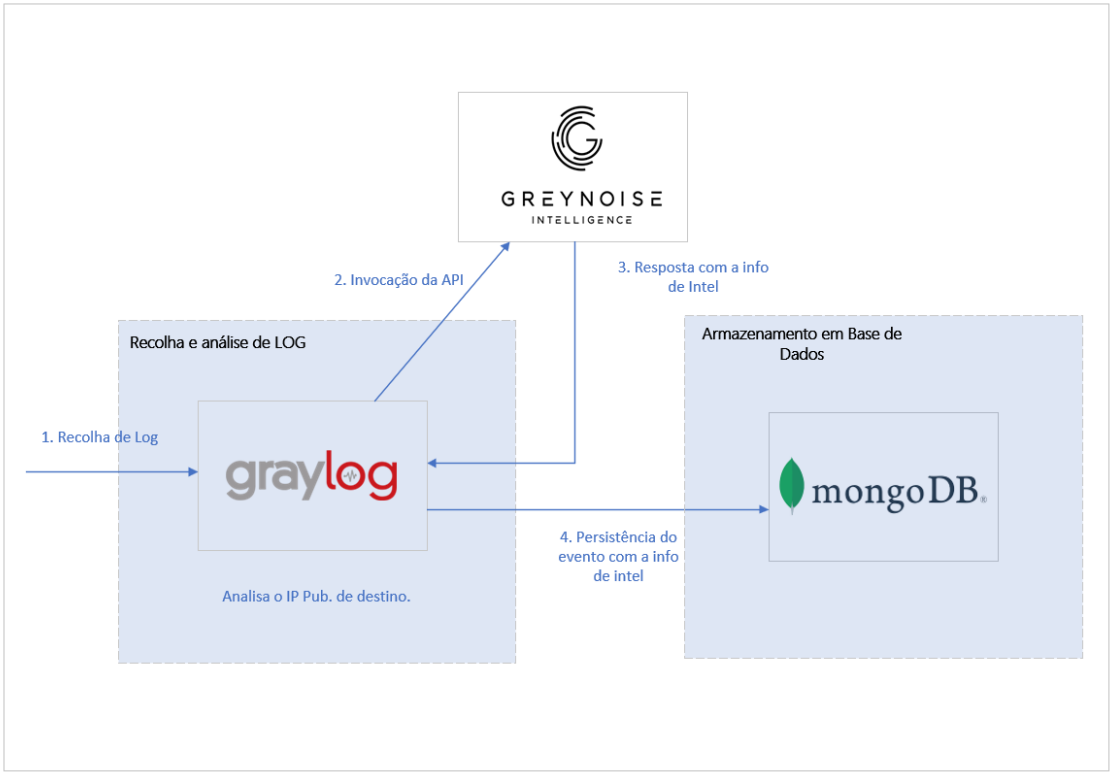

Figura 4 - Integração da API Greynoise no Graylog. Adaptado de SOCFortress (2022)

- ***ThreatFox* IoC**

ThreatFox IoC é uma plataforma em linha gratuita e de código aberto que fornece informações sobre ameaças em domínios maliciosos conhecidos e endereços IP, através da pesquisa de IOC associados a *malware* (Bannister, 2021). A plataforma agrega e analisa dados de uma vasta gama de fontes, incluindo amostras de *malware*, *e-mails* de *phishing* e outras fontes de informação sobre ameaças. O principal objetivo desta plataforma é fornecer um repositório centralizado de inteligência de ameaças que possa ser utilizado por profissionais de segurança para identificar e bloquear o tráfego malicioso nas suas redes. A plataforma fornece uma *interface* de fácil utilização que permite aos utilizadores pesquisar domínios maliciosos conhecidos e endereços IP, ver detalhes sobre as ameaças associadas e descarregar os dados do IoC para utilização nas suas próprias ferramentas de segurança. Para isso, fornece uma API que permite aos sistemas SIEM consumir os dados de inteligência de ameaças fornecidos pela plataforma, permitindo automatizar o processo de identificação e bloqueio de tráfego malicioso. Por exemplo, quando uma plataforma SIEM deteta e regista um evento, tal como uma ligação de rede suspeita ou uma tentativa de acesso a um domínio malicioso conhecido, é realizada uma verificação do domínio ou endereço IP no sentido de avaliar se está associado a qualquer ameaça conhecida. Se for encontrada uma correspondência, podendo o SIEM tomar ações automatizadas, tais como bloquear o tráfego ou alertar a equipa de SI.

2.2 *Threat hunting*

2.2.1 Definição

Threat hunting é o processo de pesquisa proativa e iterativa que, através da análise da atividade de rede, permite detetar e isolar ameaças avançadas que passam despercebidas às soluções de segurança implementadas, através da procura intencional e estruturada de provas de atividades maliciosas, que ainda não geraram alertas de segurança (Hazel, 2021). Advindo da necessidade de procurar ativamente as ameaças nos respetivos ecossistemas informáticos, alertando para o fato dos atores de ameaça poderem assumir não só a forma de ameaças externas, que podem manter a persistência (APT), mas também ameaças provindas das suas redes privadas, aproveitando-se assim e a título de exemplo os seus privilégios. Esta abordagem dita uma mudança de paradigma (Kumar, 2018), que se baseia no fato de em vez de esperar que as defesas bloqueiem os ataques ou que as violações sejam detetadas por mecanismos de alerta passivos, os departamentos de segurança informática possam evitar possíveis intrusões através da deteção e resposta sob forma pró-ativa.

Quando se implementa um processo de procura por ameaças, o primeiro passo tipicamente é perceber em que nível do *Hunting Maturity Model* a organização se encontra (Imam, 2018), com o objetivo de avaliar a sua atual qualidade e quantidade de dados recolhidos, que podem ter impacto na capacidade para a deteção das próprias ameaças, assim como a identificação de áreas a melhorar, divididos pelos seguintes estágios (SQRRL, 2015):

- Inicial (HMM0) - Colocação em funcionamento dos alertas de segurança automatizados (ferramentas SIEM, IDS, etc.) e desenvolvimento de uma equipa dedicada para resposta a incidentes.

- Mínimo (HMM1) - Recolha e centralização de registos de diferentes domínios dentro do ambiente (rede, base de dados, aplicações, etc.); Utilização do mecanismo de inteligência a ameaças na deteção e alavancagem dos IoC a partir de relatórios e autoridades publicadas.

- Procedimentos (HMM2) - Na sequência de procedimentos publicados pela procura de novos incidentes de segurança; Implementação de um calendário de procura por ameaças sob forma regular, i.e., semanal, mensal, etc. e possuir recursos humanos especializados dentro da equipa SOC.

- Inovador (HMM3) - Utiliza uma grande variedade de quadros de análise de dados, aplicando-os na identificação de atividades suspeitas; desenvolve ou publica procedimentos originais no âmbito da procura por ameaças, com base na sua experiência e/ou no seu ambiente; Utilização de uma plataforma dedicada à caça de ameaças para racionalizar o processo e reforçar a cooperação na equipa.

- Líder (HMM4) - Utilização de técnicas de ciência de dados, aprendizagem de máquinas e inteligência artificial dentro dos procedimentos de caça às ameaças; Alavanca ferramentas automatizadas para obter os resultados das atividades de caça de ameaças, no sentido de melhorar os alertas e os esforços de deteção; Implementa uma metodologia para dimensionar os procedimentos, de modo a que estes sejam aplicáveis a um âmbito mais alargado dentro da organização.

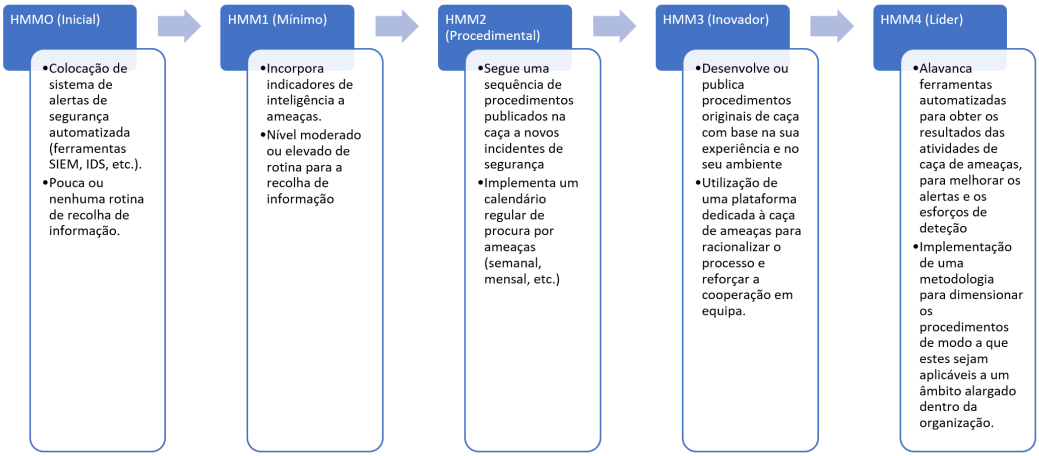

Figura 5 - Hunting Maturity Model (HMM). Adaptado de Rumiantseva (2022).

2.2.2 Metodologias *Threat hunting*

Nos próximos pontos serão descritas as metodologias adotadas na pesquisa por ameaças, sendo na sua essência as três aproximações mais comuns, ou seja, estruturada, não estruturada e situacional (Naz, 2023).

2.2.2.1 Estruturado

A pesquisa estruturada de ameaças é um processo proactivo que envolve a procura de potenciais ameaças e anomalias de segurança dentro da rede, sistemas, e aplicações de uma organização (Ariganello, 2022). O objetivo da procura estruturada de ameaças é identificar e remediar ameaças que possam não ter sido detetados numa primeira instância pelos controlos de segurança tradicionais, tais como *firewalls*, *software* antivírus, e sistemas de deteção de intrusão, combinando táticas de ataque, técnicas e procedimentos (TTPs), com os principais IOA, frequentemente alinhados com uma *framework* conhecida, como por exemplo MITRE ATT&CK, envolvendo uma abordagem metódica e estruturada. Esta abordagem inclui tipicamente os seguintes passos:

- Definição do âmbito: Determinar os sistemas, redes e aplicações que serão incluídos no exercício de *threat hunting*, o que procurar e decidir que atividade maliciosa possa coexistir no sistema sem que tenha sido detetada.

- Desenvolver hipóteses: Com base no conhecimento da organização e na inteligência da ameaça, desenvolver hipóteses sobre potenciais ameaças ou anomalias que possam existir,

considerando a especificidade de cada ambiente para determinar potenciais riscos, como as vulnerabilidades que os atores de ameaça poderão eventualmente explorar.

- Recolher e analisar dados: Recolher e analisar dados de várias fontes, tais como registos de tráfego de rede, registos de sistema, e dados de parâmetros, para identificar provas de potenciais ameaças ou anomalias.

- Investigar e validar os resultados: Validar as provas recolhidas durante a fase de análise para determinar se são indicativas de uma ameaça real ou apenas de um falso positivo e procurar os IOC ou seguir o caminho de ataque potencial para provar ou refutar a hipótese.

- Remediar e relatar: Caso seja identificada uma ameaça real, tomar as medidas adequadas para remediar e conter a ameaça, documentando os resultados e as ações tomadas.

2.2.2.2 Não estruturado

A procura não estruturada de ameaças é uma abordagem menos procedimental ou formal de *threat hunting*, sendo um trabalho de investigação em que o *threat hunter* observa o comportamento e procura possíveis anomalias (Ariganello, 2022). Em contraste com a procura estruturada de ameaças, não existe um processo ou metodologia definida para a caça não estruturada de ameaças, sendo que pode ser promovida por intuição ou por sugestões, em vez de hipóteses específicas, que envolve normalmente a revisão manual de ficheiros de registo, tráfego de rede, e outras fontes de dados, pela procura de anomalias ou indicadores de compromisso que possam ter sido perdidos por controlos de segurança automatizados, com base na sua experiência e conhecimento adquirido. Além de ser um processo moroso, existe o risco para a inexistência de ameaças ou indicadores importantes caso a pesquisa não seja minuciosa ou focalizada. Apesar da sua natureza informal, pode ser um complemento útil para a caça estruturada de ameaças e outras medidas de segurança, pelo que ao adotar uma abordagem mais flexível e criativa da caça às ameaças, os profissionais de segurança podem identificar novas ameaças e emergentes, que podem não ter sido documentadas, antecipadas ou abordadas pelas medidas de segurança tradicionais.

2.2.2.3 Situacional ou orientada por entidades

A procura situacional ou orientada por entidades é outra abordagem à caça de ameaças que se concentra em situações ou entidades específicas dentro de uma determinada organização

(Keerthana, 2023). Esta abordagem implica identificar situações ou entidades de alto risco, tais como sistemas críticos, colaboradores chave, ou dados sensíveis, e depois procurar proactivamente potenciais ameaças dentro dessas áreas. A procura de ameaças por situações ou entidades pode ser particularmente eficaz na identificação de ataques direcionados, que são concebidos para explorar vulnerabilidades específicas ou visar indivíduos ou sistemas específicos. Ao concentrarem-se em áreas de alto risco, os profissionais de segurança podem identificar e remediar proactivamente potenciais ameaças antes de serem capazes de causar danos.

A abordagem situacional ou orientada por entidades à procura de ameaças que envolve alguns passos fundamentais, sendo eles:

- Identificar situações ou entidades de alto risco: Determinar as áreas dentro da organização que são mais críticas, tais como sistemas críticos, pessoal chave, ou dados sensíveis.

- Recolher dados: Recolher dados de várias fontes, tais como registos, tráfego de rede, e dados de pontos finais, para identificar potenciais ameaças dentro dessas áreas.

- Analisar dados: Utilizar uma combinação de ferramentas automatizadas e análise manual para identificar potenciais ameaças e anomalias dentro dos dados.

- Remediação e relatórios: Se for identificada uma potencial ameaça, tomar as medidas adequadas para remediar a questão e informar sobre as conclusões e ações tomadas.

2.2.3 Modelos

Nos próximos pontos serão descritos os modelos afetos ao *threat hunting.*

2.2.3.1 *Intel-based*

O modelo *intel-based*, traduzida para português, baseada em inteligência, é uma abordagem proactiva que envolve a recolha e análise de grandes quantidades de dados de várias fontes para identificar e mitigar potenciais ameaças à segurança antes que estas possam causar danos (McGowan, 2023). Esta abordagem é tipicamente utilizada por analistas de segurança, equipas de incidentes e *threat hunters* para detetar e responder a ameaças persistentes avançadas (APTs) e outros ataques sofisticados. O principal objetivo é aproveitar o poder da inteligência de ameaças e da análise de dados para detetar comportamentos pouco habituais ou suspeitos na rede e nos pontos terminais. Esta abordagem baseia-se numa vasta gama de fontes de dados, incluindo

tráfego de rede, ficheiros de registo, telemetria de pontos terminais e *feeds* de inteligência de ameaças, para construir uma imagem completa da postura de segurança da organização e detetar anomalias. Alguns dos principais benefícios da caça baseada na informação incluem:

- Deteção precoce de ameaças: Ao recolher e analisar grandes quantidades de dados, os analistas de segurança podem identificar potenciais ameaças antes que possam causar danos significativos.

- Defesa proactiva: Baseada em informações, permite que as organizações adotem uma abordagem proactiva, em vez de esperar que os ataques ocorram.

- Melhorar a resposta incidentes: Ao identificar ameaças potenciais com antecedência, as organizações podem responder rápida e eficazmente, minimizando o impacto de quaisquer incidentes de segurança.

2.2.3.2 *Hypothesis hunting*

As equipas de *threat hunting* usam de forma regular metodologias baseadas em hipóteses que se baseiam no método científico de investigação, sendo uma abordagem à aquisição de conhecimento, que se baseia em raciocínio lógico e provas empíricas, concebida sobretudo para evitar que os preconceitos e suposições influenciassem os seus respetivos resultados (Naz, 2023). Neste sentido, cada procura por *threat hunting* tende, de forma sumária, a seguir o seguinte processo:

- Definição do Cenário de Ataque: Em vez de procurar em geral vários tipos de ameaças, o ponto de partida é definir uma ameaça específica e estritamente focada numa que pudesse estar em curso na infraestrutura. Nesta etapa, a equipa deve pensar nas técnicas globais que podem ser utilizadas, nos alvos dentro da rede vulneráveis ao ataque e nas várias vulnerabilidades passivas de exploração.

- Formulação de uma hipótese inicial: Ao pensar nos objetivos dos atores de ameaça, para cada fase da cadeia de ataque, a equipa faz uma série de "suposições informadas" sobre que ferramentas e técnicas que o ator de ameaça pode utilizar e que provas poderão ser criadas pelas suas atividades. A pesquisa pela ameaça é então estruturada para procurar provas que seriam geradas se de facto cada hipótese sequencial fosse válida.

- Identificar e reunir provas para investigar cada hipótese: Reunir as fontes de dados que serão analisadas dentro do processo de pesquisa pela ameaça. Para provar ou refutar uma hipótese, com um elevado grau de confiança, são geralmente necessárias múltiplas formas de prova, sendo necessário também documentar a proveniência dos dados para assegurar que as fontes sejam contextualizadas e consistentes.

- Alavancar a análise para revelar resultados: Durante esta fase, as provas são correlacionadas e sujeitas a técnicas analíticas e de visualização para desvendar relações no seu interior. Os caçadores de ameaças precisam de uma compreensão profunda relativamente às técnicas usadas pelos atores de ameaça, bem como de uma perceção do tráfego normal dentro dos seus ambientes, para existir uma hipótese de serem bem-sucedidos.

- Resultados do Relatório: É fundamental documentar os tipos de provas recolhidas, a natureza da análise realizada, e a lógica por detrás das conclusões a que se chega no decurso da pesquisa pela ameaça, permitindo as respetivas equipas de segurança uma eficaz comunicação com os *stakeholders*, bem como, caso existam com a equipa responsáveis por incidentes cibernéticos.

2.2.3.3 *Custom hunting*

Custom hunting é a abordagem que envolve a adaptação das atividades de procura de ameaças às necessidades e características específicas da infraestrutura informática e do ambiente de segurança de uma organização. Ao contrário *Intel-based*, que se baseia em técnicas padronizadas e em informações sobre ameaças, a personalizada envolve o desenvolvimento de ferramentas e processos personalizados que são concebidos para satisfazer as necessidades únicas de uma organização, que é tipicamente realizada por analistas de segurança e *threat hunters* que têm um profundo conhecimento da infraestrutura e da postura de segurança de uma organização (Yesyev, 2021). Estas equipas trabalham em estreita colaboração com as equipas de TI e outros intervenientes, no sentido de identificar potenciais áreas de fraqueza ou vulnerabilidade nos sistemas e aplicações da organização, por exemplo com equipas de *pen testing*, onde desenvolvem posteriormente ferramentas e processos personalizados para monitorizar proactivamente estas áreas e detetar quaisquer sinais de atividade suspeita. Um dos principais benefícios deste modelo é permitir às organizações adotar uma abordagem mais direcionada para a deteção e resposta a ameaças, ao concentrarem-se nas áreas específicas do ambiente informático que são mais críticas ou vulneráveis, podendo atribuir recursos e responder rapidamente a quaisquer ameaças que sejam detetadas. O uso deste modelo pode também ser usado em conjunto com o *Intel-based*, no sentido

de criar um programa mais abrangente de deteção e resposta a ameaças, combinando alimentações padronizadas de inteligência de ameaças com ferramentas e processos personalizados, permitindo criar um programa de caça de ameaças mais poderoso e eficaz adaptado a necessidades específicas, uma vez que permite às organizações manter-se à frente das ameaças em evolução e identificar e responder proactivamente a potenciais incidentes de segurança.

2.2.4 *Frameworks*

2.2.4.1 *MITRE ATT&CK*

MITRE ATT&CK é uma base de conhecimentos globalmente acessível de táticas e técnicas adversárias baseadas nas observações do mundo real e fornece uma matriz de táticas e técnicas utilizadas pelos atores de ameaça, para atacar os sistemas e dados de uma organização (Walkowski, 2021). A matriz *ATT&CK* é uma ferramenta gratuita que as organizações dos sectores público e privado de todas as dimensões e indústrias adotaram amplamente, sendo utilizada pelas equipas de segurança como uma ferramenta para melhorar as suas capacidades de deteção e resposta a ameaças, fornecendo uma linguagem e um quadro comum para a discussão e análise de ameaças. A matriz encontra-se dividida em vários níveis de categorias de ataque que vão desde as atividades pré-ataque, tais como: acesso inicial, métodos de execução, incluindo *malware*, armação de documentos, técnicas de evasão de defesa, como a ofuscação do aumento de privilégios, acesso a credenciais e movimento lateral.

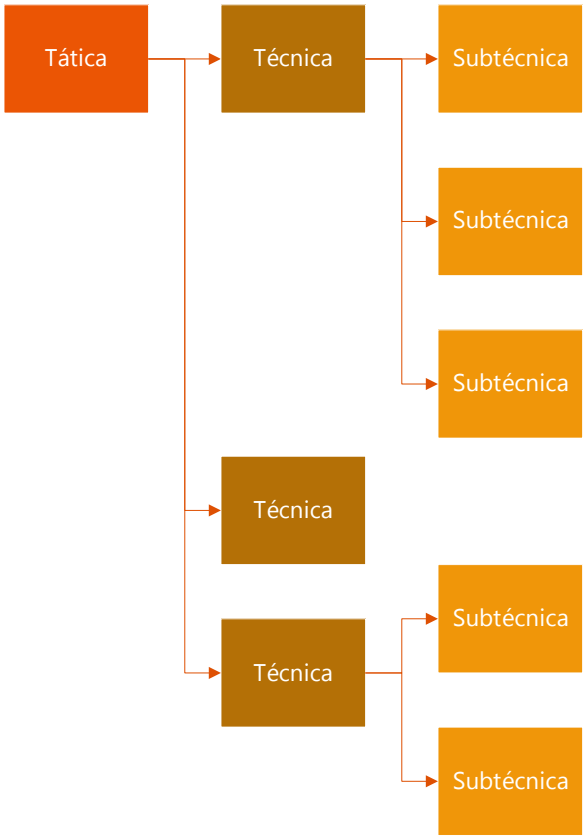

Figura 6 - Representação das colunas da matriz ATT&CK. Adaptado de Walkowski (2021).

Esta *framework* inclui uma gama de IOC para cada TTP, incluindo indicadores baseados em rede, indicadores baseados em *hosts*, e indicadores comportamentais, baseado nas seguintes componentes:

- Táticas: Descreve os objetivos técnicos imediatos que os atores de ameaça estão a tentar alcançar, como a obtenção do acesso inicial, manutenção da persistência ou estabelecimento do comando e o controlo. Invariavelmente, os atacantes têm de utilizar várias táticas para concluir com êxito um ataque.

- Técnicas: Descreve os métodos que os atores de ameaça usam para alcançar uma tática. Todas as táticas em cada matriz têm várias técnicas; a matriz *Enterprise* divide algumas técnicas em subtécnica. Um exemplo disto é a técnica pela procura de informação em bases de dados técnicas, sendo cinco as subtécnicas associadas descritas na seguinte figura.

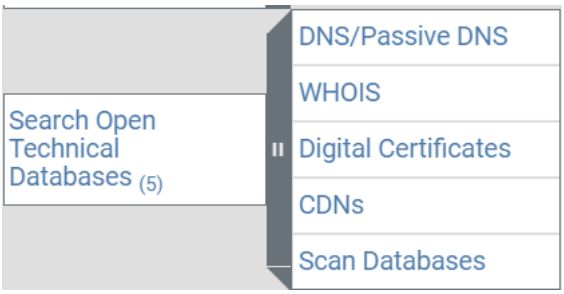

Figura 7 - Técnica de reconhecimento "Search Open Technical Database" da matriz ATT&CK Matrix for Enterprise. (CISA, 2021)

- Procedimentos: Descreve as implementações específicas das técnicas e subtécnicas utilizadas pelos APTs ou pode referir-se a *malware* específico ou outras ferramentas utilizadas pelos atores de ameaça.

2.2.4.2 *OWASP*

OWASP é o acrónimo de *Open Web Application Security Project*, e apresenta-se como uma organização sem fins lucrativos dedicada a melhorar a segurança do *software*. A estrutura OWASP é uma coleção de ferramentas, guias, e melhores práticas que ajudam os programadores a criar aplicações web seguras cada vez mais seguras (Bhardwaj, 2022).

O OWASP *Framework* inclui o OWASP Top 10, enumerando uma lista dos dez riscos mais críticos de segurança das aplicações web, incluindo por exemplo ataques por injeção, o Cross Site *Scripting* (XSS), *broken authentication* a gestão de sessões, permitindo por exemplo um ator de ameaça recolher dados de *login* de um utilizador, ou forjar dados de sessão, tais como *cookies*, para obter acesso não autorizados.

Para além do OWASP Top 10, a Estrutura OWASP também inclui o Guia de Testes OWASP, que pode ser não só uma referência útil, por exemplo, ao compreenderem os riscos de segurança mais comuns das aplicações web, fornecendo diretrizes e melhores práticas para testar a segurança das aplicações web, relevantes para as plataformas SIEM, ajudando a garantir que os sistemas são configurados para detetar e responder a determinados riscos. O OWASP pode ser utilizado em conjunto com uma plataforma SIEM, incluindo integrações incorporadas com ferramentas OWASP, tais como o OWASP ZAP (*Zed Attack Proxy*) ou a Verificação de Dependência OWASP, que pode ser utilizada para procurar vulnerabilidades em aplicações e gerar relatórios que podem ser consumidos pelo sistema SIEM (Pham B, 2020).

2.3 Cibersegurança nas PME

Portugal tem realizado progressos significativos na área da cibersegurança, com o governo e o sector privado a tomarem medidas no sentido de melhorar as defesas cibernéticas do país. Prova disso, é o forte avanço na classificação do índice Global de Cibersegurança, passando da posição 42º, na Edição de 2018, para a 14º posição, na Edição de 2021 (Andrade, 2021). Adicionalmente, foram criadas várias entidades, nomeadamente o Centro Nacional de Cibersegurança (CNCS), para coordenar os esforços nacionais de prevenção, deteção e resposta às ameaças cibernéticas, desenvolvendo uma estratégia nacional de cibersegurança destinada a melhorar a resiliência cibernética do país.

Apesar destes esforços, as empresas portuguesas ainda enfrentam uma série de desafios em matéria de cibersegurança potenciadas não só pela pandemia (COVID-19), como também pelo reforço da digitalização em algumas indústrias e pela instabilidade geopolítica (Ferreira, 2022), destacando-se os seguintes:

- Falta de sensibilização: Muitas empresas em Portugal ainda não compreendem totalmente a importância da cibersegurança ou o potencial impacto de um ataque cibernético, podendo levar a uma falta de investimento em medidas de cibersegurança, falta de formação e sensibilização dos empregados.
- Cibercriminalidade: Como muitos outros países, Portugal enfrenta uma ameaça crescente desta criminalidade, onde são utilizadas técnicas sofisticadas para atingir empresas e indivíduos e que podem resultar em perdas financeiras significativas, danos à reputação, e consequências legais e regulamentares.
- Regulamentação: As empresas em Portugal estão sujeitas a uma série de regulamentos de cibersegurança da UE e nacionais, que podem ser complexos e difíceis de implementar. O não cumprimento destes regulamentos pode resultar em sanções e multas significativas.
- Falta de competências: Escassez de profissionais de cibersegurança, o que poderá ser uma potencial dificuldade para as PME recrutarem o talento necessário para implementar medidas eficazes na defesa de ameaças cibernéticas.

