

Cibersegurança para PME – Módulo I

Licenciatura em Engenharia Informática

Victor Hugo Boarato

Pierre Morgado

Leiria, setembro de 2021

Cibersegurança para PME – Módulo I

Licenciatura em Engenharia Informática

Victor Hugo Boarato

Pierre Morgado

Trabalho de Projeto da unidade curricular de Projeto Informático realizado sob a orientação
do Professor Doutor Carlos Rabadão e do Professor Doutor Leonel Santos.

Leiria, setembro de 2021

Resumo

Atualmente, os sistemas e as redes são cada vez maiores e mais complexas, com um enorme crescimento de dispositivos conectados à Internet, isto implica que a sua proteção contra atividades maliciosas seja uma tarefa complexa e de grande importância.

Nesse cenário, as empresas que pretendem proteger os seus dados e a sua propriedade intelectual, a identidade dos seus clientes e manter o ritmo de trabalho sem interrupções, precisam de desenvolver tarefas que não se limitem apenas na monitorização de registos e dados de fluxo da rede. Além disso, têm de potenciar ferramentas necessárias para detetar e analisar estas atividades de uma forma heurística e comportamental.

Nesta componente os *Security Information and Event Management* (SIEM) são vistos como ferramentas de grande utilidade no combate de ataques informáticos, não deixando de ter os seus pontos fracos, algo que pode ser mitigado com a integração de sistemas *Threat Intelligence Platforms* (TIP).

No âmbito deste trabalho, foram exploradas as diversas ofertas *open source* de sistemas SIEM e TIP, realizando um comparativo entre as várias opções, com o objetivo final de ser implementado um protótipo utilizando os recursos que mais nos adequam, adequadamente justificado.

Palavras-chave: Cibersegurança, *Security Information and Event Management*, *Threat Intelligence Platforms*, *open source*, *Logs*

Abstract

Currently, systems and networks are increasingly larger and more complex, with a huge growth of devices connected to the Internet, this implies that their protection against malicious activities is a complex task of great importance.

In this scenario, companies that want to protect their data and their intellectual property, the identity of their customers and keep the work pace uninterrupted, need to develop tasks that are not limited only to monitoring records and network *flow* data. Furthermore, they have to leverage the tools needed to detect and analyze these activities in a heuristic and behavioral way.

In this component, Security Information and Event Management (SIEM) are seen as very useful tools in combating computer attacks, not forgetting their weaknesses, something that can be mitigated with the integration of Threat Intelligence Platforms (TIP) systems.

Within the scope of this work, the various open source offers of SIEM and TIP systems were explored, making a comparison between the various options, with the final objective of implementing a prototype using the resources that best suit us, properly justified.

Keywords: Cybersecurity, Security Information and Event Management, Threat Intelligence Platforms, *open source, Logs*

Lista de Figuras

Figura 1 - Pilares da Segurança da Informação retidado de (oliveira, 2021)	4
Figura 2 - Pesquisa sobre as ameaças mais relevantes, retirado de (Help, 2021).....	9
Figura 3 - Relatório do Quadrante Magico Gartner, retirado de (Gartner, 2021).....	10
Figura 4 - Arquitetura da solução USM Anywhere (AT&T, 2021)	12
Figura 5 - Arquitetura do <i>Elastic Stack</i>	16
Figura 6 - <i>Flow</i> dos <i>Logs</i> do <i>Elastic Stack</i>	16
Figura 7 - Licenciamento do <i>Elastic Stack</i>	18
Figura 8 - Várias Funcionalidades das Licenças do Elastic Stack.....	19
Figura 9 - Arquitetura do Splunk	22
Figura 10 - Arquitetura do MozDef	26
Figura 11 - Funcionamento do SIEMonster	29
Figura 12 - <i>Flow</i> dos <i>Logs</i> no Siemonster.....	30
Figura 13 - Vários recursos do SIEMonster.....	30
Figura 14 - Várias licenças do Siemonster (Siemonster, 2021).....	34
Figura 15 - Diagrama do funcionamento de um SIEM com TIP, (Prytuluk, 2021)	41
Figura 16 - Arquitetura abstrata do funcionamento de um SIEM com integração TIP	48
Figura 17 - Funcionamento lógico do <i>Elastic Stack</i>	49
Figura 18 - aceder à porta 9200 (Elasticsearch)	50
Figura 19 - Menu Principal do <i>Kibana</i>	52
Figura 20 - Criar um user no Kibana.....	53
Figura 21 - Dashboard do Auditbeat	54
Figura 22- Como os dados são recolhidos no Filebeat (elastic f. , 2021)	55
Figura 23 - Menu Discover do Kibana onde se pode visualizar os logs do Filebeat com as tags	56
Figura 24 – Verificação dos vários monitors no Heartbeat	57
Figura 25 - Arquitetura da solução.....	61
Figura 26 - Esquema da recolha de métricas do servidor Apache.....	64
Figura 27 - Esquema Lógico da recolha de métricas com redundância	65
Figura 28 - Esquema do funcionamento de um alerta do Elastalert	66