Além destes desafios, é revelante perceber como têm evoluído os ataques às PME, sendo que em 2022, 61% de todos os ciberataques visaram especificamente as PME (IT SECURITY, 2023), e onde no ano anterior o CNCS registou 847 ataques no primeiro semestre de 2021, um aumento de 23% em comparação com 2020 e um aumento de 124% relativamente a 2019 (Fernandes, 2021).

2.3.1 PME

Em Portugal, a definição de PME está estabelecida no Decreto-Lei n.º 372/2007, de 6 de novembro, que adapta a Recomendação da Comissão Europeia 2003/361/CE, de 6 de maio de 2003. Este decreto-lei define os critérios para a classificação de micro, pequenas e médias empresas com base no número de empregados e no volume de negócios ou balanço total anual DR (2007). As definições são as seguintes:

- Microempresa:
  Número de empregados: Menos de 10, Volume de negócios anual: Até 2 milhões de euros. Balanço total anual: Até 2 milhões de euros.
- Pequena Empresa:
  Número de empregados: Menos de 50. Volume de negócios anual: Até 10 milhões de euros. Balanço total anual: Até 10 milhões de euros.
- Média Empresa:
  Número de empregados: Menos de 250. Volume de negócios anual: Até 50 milhões de euros. Balanço total anual: Até 43 milhões de euros.

Estas definições ajudam a categorizar as empresas para efeitos de políticas de apoio, financiamento, regulamentação e estatísticas econômicas.

No período atual, são várias as entidades quer ao nível nacional ou europeu, com atuação devidamente regulamentada, que produzem documentação baseadas em recomendações nesta matéria, também aplicáveis às PME, descritas nos seguintes subcapítulos.

2.3.2 Centro Nacional de Cibersegurança

Tendo sido criado a 6 de outubro de 2014, na altura designado por CNCSeg, dentro do Gabinete Nacional de Cibersegurança e através do Decreto-Lei n.º 69/2014, de 9 de maio (PGDL, 2014) o CNCS adquire a sua designação atual através do Decreto-Lei n.º 136/2017, de 6 de novembro (PGDL, 2017). Atuando como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança, o seu *website* fornece informações sobre políticas e iniciativas em Portugal com importância relevante nesta matéria (CNCS A, 2023).

2.3.3 Roteiro para as Capacidades Mínimas de 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 especial enfoque nas pequenas e médias empresas. Nesse modelo, denominado por "Roteiro para as Capacidades Mínimas em Cibersegurança" (CNCS B, 2023), apresenta um conjunto de ações, sendo uma de especial relevância para esta dissertação, a A 2.5 – Recolha centralizada de registos (*logs*), realçando a importância desta metodologia como o principal instrumento de análise e investigação de um incidente de cibersegurança e a ação A 3.8 "Instalação e configuração de um *Security Information and Event Management* (SIEM)" visando a facilitação da análise em tempo real e acelerando a tomada de ações defensivas.

2.3.4 Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

A Equipa Portuguesa de Resposta a Emergências Informáticas (CERT.PT) fornece informações sobre ameaças e vulnerabilidades de segurança cibernética em Portugal, contendo notas e informações relevantes para o panorama geral das ameaças, no seu RFC 2350 (CNCS C, 2023).

2.3.5 Comissão Nacional de Proteção de Dados

A Comissão Nacional de Proteção de Dados (CNPD) oferece informações sobre a regulamentação em matéria de cibersegurança e o seu cumprimento em Portugal. A CNPD controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019 (PGDL, 2019), da Lei 59/2019 (PGDL, 2019) e da Lei 41/2004 (PGDL, 2004), bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias dos pessoais singulares no âmbito dos tratamentos dos seus dados pessoais. A CNPD promove e emite também orientações às empresas sobre medidas de segurança a adotar em caso de ciberataque, no sentido de minimizar as consequências e salvaguardar os direitos das pessoas (Lusa, 2023).

2.3.6 Agência Europeia para a Segurança das Redes e da Informação

A ENISA representa a Agência da União Europeia para a cibersegurança e é um centro de especialização que apoia os estados membros e instituições da UE na área da cibersegurança. A

ENISA foi criada em 2004, e desde então tem desempenhado um papel importante na promoção da cibersegurança e resiliência em toda a UE. O principal objetivo da ENISA é melhorar as capacidades cibernéticas dos estados membros e instituições da UE, e melhorar o nível global em toda a Europa (Mishra, 2021), através da prestação dos seguintes serviços:

- Aconselhamento sobre políticas e legislação de cibersegurança da UE.
- Apoio ao desenvolvimento de estratégias e capacidades nacionais de cibersegurança.
- Realização de investigação e análise sobre questões e tendências da cibersegurança.
- Facilitar a partilha de informação e a colaboração entre estados membros e instituições da UE.
- Prestar assistência técnica e conhecimentos especializados aos estados membros e instituições da UE.

A título de exemplo, a ENISA faz referência no documento "*Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*" o uso das plataformas SIEM, categorizada no nível de sofisticação 2, integrado nas medidas de segurança e procedimentos padrão da indústria para deteção e resposta a incidentes em 2016 e reconhecendo em 2022 a função *Cybersecurity* SIEM *Manager*, na versão *Draft* do *European Cybersecurity Skills Framework*.

2.4 *System Information and Event Management* (SIEM)

Uma plataforma de gestão da informação e eventos de segurança (*System Information and Event Management* - SIEM) é um *software* que melhora a conscientização de segurança nos ambientes das tecnologias da informação, combinando a gestão das informações de segurança (SIM) e a gestão dos eventos de segurança (SEM) (Fruhlinger, 2022). As soluções SIEM elevam a deteção de ameaças, a conformidade e a gestão de incidentes de segurança por meio da recolha e análise de eventos de segurança em tempo real, sendo os ficheiros de log a principal fonte de dados para a capacidade de observação da rede, sendo que são gerados por computador e que contém informações sobre padrões de uso, atividades e operações num determinado sistema operativo, aplicativo, servidor ou outro dispositivo.

2.4.1 Características

Podemos considerar como características básicas de um sistema de Gestão de Informação e Eventos de Segurança (SIEM) as seguintes:

- Recolha e análise em tempo real de dados relacionados com a segurança de várias fontes, tais como dispositivos de rede, servidores e aplicações.

- Correlação de eventos de segurança para identificar potenciais ameaças ou ataques de segurança.

- Capacidade de gerar alertas e notificações para atividades ou incidentes suspeitos.

- Gestão e armazenamento centralizado de registos e eventos de segurança para relatórios de conformidade e análise forense.

- Integração com outras ferramentas de segurança, tais como *firewalls*, sistemas de deteção de intrusão, e *scanners* de vulnerabilidade.

- Capacidade de análise do comportamento de utilizadores e entidades (UEBA) para detetar anomalias e atividade invulgar.

- Regras personalizáveis e motores de correlação para apoiar requisitos de segurança específicos.

- Relatórios e visualizações avançadas para a análise de dados de segurança.

- Escalabilidade para lidar com grandes quantidades de dados de segurança.

- Medidas de segurança robustas para assegurar a confidencialidade e integridade dos dados de segurança.

2.4.2 Arquitetura

A arquitetura de uma plataforma SIEM (*Security Information and Event Management*) refere-se à conceção e implementação de um sistema de segurança, que agrega e analisa dados relacionados com a segurança de múltiplas fontes em tempo real. A arquitetura típica do SIEM inclui os seguintes componentes (Laue, 2022):

- Recolha de dados: Relacionados com a segurança provinda de várias fontes, tais como dispositivos de rede, servidores, aplicações e ferramentas de segurança. Os dados recolhidos são depois normalizados, enriquecidos e filtrados com o objetivo de remover duplicados e informações irrelevantes.

- Armazenamento de dados: Responsável pelo armazenamento dos dados recolhidos e processados relacionados com a segurança num repositório centralizado. Isto permite às equipas de segurança aceder e analisar os dados conforme necessário.

- Mecanismo de correlação: Responsável pela análise dos dados de segurança recolhidos e pela geração de eventos de segurança com base em regras e políticas pré-definidas. O motor de correlação, através da aplicação de algoritmos, identificando padrões e relações nos dados, que ajudam a identificar potenciais ameaças e incidentes de segurança.

- Gestão de eventos: Gere e prioriza dos eventos de segurança gerados nos equipamentos, é usado para automatizar muitas das tarefas manuais associadas à resposta a incidentes, tais como ativar alertas e gerar relatórios.

- Relatórios e análises: Com objetivo na visibilidade em tempo real da postura de segurança, é utilizado para gerar relatórios históricos e analisar tendências em dados relacionados com a segurança.

- Integração com outras ferramentas de segurança: A arquitetura SIEM tipicamente permite a integração com outras ferramentas de segurança, tais como sistemas de deteção de intrusão (IDS), *firewalls*, e ferramentas de gestão de informação e eventos de segurança (SIEM).

As arquiteturas modernas de SIEM, neste contexto, ganham um papel de extrema relevância, no sentido de fornecer às equipas de segurança visibilidade em tempo real da postura de segurança da organização, ao agregar e analisar dados relacionados com a segurança de múltiplas fontes, permitindo identificar com maior rapidez as potenciais ameaças à segurança informática, garantindo uma resposta a incidentes de segurança mais eficaz, quando comparado com as ferramentas tradicionais (Pham A, 2020).

2.4.3 Modelos de serviço

Uma solução de Gestão de Informação e Eventos de Segurança (SIEM) pode ser oferecida como um serviço através de diferentes modelos (Simmons, 2019), como por exemplo:

- *On-Premises* ou instalação local: A solução é instalada e mantida na própria infraestrutura da empresa ou organização.

- Alojado na nuvem (*cloud*): A solução é alojada e mantida por um fornecedor externo e acedida através da nuvem, fornecida sob modelo *software as a service* (SaaS).

- SIEM gerido: A solução é gerida por um terceiro fornecedor, que se encarrega da sua instalação, configuração e manutenção.

- SIEM Híbrido: Uma combinação de SIEM *On-Premises* e SIEM baseado na nuvem, aproveitando os benefícios de ambos os modelos.

2.4.4 Integrações com outras ferramentas de segurança

A integração da Informação de Segurança e Gestão de Eventos (SIEM) com outras ferramentas de segurança pode fornecer às organizações uma estratégia mais abrangente e eficaz de cibersegurança, mais presente nas apelidadas de *Next-Generation* SIEM (Stone, 2022), distinguindo-se pela sua capacidade na deteção de atividade anómala em múltiplas redes e sistemas, identificação dos atores maliciosos e as suas atividades, pela monitorização das alterações nos padrões de tráfego da rede e na ingestão de *terabytes* de dados de forma rápida e eficiente. Alguns exemplos de como estas plataformas SIEM podem ser integradas com outras ferramentas de segurança:

- Deteção e Resposta de Pontos Finais (*Endpoint Detection and Response*): Integração com soluções de EDR para proporcionar visibilidade em tempo real na atividade de rede, detetando e respondendo a ameaças ao nível do dispositivo, permitindo uma procura proactiva às ameaças e uma resposta a incidentes mais eficiente.

- *Firewall*: O SIEM pode ser integrado com *firewalls* para fornecer monitorização em tempo real do tráfego da rede e identificar potenciais ameaças. Esta integração pode ajudar as organizações a detetar e bloquear o tráfego malicioso e impedir a exfiltração de dados.

- Gestão de Identidade e Acesso (IAM): Integração com soluções IAM para monitorizar a atividade dos utilizadores e identificar potenciais ameaças ou comportamentos suspeitos. Esta integração visa detetar e responder a ameaças internas ou a contas de utilizadores comprometidas.

- Inteligência de Ameaças: Integração com informações sobre ameaças para fornecer informações em tempo real sobre ameaças e vulnerabilidades emergentes, identificando e mitigando proactivamente potenciais ameaças.

2.5 O papel da tecnologia SIEM no contexto *Threat hunting*

Esta tecnologia desempenha um papel relevante, ao proporcionar a capacidade de identificar e responder rapidamente a potenciais ameaças à segurança, através da combinação e análise de grandes quantidades de dados de registo de várias fontes. Várias possíveis aplicabilidades da tecnologia na procura de ameaças, são descritos nos seguintes pontos-chave (Vincent, 2022):

- Correlação de eventos: como por exemplo, *firewalls*, sistemas de deteção de intrusão, e *software* de proteção de *endpoints*, para ajudar a detetar ameaças que podem não ser facilmente visíveis num só registo isolado.

- Deteção de ameaças: As configurações para detetar ameaças e anomalias conhecidas, tais como infeções por *malware*, padrões de tráfego de rede suspeitos, e tentativas de acesso não autorizado, através da aplicação de regras e algoritmos predefinidos.

- Investigação e resposta: Fornecer um repositório centralizado de dados de registo de segurança que podem ser facilmente pesquisados e analisados, facilitando às equipas de segurança a investigação e resposta a potenciais incidentes de segurança.

- Ameaça de inteligência: Integrado com informações sobre ameaças para fornecer informações em tempo real sobre ameaças novas e emergentes, permitindo às equipas de segurança tomar medidas proactivas para proteger a sua organização.

Assim, destaca-se como principais capacidades, a agregação, análise e corelacionamento de dados de segurança de múltiplas fontes em tempo real, permitindo as equipas de segurança a identificar e responder rapidamente a potenciais ameaças à segurança.

3. Metodologia de aplicação

O modelo escolhido para metodologia aplicada foi o modelo de gestão de alteração *Lewin´s*, desenvolvido em 1940 por *Kurt Lewin*, aplicado ainda aos dias de hoje, sendo uma *framework* amplamente usada para compreender e gerir alterações organizacionais, composto por 3 fases, descongelamento, mudança e congelamento, promovendo em todo o processo o envolvimento dos *stakeholders* (Malik, 2022).

Neste processo, foram identificadas as seguintes fases e objetivos no contexto da empresa, críticas para a obtenção da mudança:

1. Alteração do comportamento e as competências do grupo de trabalho.
2. Alterar os processos, estruturas e sistemas da organização.
3. Mudança da cultura da organização.
4. Alteração da tecnologia utilizada.
5. Avaliação dos resultados.

Na primeira fase, foram reunidas várias áreas tecnológicas da empresa, endereçando algumas dificuldades já decorrentes da operação e previamente identificadas, sendo elas:

- Dificuldade na identificação de um determinado serviço na infraestrutura informática, na ocorrência de incidentes.
- Análise de *Logs* complexa e demorada, devido à dispersão da informação.
- Processo moroso relativo à correlação da informação obtida de várias fontes e tecnologias.
- Inexistência de uma componente de integração automática de inteligência a ameaças.

Identificada a necessidade de mudança e consequente preparação de todos os *stakeholders*, deu-se inicio à segunda fase, denominada por Mudança, envolvendo implementação do protótipo para a recolha, monitorização e correlação dos eventos da atividade da rede e dos *logs* de sistema para comportamentos anómalos com o objetivo de mitigar as dificuldades supracitadas e indicar a presença de uma ameaça, incidindo a nossa análise nas ligações IP, atividade de processos e pedidos DNS através dos IOC comummente conhecidos, através da utilização de técnicas para analisar grandes quantidades de dados em tempo real e identificar padrões de atividade que

possam ser indicativos de uma ameaça, analisando os resultados das pesquisas da plataforma SIEM com os principais IOC´s, considerando os mais relevantes para este protótipo, os seguintes:

Indicador Chave de Risco	Risco	Probabilidade	Impacto
Total de registos de *Log* por segundo.	Médio	Baixa	Médio
Inícios de sessão remotos falhados.	Alto	Alta	Baixo
Inícios de sessão com credenciais de administração	Alto	Baixa	Alto
***Restart / Shutdown* do Sistema Operativo**	Médio	Baixa	Médio
Tráfego com origem/destino suspeito	Médio	Média	Médio
Uso de portas incomuns	Médio	Média	Alto

Tabela 1 - Indicies de comprometimento para o ambiente escolhido. Fonte: Autor

Relativamente à razão para o uso do SIEM da *Graylog*, adveio por uma questão histórica, motivada inicialmente pela necessidade em centralizar os *logs* das aplicações de negócio, para uma posterior análise e correlação, conferindo independência aos sistemas em produção, reduzindo também a probabilidade de qualquer impacto no desempenho. Os seguintes pontos pretendem descrever a metodologia aplicada, com o objetivo de demonstrar a utilidade da tecnologia SIEM em contexto real, possibilitando a deteção de possíveis ameaças cibernéticas, focando-se especialmente nos estágios iniciais das ameaças, através de numa análise incisiva ao tráfego das comunicações TCP/IP.

4. Protótipo

4.1 Configuração da plataforma SIEM

Este subcapítulo pretende descrever uma visão geral de como a plataforma SIEM foi configurada, incluindo que fontes de registo (*log*) foram recolhidas, que alertas foram configurados, e que *feeds* de inteligência de ameaças foram integrados.

4.1.1 Especificação e planeamento

Depois de especificados os requisitos e definidos os objetivos da plataforma SIEM, foi selecionada a aplicação *Graylog*, tendo em conta a dispersão dos sistemas operativos das fontes de registo (*logs*) que careciam de integração no sistema, maioritariamente *Unix, Linux e Windows*. Nesta fase é importante uma correta identificação do inventário de ativos, garantindo a maior abrangência possível, senão a sua totalidade. Neste caso de estudo, o inventário foi realizado através também de uma plataforma *Open-Source, OCS Inventory*, no APÊNDICE VI – Plataforma *OpenSource OCS Inventory*, o *software* de gestão de inventário de computadores e redes de código aberto, que permite recolher informações sobre bens de *hardware* e *software* em computadores em rede e outros dispositivos, incluindo servidores, impressoras, e dispositivos móveis. Com esta plataforma, após a identificação e registo de todos os ativos de rede, o processo de identificação torna-se muito mais simples, na medida em que teremos toda a informação sobre o ativo, caso seja conhecido na rede.

4.1.2 Instalação da plataforma SIEM

Uma vez selecionada a solução SIEM, o passo seguinte foi instalar a plataforma SIEM no servidor designado para o efeito, sendo que neste caso foi optado por uma instalação minimalista, apenas com uma instância, de modo a tornar esta solução o menos complexa possível. Sendo o *Graylog* uma aplicação *Open Source*, a base do sistema operativo escolhido foi o *Ubuntu*, versão 22.04, devido não só a familiaridade e conhecimento prévio no âmbito da experiência profissional do autor, que aliado à existência de um manual de instalação disponibilizado pelo próprio fabricante do *software*, revelou-se a decisão mais adequada. O processo de instalação foi bastante simples e envolveu a execução de um conjunto de comandos e scripts, assim como a configuração das configurações básicas do sistema disponibilizadas pelo fabricante (*https://go2docs.graylog.org/50/downloading_and_installing_graylog/ubuntu_installation.html*)
.

4.1.3 Configuração dos *logs*

Após a instalação da solução SIEM, o passo seguinte foi ativar e configurar as fontes de registo para o encaminhamento dos *logs* para os respetivos *inputs* da plataforma SIEM. Incluiu configurar o reencaminhamento do registo nos dispositivos que geram os dados de registo, como por exemplo *firewalls*, servidores e terminais, configurando a solução SIEM para receber e processar os dados de registo através dos *inputs* criados para o efeito e descritos em maior detalhe no capítulo (5.2.2 *Inputs*). Como amostra, foram selecionados cerca de 40 equipamentos, entre servidores *front* e *back-end*, *switch´s* e *firewalls*, que compõem a rede de uma empresa de desenvolvimento de *software*, servindo por isso de um exemplo em contexto real, descritos na tabela 2.

Tipo	Função	Quantidade
Virtual Server	*Application Server*	10
Virtual Server	*WebServer*	8
Virtual Server	*DatabaseServer*	6
Virtual Server	*Email Server*	3
Physical Server	*Hypervisor*	8
Virtual Server	*Domain Controller*	4
Network Device	*Firewall*	3
Network Device	*Access Point*	8

Tabela 2 - Tabela de tipos e quantidades de equipamentos configurados. Fonte: Autor

4.1.4 Normalização dos *logs*

Após o encaminhamento dos registos *log*, em alguns casos foi necessário proceder à sua normalização. Apesar de existirem normas bem conhecidas, as fontes de registo variam muito no formato e esquema, tornando difícil a execução de consultas padrão para coisas como um IP de fonte específica quando esse campo pode aparecer de muitas maneiras diferentes dependendo dos registos: *source_ip, srcip, src_ip, originating IP*, entre outros. Neste sentido, foram criadas regras de *pipeline* para renomear todos estes campos semelhantes para um nome de campo padrão, processo este que se chama tipicamente normalização do processo, conforme APÊNDICE II – Extratores configurados a normalização dos Logs configurados para a normalização dos *Logs*.

4.1.5 Criação de regras

Uma vez configuradas as fontes de registo, o passo seguinte foi a criação de regras SIEM, que serão utilizadas para analisar os dados de registo e gerar alertas. Esta fase implica definir as condições que devem ser cumpridas para que um alerta seja gerado, tal como um evento específico que ocorra num dispositivo específico. Por exemplo, a definição de um alerta sempre que uma conta de domínio fosse bloqueada. Os alertas especificados e definidos para a análise no contexto desta dissertação estão descritos na tabela 3.

Tipo de Alerta	Parametrização
Reinício de servidor	winlogbeat_event_code:1074
Uso de conta de administração	winlogbeat_winlog_event_data_TargetUserName:*
Bloqueio de conta	Pesquisa e alerta pelo evento: winlogbeat_event_code:4740
Nº excessivo de inícios de sessão falhados	Nº de eventos winlogbeat_event_code:4625
Certificado expirado	winlogbeat_event_code must match exactly 64 and winlogbeat_log_level must match exactly warning

Tabela 3 - Tabela de alertas configurados. Fonte: Autor

4.1.6 Teste

Após a criação das regras SIEM, procedeu-se ao teste do sistema para assegurar que está a receber e a processar corretamente os dados de registo, gerando alertas, e tomando as ações definidas, envolvendo por isso a simulação de vários eventos de segurança e a validação de que a solução SIEM está a detetar e a alertar sobre esses eventos, presentes no APÊNDICE III – Histórico de alertas e eventos.

4.1.7 Integração com inteligência de ameaças

Finalmente, integrar as informações de ameaças no sistema SIEM, através do uso de *feeds* que contêm informações sobre ameaças, no sentido de aumentar as capacidades de deteção e

melhorar a precisão dos alertas. Embora existam inúmeros, para este projeto foram integrados os seguintes:

- Geolocalização (GeoIP): A recolha de registos log que contêm endereços IP é bastante comum, deste as *firewalls*, servidores *web*, rede *Wi-Fi* e dispositivos terminais, inclusive endereços IP públicos. Ter dados adicionais sobre esses registos, nomeadamente a Geolocalização do endereço IP, ajuda a investigar e compreender os padrões de tráfego da rede. Por exemplo, se conseguirmos apresentar os registos num mapa mundial, é possível identificar rapidamente comunicações com países com os quais não comunicamos habitualmente, detetando rapidamente comunicações suspeitas, em maior detalhe no APÊNDICE V – Configuração do GEO IP no *Graylog*.

- Informação de registo Whois (*Whois for IP's*): É um protocolo de resposta utilizado para consultar as bases de dados que contêm a informação dos utilizadores registados relativos aos endereços IP. O mesmo protocolo de consulta é utilizado para consultar as bases de dados que contêm a informação do nome de domínio e que tipicamente tem uma série de informação associada, como por exemplo: Informações de contacto do proprietário de um endereço IP; A informação sobre o Registo Regional da Internet (RIR) que atribui o endereço IP dado; Os números do sistema autónomo (AS); O proprietário designado, informações de contacto, localização, e os detalhes da comunicação de abusos; O número total de endereços IP atribuídos no bloco ou blocos atribuídos ao proprietário do IP em questão.

- Deteção de *malware* (*Greynoise*): Através do uso de *plugins*, foi possível a integração com a plataforma *Greynoise* para partilhar e solicitar indicadores de comprometimento (*IoCs*) associados a diferentes estirpes de *malware*, analisando se os *IP's* ou domínios de origem das ligações registadas estão referenciados nas respetivas listas por uso habitual de *malware*, representado no APÊNDICE IV – Configuração da *API Greynoise*, categorizando o tráfego como benigno, malicioso ou desconhecido.

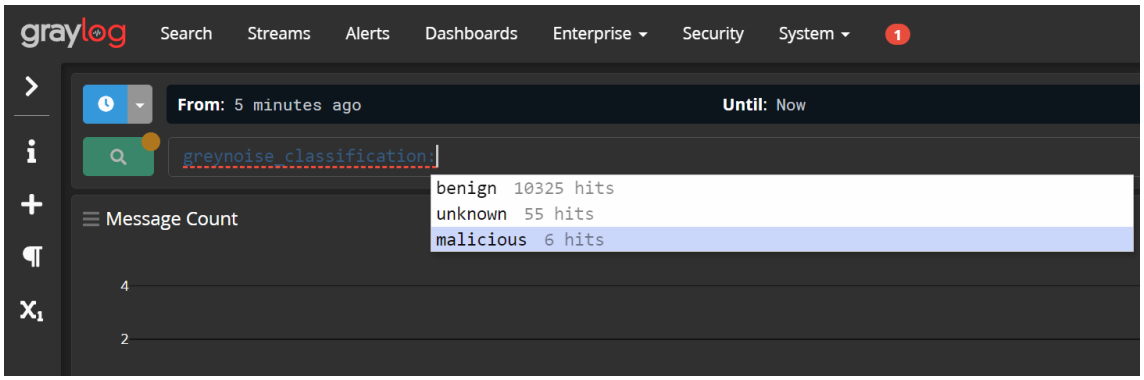

Figura 8 - Classificação do tráfego pela API Greynoise. Fonte: Autor

• *Allienvault OTX*: Esta plataforma permite aos utilizadores partilhar e aceder a informações sobre agentes de ameaça, IoC´s e outros dados relacionados com cibersegurança. Os utilizadores podem contribuir com a sua própria inteligência, subscrever *feeds* de outros utilizadores, e aceder a informações públicas e privadas sobre ameaças a partir de uma variedade de fontes. Uma das principais características do *AlienVault OTX* é a sua capacidade de fornecer contexto para ameaçar os dados das informações. A plataforma utiliza aprendizagem mecânica e outras técnicas para analisar e correlacionar dados de ameaças de múltiplas fontes, ajudando os utilizadores a identificar padrões e ligações que de outra forma poderiam ser negligenciados. Para além das suas capacidades de partilha de informações sobre ameaças, *AlienVault OTX* inclui também uma série de outras características, tais como deteção e resposta automatizada a ameaças, orquestração e automatização de segurança, e gestão de vulnerabilidades. Estas características permitem às organizações automatizar e racionalizar as suas operações de cibersegurança, melhorando a sua postura global de segurança.