Figura 29 - Esquema Genérico do <i>flow</i> dos Feeds do TIP.....	66
Figura 30 - Esquema do <i>flow</i> dos <i>feeds</i> do Misp.....	68
Figura 31 - Localização da Auth Key no MISP.....	68
Figura 32 -- Flow dos <i>feeds</i> do TIP na solução	69
Figura 33 - Subscrição de <i>feeds</i> no OTX.....	69
Figura 34 - <i>Dashboard</i> do OTX	71
Figura 35 - Vários <i>feeds</i> para subscrever no OTX.....	71
Figura 36 - OTX key para receber os <i>feeds</i>	72
Figura 37 - Informação que irá ser enviada pelos <i>feeds</i> do OTX.....	72
Figura 38 - Log recebido no Filebeat com IP recebido pelos <i>feeds</i> do OTX.....	73
Figura 39 - Esquema de ataque <i>Brute-force</i>	74
Figura 40 - Comando hydra para ataque <i>brute-force</i>	74
Figura 41 - várias tentativas de autenticação no menu SSH Login Attempts	75
Figura 42 – Esquema ataque DDOs.....	76
Figura 43 - Comando ataque DDoS.....	76
Figura 44 - Dashboard Access and error logs.....	77
Figura 45 - Esquema de ataque SynFlood	78
Figura 46 - Comando ataque Synflood	78
Figura 48 - Picos de pacotes recebidos (Por IP)	79
Figura 47 - Pico de Pacotes recebidos pelo ataque SY flood.....	79
Figura 49 – Comando para execução do PsExec	80
Figura 50 - Verificação do ataque Psexec pelo Winlogbeat	81
Figura 51 - Verificação do ataque PsExec através do menu Detections do Kibana	81
Figura 52 - Alerta no Slack do Ataque PsExec	82
Figura 53 - Métricas mostradas no Metricbeat	82
Figura 54 - Metrics mostradas no Metricbeat por tags.....	83
Figura 55 - Visao Global do Sistema no Netdata	84
Figura 56 - Metrics no Prometheus pelas várias tags.....	85
Figura 57 - Visão inicial do Netdata.....	86
Figura 58 - Targets no Prometheus.....	87

Figura 59 - Grafico com o uso do cpu das diferentes máquinas.....	87
Figura 60 - <i>Dashboard</i> com as métricas no Grafana.....	88
Figura 61 - Datasource / Job/ <i>Host</i> no Grafana	89
Figura 62 - Esquema do Funcionamento logico entre o Netdata/Prometheus/Grafana.....	89
Figura 63 - Aumento nas métricas do tráfego da rede quando um ataque ‘ <i>SYN Flood</i> é feito.....	90
Figura 64 - Menu de login do MISP.....	91
Figura 65 - Listar <i>feeds</i> no Misp	91
Figura 66 - Adicionar Feeds para o Misp.....	92
Figura 67 - Feeds adicionados ao MISP.....	92
Figura 68 - Lista de Atributos no Misp	93
Figura 69 - Dashboard no Kibana com a informação recebida pelos feeds.....	93
Figura 70 - Criar regra no Kibana	94
Figura 71 - Alerta no Slack descrevendo as condições	94
Figura 72 - Criar Regra com os tags recebidas pelos feeds do OTX.....	95
Figura 73 - Alerta no Slack coicidindo as tags do OTX.....	95
Figura 74 - Criar Relatório	96
Figura 75 - Gerar relatório em formato CSV com as pesquisas realizadas	96
Figura 76 - Relatórios Listados	97

Lista de tabelas

Tabela 1 - Características dos vários SIEMS.....	36
Tabela 2 - Requisitos de Hardware das soluções SIEM	37
Tabela 3 - Soluções TIP mais utilizadas	42
Tabela 4 - Descrição das várias máquinas da solução	62

Lista de siglas e acrónimos

API Application Programming Interface

ESTG Escola Superior de Tecnologia e Gestão

ICMP Internet Control Message Protocol

IOC Indicadores de Compromisso

IPLeiria Instituto Politécnico de Leiria

JSON Javascript Object Notation

LMS Log Management System

OSINT Open source intelligence

PME Pequenas Médias Empresas

SEC Security Event Correlation

SEM Security Event Management

SIEM	Security Information Event Management
SIM	Security Information Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SPL	Search Processing Language
TIP	Threat Intelligence Platform
UEBA	User and Entity Behavior Analytics

Índice

Resumo.....	ii
Abstract.....	iii
Lista de Figuras.....	iv
Lista de tabelas.....	vii
Lista de siglas e acrónimos	viii
1. Introdução	1
2. Eventos de Segurança.....	3
2.1. Ataque Informático	4
2.2. <i>Logs</i>	5
2.3. Security Information and Event Management	7
2.3.1. Funções de um sistema SIEM	8
2.3.2. Soluções SIEM	9
2.3.2.1. OSSIM.....	11
2.3.2.2. Elastic Stack	15
2.3.2.3. SPLUNK.....	21
2.3.2.4. MozDef.....	26
2.3.2.5. SIEMONSTER.....	29
2.4. Comparações das soluções SIEM.....	35
2.5. Características mais relevantes num SIEM	37
2.6. Threat Intelligence.....	38
2.6.1. Threat Intelligence Platform (TIP)	39
2.6.2. Como os TIP podem complementar um SIEM	40
2.6.3. Como funciona a integração TIP no SIEM	40
2.6.4. Soluções TIP.....	42
2.7. Síntese	45

3.	Arquitetura e <i>Elastic Stack</i>	48
3.1.	Arquitetura lógica	48
3.2.	<i>Elastic Stack</i>	49
3.2.1.1.	Elasticsearch.....	50
3.2.1.2.	Logstash	51
3.2.1.3.	Kibana	51
3.2.1.4.	Beats	54
3.3.	Síntese	59
4.	Implementação e testes	60
4.1.	Protótipo.....	61
4.1.1.	Especificações técnicas do protótipo.....	62
4.1.2.	Instalação do <i>Elastic Stack</i>	64
4.1.3.	Instalação e configurações dos <i>Beats</i>	64
4.1.4.	Instalação e configuração do Elastalert	65
4.2.	Integração do TIP no SIEM	66
4.2.1.	TIP MISP.....	67
4.2.2.	TIP OTX.....	69
4.3.	TESTES.....	73
4.3.1.	Ataques simulados.....	74
4.3.2.	Monitorização e recolha de métricas.....	82
4.3.3.	TIP	91
4.3.4.	Relatórios	96
4.4.	Síntese	97
5.	Conclusão	99
5.1.	Análise crítica e proposta de melhorias.....	102
6.	Bibliografia	104
Anexo A – Instalação do <i>Elastic Stack</i>		111
Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus.....		125

Anexo C – Certificado SSL	135
Anexo D – TLS	138
Anexo E – Instalação do Elastalert.....	140
Anexo F - Alertas do <i>Kibana</i>	144

1. Introdução

Atualmente, a complexidade dos problemas colocados pela cibersegurança tem aumentado, principalmente se tivermos em conta a pandemia que começou em 2020, e passado pouco mais de um ano, podemos ver os problemas que isso trouxe na área da segurança informática (Grustniy, 2021).

Seja em teletrabalho ou dentro da empresa, é extremamente importante estabelecer regras de segurança e ter meios de detetar qualquer tipo de ataque.

No âmbito da unidade curricular do Projeto Informático do curso de Licenciatura Informática da Escola Superior de Tecnologia e Gestão do Instituto politécnico de leiria, foi elaborado o presente relatório sobre cibersegurança pra pequenas médias empresas (PME).

Nesse âmbito, este trabalho irá abordar diferentes soluções de SIEM e TIP *open source*, de forma a ser possível implementar em qualquer empresa sem custos de licenciamento, mas com as funcionalidades necessárias para obter uma proteção contra ataques informáticos.

O objetivo deste trabalho é explorar e demonstrar a importância dos sistemas de *Security Information Event Management* (SIEM), juntamente com as plataformas de *Threat Intelligence* (TIP) utilizadas pelos *Security Operations Center* (SOC).

Metodologia

Devida às limitações implicadas pela pandemia, o presente trabalho foi realizado totalmente à distância, sendo que a solução final foi feita em apenas uma máquina.

O trabalho foi feito em três etapas: pesquisa, comparações e desenvolvimento de um protótipo.

Tendo realizado a pesquisa bibliográfica necessária para perceber o funcionamento de um SIEM e de uma TIP, foi implementado um protótipo de forma a aplicar esses conhecimentos.

Estrutura do relatório

Na introdução, foi referido o problema referente ao trabalho, assim como os seus objetivos.

No segundo capítulo será feita uma introdução aos SIEM e às suas funções, seguido por uma análise comparativa de algumas das soluções *open source* mais utilizadas.

Num terceiro capítulo é abordado as TIP, com intuito de mostrar como estas plataformas podem complementar um SIEM.

No quarto capítulo é feita a descrição da solução proposta, onde iremos elaborar um cenário de testes e será documentado as configurações realizadas para obter os resultados desejados.

Por último, vamos ter o capítulo das conclusões, onde é feito um levantamento das principais ideias abordadas neste trabalho, são descritos os resultados obtidos. São comentadas as limitações da implementação do cenário proposto, assim como ideias para melhorias futuras.

2. Eventos de Segurança

Este capítulo irá focar-se na segurança informática, mais precisamente a segurança do software. Esta vertente, com o passar dos anos, tem vindo a tornar-se mais relevante.

Quando a Internet foi primeiramente desenvolvida, não se pensava na sua segurança. Com o crescimento da rede de computadores este conceito passou a ser considerado para quem a utiliza diariamente.

Existem dois tipos de segurança que ainda hoje criam incertezas nos seus conceitos, a segurança da informação e segurança informática. Estes apesar de serem complementares, tem objetivos diferentes. A segurança informática trata-se da proteção ao nível dos sistemas informáticos, onde a informação é geralmente armazenada e difundida. Por outro lado, a segurança da informação tem a responsabilidade na proteção da informação armazenada de distintas formas entre os diferentes canais (Santos, 2016).

Podemos então afirmar que a segurança informática está relacionada com a confidencialidade, integridade, disponibilidade, irrefutabilidade, responsabilidade, autenticidade e confiabilidade dos recursos da informação, pela norma, ISO/IEC 13335-1 de 2004 (Torres, 2014).

A segurança da informação, por outro lado, não se trata apenas da proteção da informação armazenada nos computadores, mas também dos outros canais, como documentos impressos ou escritos. A norma internacional ISSO/IEC 27002 define-a como sendo a preservação da confidencialidade, integridade e disponibilidade (Torres, 2014).

Estes três pilares da segurança da informação podem ser explicados da seguinte forma:

- **Confidencialidade** – Garantir que a informação não é exposta às pessoas ou entidades sem autorização;
- **Integridade** — Corresponde à preservação dos dados, sem que haja uma interferência externa que os possa comprometer;

- **Disponibilidade** – Assegurar que os dados e sistemas possam ser acedidos a qualquer momento com a devida autorização.



Figura 1 - Pilares da Segurança da Informação retidoado de (oliveira, 2021)

Como já foi referido anteriormente, este trabalho é focado na segurança informática, para isso é importante introduzir alguns conceitos fundamentais envolvidos nas ameaças informáticas. Os seguintes tópicos visam explicar esses conceitos.

2.1. Ataque Informático

Um ataque informático é uma tentativa maliciosa e deliberada por indivíduos ou organizações de violar o sistema informático de outro individuo ou organização (Cisco, s.d.).

Existem dois tipos de ataques: **passivos** e **ativos**.

O primeiro tipo de ataque é o ataque passivo. Ataques passivos podem monitorar, observar ou construir o uso de dados do sistema para certas funções. No entanto, não tem efeito sobre os recursos do sistema e os dados podem permanecer inalterados. É difícil para as vítimas perceberem ataques passivos porque esse tipo de ataque é realizado em segredo. O objetivo dos ataques passivos é obter dados ou fazer a varredura em busca de portas abertas e vulnerabilidades de rede (Bhattacharya, 2021).

Ataques ativos podem ser ataques à rede, durante os quais o invasor modifica ou altera o conteúdo e afeta os recursos do sistema. Isso pode causar danos à vítima. Os invasores podem realizar ataques passivos para recolher informações antes de iniciar um ataque violento. O invasor tentou parar e forçar o sistema a travar. A vítima pode ser notificada para tomar a iniciativa de atacar. Esse tipo de ataque pode ameaçar sua integridade e acessibilidade. Ataques de força bruta são mais difíceis de realizar do que ataques passivos. Exemplos deste tipo de ataque são: *Denial-of-Service* (DoS), *ICMP flood*, *SYN Flood* e ataques Trojan (Bhattacharya, 2021).