4.2 Ferramentas tecnológicas

Neste projeto foi usada uma das ferramentas SIEM disponibilizadas no mercado, o *Graylog*, para agregar e centralizar todos os *logs* recolhidos de vários servidores, na sua grande maioria virtualizados, com o *hypervisor* da *Microsoft Hyper-V*. Na mesma vertente e para auxiliar na identificação das ameaças, são usadas outras plataformas tipicamente de acesso *Web* para confirmação das suspeitas, descritas comumente por ferramentas OSINT.

4.2.1 *Graylog*

Para estes casos práticos, foi configurada a versão mais simplicista do *Graylog*, de acesso gratuito, cuja arquitetura se encontra refletida na seguinte figura, sendo uma configuração mínima de que pode ser usada para configurações com menos exigência, não críticas ou neste caso, de

teste. Como nenhuma das componentes é redundante, torna-se relativamente fácil e rápida a configuração das componentes.

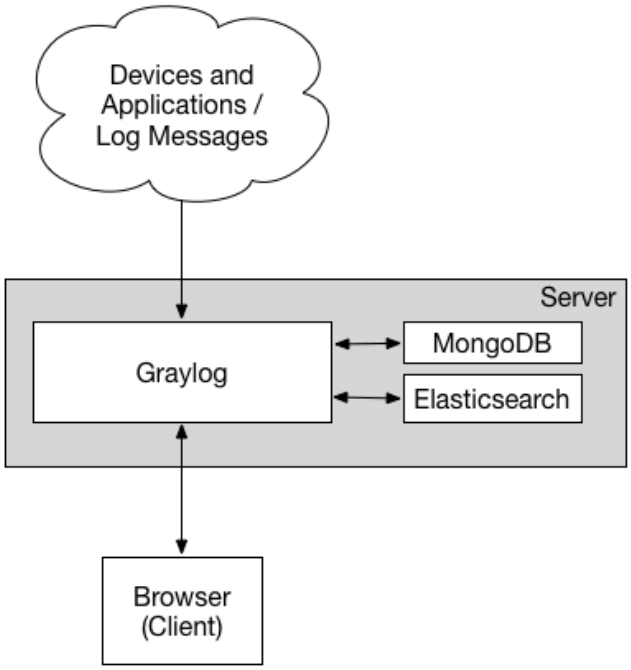

Figura 9 - Arquitetura Graylog. Fonte: Graylog (2021).

Numa visão mais lata da solução, a informação é recolhida através de agentes, sendo depois processada, indexada e armazenada centralmente numa base de dados num nó de dados, neste caso baseado em *Elasticsearch*. Este nó de informação permite indexar e pesquisar todas as mensagens na base de dados de mensagens do *Graylog*. Como os dados estão acessíveis a partir deste nó de dados, não está dependente de uma ferramenta de pesquisa independente, o que confere flexibilidade na personalização das próprias consultas de pesquisa. A componente *Graylog Server* situa-se no meio e funciona em torno do seu nó de dados, que é um motor de pesquisa de texto completo e não um sistema de gestão de *logs*, construindo também uma camada de abstração no topo, para disponibilizar o acesso aos dados, sem ter de selecionar índices e escrever filtros de seleção de intervalo de tempo. Neste sentido, é apenas suficiente a submissão da consulta de pesquisa. Para armazenar dados, o *Graylog* utiliza um motor de base-de-dados *opensource*, a *MongoDB*, onde serão registados os metadados, tais como informação do utilizador e configurações de fluxo.

4.2.2 *Inputs*

O *Graylog* injeta *logs* das aplicações, servidores, *routers* ou *switches* utilizando uma ou várias entradas. Estas entradas podem utilizar protocolos TCP ou UDP e podem receber diferentes

formatos de dados como GELF, CEF, *Syslog* ou RAW. Neste sentido foram criadas várias entradas dependendo do tipo de equipamento, protocolo e estrutura de *log*, em maior detalhe no APÊNDICE I – Inputs configurados para a recolha de dados.

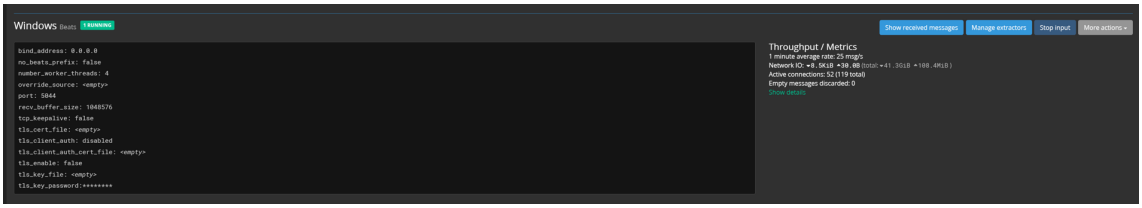

Figura 10 - Exemplo de um input do tipo Beats. Fonte: Autor

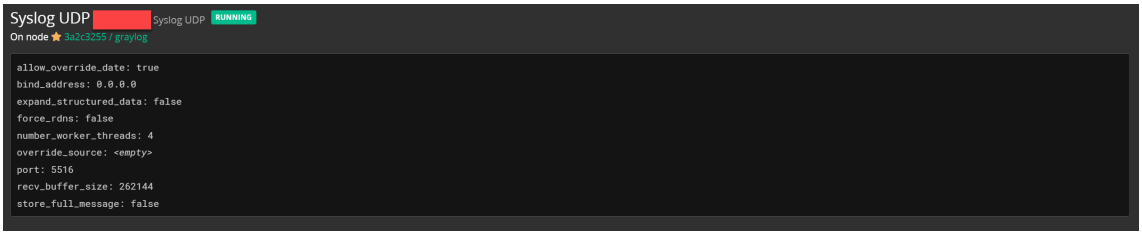

Figura 11 - Exemplo de um input do tipo Syslog UDP. Fonte: Autor

4.2.3 *Extractor*

Sendo que existem equipamentos ou aplicações que não cumprem as normas RFC3164, RFC5424, os extratores permitem extrair e normalizar os dados de qualquer texto da mensagem recebida (não importa de que formato ou se um campo já extraído) para campos de mensagens, para posterior indexação, conforme APÊNDICE II – Extratores configurados a normalização dos *Logs* e conforme exemplo na figura 14, que foi necessário proceder à extração dos campos IP de origem, IP de destino, Porto de origem e Porto de destino, para posterior indexação, conforme figura 16.

Figura 12 - Lista de extratores para um input em específico, neste caso uma firewall. Fonte: Autor

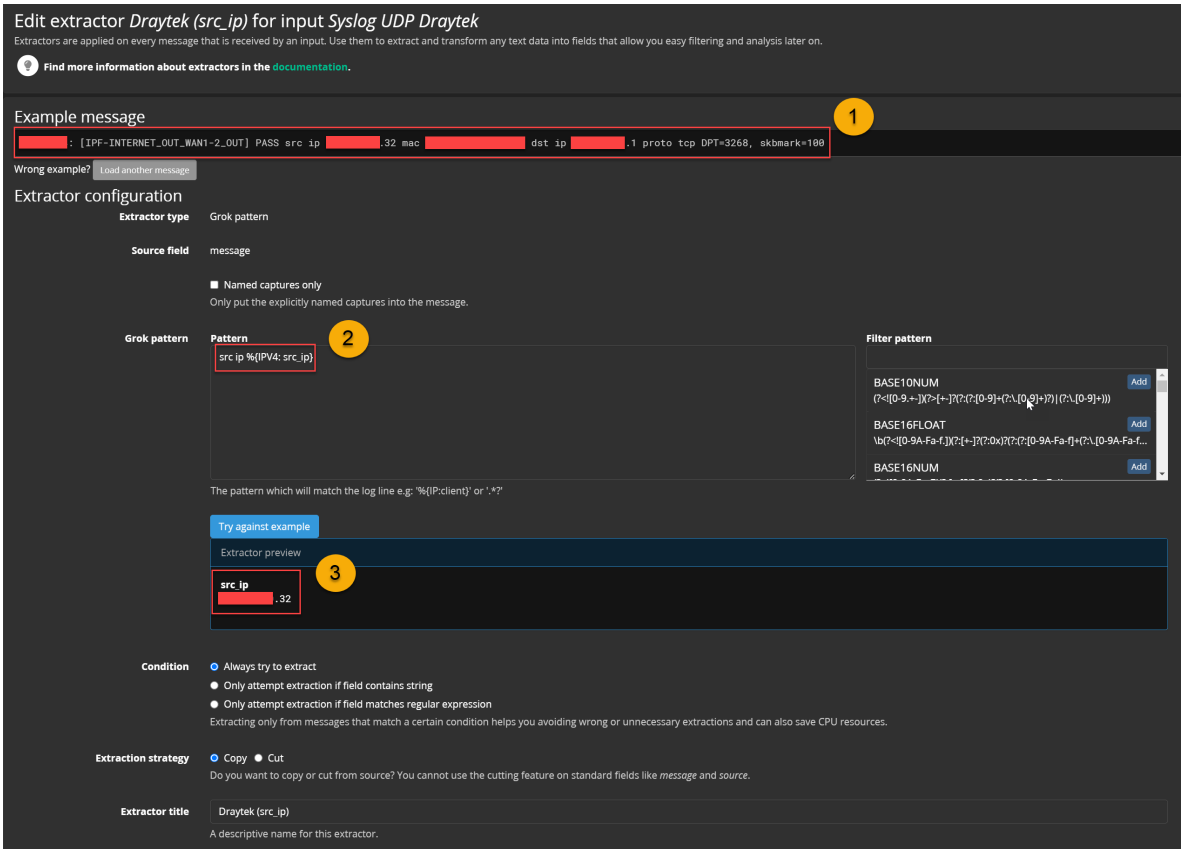

Figura 13 - Exemplo de um extrator para os logs de um equipamento de rede, neste caso uma firewall. Fonte: Autor

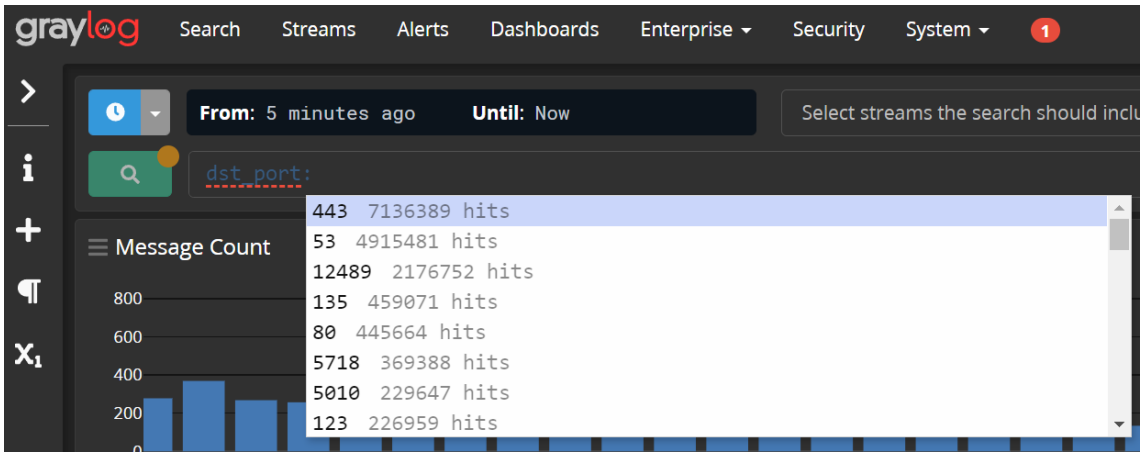

Figura 14 - Uso do porto de destino após normalização e indexação. Fonte: Autor

4.2.4 *Stream*

Uma *stream* (fluxo) é um mecanismo que encaminha as mensagens em categorias em tempo real enquanto estão a ser processadas. É possível definir regras na aplicação para encaminhar mensagens para determinados fluxos, dividindo e categorizando a informação. Para este projeto foram criadas várias, com a lógica de realizar divisão dependente da função ou tecnologia, de acordo com a figura 15, facilitando a pesquisa, como por exemplo, através da escolha da *Stream – Expired Certificates*, figura 16, teremos acesso imediato aos eventos relativos a servidores que estão a operar com certificados expirados. Para tal, foi necessário criar a *Stream* com as regras definidas na figura 17.

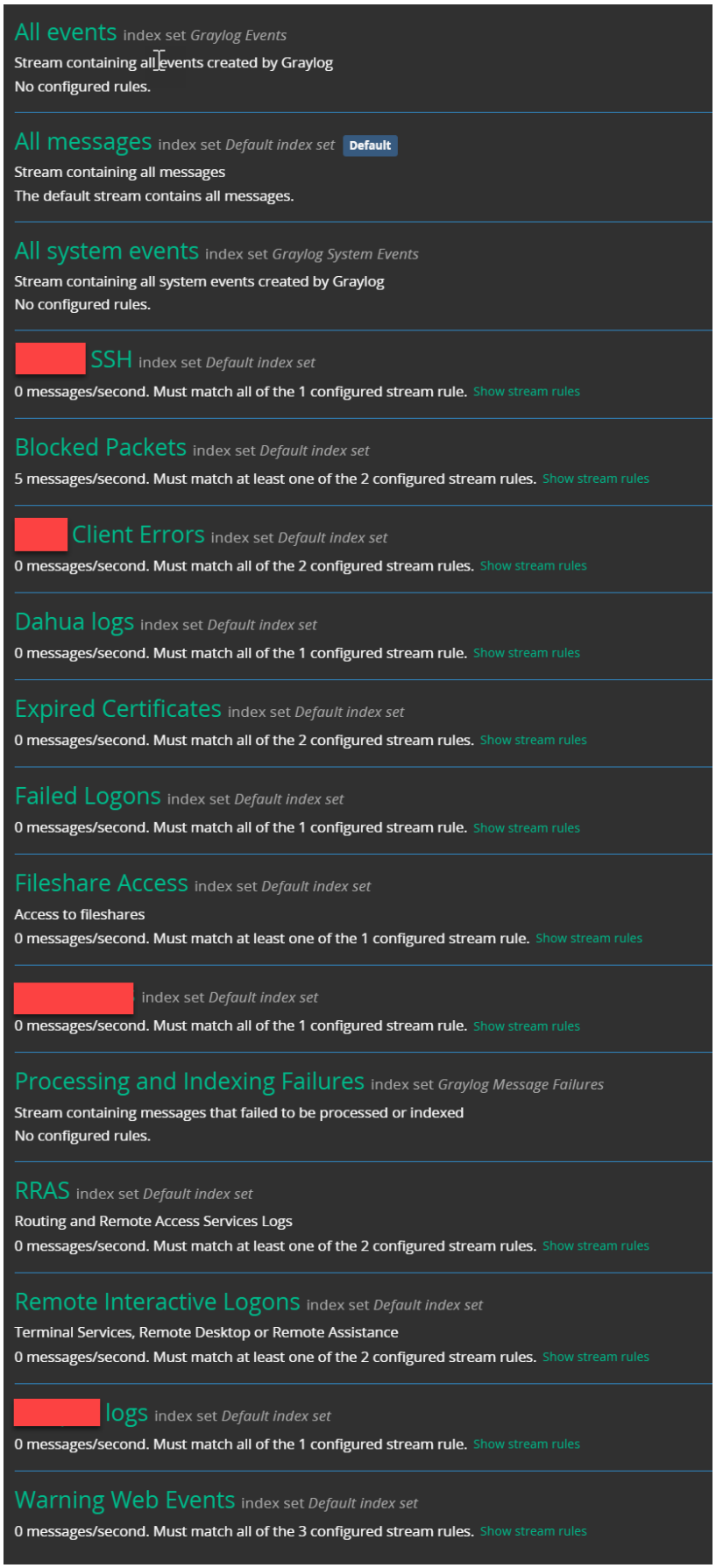

Figura 15 - Streams configurados para este projeto. Fonte: Autor

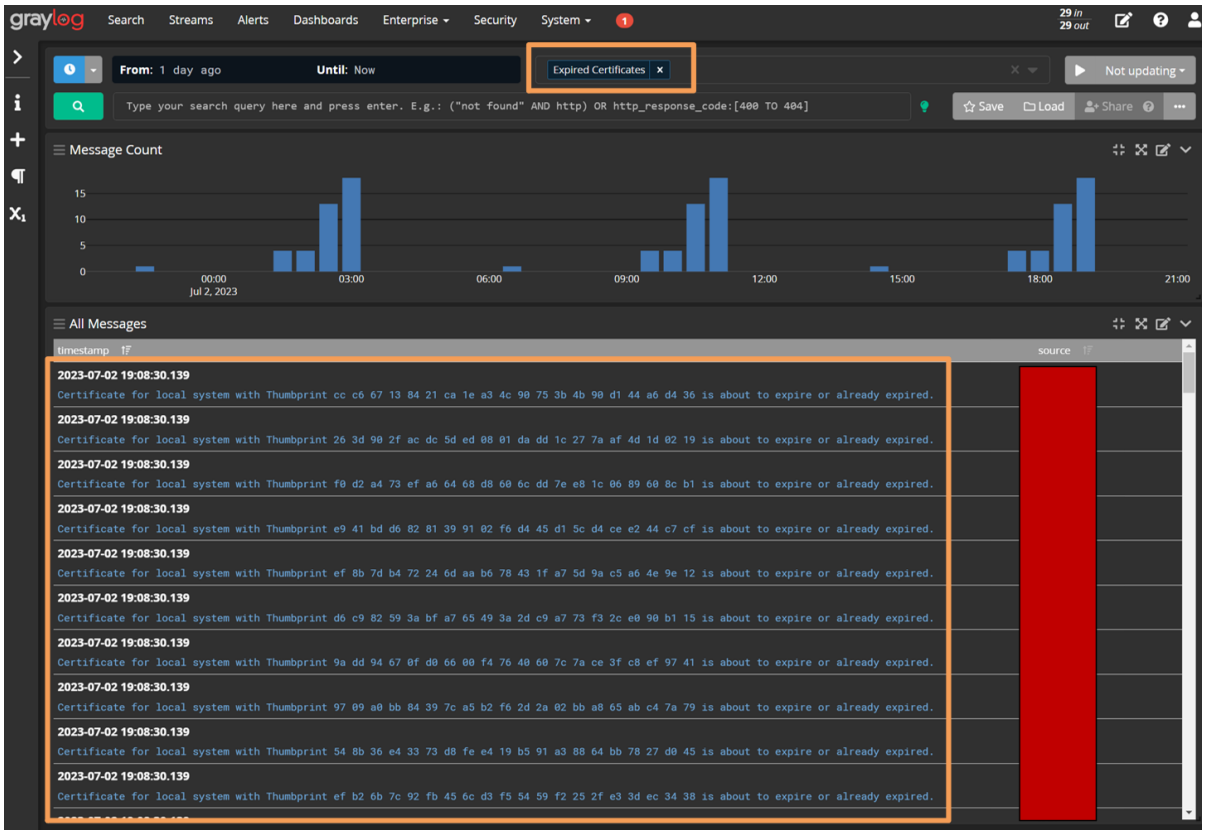

Figura 156 - Uso do filtro Expired Certificates após configuração. Fonte: Autor

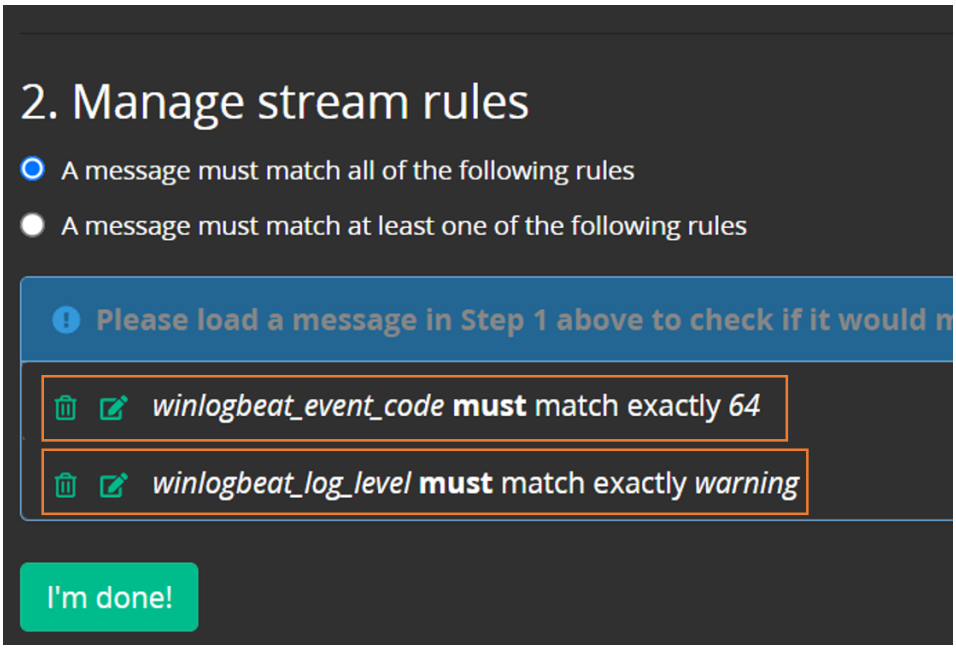

Figura 167 - Regras configuradas para a Stream Expired Certificates. Fonte: Autor

4.2.5 *Sidecars*

Para a recolha de *logs* nos ambientes *Windows*, fez-se uso da componente denominada por *Sidecar*, que é um sistema de gestão de configuração, que atua no *backend*. O *Graylog* acaba por servir como um núcleo centralizado, contendo as configurações dos coletores de log. O *Sidecar* pode funcionar como um serviço (para sistemas *Windows*) ou *daemon* (*Linux*) que atua na recolha dos *logs* para o *input* configurado para o efeito.

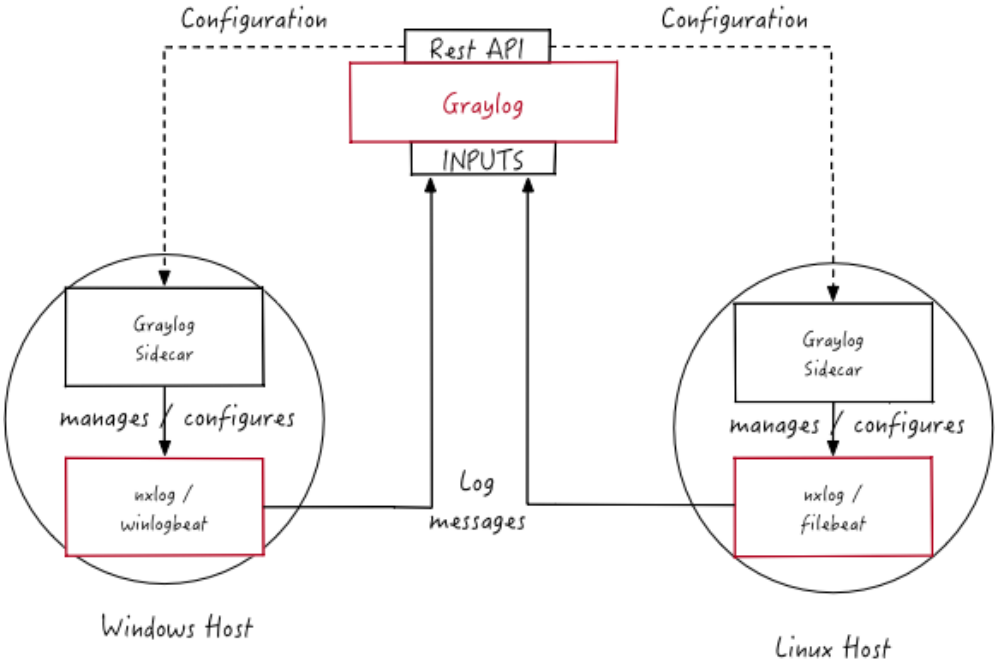

Figura 17 - Arquitetura do Sidecar. Fonte:(Graylog, 2021)

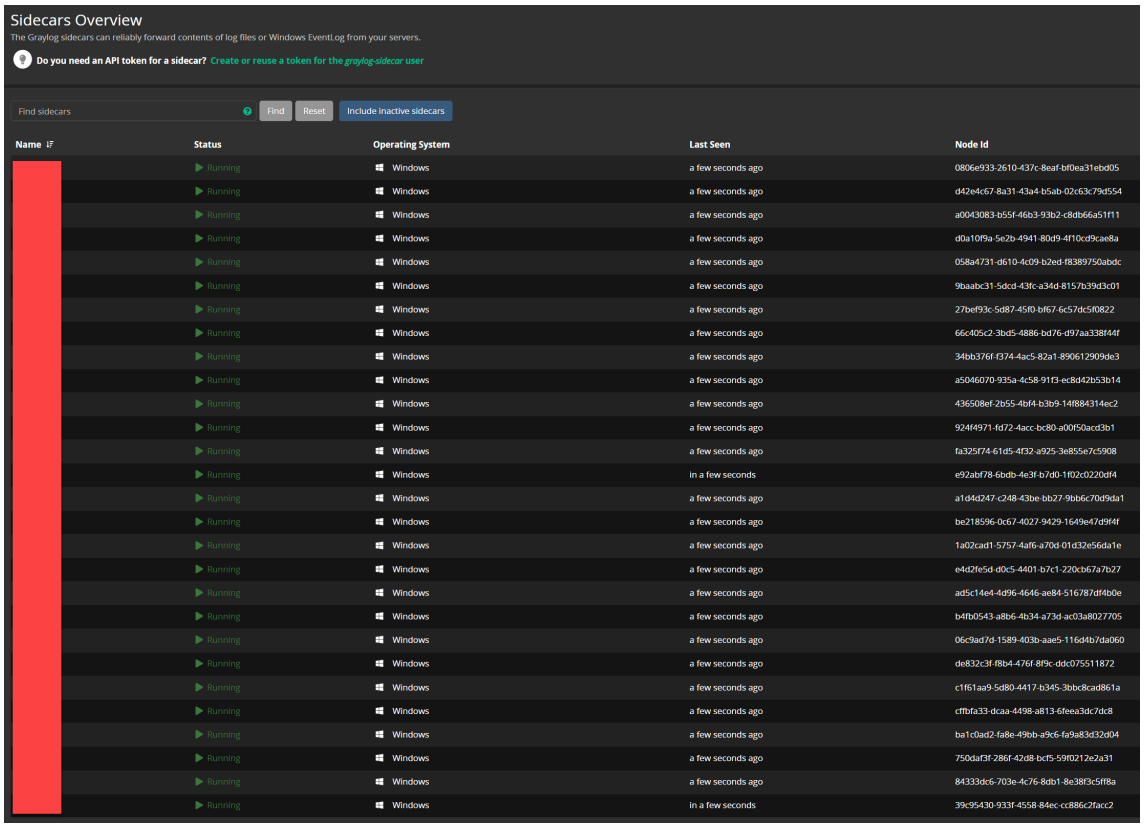

Figura 18 - Lista de Sidecars configurados para recolha de logs. Fonte: Autor

4.3 *Winlogbeat*

O *Winlogbeat* é um agente de envio de registos de eventos específico do *Windows*, instalado como um serviço do sistema operativo. Pode ser utilizado para recolher e enviar registos de eventos para um ou mais destinos, que neste caso terá a função de enviar os *logs* pretendidos para a plataforma de SIEM, conforme registo de *log* no Apêndice VII – Exemplo de log *Winlogbeat*.

4.3.1 *Filebeat*

Para a recolha de outros tipos de *logs*, nomeadamente os que são tipicamente registados em *filesystem* foi escolhido o agente *Filebeat*, como por exemplo para o envio dos *logs* referentes ao IIS (servidores *web*) e DNS.

4.4 *Dashboards*

A construção de *dashboards* permitiu uma forma de disponibilizar a informação de acordo com pesquisas pré-definidas e sob formas de visualização mais eficazes e rápidas para a análise da informação processada e correlacionada. Na figura 20, por exemplo, podemos constatar a facilidade de analisar a origem das comunicações para a nossa infraestrutura, pela sua representação no mapa, detetando assim possíveis ameaças não só com base na localização, mas também na frequência das ligações.

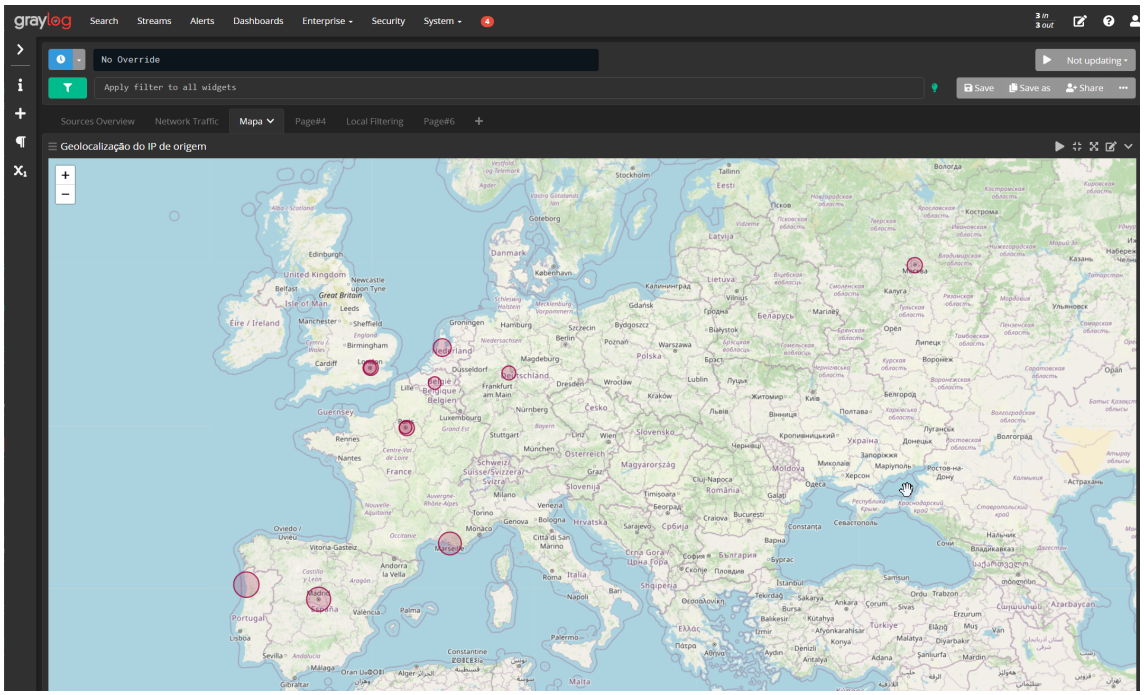

Figura 19 - Dashboard da Geolocalização por IP de origem. Fonte: Autor

Na figura 21 foi possível contruir um *dashboard* que permitisse visualizar em tempo real todo o tráfego da rede, relacionando informação de dezenas de equipamentos, classificando-os também mediante a quantidade de tráfego gerado.

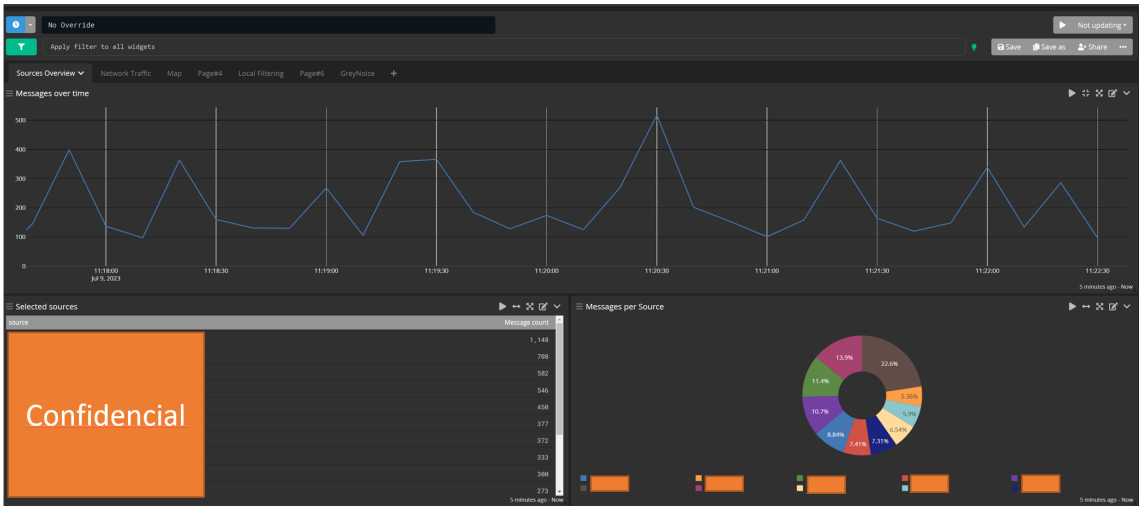

Figura 20 - Dashboard do volume de tráfego gerado em tempo real. Fonte: Autor

Na figura 22, à semelhança da figura 21, mas incluindo maior detalhe das comunicações, incluindo os respetivos IP´s, portos de origem e destino, país de origem e destino e número que mensagens processadas por segundo.

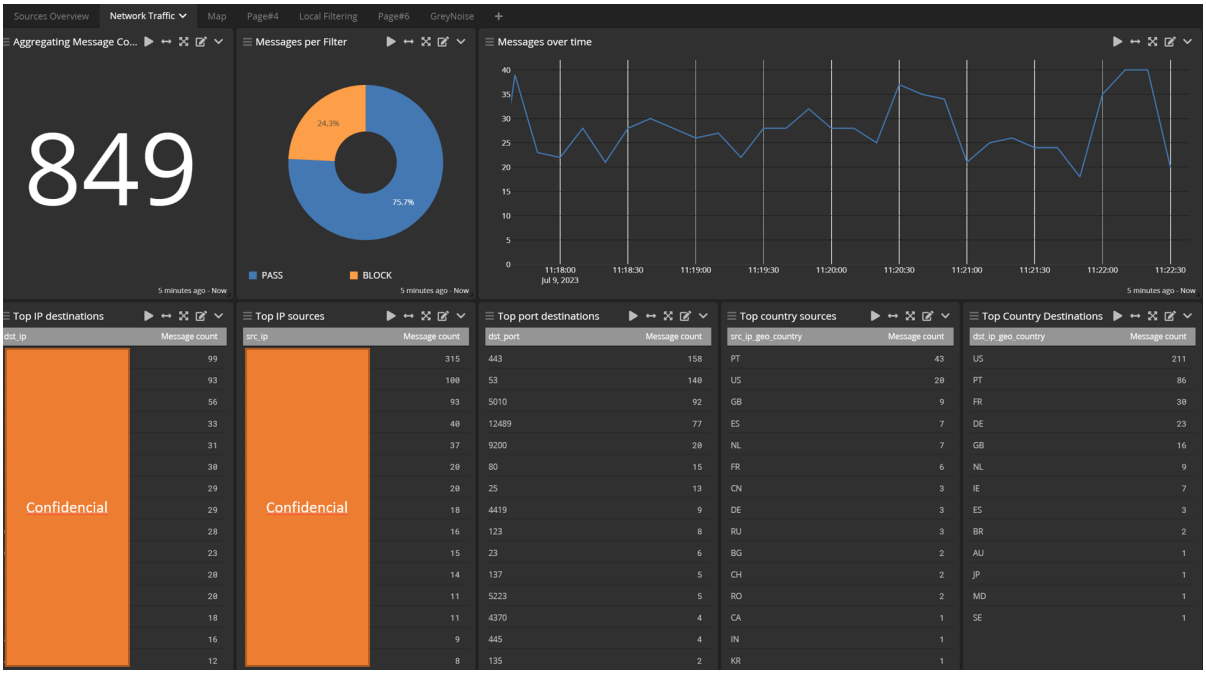

Figura 21 - Dashboard do tráfego em modo detalhado relativo à rede. Fonte: Autor

Na figura 23, um *dashboard* com a mesma informação, mas relacionada apenas a 1 *host*, para uma análise mais incisiva.

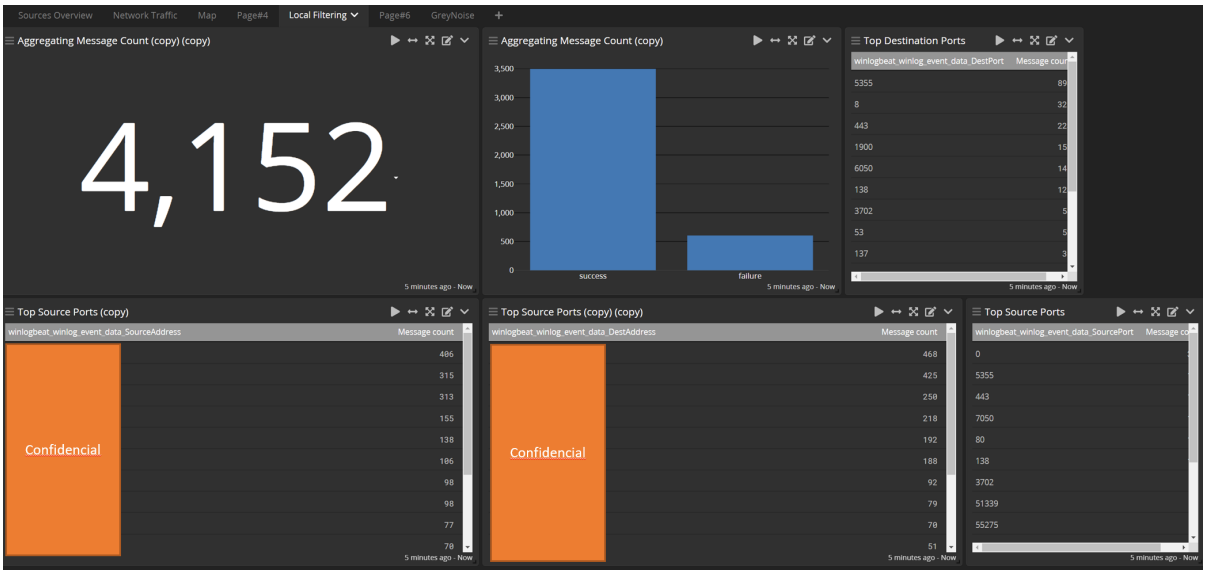

Figura 22 - Dashboard do tráfego em modo detalhado relativo a um host em específico. Fonte: Autor

Na figura 24, um *dashboard* relativo apenas aos servidores *web*, permitindo em tempo real aferir os acessos e URLs solicitados, sendo rapidamente percetível identificar os IPs de origem de possíveis atores maliciosos que tentam aceder a URLs reservados.

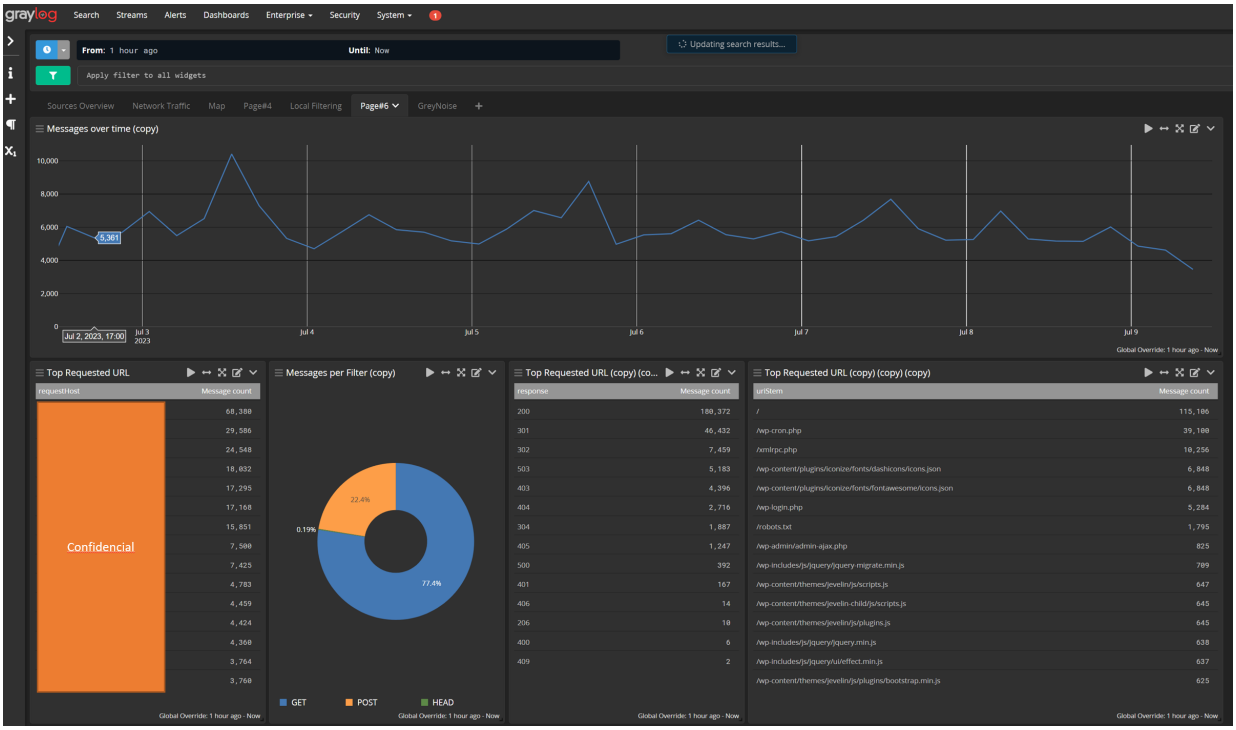

Figura 23 - Dashboard do tráfego dos acessos relativos aos webservers. Fonte: Autor

Na figura 25, um *dashboard* relativo ao processamento da informação com a informação de inteligência a ameaças *Greynoise*, classificando o tráfego, onde rapidamente se percebe que apenas 0,0952% do tráfego na última hora tem intenção desconhecida, sendo por isso passível de análise.

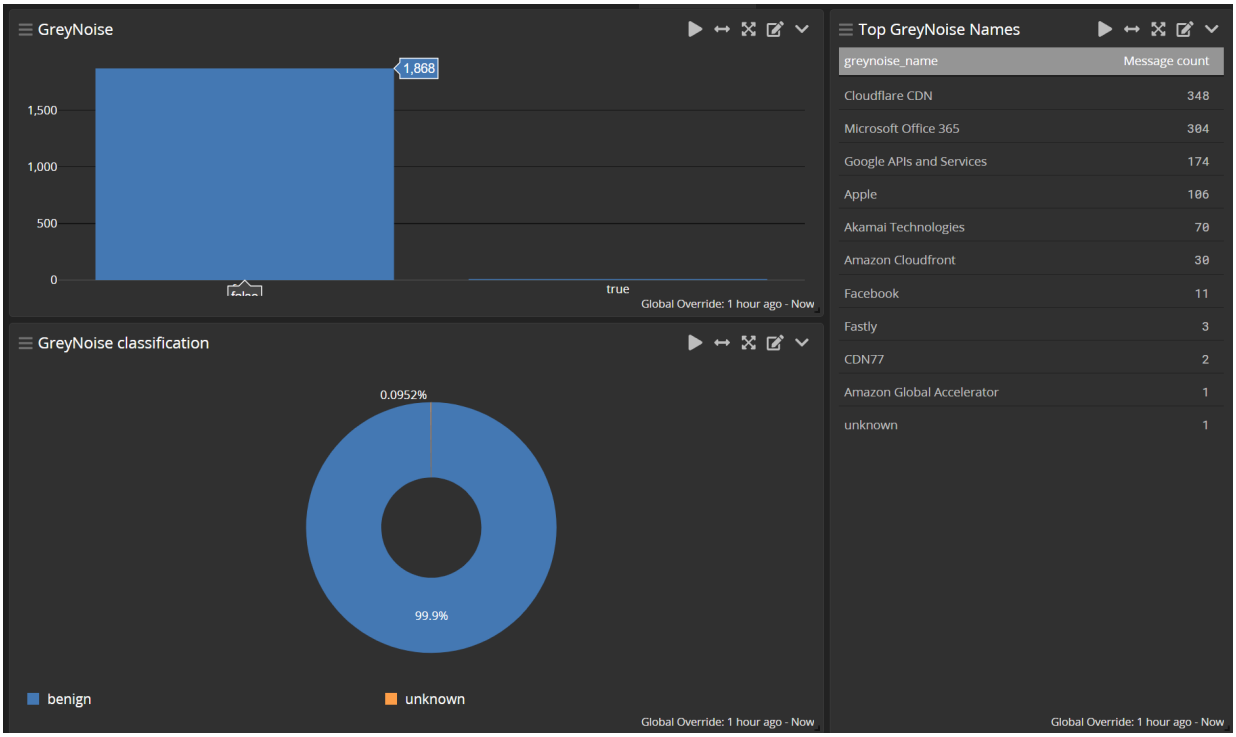

Figura 24 -Dashboard à classificação do Greynoise. Fonte: Autor

4.5 Avaliação

4.5.1 Cenário prático 1 – Exemplo de caça a ameaça através da metodologia não estruturada

Ao analisar aleatoriamente o tráfego recebido, a plataforma SIEM dispõe na pesquisa, a funcionalidade *autocomplete*, visível na figura 26, com um totalizador dos eventos registados em base de dados. Neste sentido, é possível perceber numa primeira instância as ligações mais expressivas em termos quantitativos e daí prosseguir com uma pesquisa de uma potencial ameaça com uma metodologia não estruturada.

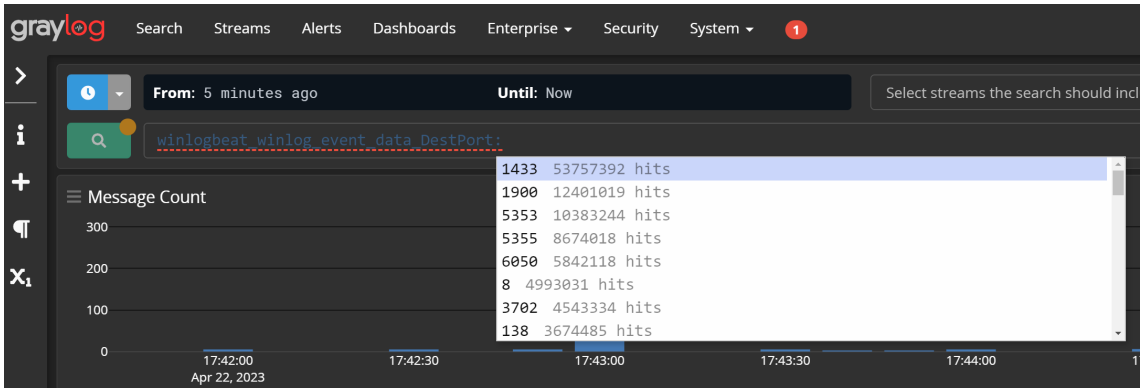

Figura 25 - Pesquisa usando funcionalidade autocomplete. Fonte: Autor

Continuando a nossa pesquisa, deparamo-nos na figura 26 e 27, com uma série de tráfego, tipicamente com destino no endereço de *broadcast* 224.0.0.252 com destino ao porto 5355, provindo de múltiplos servidores, em que inclusive uns são autorizados e outros bloqueados.

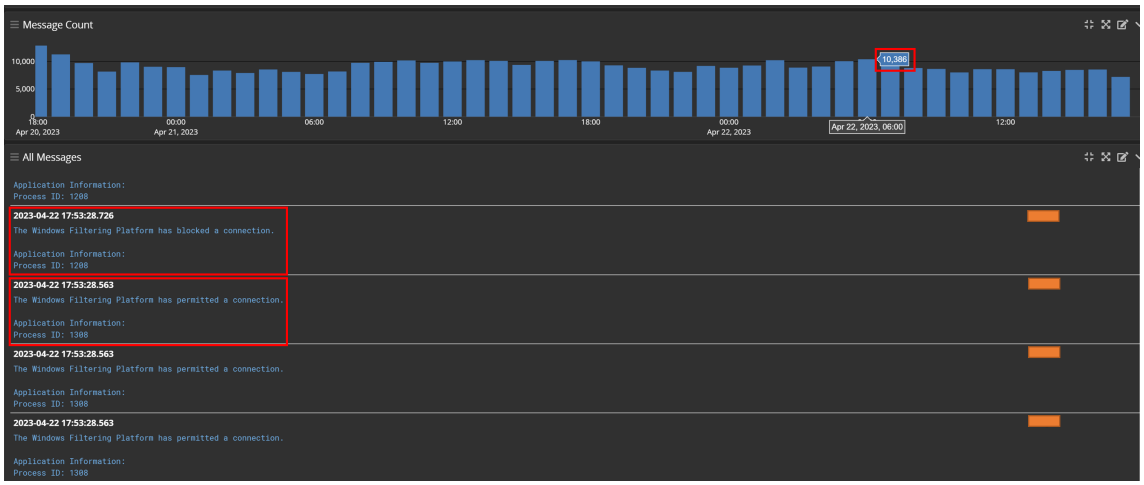

Figura 26 - Resultado do filtro relativo às comunicações com porto de destino 5355. Fonte: Autor

```
message
The Windows Filtering Platform has blocked a connection.

Application Information:
        Process ID:             1208
        Application Name:       \device\harddiskvolume4\windows\system32\svchost.exe

Network Information:
        Direction:              Inbound
        Source Address:         [redacted]
        Source Port:            56891
        Destination Address:    224.0.0.252
        Destination Port:               5355
        Protocol:               17

Filter Information:
        Filter Run-Time ID:     482960
        Layer Name:             Receive/Accept
        Layer Run-Time ID:      44
```

Figura 27 - Resultado do filtro relativo às comunicações com porto de destino 5355. Fonte: Autor

Nesta fase, importa perceber que comunicações estão associadas a este porto e se representam uma ameaça atual ou futura. Realizando uma rápida pesquisa percebemos que este padrão de tráfego está associado tipicamente ao serviço nativo SSDP (*Simple Service Discovery Protocol*) do sistema operativo *Windows*, usado para procurar outras máquinas na mesma rede em que o protocolo está fazendo parte no UPnP (*Universal Plug and Play*) permitindo a ligação entre diversos dispositivos na mesma rede sem configurações adicionais como o DNS (*Domain Name System*), essencial na maior parte das redes corporativas. Numa pesquisa mais alargada, percebe-se que este serviço não só já não é usado nas redes modernas, como também fica exposto

a ataques do tipo "*man-in-middle*", sendo recomendada por isso a sua desativação como forma de mitigação (Bradley, 2019).

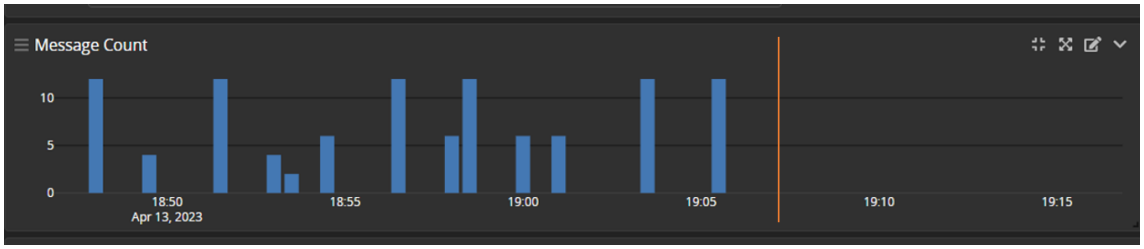

Figura 28 - Filtro temporal com o período antes e depois da desativação do serviço.
Fonte: Autor

5. Resultados

Após a colocação do protótipo em produção, foi possível recolher e determinar os dados representados nas seguintes alíneas, importantes para o estabelecimento de padrões, que poderão indiciar possíveis deteções de comunicações suspeitas, eventos de erro ou alerta, tendo como apreciação dois fatores principais, por um lado o estabelecimento de padrões relativos dos eventos e respetivas comunicações e, por outro, validar se a informação apresentada é relevante no contexto de ameaça cibernética, nomeadamente na sua deteção e mitigação.

a) Volume de tráfego

Foi percetível um volume recolhido de tráfego com um mínimo de 1.359.498 e no máximo de 2.135.925 mensagens.