2.2. Logs

A gestão de *logs* trata-se de preparar sistematicamente os *logs* do sistema e da rede recolhidos pela empresa (Barajas, 2020). Os *logs* guardados, regra geral, têm a sua data e hora marcados e registam tudo o que está a acontecer nos bastidores dos sistemas (Carstensen, 2019). Podemos ter diversos tipos de *logs*, com finalidade diversas, entre eles: *logs* de auditoria, *logs* de transações, *logs* de eventos, *logs* de erros, *logs* de mensagens são alguns exemplos principais (Carstensen, 2019).

PROCESSO DO GERIR DE LOGS

O processo de administração de *logs* pode ser dividido em seis etapas. Segue-se, para já, uma descrição resumida de cada uma das etapas, acompanhada de uma breve explicação sobre o que estas representam.

- **Coleção de logs** – devem ser recolhidos e armazenados *logs* de diferentes partes do ambiente IT, tal como dos sistemas operativos, servidores, *switches* e routers. A coleção de *logs* mais eficiente é a personalização do que é recolhido pela organização, de forma a eliminar possíveis repetições, salvando assim o espaço disponível (Carstensen, 2019).
- **Armazenamento** – uma vez recolhidos, existe a necessidade de armazenar e encriptar os registos. Destaca-se aqui a importância do processo de normalização uma vez que transforma todos os *logs* recebidos num formato comum, permitindo assim que possam ser analisados de um modo mais eficiente (Carstensen, 2019).

- **Armazenamento a longo prazo** – uma vez que por vezes se torna necessário consultar *logs* mais antigos, nomeadamente caso haja um ataque informático e seja necessária à sua investigação, torna-se importante desenvolver uma estratégia de armazenamento a longo prazo. Como foi dito no tópico anterior, ressalta aqui o problema relacionado com os elevados custos de armazenamento. Ora, a maneira mais eficaz de superar tal problema, é seguir melhores práticas de armazenamento e regulamentar o sector, armazenando os dados pelo período de, pelo menos, um ano (Carstensen, 2019).
- **Rotação de logs** – a rotação de *logs* ocupa-se de mover, redimensionar ou apagar *logs* desnecessários, resolvendo assim alguns dos problemas mencionados anteriormente (Carstensen, 2019).
- **Análise de logs** – segue-se uma análise dos *logs* que, efetivamente, irão ser utilizados. É de extrema relevância que as entidades consigam realizar pesquisas de *logs* guardados, seja via *plaintext*, REGEX ou API *queries* (Bisson, 2017).
- **Relatórios** – por último, os *logs* devem ser distribuídos para diferentes utilizadores através de *dashboards*, relatórios ou e-mails. O objetivo desta etapa é facilitar a troca de dados com os diferentes sistemas e a equipa de segurança (Bisson, 2017).

2.3. Security Information and Event Management

O SIEM é atualmente uma indústria valorizada em mais de US \$ 2 bilhões, no entanto, apenas 21,9% das empresas tiram o melhor proveito da sua solução SIEM, de acordo com uma pesquisa realizada pela 451 Research (Research, 2015).

As ferramentas SIEM são essenciais na segurança de dados. Elas agregam dados de diferentes sistemas, que são analisados para detetar comportamentos anormais ou potenciais ataques informáticos. Para percebermos o funcionamento de um SIEM, primeiro temos de ter em conta o SEM e o SIM, *Security Event Management* e *Security Information Management* respetivamente. No que diz respeito à segurança, ambas partilham tecnologias como *Log Management System* (LMS), *Security Event Correlation* (SEC), sendo o objetivo disto a análise e armazenamento de *logs* referentes a acontecimentos da rede.

De forma sucinta, pode-se afirmar que um SIM foca-se no armazenamento de dados/*logs* para serem analisados futuramente. As soluções SIM correm nos sistemas a serem monitorados que, por sua vez regista e envia informações a um servidor SIM central, onde os administradores podem consultar em tempo real os *logs* (Security_guest, 2019).

Por sua vez, o SEM é uma melhoria do SIM, pois é capaz de avaliar as entradas de *logs* mais relevantes, informando quais os acontecimentos devem ser analisados de imediato/tempo real. O objetivo principal de uma ferramenta SEM é identificar alertas ou eventos significativos, como login de administrador fora do horário de trabalho.

Visto individualmente, essas técnicas não conseguem nos indicar o que está a acontecer com a rede em tempo real. No entanto, a combinação dessas técnicas, pode fornecer um SIEM eficaz. De acordo com Stephen Watts, bmc blogs, um SIEM bem equilibrado deve possuir as seguintes características (Watts, 2018).

- A agregação, análise e relatório de saída de log de redes, sistemas operativos, bancos de dados e aplicativos;
- Aplicativos que verificam identidades e gerenciam o acesso;
- Gerir de vulnerabilidades e análise forense;
- Conformidade política;
- Notificações de ameaças externas;
- Painéis personalizáveis.

2.3.1. Funções de um sistema SIEM

Além das características mencionadas anteriormente, o Gartner (Petters, 2020) identifica três recursos essenciais para o SIEM, estes sendo a deteção de ameaças, investigação e tempo de resposta. Outras funcionalidades comuns vistas num SIEM moderno, de acordo com (Team, 2020) são.