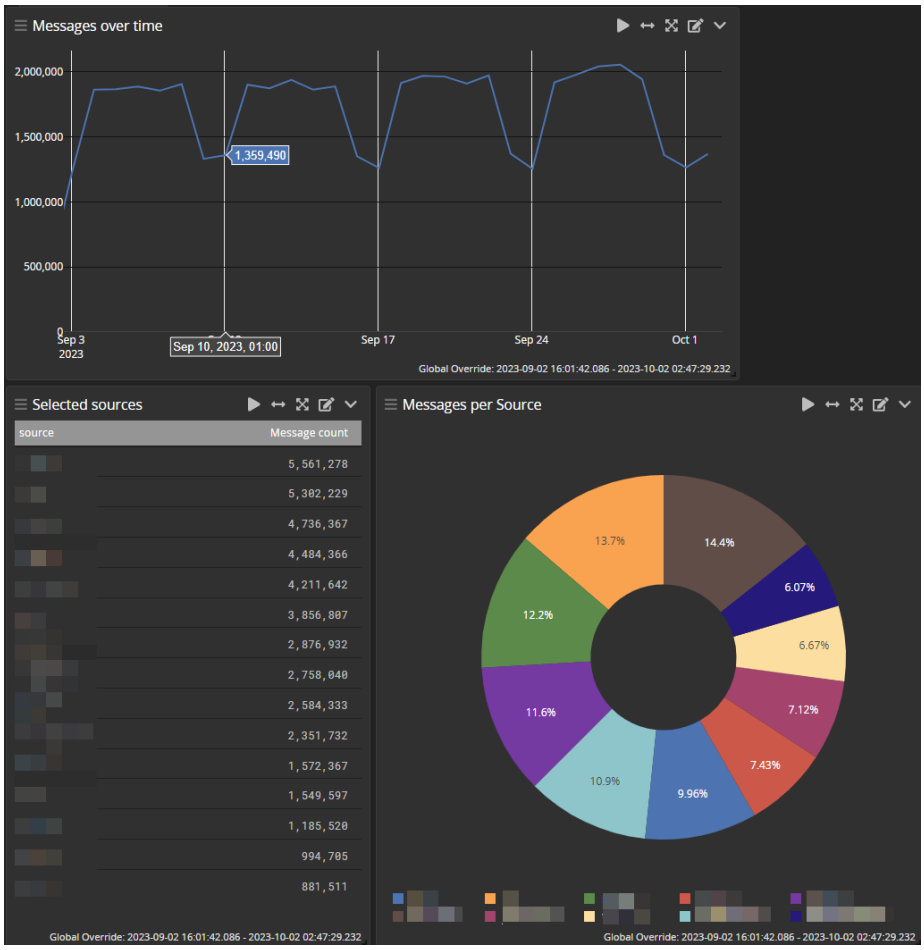

Figura 29 - Total de mensagens durante o mês de setembro e respetivas origens.
Fonte: Autor

b) **Percentagem de tráfego autorizado e não autorizado.**

Foi possível determinar a percentagem de tráfego autorizado, cerca de 93,7% e o tráfego bloqueado, cerca de 6,25%.

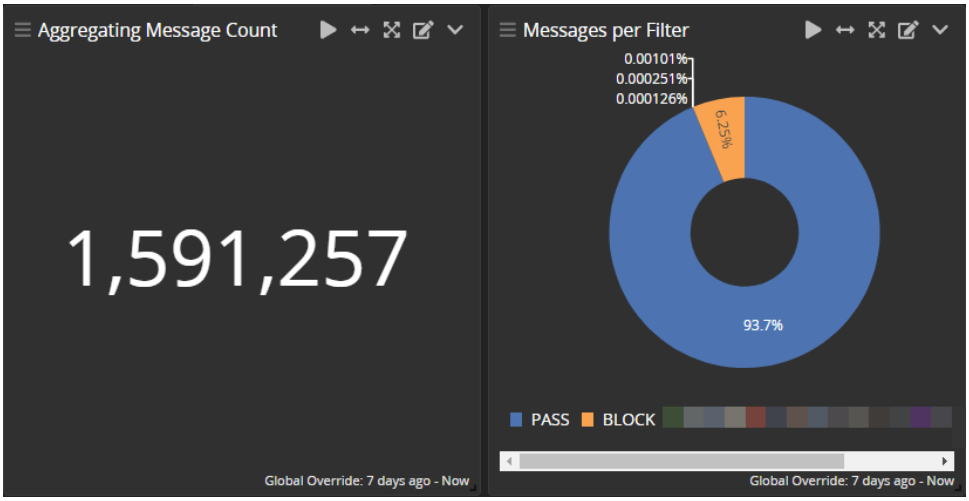

Figura 30 - Dashboard do volume de mensagens recolhidas. Fonte: Autor

c) ***Ranking* de equipamentos que mais tráfego geraram.**

Foi possível perceber, em qualquer altura selecionada ou em tempo real, os equipamentos que mais tráfego geraram, tanto relativamente ao tráfego que receberam, como o que geraram.

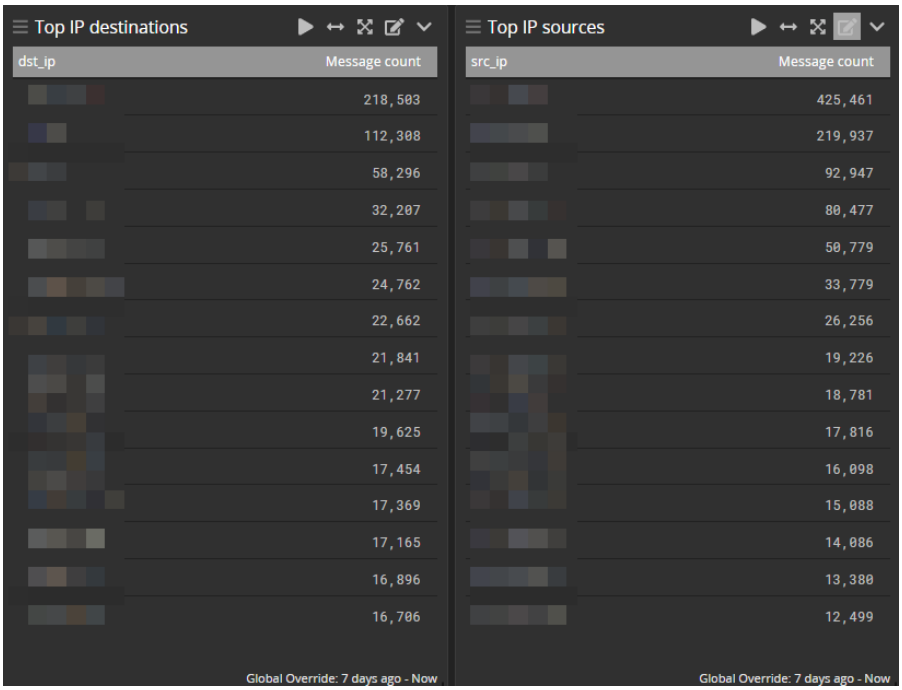

Figura 31 - Lista de endereços de destino ordenados por volume de tráfego. Fonte: Autor

d) **Portas de comunicação usadas.**

Foi possível perceber, em qualquer altura selecionada ou em tempo real, as portas de comunicação mais usadas, tanto relativamente às portas de origem, como às portas de destino.

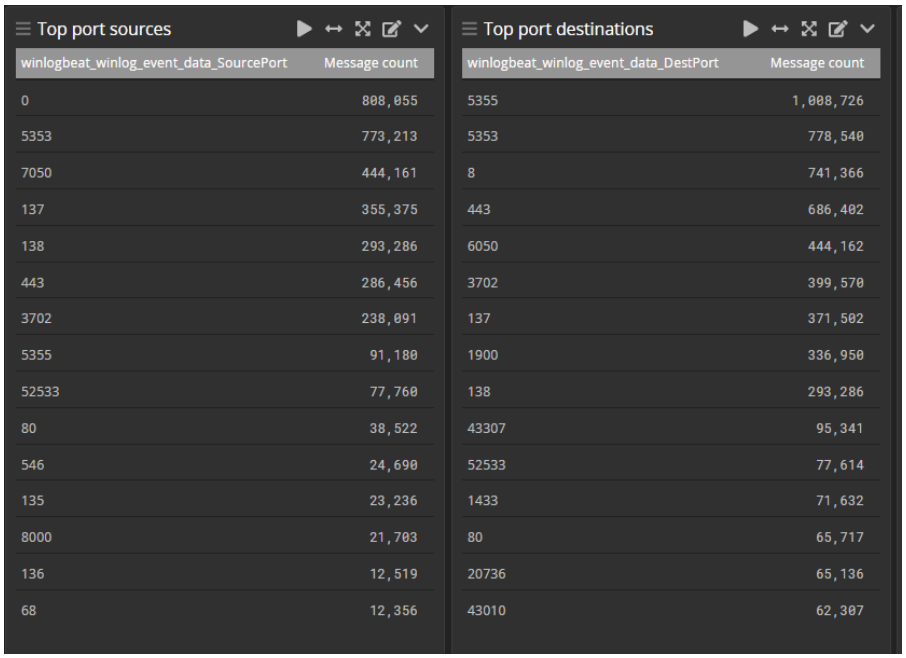

Figura 32 - Lista de portos usados, ordenados por volume de tráfego. Fonte: Autor

e) **Número de eventos relativos a autenticações falhadas.**

Relativamente ao número de eventos de autenticações falhadas, numa rápida visualização gráfica foi possível observar a obtenção de um máximo, no dia 28 de setembro 2023, face a um mínimo de 1188 eventos, no dia 1 de setembro 2023, evidencias que ajudam a circunscrever a análise de uma possível ameaça.

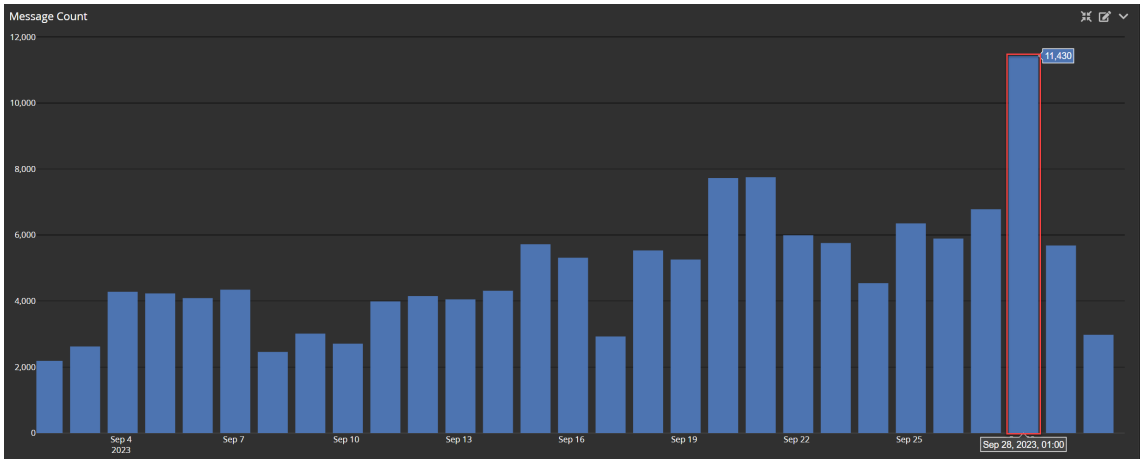

Figura 33 - Volume de tráfego diário, representado em gráfico de barras. Fonte: Autor

f) **Classificação do agente inteligente de ameaças.**

Durante o mesmo período, foram detetados 6 eventos com destino IP classificado como maligno, pelo agente de inteligência a ameaças *Greynoise.*

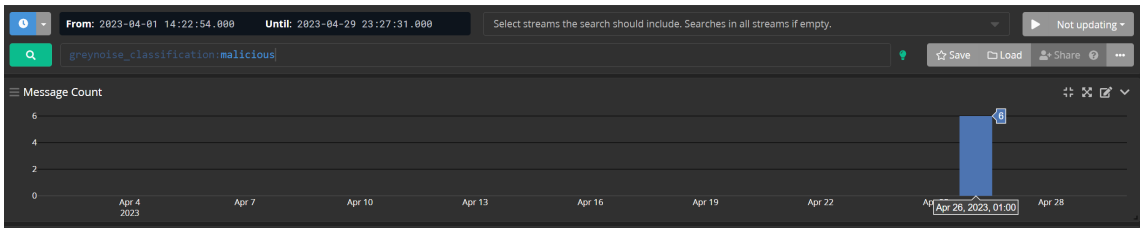

Figura 34 - Eventos detetados, classificados pela inteligência a ameaças Greynoise.
Fonte: Autor

g) **Número de eventos relativos a contas bloqueadas**

Contabilizaram-se durante o período mencionado, um total de 37 eventos relativos a contas que foram bloqueadas após terem excedido o máximo de tentativas (3).

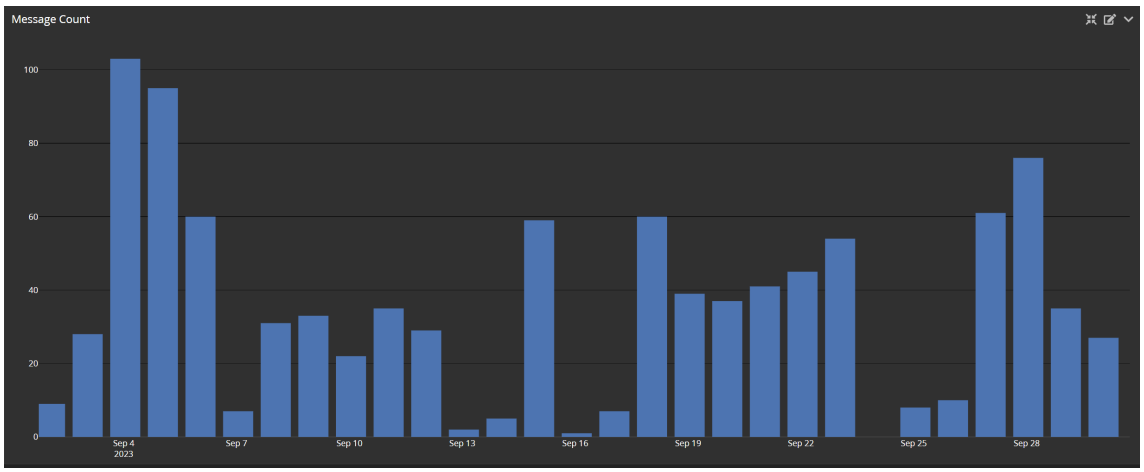

Figura 35 - Eventos de acessos bloqueados diários, representado em gráfico de barras.
Fonte: Autor

h) **Número de eventos relacionados com reinício de servidores.**

Contabilizaram-se durante o período mencionado, um total de 7 eventos relativos a reinícios de servidores, tendo sido o total de manutenções planeadas e previstas.

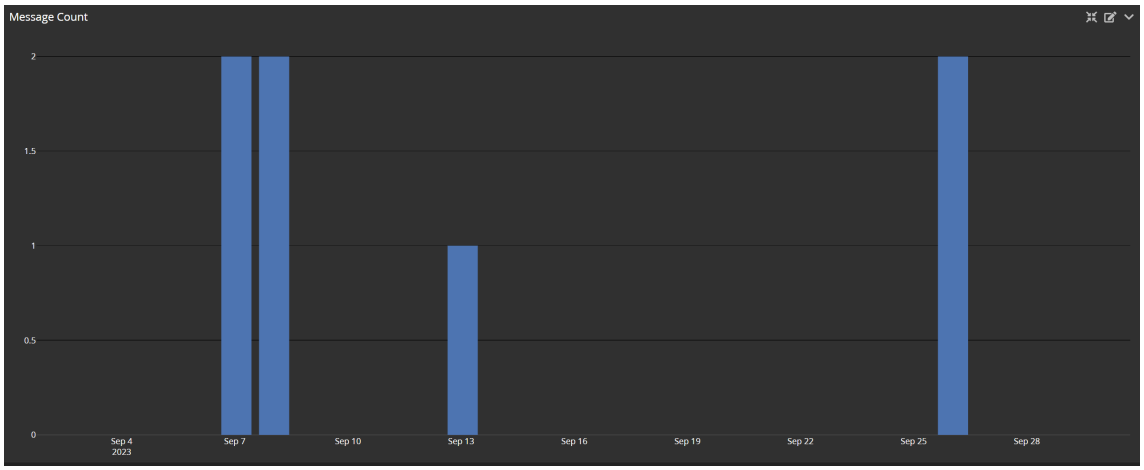

Figura 36 - Eventos gerados pelo reinício de servidores, representado em gráfico de barras. Fonte: Autor

i) **Número de eventos relacionados com a utilização de contas de administração.**

Contabilizaram-se durante o período mencionado, um total de 84 eventos relativos ao uso de credenciais com privilégios de administração.

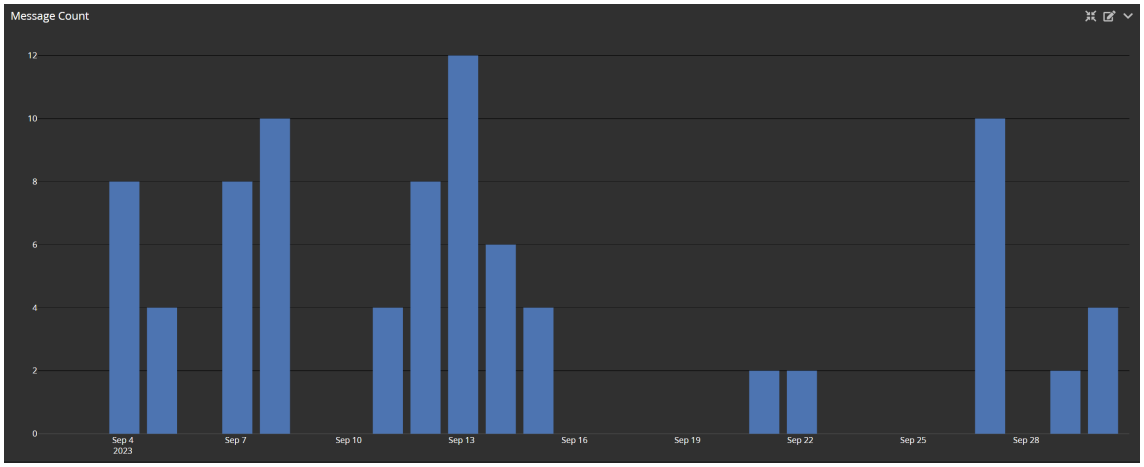

Figura 37 - Eventos relativo ao uso de credenciais de administração. Fonte:Autor

Quanto aos alertas configurados, definidos na Tabela 3, durante o primeiro mês de operação em produção (Setembro 2023), foi possível determinar os seguintes números quanto a notificações enviadas pelo SIEM, na seguinte tabela.

Tipo de Alerta	Quantidade de alertas
Reinício de servidor	6
Uso de conta de administração	152
Bloqueio de conta	1019
Nº de autenticações falhadas	141345
Certificados expirados	2921

Tabela 4- Tabela de alertas configurados e ocorrências verificadas. Fonte: Autor

6. Discussão

A avaliação da implementação da plataforma SIEM na organização selecionada para o estudo de caso, ofereceu informações relevantes sobre a eficácia desta tecnologia na cibersegurança e respetivamente no impacto na postura geral de segurança da organização. Esta secção de discussão analisa as principais conclusões, implicações e recomendações com base na análise deste projeto.

a) Eficácia da implementação da plataforma

A análise revela que a implementação do SIEM abordou eficazmente vários aspetos críticos da postura de cibersegurança da organização. Os principais objetivos deste projeto, que incluíam o reforço das capacidades de deteção e resposta a ameaças, o alinhamento das políticas de segurança e a melhoria da gestão de incidentes, foram amplamente alcançados. O sistema SIEM correlacionou e analisou eficientemente os dados de eventos de segurança de várias fontes, fornecendo à organização uma visão abrangente do seu panorama de segurança e *insights* importantes sobre o seu trafego e eventos de vários sistemas em tempo real, o que contribuiu para uma identificação mais proactiva das ameaças e tempos de resposta a incidentes mais rápidos, cruciais para a tomada de medidas de mitigação. A plataforma tornou-se doravante essencial para a validação das regras configuradas nos equipamentos e da política de segurança aplicada, garantindo assim a sua conformidade.

b) Desafios

No entanto, reconhecendo os desafios encontrados durante o processo de implementação do SIEM, denotou-se a complexidade técnica relacionada com a integração de dados, normalização dos dados e a resistência inicial à mudança por parte de alguns colaboradores, em reconhecer a vantagem e necessidade da ferramenta. Estes desafios sublinham a importância de um planeamento minucioso, da adesão das partes interessadas e da atribuição de recursos adequados a este tipo de projetos.

c) Impacto na cibersegurança

A implementação do SIEM teve um impacto notável na postura de segurança cibernética da organização. A análise dos dados de incidentes de segurança indicou em primeiro lugar uma consciencialização para o tráfego que circula na rede e respetiva proveniência, para potenciar

uma análise específica de cada evidencia encontrada, contribuindo para uma possível diminuição do tempo de permanência das ameaças na rede da organização. Isto sugere que o sistema SIEM evidencia eficazmente possíveis incidentes de segurança, contribuindo para melhorar a resiliência da cibersegurança, assim como a garantia de todas as evidencias para futura analise e contribuição para a melhoria continua do projeto, nomeadamente da adaptação à realidade da empresa, com desenvolvimentos e alarmística específica.

d) Tempo investido

O tempo investido é o reverso da medalha quando falamos de soluções *open-source* sem custo de licenciamento, onde se verificou que consome mais tempo na instalação e configuração inicial, sem a possibilidade de *Wizards,* mais exigente nas configurações de personalização, maioritariamente executadas em baixo nível, mas com a ressalva de que neste fabricante existiu um bom suporte, atualizações frequentes, manuais, procedimentos e um fórum comunitário que contribuiu eficazmente para a ultrapassagem das dificuldades encontradas e das que ainda advirão do decorrer da melhoria continua da plataforma.

7. Conclusão

Este projeto foi criado para estudar uma possível aplicação prática de um sistema SIEM, com o intuito de perceber a sua eficácia na deteção e mitigação de ciberameaças para as PME, nomeadamente possíveis ataques ainda em estágios iniciais, permitindo uma ação e vigilância proativas. Pese embora por si só a ferramenta não confira proteção, sendo necessário um conjunto de conhecimento inerente à área para a administrar, ficou demonstrado que a Informação de Segurança e Gestão de Eventos (SIEM) demonstrou ser uma ferramenta diferenciadora e necessária, que garante mais eficácia e eficiência da deteção de eventos anómalos, destacando-se com as seguintes vantagens:

- Gestão Centralizada de Registos: Permitiu recolher e analisar registos de múltiplas fontes, tais como dispositivos de rede, servidores, aplicações, e pontos finais. Esta abordagem centralizada ajudou a identificar possíveis incidentes de segurança de forma mais rápida e eficaz.

- Deteção de Ameaças: Foi possível executar análises avançadas para detetar ameaças que as soluções de segurança tradicionais tipicamente não possuem, analisando dados de múltiplas fontes para a identificação de padrões, anomalias e comportamentos suspeitos que possam indiciar uma ameaça cibernética.

- Monitorização em tempo real: Forneceu monitorização em tempo real de eventos de segurança, podendo alertar eficazmente para potenciais ameaças à medida que estas ocorrem, permitindo uma resposta mais rápida a incidentes, reduzindo assim o tempo para a sua mitigação/defesa.

- Relatórios de conformidade: Embora a versão instalada não permita a extração de relatórios, sendo que é necessária uma licença *Enterprise*, a plataforma permite gerar relatórios de conformidade para ajudar a cumprir os requisitos regulamentares e de conformidade.

- Resposta a Incidentes: Permite fornecer ferramentas para investigar e responder a incidentes de segurança, ajudando identificar a origem de um ataque, a possível extensão dos danos, e fornecer orientações sobre como mitigar a ameaça, através da inclusão de API de *Threat Intelligence.*

- Gestão centralizada: Foi possível centralizar e correlacionar todos os eventos locais de cada dispositivo, inclusive eventos de segurança, a partir de uma única consola, simplificando a gestão e reduzindo a complexidade.

Existindo de facto várias soluções no mercado, baseadas na mesma tecnologia, comprovou-se que este tipo de soluções confere uma vantagem num contexto de cibersegurança, através da gestão centralizada de registos, deteção de ameaças, monitorização em tempo real, relatórios de conformidade, resposta a incidentes e a capacidades de gestão centralizada que podem ajudar as organizações a melhorar a postura de segurança cibernética, na maior parte dos estágios dos ataques. Os recursos dedicados à instância virtual, foram constantemente atualizados, por forma a permitir uma visualização mais fluida e consequente rapidez nos alertas, devido ao aumento de desempenho no processamento dos eventos.

Como pontos menos positivos, destaca-se a necessidade e quantidade de tempo investido a título recorrente para adaptar sistematicamente a ferramenta tanto à realidade cibernética, como as possíveis mudanças na infraestrutura interna, consumindo e fazendo quase como um trabalho a tempo inteiro a sua adaptação, sob pena de se tornar ineficaz com o tempo. Neste sentido, pode-se resumir da seguinte forma:

- Complexidade: Dependendo da infraestrutura de cada PME, a implementação e manutenção da plataforma SIEM pode ser complexa e intensiva em recursos, exigindo conhecimento e formação especializados.

- Falsos positivos: Podem gerar um número elevado de falsos positivos, podendo causar descrédito nos alertas e consequente eficácia do sistema, principalmente quando mal parametrizado.

- Custo: Pode ser dispendioso, particularmente para organizações mais pequenas ou com orçamentos limitados de TI, que pretendam mais funcionalidades das fornecidas nas ferramentas básicas, como referido anteriormente relativamente aos relatórios de conformidade.

- Integração: Requer integração com outras tecnologias e sistemas de segurança, o que pode ser desafiante e demorado.

- Gestão da informação: Requer planeamento para a gestão da informação recolhida, uma vez que poder-nos-emos deparar rapidamente com largos *datasets* de *Gigabtytes/Terabytes.* No

decorrer do projeto, foi necessário recorrer por diversas vezes ao aumento dos volumes lógicos de armazenamento, ficando no final com uma alocação de aproximadamente 1 *terabyte* e aumento de memória RAM, para 32GB no sentido de tornar a plataforma mais responsiva.

Resumindo, foi possível demonstrar, que uma implementação bem executada deste tipo de soluções pode melhorar significativamente a postura de cibersegurança de uma organização. As conclusões e recomendações apresentadas neste estudo contribuem para o conjunto de conhecimentos sobre a tecnologia SIEM e o seu papel na proteção das organizações contra as ciberameaças.

7.1 Trabalho Futuro

Em trabalhos futuros, considera-se relevante e interessante integrar um sistema de IDS (*SURRICATA ou SNORT*) para uma análise e modelação das regras de gestão do tráfego de rede sob forma autónoma e em tempo real, no sentido de existir adaptação das regras de tráfego consoante o nível de ameaça declarado.

Ao nível da otimização dos pedidos, nomeadamente às respetivas APIs de informação de inteligência, torna-se necessário invocá-las apenas para endereços públicos, por uma questão de gestão de pedidos e consequentemente redução do respetivo tráfego.

Face ao resultado obtido, expandir o estudo por forma a abranger mais PME, poderá revelar-se fundamental para fortalecer a cibersegurança no ecossistema empresarial português. Dado que as PME representam 99,9% do tecido empresarial em Portugal, conforme definido pelo Decreto-Lei n.º 372/2007, de 6 de novembro, é imperativo que estas organizações adotem tecnologias avançadas de segurança para mitigar riscos cibernéticos e a ampliação deste estudo a mais PME, permitirá eventualmente identificar as necessidades específicas, assim como mitigar os desafios enfrentados por estas empresas na implementação de SIEM, promovendo práticas de segurança mais robustas e adaptadas aos seus recursos limitados. Além disso, ao integrar mais PME no estudo, será possível criar um conjunto de dados mais abrangente, facilitando a elaboração de estratégias de segurança cibernética mais eficazes e a promoção de uma cultura de segurança digital entre as pequenas e médias empresas, podendo inclusive contribuir para o reforço do resultado obtido.

Referências

Adejumola, R. (2022). What Is Shodan and How Can It Improve Your Online Security? Consultado em 4 de março de 2023. Disponível em: https://www.makeuseof.com/what-is-shodan/

Al-Duwairi, B. (2019). SIEM-based detection and mitigation of IoT-botnet DDoS attacks. Consultado em 4 de março de 2023. Disponível em: https://core.ac.uk/download/pdf/329119316.pdf

Andrade, F. (2021). Cibersegurança: Portugal regista melhorias no desempenho e sobe para o 14º lugar do ranking global. Consultado em 4 de março de 2023. Disponível em: https://tek.sapo.pt/noticias/internet/artigos/ciberseguranca-portugal-regista-melhorias-no-desempenho-e-sobe-para-o-14o-lugar-do-ranking-global

Ariganello, J. (2022). Threat Hunting: Eight Tactics to Accelerating Threat Hunting. Consultado em 05 de maio de 2023. Disponível em: https://www.anomali.com/blog/threat-hunting-eight-tactics-to-a-accelerating-threat-hunting

Bannister, A. (2021). Abuse.ch creator launches ThreatFox, a platform for sharing malware indicators of compromise. Consultado em 23 de abril de 2023. Disponível em: https://portswigger.net/daily-swig/abuse-ch-creator-launches-threatfox-a-platform-for-sharing-malware-indicators-of-compromise

Baker, K. (2023). WHAT IS CYBER THREAT INTELLIGENCE? Consultado em 23 de abril de 2023. Disponível em: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Bazzel, M. (2022). Open Source Intelligence Techiques: Resources for searching and Analyzing Online Information. Consultado em 23 de abril de 2023. Disponível em: https://IntelTechniques.com

Bhardwaj, P. (2022). What is Open Web Application Security Project (OWASP)? Consultado em 8 de abril de 2023. Disponível em: https://www.tutorialspoint.com/what-is-open-web-application-security-project-owasp

Bradley, S. (2019). How to disable LLMNR in Windows Server. Consultado em 22 de abril de 2023. Disponível em: https://www.csoonline.com/article/3449156/how-to-disable-llmnr-in-windows-server.html

Brandefense (2022). European Focused Threat Actors – APT Groups. Consultado em 23 de abril de 2023. Disponível em: https://brandefense.io/blog/apt-groups/european-focused-threat-actors/

Brooke, L. (2022). How Cyber Security Helps Identify Internet Frauds and Crimes. Consultado em 4 de março de 2023. Disponível em: https://www.logsign.com/blog/cyber-security-for-internet-frauds-with-siem-solutions/

CISA (2021). Best Practices for MITRE ATT&CK®. Consultado em 23 de abril de 2023. Disponível em: https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

Clarke, C. (2023). 6-Step Ransomware Response Plan. Consultado em 23 de setembro de 2023. Disponível em: https://www.veeam.com/blog/ransomware-response-plan.html

CNCS A (2023). HISTÓRIA DO CNCS. Consultado em 23 de abril de 2023. Disponível em: https://www.cncs.gov.pt/pt/sobre-nos/

CNCS B (2023). Roteiro para as Capacidades Mínimas de Cibersegurança. Consultado em 23 de abril de 2023. Disponível em: https://www.cncs.gov.pt/pt/roteiro-capacidades-minimas-ciberseguranaa/

CNCS C (2023). RFC 2350. Consultado em 23 de abril de 2023. Disponível em: https://www.cncs.gov.pt/pt/certpt/rfc-2350/

Cynet (2022). NIST incident response plan: Building your own IR process based on NIST guidelines. Incident Response. Consultado em 23 de abril de 2023. Disponível em: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

Dimaggio, J. (2022). The Art of Cyberwarfare – An Investigator´s Guide to Espionage, Ransomware, and Ornanized Cybercrime (pp. 109 - 111). San Francisco, No Starch Press Inc.

Donnan, L. (2022). What Is GreyNoise? And How They Approach Threat Intelligence. Consultado em 02 de julho de 2023. Disponível em: https://option3.com/what-is-greynoise/

DR (2007). Decreto-Lei n.º 372/2007, de 6 de novembro, consultado em 26 de junho de 2024. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/372-2007-629439

Eley, K. (2023). SIEM Platform Helps Proactive Cyber Security Strategy. Consultado em 05 de maio de 2023. Disponível em: https://businessplus.ie/industry-type/technology/cyber-security-strategy/

Ferreira, C. (2022). Investimento continua longe do desejável para os desafios de cibersegurança que as empresas enfrentam. Consultado em 7 de março de 2023. Disponível em: https://tek.sapo.pt/noticias/computadores/artigos/investimento-continua-longe-do-desejavel-para-os-desafios-de-ciberseguranca-que-as-empresas-enfrentam

Fernandes, F. (2021). Ataques informáticos já atingem as PME. Consultado em 05 de maio de 2023. Disponível em: https://www.jornaldenegocios.pt/negocios-iniciativas/seguros/detalhe/ataques-informaticos-ja-atingem-as-pme

Fruhlinger, J. (2022). What is SIEM? Security information and event management explained. Consultado em 6 de março de 2023. Disponível em: https://www.csoonline.com/article/2124604/what-is-siem-security-information-and-event-management-explained.html

Graylog. (2021). *Graylog Sidecar*. Consultado em 4 de março de 2023. Disponível em: https://archivedocs.graylog.org/en/latest/pages/sidecar.html

Greynoise. (2021). *Understanding GreyNoise Classifications*. Consultado em 4 de março de 2023. Disponível em: https://docs.greynoise.io/docs/understanding-greynoise-classifications

Gupta, D. (2021). How IoT is Making DDoS Attacks More Dangerous?. Consultado em 4 de março de 2023. Disponível em: https://insights2techinfo.com/how-iot-is-making-ddos-attacks-more-dangerous/

Hanna, K. (2021). Attack surface, definition. Consultado em 6 de março de 2023. Disponível em: https://www.techtarget.com/whatis/definition/attack-surface

Hazel, T. (2021). Threat Hunting Frameworks and Methodologies: An Introductory Guide Consultado em 12 de fevereiro de 2023. Disponível em: https://www.chaossearch.io/blog/threat-hunting-methods-and-frameworks

Horenbeeck, M. (2023). The importance of attack surface reduction for Active Directory. Consultado em 8 de abril de 2023. Disponível em: https://blog.quest.com/the-importance-of-attack-surface-reduction-for-active-directory/

Huntley, S. (2023). Fog of war: how the Ukraine conflict transformed the cyber threat landscape. Consultado em 8 de abril de 2023. Disponível em: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

IANS. (2022). How to Use Your SIEM to Detect Ransomware Attacks. Consultado em 4 de março de 2023. Disponível em: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/01/28/how-to-use-your-siem-to-detect-ransomware-attacks

IANS. (2021). Three Security Initiatives to Consider in 2022. Consultado em 4 de março de 2023. Disponível em: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/12/02/three-security-initiatives-to-consider-in-2022

IT SECURITY. (2023). Maioria dos ciberataques visam PME. Consultado em 4 de março de 2023. Disponível em: https://www.itsecurity.pt/news/analysis/maioria-dos-ciberataques-visam-pme

Ingerslev, J. (2021). Critical Infrastructure and Cyber Risk: Single Points of Failure. Consultado em 4 de março de 2023. Disponível em: https://www.linkedin.com/pulse/critical-infrastructure-cyber-risk-single-points-jacob-ingerslev?trk=read_related_article-card_title

Imam, F. (2018). Threat hunting maturity model. Consultado em 4 de março de 2023. Disponível em: https://resources.infosecinstitute.com/topics/threat-hunting/threat-hunting-maturity-model/

Irwin, L. (2021). How to protect your organization after a ransomware attack. Consultado em 4 de março de 2023. Disponível em: https://www.itgovernance.co.uk/blog/how-to-handle-a-ransomware-attack

Kerner, S. (2023). Ransomware trends, statistics and facts in 2023. Consultado em 4 de março de 2023. Disponível em: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

Keerthana, E. (2023). Threat Hunting: Methodologies, Tools and TipsConsultado em 05 de maio de 2023. Disponível em: https://www.infosectrain.com/blog/threat-hunting-methodologies-tools-and-tips/

Kidd, C. (2022). Cyber Kill Chains Explained: Phases, Pros/Cons & Security Tactics. Consultado em 6 de março de 2023. Disponível em: https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Korolov, M. (2021). Supply chain attacks show why you should be wary of third-party providers. Consultado em 6 de março de 2023. Disponível em: https://www.csoonline.com/article/561323/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

Kost, E. (2022). O que é cibersegurança? Consultado em 4 de março de 2023. Disponível em: https://tecnoblog.net/responde/o-que-e-ciberseguranca/

Kovacs, L. (2021). What are Indicators of Attack (IOAs)? How they Differ from IOCs. Consultado em 4 de março de 2023. Disponível em: https://www.upguard.com/blog/what-are-indicators-of-attack

Kreisa, M. (2023). How to use the incident response lifecycle to thwart cyberattacks. Consultado em 4 de novembro de 2023. Disponível em: https://www.pdq.com/blog/how-to-use-incident-response-lifecycle/

Kumar, M. (2018). A New Paradigm For Cyber Threat Hunting. Consultado em 4 de março de 2023. Disponível em: https://thehackernews.com/2018/06/cyber-threat-hunting.html

Laue, T. (2022). A SIEM Architecture for Advanced Anomaly Detection. Consultado em 22 de abril de 2023. Disponível em: https://www.ronpub.com/OJBD_2022v6i1n02_Laue.pdf

Liu, T. (2022). A Guide for Defending Against Supply Chain Attacks. Consultado em 4 de março de 2023. Disponível em: https://www.semi.org/zh/txonenetworks_a_guide_for_defending_against_supply_chain_attacks

Lusa. (2023). Proteção de Dados emite recomendações às empresas sobre segurança em ciberataques. Consultado em 8 de abril de 2023. Disponível em: https://eco.sapo.pt/2023/02/03/protecao-de-dados-emite-recomendacoes-as-empresas-sobre-seguranca-em-ciberataques/

Magnusson, A. (2023). What is an Attack Surface? (And the Best Way to Reduce It) Consultado em 15 de outubro de 2023. Disponível em: https://www.strongdm.com/blog/attack-surface

Malik, P. (2022). Lewin's 3-Stage Model of Change Theory: Overview. Consultado em 4 de março de 2023. Disponível em: https://whatfix.com/blog/lewins-change-model/

Martins, A. (2023). What Is Cyber Threat Intelligence, and Why Do You Need It? Consultado em 25 de fevereiro de 2023. Disponível em: https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html

Martin, S. (2021). Supply Chain Attacks: How To Combat This Growing Threat. Consultado em 4 de março de 2023. Disponível em: https://www.csiweb.com/what-to-know/content-hub/blog/supply-chain-attacks-how-to-combat-this-growing-threat/

Mcbride, E. (2023). The dark web's criminal minds see Internet of Things as next big hacking prize. Consultado em 4 de março de 2023. Disponível em: https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html

McCarthy, M. (2023). What Is a Threat Actor?. Consultado em 4 de março de 2023. Disponível em: https://www.strongdm.com/what-is/threat-actor

McGowan, E. (2023). A Beginner's Guide to Cyber Threat Hunting. Consultado em 5 de março de 2022. Disponível em: https://blog.acer.com/en/discussion/496/a-beginner-s-guide-to-cyber-threat-hunting

Medeiros, N. (2022). Fator Humano na Cibersegurança. Consultado em 1 de outubro de 2023. Disponível em: https://www.pbs.up.pt/pt/artigos-e-eventos/artigos/artigo-o-fator-humano-na-ciberseguranca/

Mishra, R. (2021). What is ENISA and how has it helped enforce cyber laws in the EU. Consultado em 8 de abril de 2023. Disponível em: https://blog.ipleaders.in/what-is-enisa-and-how-has-it-helped-enforce-cyber-laws-in-the-eu/

Naz, Z. (2023). Cyber Threat Hunting: Types, Methodologies, Best Practices. Consultado em 5 de março de 2023. Disponível em: https://www.knowledgehut.com/blog/security/cyber-threat-hunting

Nazarov, R. (2022). Indicators of compromise (IOCs): how we collect and use them. Consultado em 4 de março de 2023. Disponível em: https://securelist.com/how-to-collect-and-use-indicators-of-compromise/108184/

Palmer, D. (2022). What is ransomware? Everything you need to know about one of the biggest menaces on the web. Consultado em 4 de março de 2023. Disponível em: https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

Palmer, D. (2023). What is phishing? Everything you need to know to protect against scam emails - and worse. Consultado em 4 de março de 2023. Disponível em: https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/

Pires, A. (2023). How the cybersecurity culture changes the direction of a company. Consultado em 1 de outubro de 2023. Disponível em: https://skyone.solutions/en/hub/cybersecurity-culture/

PGDL (2004). Lei n.º 41/2004, de 18 de Agosto. Consultado em 23 de abril de 2023. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=707&tabela=leis&so_miolo=

PGDL (2014). Lei n.º 69/2014, de 29 de Agosto . Consultado em 23 de abril de 2023. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=2213&pagina=1&ficha=1

PGDL (2017). DL n.º 136/2017, de 06 de Novembro. Consultado em 23 de abril de 2023. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=selected&nid=2803&tabela=leis&pagina=1&ficha=1&nversao=

PGDL (2019). Lei n.º 58/2019, de 08 de Agosto. Consultado em 23 de abril de 2023. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=

PGDL (2019). Lei n.º 59/2019, de 08 de Agosto. Consultado em 23 de abril de 2023. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3123A0001&nid=3123&tabela=leis&pagina=1&ficha=1&so_miolo=?area=Identifica%E7%E3o%20civil%20e%20criminal&nversao=

Pham A, T. (2020). Replace Your SIEM: Traditional vs. Modern SIEM. Consultado em 23 de abril de 2023. Disponível em: https://www.blumira.com/replace-your-siem-traditional-vs-modern-siem/

Pham B, T. (2020). OWASP Top 10: Automate Logging & Monitoring for Application Security. Consultado em 23 de abril de 2023. Disponível em: https://www.blumira.com/owasp-top-10/

Pontual (2023). CIBERSEGURANÇA PARA PME – PORQUE TEM DE INVESTIR JÁ. Consultado em 23 de abril de 2023. Disponível em: https://www.pontualsoftware.com/ciberseguranca-para-pme/

Roberts, I. (2022). What are Indicators of Compromise?. Consultado em 25 de fevereiro de 2023. Disponível em: https://www.lepide.com/blog/what-are-indicators-of-compromise/

Roy, R. (2021). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Consultado em 25 de fevereiro de 2023. Disponível em: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/

Rumiantseva, O. (2022). Threat Hunting Maturity Model Explained With Examples. Consultado em 6 de março de 2023. Disponível em: https://socprime.com/blog/threat-hunting-maturity-model-explained-with-examples/

Scarfone, K. (2022). How to develop a cybersecurity strategy: Step-by-step guide. Consultado em 4 de março de 2023. Disponível em: https://www.techtarget.com/searchsecurity/tip/How-to-develop-a-cybersecurity-strategy-Step-by-step-guide

Simmons, K. (2019). The IT Leaders' Guide to Choosing the Right SIEM Deployment Method. Consultado em 12 de fevereiro de 2023. Disponível em: https://armorpoint.com/2019/04/04/the-it-leaders-guide-to-choosing-the-right-siem-deployment-method/

SOCFortress. (2022). *Part 8. Firewall Threat Intel With GreyNoise.* Consultado em 01 de outubro de 2023. https://socfortress.medium.com/part-8-firewall-threat-intel-with-greynoise-210245407a4b

Sousa, A. (2022). Estudo Sage: 59% das PME mais dependente da tecnologia depois da pandemia. Consultado em 01 de outubro de 2023. Disponível em: https://jornaleconomico.pt/noticias/estudo-sage-59-das-pme-mais-dependente-da-tecnologia-depois-da-pandemia-895265/

Stone, M. (2022). 4 Most Common Cyberattack Patterns from 2022. Consultado em 21 de fevereiro de 2023. Disponível em: https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022/

Stouffer, C. (2021). Hacktivism: An overview plus high-profile groups and examples. Consultado em 23 de abril de 2023. Disponível em: https://us.norton.com/blog/emerging-threats/hacktivism#

Sqrrl (2015). The Cyber Hunting Maturity Model. Consultado em 23 de abril de 2023. Disponível em: https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5

Tunggal, A. (2023). Common Attack Vectors in 2023. Consultado em 6 de março de 2023. Disponível em: https://www.upguard.com/blog/attack-vector

Unni, A. (2022). How To Develop A Strong Cybersecurity Strategy. Consultado em 4 de março de 2023. Disponível em: https://www.stickmancyber.com/cybersecurity-blog/how-to-develop-a-strong-cybersecurity-strategy

Vankirk, S. (2022). What Are the Most Important Types of Cyberthreats? Consultado em 4 de março de 2023. Disponível em: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-threat-intelligence-program/

Vincent, S. (2023). Threat Hunting: 7 Ways to Reduce Risk. Consultado em 5 de março de 2022. Disponível em: https://www.techopedia.com/threat-hunting-8-ways-to-reduce-risk/2/34903

Walkowski, D. (2021). MITRE ATT&CK: What It Is, How it Works, Who Uses It and Why. Consultado em 4 de março de 2023. Disponível em: https://www.f5.com/labs/learning-center/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why

Wolff, J. (2021). How the NotPetya attack is reshaping cyber insurance. Consultado em 4 de março de 2023. Disponível em: https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/

Yadav, D. (2023). Cyber Threat Intelligence: Goals, Challenges, Best Practices. Consultado em 5 de março de 2023. Disponível em: https://www.knowledgehut.com/blog/security/cyber-threat-intelligence

Yesyev, A. (2021). Successful threat hunting requires a visible, intelligent network. Consultado em 5 de março de 2023. Disponível em: https://accedian.com/blog/successful-threat-hunting-requires-a-visible-intelligent-network/

Glossário

Zero-day - Um ataque de dia zero, também conhecido como exploração de dia zero, é um tipo de ataque cibernético que explora uma vulnerabilidade ou fraqueza numa aplicação ou sistema de *software* que é desconhecido do programador ou fornecedor de *software*. Isto significa que os atacantes podem tirar partido desta vulnerabilidade antes de uma correção ou atualização de segurança ser desenvolvida e divulgada ao público.

Hacking - Refere-se ao ato de obter acesso não autorizado a sistemas, redes ou dispositivos informáticos com a intenção de manipular, roubar, ou destruir dados, ou perturbar as operações do sistema.

Honeypots - São sistemas ou aplicações de engodo que são especificamente concebidos para atrair e apanhar atores de ameaça. O objetivo de um *honeypot* é detetar e estudar as tácitas, técnicas e procedimentos utilizados, bem como desviar a sua atenção dos sistemas de produção reais.

Backend - É a parte da aplicação que não é visível para o utilizador e é responsável pelo tratamento da lógica e gestão dos dados nos bastidores. Processa os pedidos dos utilizadores, recupera dados da base de dados e envia os resultados de volta para o *front-end* para exibição ao utilizador.

Backdoors - Refere-se a um ponto de entrada escondido ou método de acesso a um sistema informático, aplicação ou rede que ultrapassa as medidas normais de segurança e são frequentemente criados por atacantes para obter acesso não autorizado a um sistema ou rede e permanecem indetetáveis enquanto realizam atividades maliciosas, tais como roubar dados sensíveis, instalar *malware*, ou lançar ataques contra outros sistemas.

Apêndices

APÊNDICE I – *Inputs* configurados para a recolha de dados

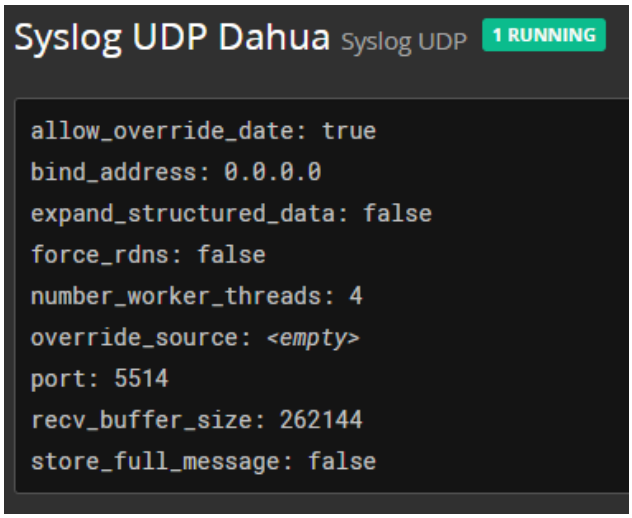

Figura 38 - Input para a recolha de dados dos equipamentos Dahua.

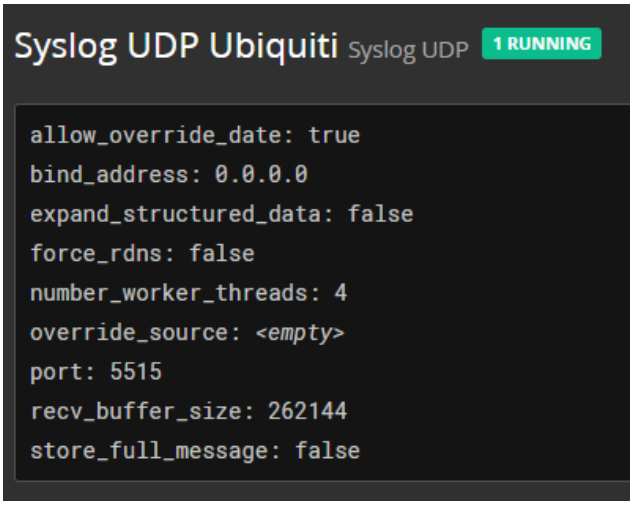

Figura 39 - Input para a recolha de dados dos equipamentos Ubiquiti.

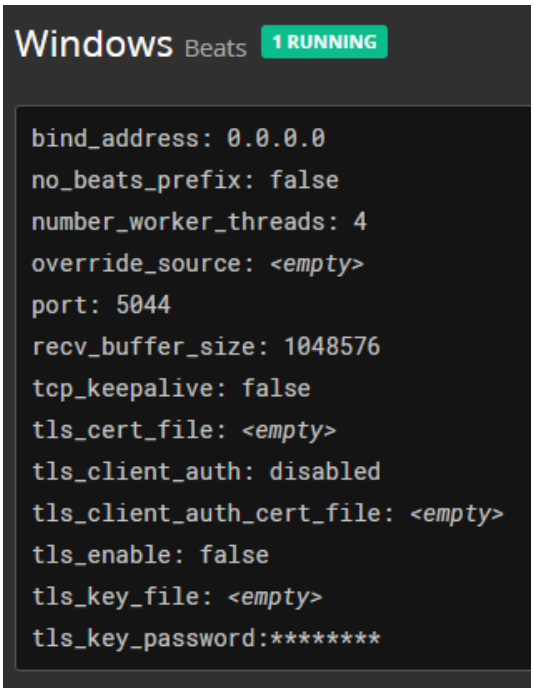

Figura 40 - Input para a recolha de dados dos equipamentos com sistema operativo Windows.

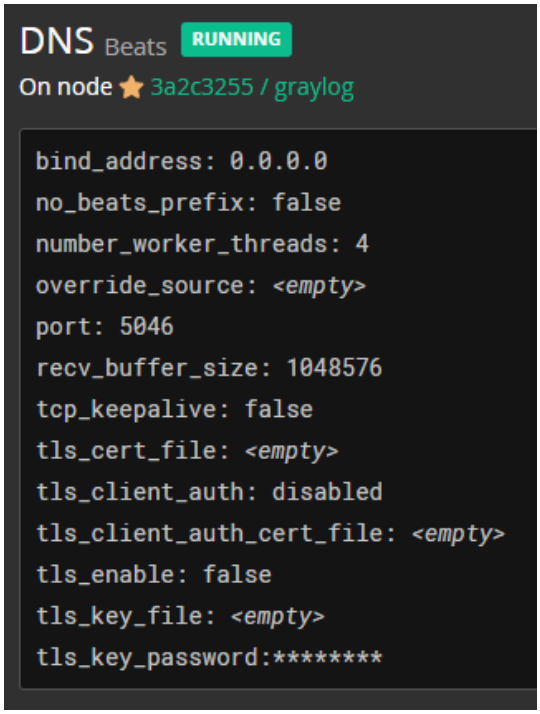

Figura 41 - Input para a recolha de dados via Beats, neste caso para os logs DNS.

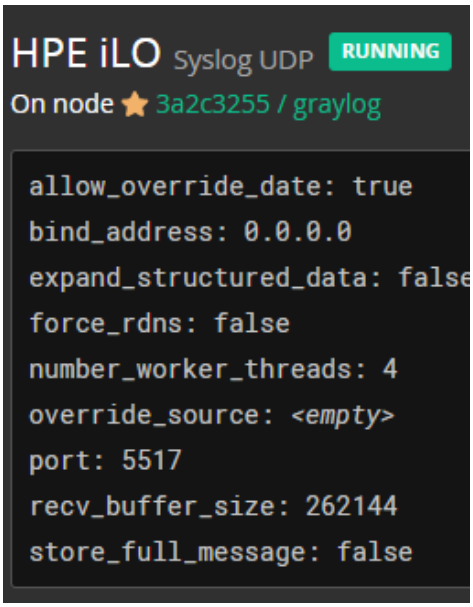

Figura 42 - Input para a recolha de dados dos equipamentos HPE com interfaces iLO (Servidores HP).

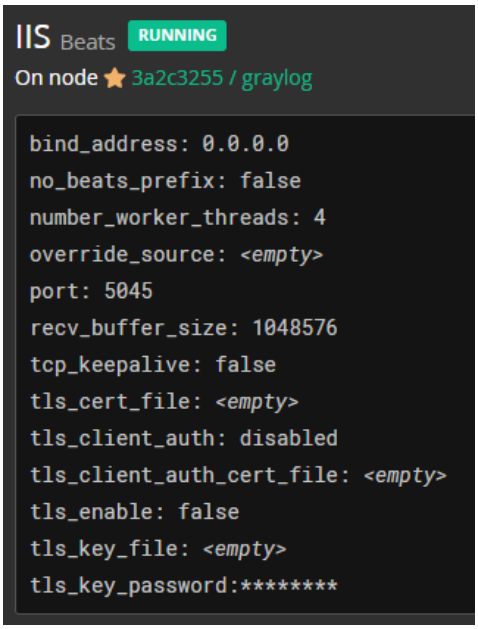

Figura 43 - Input para a recolha de dados via Beats, neste caso para os logs do IIS (Servidores Web).