- **Infraestrutura capaz de grande armazenamento com escalabilidade** – Dada a quantidade de dados recolhidos e processados por uma plataforma SIEM para um grande número de clientes, uma arquitetura escalável é necessária;
- **Recolha de logs ilimitada e tratamento rápido de logs** – As ameaças podem ter origem em diversas fontes de dados, os principais sendo dados da *cloud*, dados de rede, dados de log. Idealmente, uma solução SIEM deve ser capaz de recolher dados de todas as fontes e processá-los para correlação e análise;
- **Visualização** – As plataformas SIEM devem conter diferentes painéis para a visualização detalhada das ocorrências e estatísticas para tornar mais fácil que a equipa de segurança processe os dados;
- **Deteção precoce e caça a ameaças** – Após serem recolhidos os dados, é preciso esperar que o SIEM forneça um alto nível de desenvolvimento para produzir resultados uteis dos dados recolhidos, um SIEM moderno deve ser capaz de ajudar os profissionais de segurança a entender todo o contexto no mínimo tempo possível;
- **Triagem de incidentes e investigação avançada** – As plataformas SIEM pode, dependendo do tamanho da empresa, registar milhares de *logs* em uma semana. Um SIEM ideal deve ser capaz de eliminar os falsos positivos com eficácia e apresentar eventos com alto risco e critico. Para isso alertas devem permitir que os trabalhadores filtrem eventos de segurança rapidamente;
- **Analise de comportamento avançada** – Para que o SIEM dê suporte ao User and Entity Behavior Analytics (UEBA), é preciso primeiro entender como é o comportamento normal. Posteriormente, através de *machine learning* e análises estatísticas, é possível identificar comportamentos anormais;

- **Proteção de dados rápida e eficaz** – As soluções SIEM monitorizam constantemente os dados de log de entrada da infraestrutura da organização em tempo real. O SIEM deve procurar comportamentos maliciosos e atividades anormais, e alertar os profissionais de segurança com informações relevantes;
- **Resposta automatizada** – Este tipo de recurso é mais conhecido por SOAR, é uma ferramenta que pode ser implementada em conjunto com uma plataforma SIEM e ajuda na automatização de tarefas repetitivas, rastreando e priorizando incidentes, documentação automática e comunicação, aumentando a partilha de conhecimento entre os trabalhadores.

2.3.2. Soluções SIEM

De acordo com uma pesquisa feita pela Rapid7 sobre deteção e resposta a incidentes, mais de 50% das pessoas responderam que usam algum tipo de SIEM (Help, 2021), outra pesquisa feita pela AlienVault, cujos resultados se podem observar na Figura 1, mostrou que a maioria das empresas está preocupada com ameaças de segurança na *cloud*, 55% das empresas preocupam-se com *phishing* e 45% com *ransomware*.

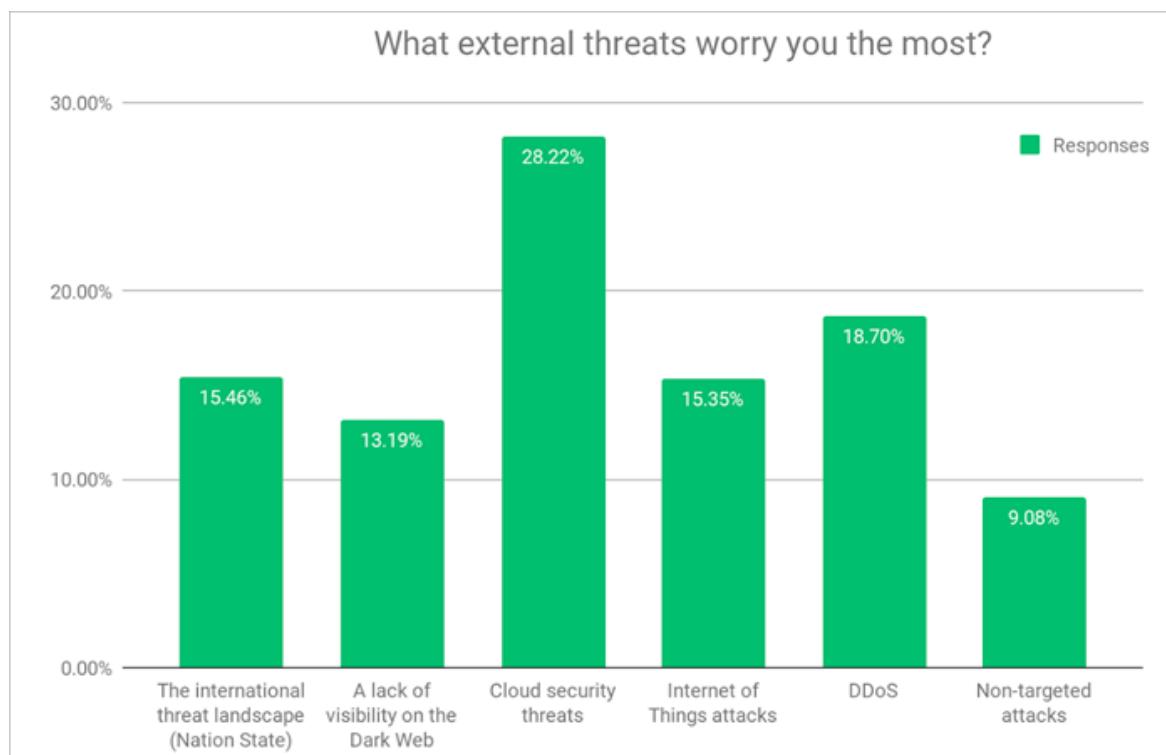


Figura 2 - Pesquisa sobre as ameaças mais relevantes, retirado de (Help, 2021)

Os números de ferramentas SIEM tem aumentado ao longo dos anos, assim como suas capacidades. Nem todos os sistemas SIEM são construídos da mesma forma, basta vermos os produtos disponíveis na Figura 3, onde são apresentadas algumas soluções. De acordo com o relatório anual do Gartner 2019/2020, os líderes de mercado são: Splunk, IBM, Exabeam, LogRhythm, Rapid7, Securonix e Dell Technologies (RSA). Em 2019/2020, nenhuma opção desafiadora foi relatada porque as opções principais aumentaram significativamente.

O mesmo relatório propôs uma solução considerada previdente, o LogPoint. No final, os documentos mencionados acima confirmam que a solução encontrou um local adequado nas



Figura 3 - Relatório do Quadrante Magico Gartner, retirado de (Gartner, 2021)

seguintes áreas Mercados: FireEye, AT&T Cybersecurity, Micro Focus, McAfee, HanSight, Fortinet, ManageEngine e SolarWinds.