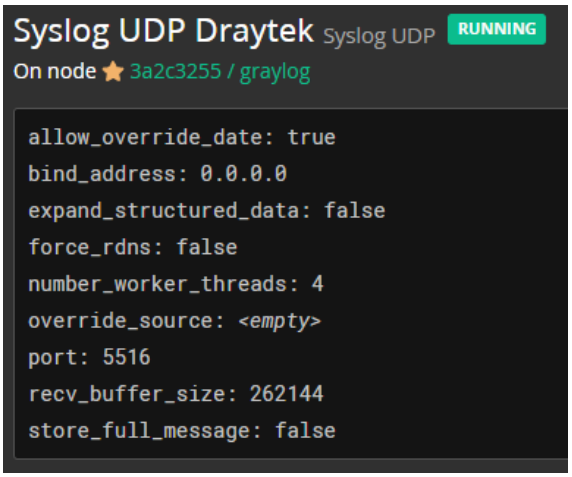

Figura 44 - Input para a recolha de dados para equipamentos Draytek.

APÊNDICE II – Extratores configurados a normalização dos *Logs*

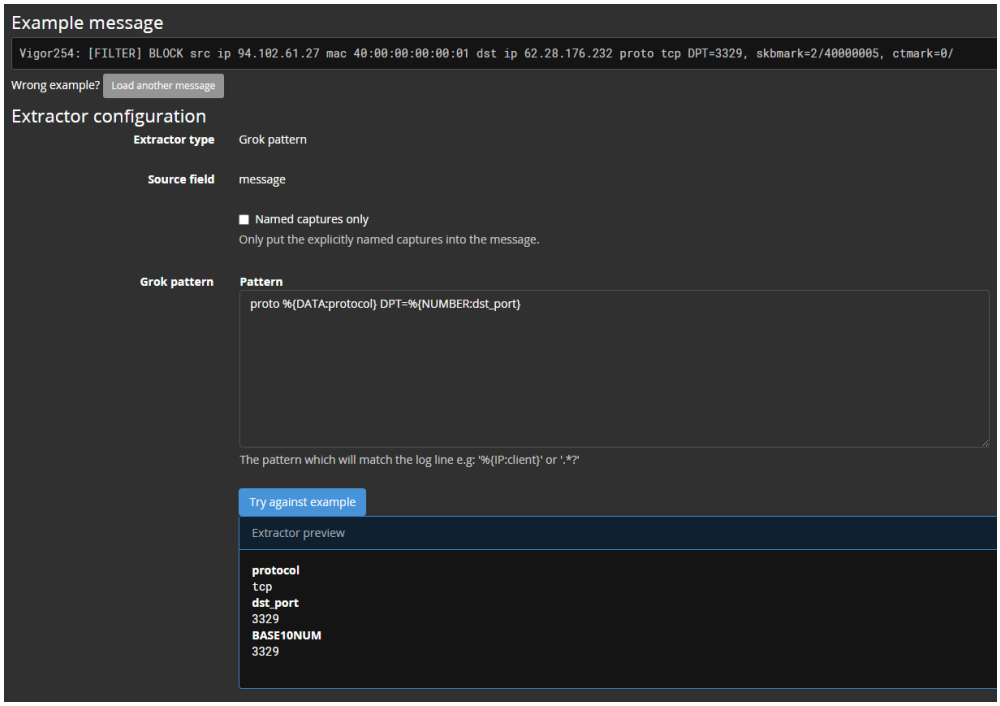

Figura 45 - Extrator do tipo grok pattern para a normalização da porta de destino e protocolo dos equipamentos Draytek.

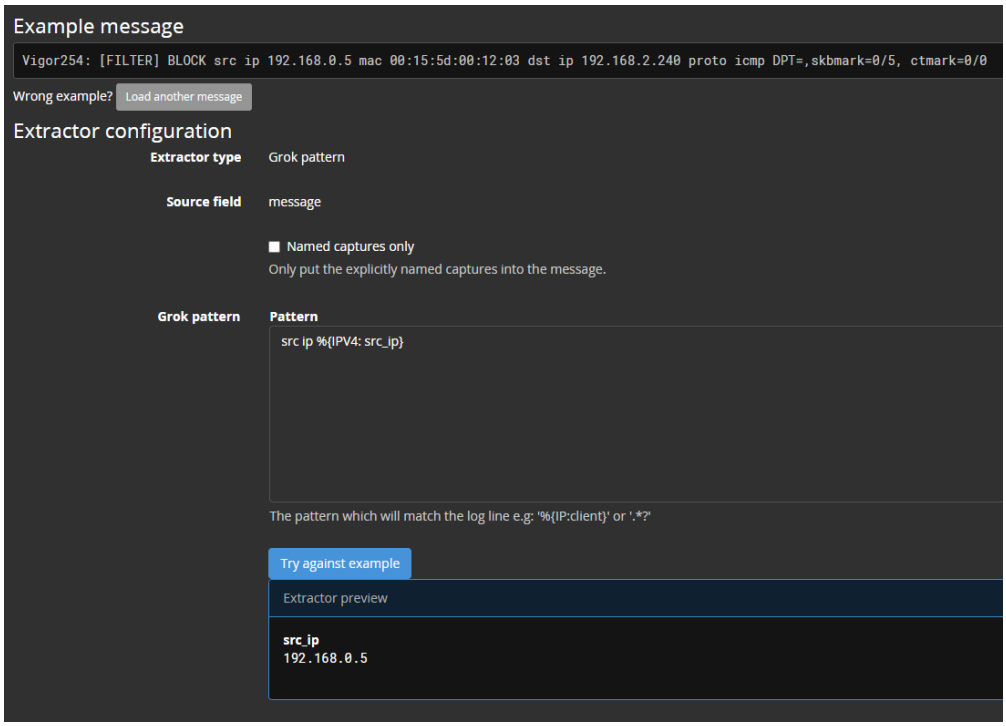

Figura 46 - Extrator do tipo grok pattern para a normalização do ip de origem dos equipamentos Draytek.

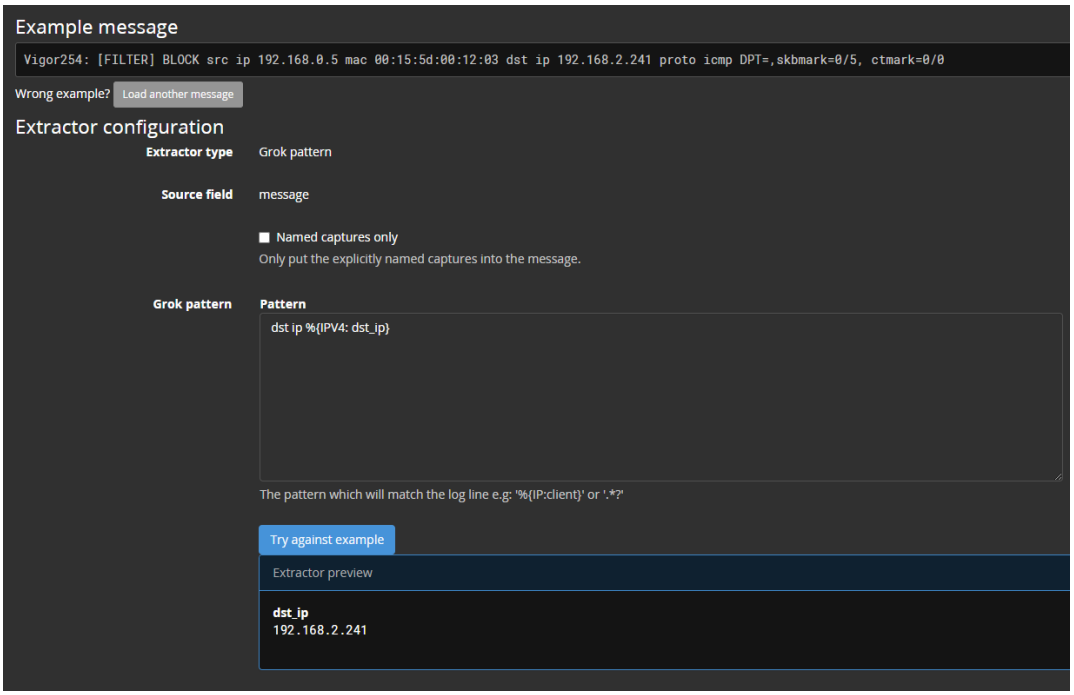

Figura 47 - Extrator do tipo grok pattern para a normalização do ip de destino dos equipamentos Draytek.

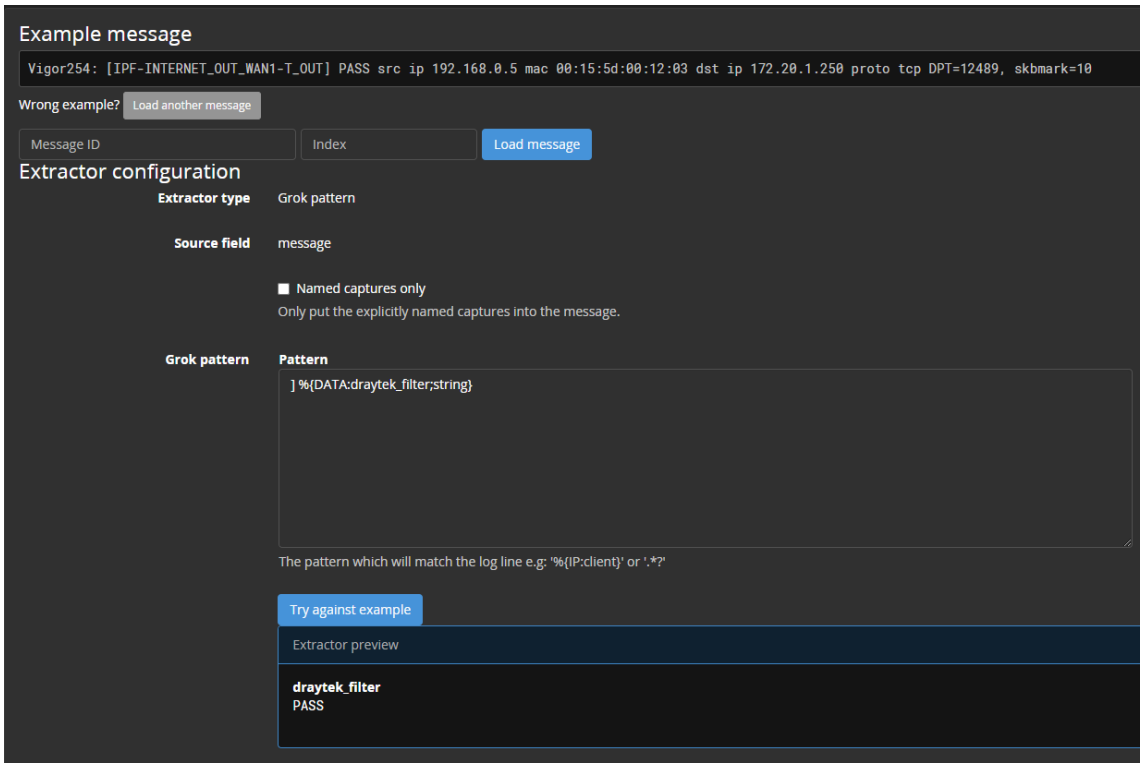

Figura 48 - Extrator do tipo grok pattern para a normalização do filtro aplicado dos equipamentos Draytek.

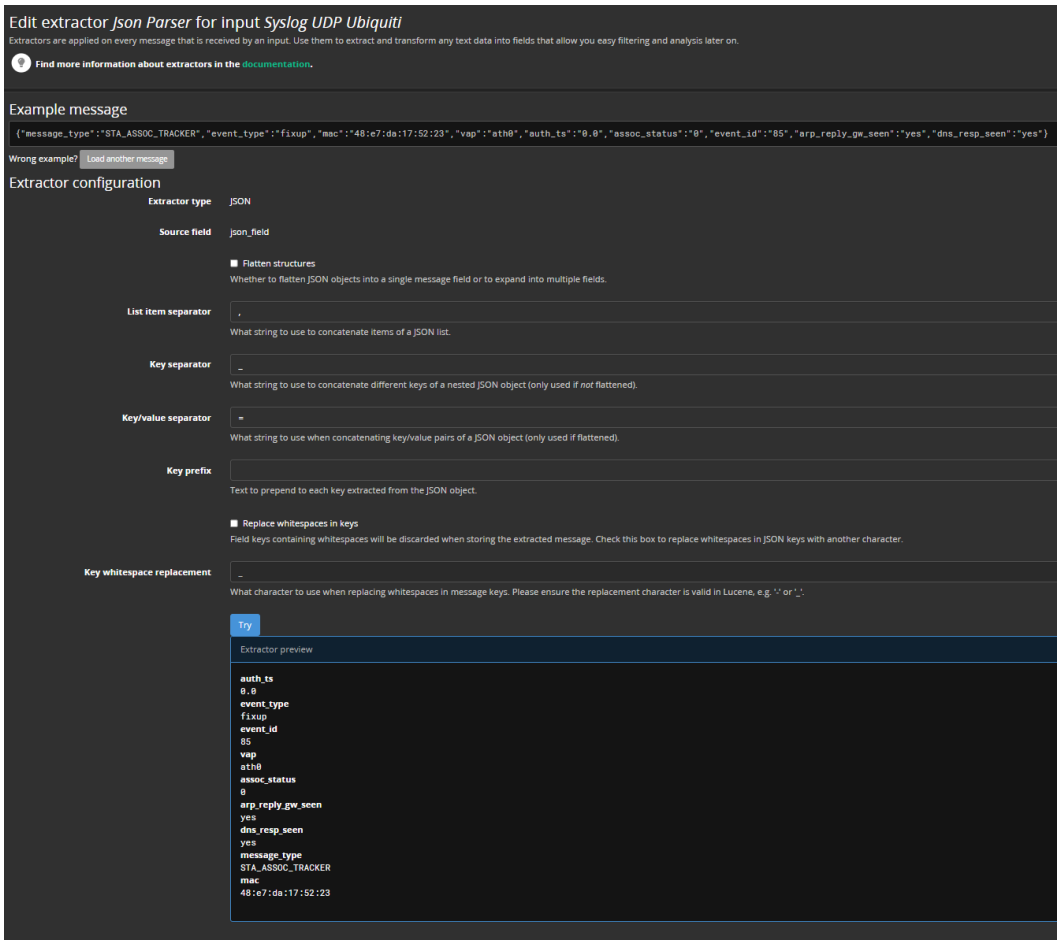

Figura 49 - Extrator do tipo json parser para a normalização do filtro aplicado dos equipamentos Ubiquiti.

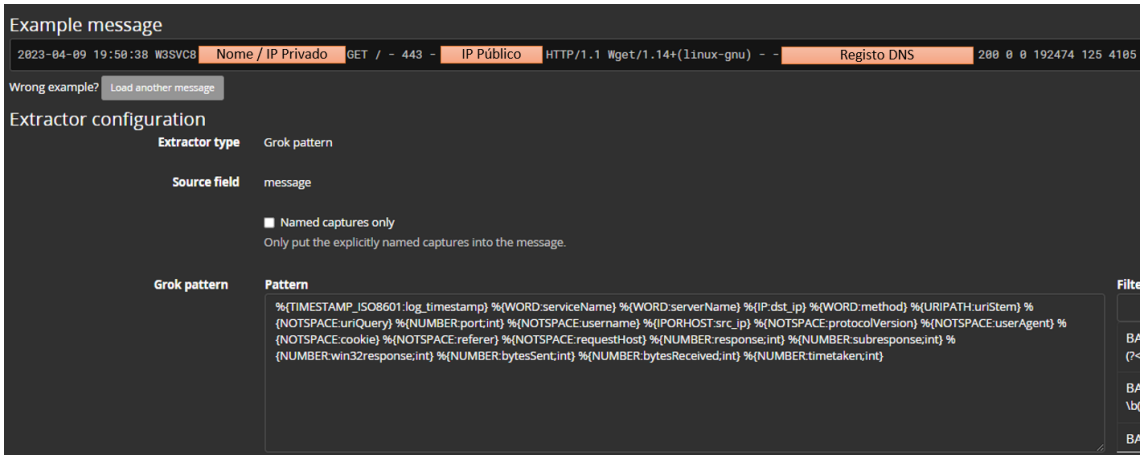

Figura 50 - Extrator do tipo grok pattern para a normalização dos logs provenientes do IIS.

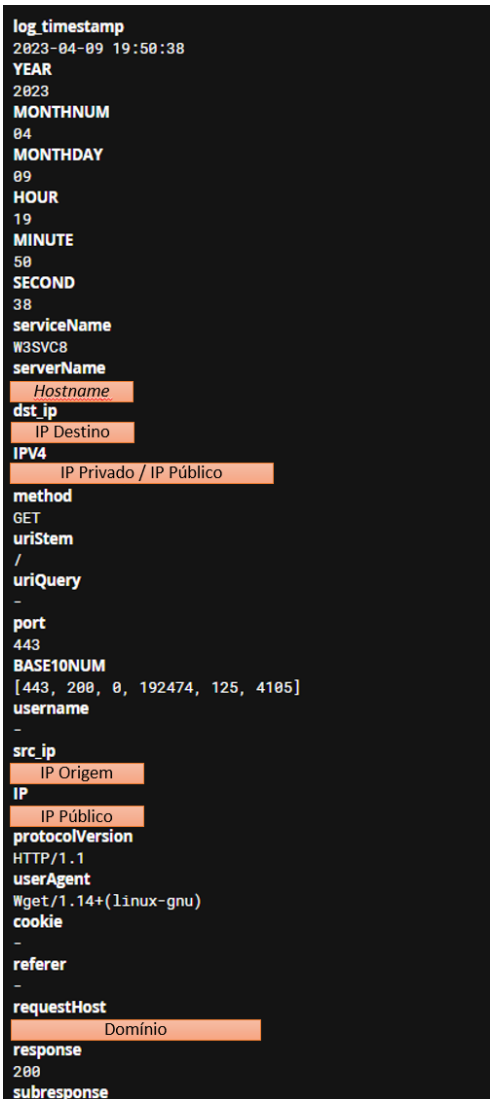

Figura 51 - Resultado do tipo grok pattern para a normalização dos logs provenientes do IIS.

APÊNDICE III – Histórico de alertas e eventos

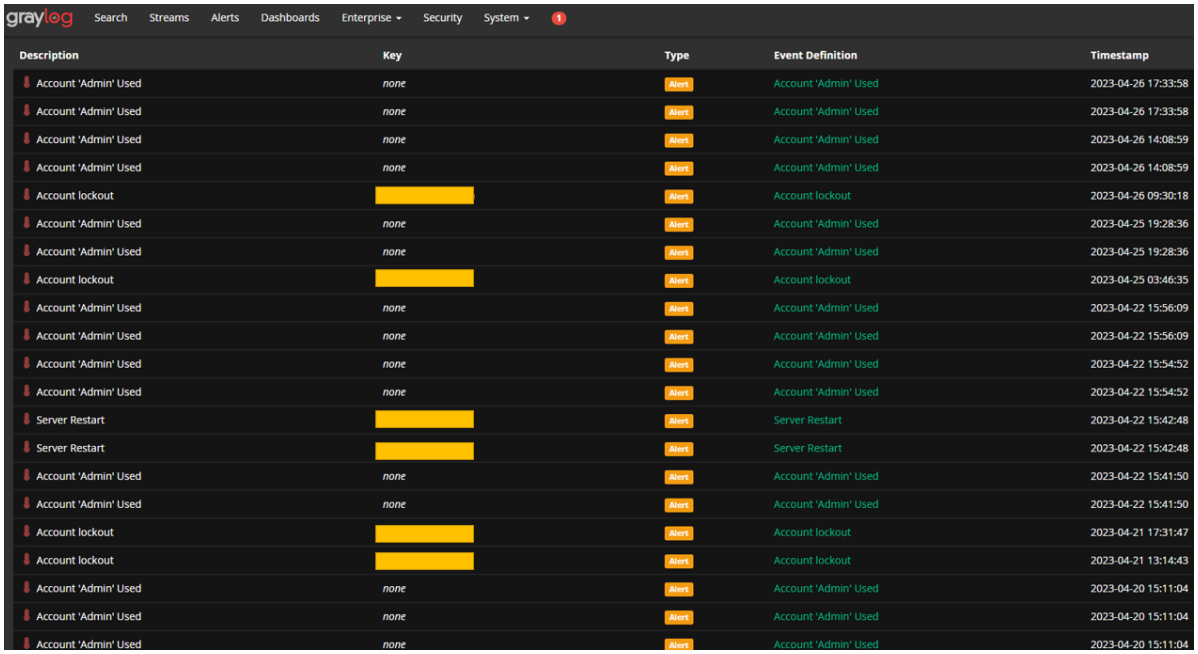

Figura 52 - Resultado do tipo grok pattern para a normalização dos logs provenientes do IIS.

APÊNDICE IV – Configuração da API *Greynoise*

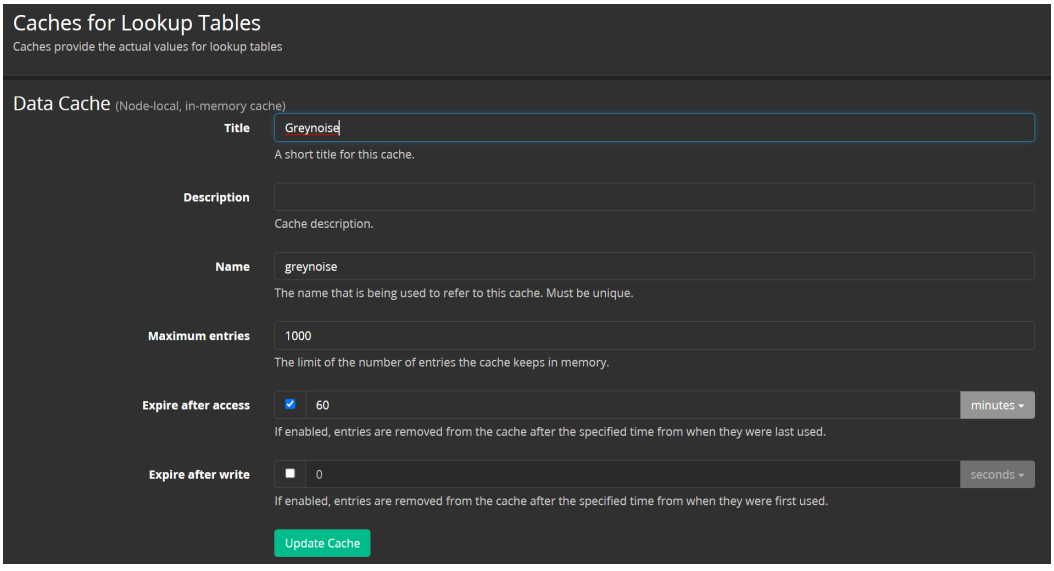

Figura 53 - Criação da Data Cache – Greynoise.

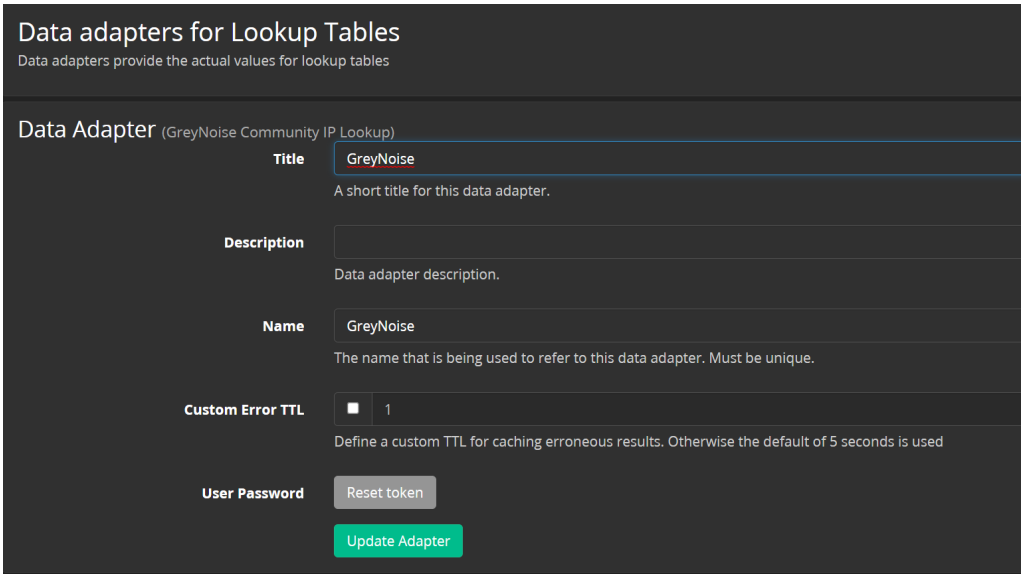

Figura 54 - Criação do Data Adapter – Greynoise.

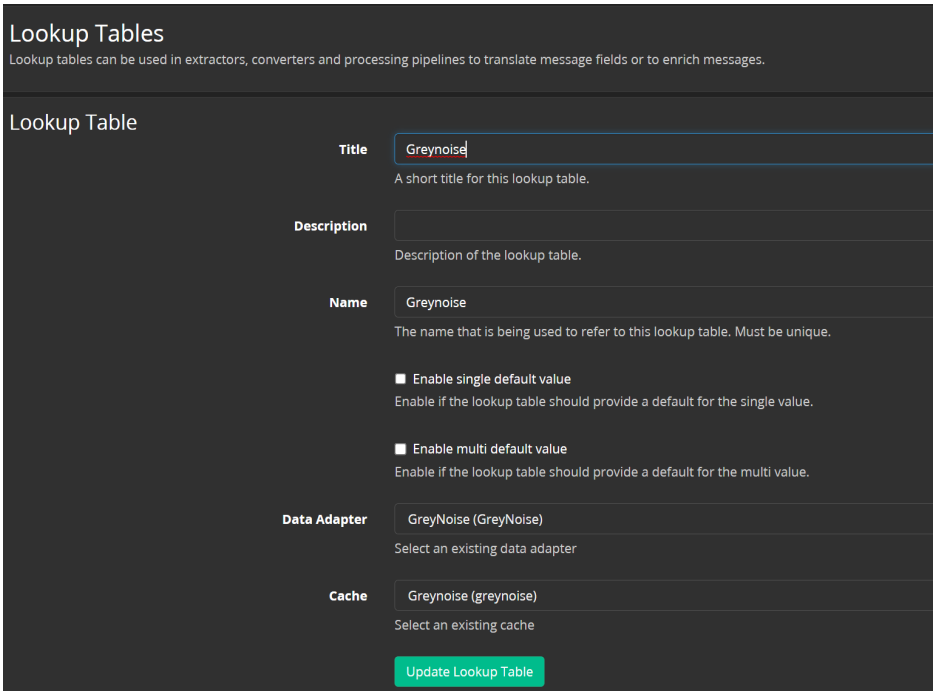

Figura 55 - Criação do Lookup Table – Greynoise.

APÊNDICE IV – Classificação de eventos usando a API *Greynoise*

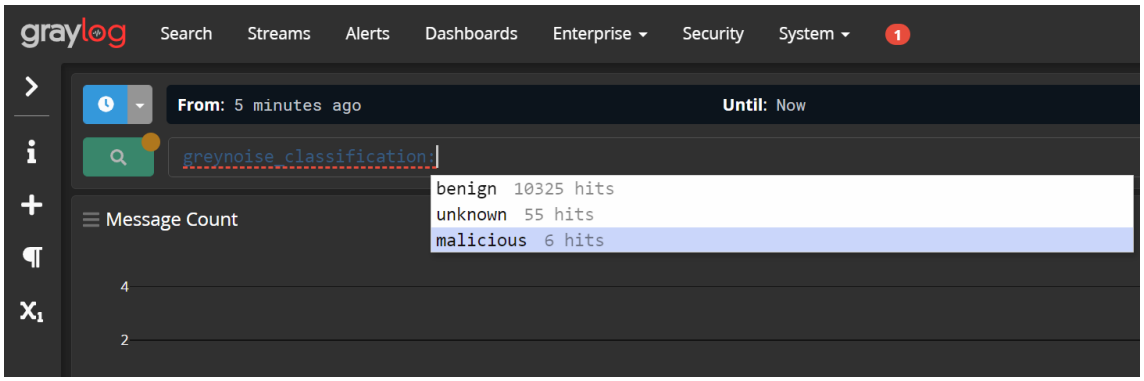

Figura 56 - Procura por classificação de ligações IP, usando o Graynoise.

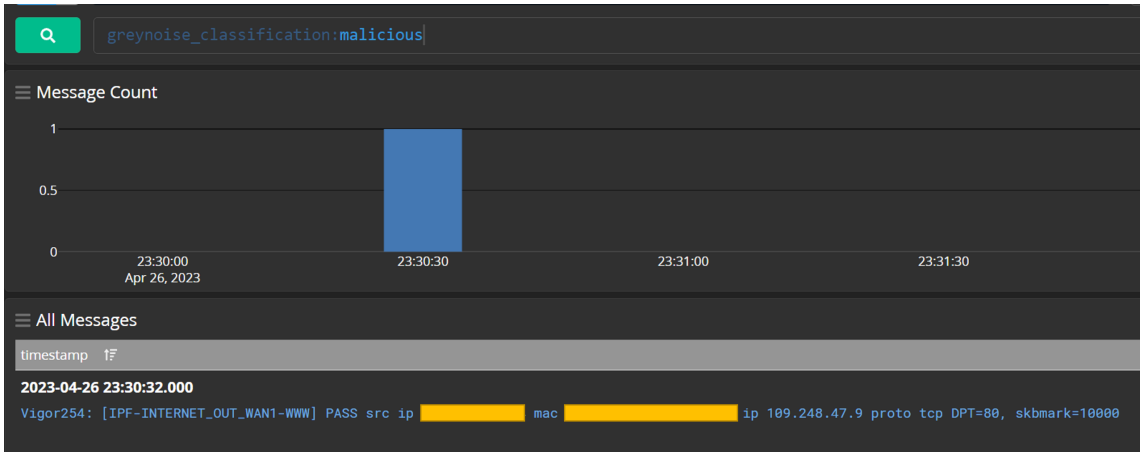

Figura 57 - Procura por classificação de ligações IP, usando o Graynoise e o filtro malicious.

APÊNDICE V – Configuração do GEO IP no *Graylog*

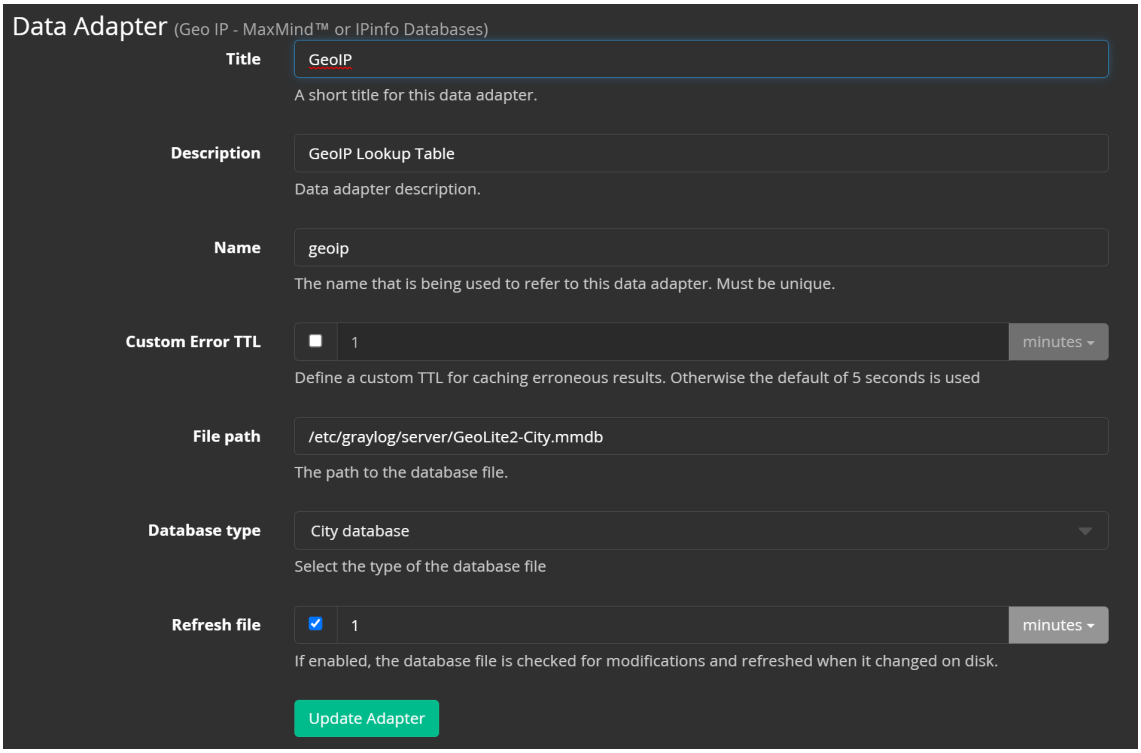

Figura 58 - Configuração do Data Adapter para a consulta da Base de Dados de geolocalização.

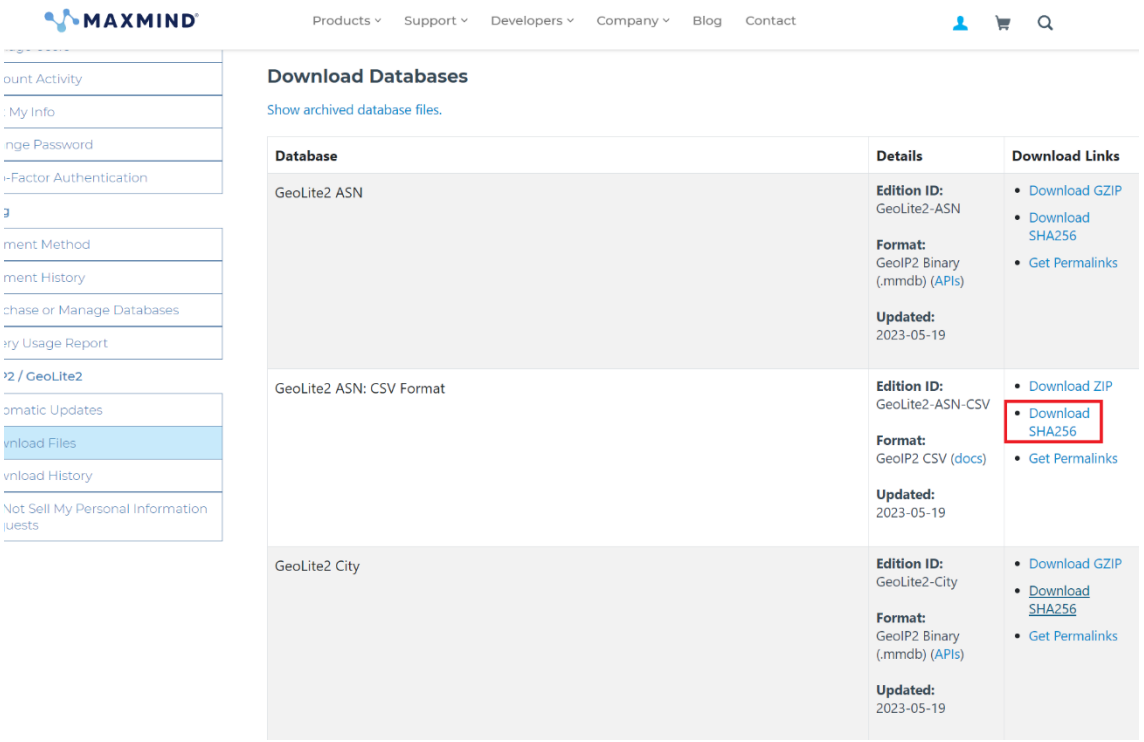

Figura 59 - Download da base de dados GeoLite2 City retiradas do seguinte URL: https://dev.maxmind.com/geoip/geolite2-free-geolocation-data)

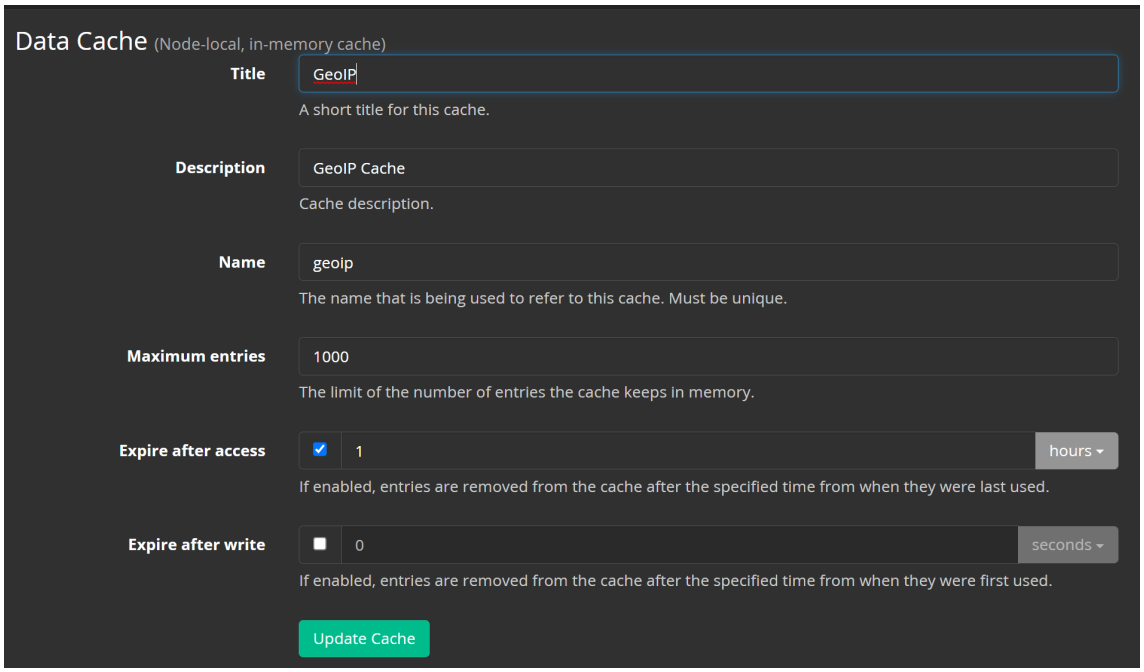

Figura 60 - Configuração da cache para a tabela geoip.

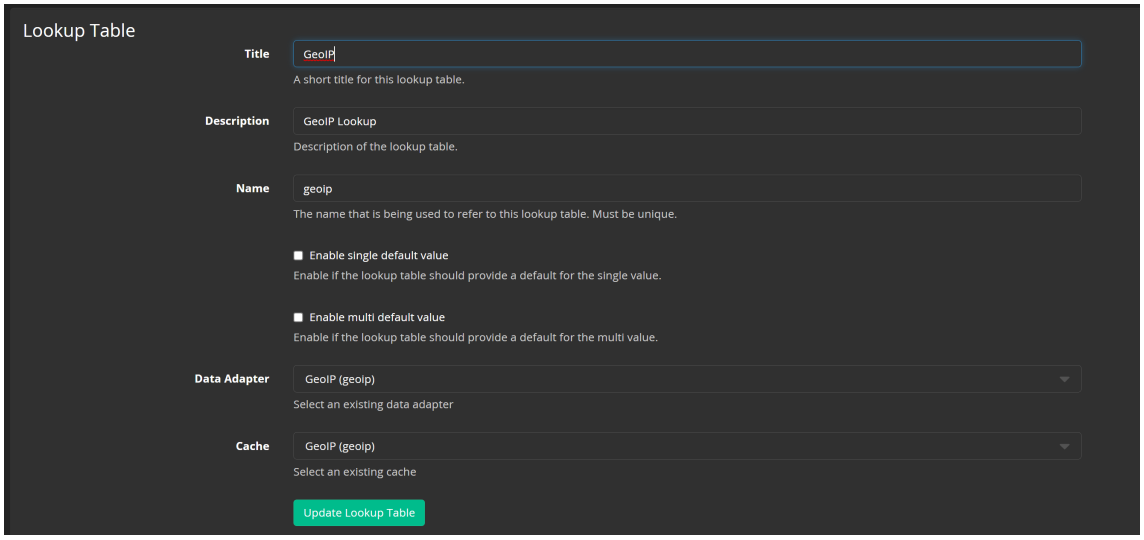

Figura 61 - Criação da tabela em si, usando o adaptador e cache criados anteriormente.

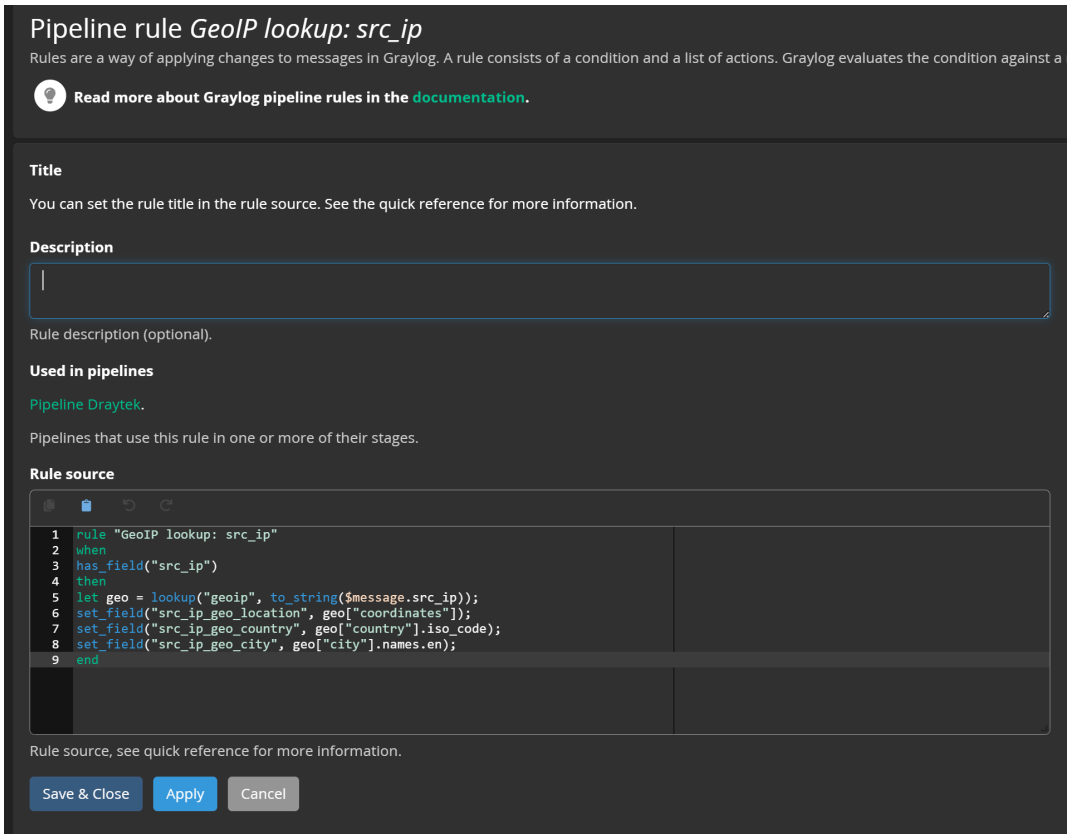

Figura 62 - Criação da regra de pipeline para a inclusão dos parâmetros geo_location, geo_country e geo_city, sempre que uma entrada contenha o parâmetro src_ip.

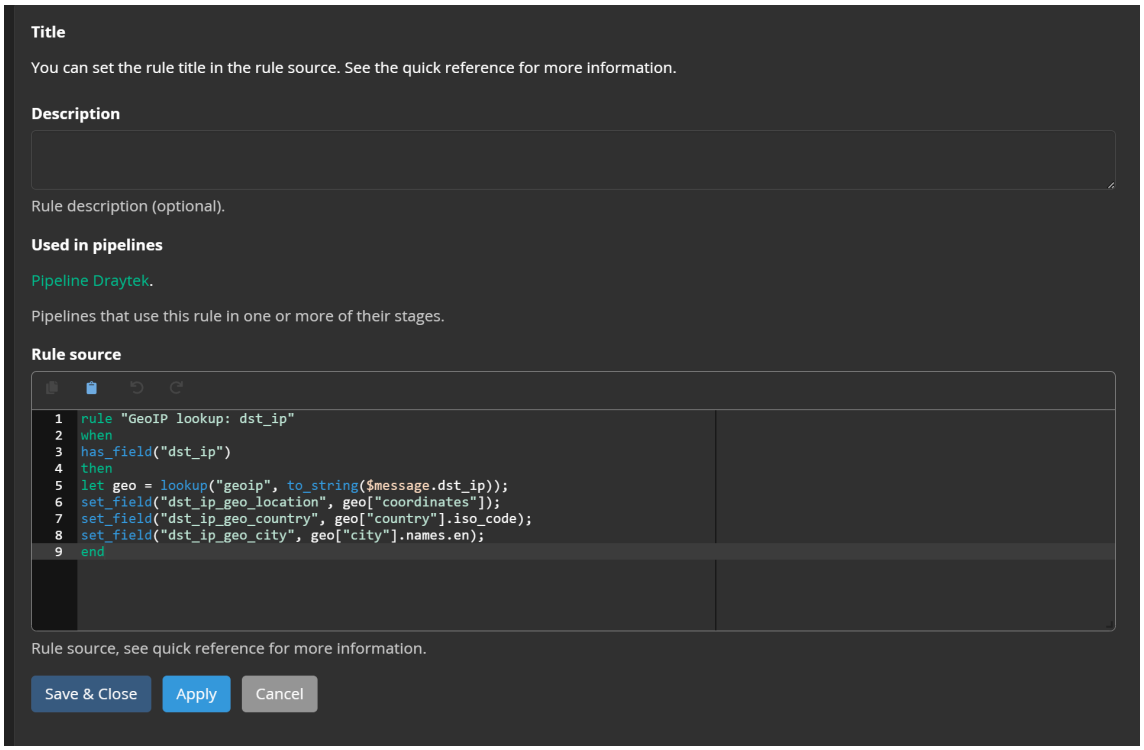

Figura 63 - Criação da regra de pipeline para a inclusão dos parâmetros geo_location, geo_country e geo_city, sempre que uma entrada contenha o parâmetro dst_ip.

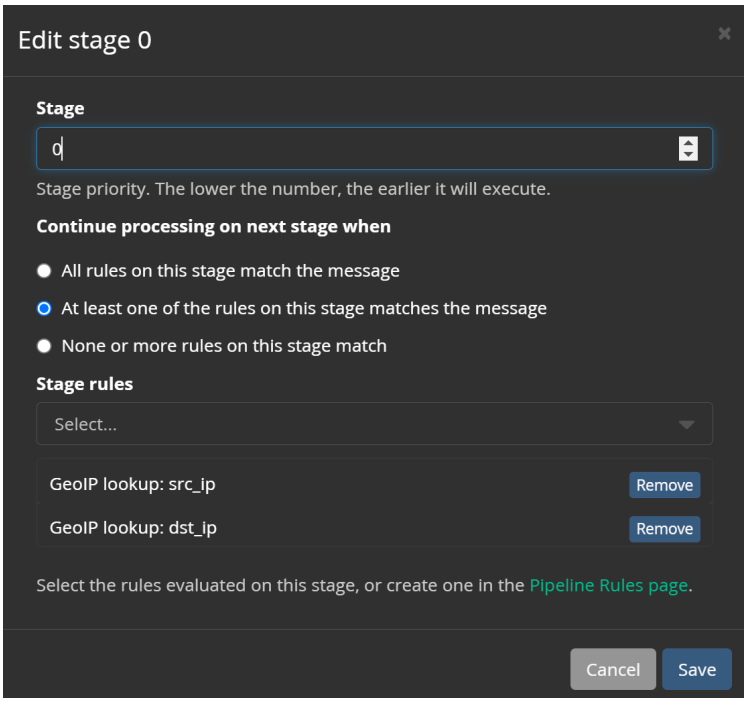

Figura 64 - Adição das regras à fase 0 do pipeline.

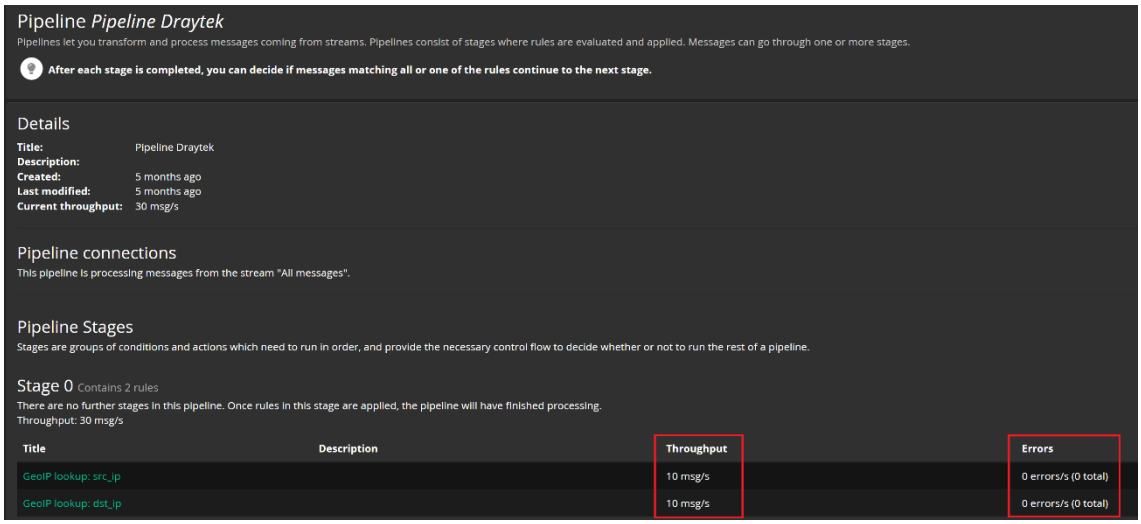

Figura 65 - Confirmação do funcionamento das regras no pipeline Draytek.

APÊNDICE VI – Plataforma *OpenSource* OCS *Inventory*

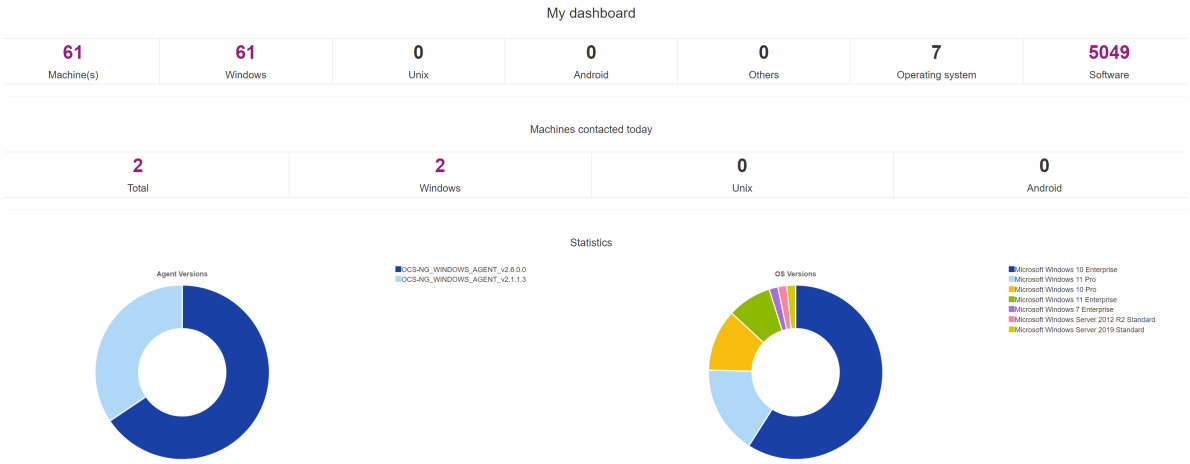

Figura 66 - Dashboard da plataforma de inventário OpenSource- OCS Inventory

APÊNDICE VII – Exemplo de log *Winlogbeat*

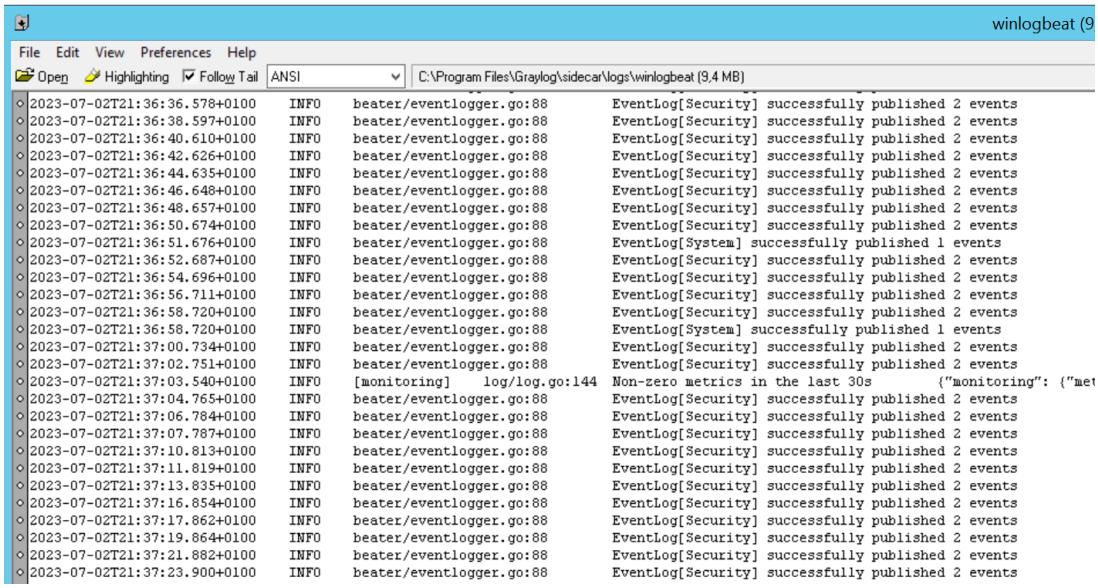

Figura 67 - Exemplo do log produzido pelo Winlogbeat.