As soluções acima mencionadas podem ser listadas como tendo licenças de *open source*: OSSIM da AT&T Cybersecurity, *Elastic Stack*, Splunk Free, MozDef da Mozilla e SIEMonster.

De seguida é feita uma pesquisa sobre as principais características das soluções escolhidas, estando organizado pela seguinte maneira: arquitetura, funcionalidades, vantagens e desvantagens e licenciamento, caso aplicável.

2.3.2.1. OSSIM

A AT&T Cybersecurity oferece vários serviços relacionados com a segurança, de entre os quais dois SIEM, sendo que um é *open source*, o AlienVault OSSIM, e um produto pago, o USM Anywhere (S., 2020).

A solução *open source* da empresa AT&T, designada por AlienVault OSSIM, é atualmente a solução *open source* SIEM mais utilizada mundialmente. O OSSIM aproveita do poder do Open Threat Exchange (OTX), permitindo que os utilizadores contribuam e recebam atualizações em tempo real sobre atividades maliciosas.

O OSSIM inclui os principais componentes de um SIEM, a recolha de eventos, normalização e correlação e outras das quais incluem (OSSIM: The Open Source SIEM | AlienVault, s.d.):

- Descoberta de ativos e inventário;
- Avaliação de vulnerabilidade;
- Monitorização comportamental;
- Correlação de eventos SIEM;
- Deteção de intruso.

Através da interface gráfica, o utilizador consegue verificar os limites de backup e para o armazenamento, ou seja, é possível definir em relação aos *logs* o tempo máximo de retenção na base de dados, sendo que estes são automaticamente eliminados após o término do período definido.

Arquitetura

Como uma plataforma de segurança unificada, o USM Appliance combina várias tecnologias de segurança em uma plataforma integrada. O Dispositivo USM pode ser integrado como uma única plataforma ou distribuído em vários servidores (virtuais ou de hardware) para fornecer escalabilidade e disponibilidade adicionais. A figura a seguir apresenta uma visão geral de alto nível da arquitetura do sistema.

Na Figura 4 pode-se verificar os componentes da arquitetura da solução USM Anywhere, cujo tem uma grande semelhança na arquitetura OSSIM pois não tem o USM Logger (AT&T, 2021)

Os sensores são instalados na infraestrutura e os dados recolhidos entre os dispositivos são normalizados e enviados para o servidor, onde são agregados e correlacionados os *logs* no servidor, para depois se administrar e gerir a rede criando relatórios e administrando os eventos de segurança na interface WEB (Vazão, 2020).

Após o USM Appliance Sensor transformar os dados em fluxos de *logs*, eles são agrupados consoante os campos dos dados e enviados para o USM appliance Server, de seguida são correlacionados os *logs* e avaliado os riscos que podem estar contidos na informação dada pelos mesmos mais tarde enviando para o USM Appliance Logger que regista e armazena os *logs* para que mais tarde sejam feitas as análises forenses (AT&T, 2021).

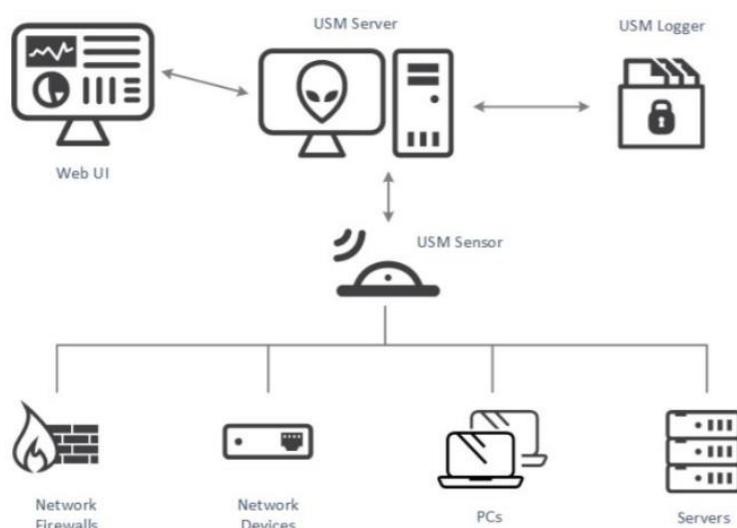


Figura 4 - Arquitetura da solução USM Anywhere (AT&T, 2021)

Funcionalidades

Como mencionado anteriormente, o OSSIM e o USM Anywhere têm várias semelhanças nas funcionalidades, das quais as mais relevantes são (Vazão, 2020):

Descoberta e inventário de ativos – por meio da descoberta e inventário de ativos pode-se analisar a rede, detetar mudanças em ativos e marcar ativos desconhecidos na rede. A solução OSSIM armazena informações sobre cada ativo, Tais como: IP interno, sistema operativo, modelo e endereço MAC

Identificação de vulnerabilidades – A avaliação de vulnerabilidades pode realizada com ou sem usar autenticação de administrador de rede. A identificação de vulnerabilidades e conformidade são comparadas entre o software instalado no ativo e o que aparece no base de dados de vulnerabilidades. Finalmente, uma avaliação de vulnerabilidade pode ser definida para que possa funcionar regularmente;

Deteção de intrusões – esta função monitoriza a atividade na rede, para identificar atividades suspeitas. A deteção de atividades suspeitas na solução OSSIM é implementada através de um HIDS e um NIDS.

Monitorização de comportamento – os dados utilizados para monitorar a rede são recolhidos pelos equipamentos de rede, por meio da monitorização da disponibilidade dos ativos e do *port mirroring*. Os padrões de tráfego recolhidos e os dados de fluxo de rede permitem a deteção de condições anormais que podem indicar violações das políticas de segurança;

Correlação de eventos SIEM – esta solução permite correlacionar *logs* de tráfego Rede, a atividade do *host* e outros indicadores utilizados para identificar atividades suspeitas;

Suporte da solução através de blogs – A solução possui uma comunidade que dá suporte a todos os produtos, inclusive a solução OSSIM;

Open Threat Exchange – é uma plataforma que permite aos utilizadores compartilhar ameaças entre soluções globais.

A solução USM possui outras funcionalidades que não se encontram no OSSIM (Cybersecurity, Compare AlienVault Products, 2021): gestão de *logs*; monitorização de segurança em *cloud*; inteligência continua de ameaças; painéis de análise avançada e visualização de dados; entre outros.

Vantagens e Desvantagens

Como foi mencionado acima, o OSSIM permite gerir infraestruturas de rede através do Open Threat Exchange, correlacionar *logs* e criar regras para a deteção de atividades suspeitas. Algumas vantagens e desvantagens são de seguida apresentadas, a partir da opinião de utilizadores (TrustRadius, s.d.).

Vantagens

- Atualização em tempo real de ameaças;
- Identificação de ativos;
- Correlação de *logs*;
- Definição de regras complexas (identificar ações suspeitas);
- Fácil de instalar.

Desvantagens

- Pouco escalável (uma única appliance);
- Retenção de *logs* limitado;
- Limitado a um servidor (Não tem redundância);
- Terminologias difíceis de perceber;
- Pouco armazenamento na versão gratuita.

Licenciamento

Pelo website da AT&T Cybersecurity, é nos fornecida a informação de que o OSSIM possui uma licença *open source* como já foi mencionado (Cybersecurity, OSSIM: The Open Source SIEM | AlienVault, 2021). Enquanto a solução USM Anywhere são fornecidos três tipos de licença: a Essentials a partir de US \$ 1075 por mês; a Standard, a partir de US \$ 1695 por mês; e a Premium, a partir de US \$ 2595 por mês (Cybersecurity, AlienVault Pricing - Affordable Plans to Fit Any Budget, 2021).

2.3.2.2. Elastic Stack

Elastic Stack é o resultado do acrônimo dos principais três produtos *open source*: *Elasticsearch*, o *Logstash* e o *Kibana*, sendo que mais tarde foram adicionados os *Beats*.

Esta solução poderá não se considerar um SIEM pois não se considera que tem as mesmas funcionalidades que as outras soluções, no entanto, a mesma já dispõe de um módulo SIEM.

A solução *Elastic Stack* é a plataforma de gestão de *logs* e bloco *open source* para SIEM. Garante organização com uma plataforma que recolha e processa dados de múltiplas origens, guarda os dados numa base de dados que vai escalando à medida que os dados aumentam, juntamente com uma variedade de ferramentas para analisar os dados.

Elastic Stack tem muitos seguidores, portanto, fornece um grande número de plug-ins e extensões para vários produtos.

Elastic Stack fornece várias funções de processamento de dados, flexíveis e suporta vários formatos. Por exemplo, se se planeja enviar dados para *Elasticsearch*, a saída deve estar no formato JSON (Javascript Object Notation) porque usa JSON para armazenar arquivos (Zarzosa, 2017).

É de salientar que esta solução é amplamente utilizada como uma plataforma de gestão de *logs* (Vazão, 2020).

Arquitetura

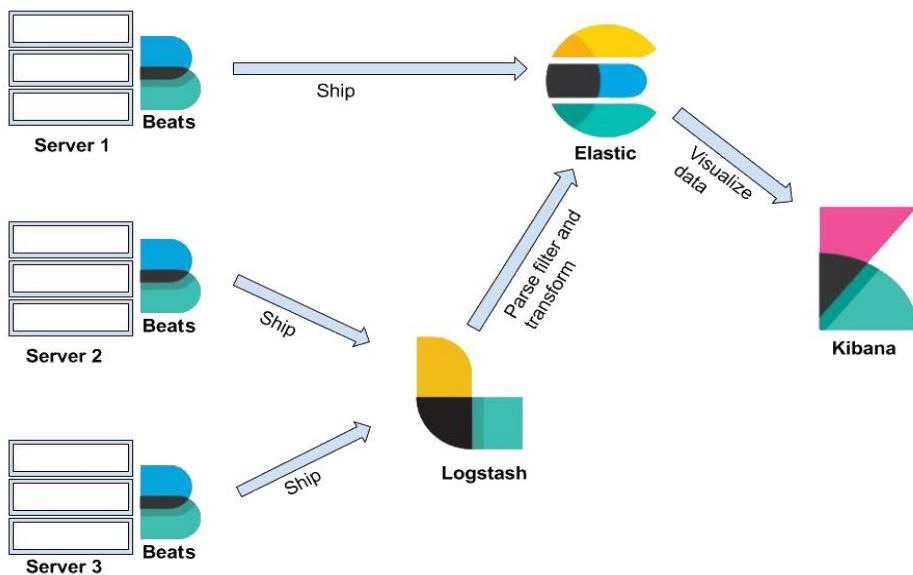


Figura 5 - Arquitetura do Elastic Stack

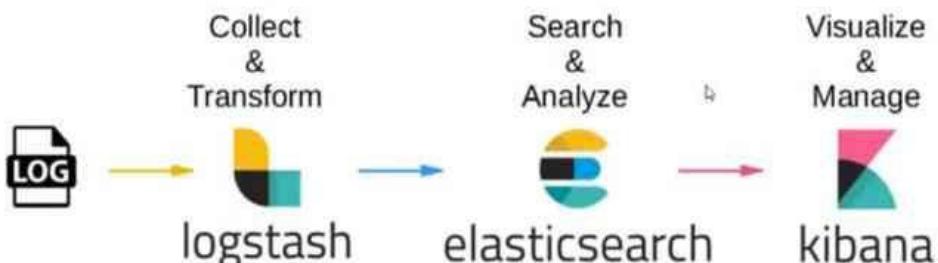


Figura 6 - Flow dos Logs do Elastic Stack

no *Elastic Stack*, o *Beats* e o *Logstash* enviam dados para o *Elasticsearch*, onde os dados são armazenados. *Kibana* é o User Interface do *Elastic Stack*; ele lê os dados do *Elasticsearch* para criar gráficos e muito mais.

Conforme mostrado na Figura 5, a arquitetura geral do *Elastic Stack* consiste em *Beats*, *Logstash*, *Elasticsearch* e *Kibana*. Os *Beats* são responsáveis por enviar dados para *Elasticsearch* e *Logstash*, e então se pode visualizar os dados do *Elasticsearch* no *Kibana*.

Como mencionado anteriormente, *Elasticsearch* permite que se execute análises Dados em tempo real, a partir de várias fontes de dados, escalonáveis E torna possível realizar pesquisas de "texto completo", que por sua vez, *Kibana* tem a capacidade A principal função é permitir a visualização dos dados do *Elasticsearch* (Srivastava, 2019). Por meio do *Kibana*, se também pode realizar vários tipos de pesquisa e visualizar dados em vários formatos (Srivastava, 2019). Observando a figura 6, o *Logstash* recolhe, analisa, melhora e transforma os dados e, em seguida, o envia os mesmos para o *Elasticsearch*.

Funcionalidades

O *Elastic Stack* Possui várias funcionalidades, estas são as que achamos mais relevantes:

- Uma interface intuitiva e personalizável
- Fornece bibliotecas para várias linguagens de programação tais como Ruby, Python, PHP, Perl, .NET, Java e JavaScript;
- Consegue fazer uma análise de dados em tempo real;
- Fornece escalabilidade de alta disponibilidade;
- Permite que se execute pesquisa de texto completo;
- Fornece funções de monitorização;
- Segurança;
- Alertas;
- Relatórios;
- Gráficos.

Deve-se observar que *Elastic Stack* é um produto *open source* altamente personalizável e um dos mais populares para a gestão e monitorização de *logs*.

Licenciamento

Atualmente nas versões mais recentes do *Elastic Stack*, como a 7.11, dispõe de uma licença SSPL, criada pela MongoDB. No entanto, em 2021 foi anunciado a licença Elastic License v2, não *copyleft*, que concede o direito de “usar, copiar, distribuir, disponibilizar e preparar trabalhos derivados do software” (Banon, 2021). A Elastic License v2 aplica-se ao *Elasticsearch* e ao *Kibana*.

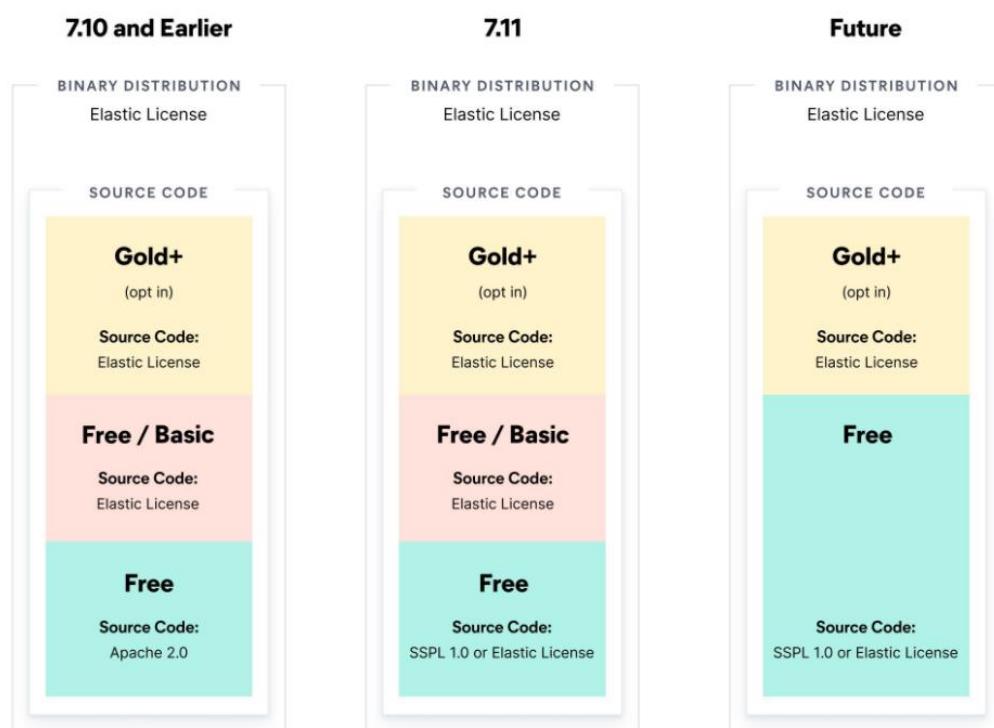


Figura 7 - Licenciamento do *Elastic Stack*

Com a solução *open source* já se tem acesso a várias funcionalidades tais como: *cluster*, alta disponibilidade, balanceamento automático de dados e a pesquisa entre *clusters*.

Contudo, existem ainda mais funcionalidades apenas disponíveis nas licenças pagas, que é o caso da solução Standard, Gold, Platinum e Enterprise, mostradas na próxima figura.

Standard	Gold	Platinum	Enterprise
Um ótimo ponto de partida	Supor te dedicado e recursos aprimorados	Funcionalidade avançada com suporte 24 horas por dia, 7 dias por semana	Supor te de camada de dados e proteção de endpoint
Funcionalidades:	Tudo do Standard e mais:	Tudo do Gold e mais:	Tudo do Platinum e mais:
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Segurança principal do Elastic Stack <input checked="" type="checkbox"/> Recursos de solução da Elastic para busca empresarial, observabilidade e segurança <input checked="" type="checkbox"/> Kibana Lens, Elastic Maps e Canvas <input checked="" type="checkbox"/> Alerta e ações na stack <input checked="" type="checkbox"/> Recursos principais gratuitos e abertos 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Relatórios <input checked="" type="checkbox"/> Ações de alerta de terceiros <input checked="" type="checkbox"/> Watcher² <p>SUPORTE</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Suporte em horário comercial <input checked="" type="checkbox"/> Suporte pela Web e por telefone <input checked="" type="checkbox"/> SLAs de tempo de resposta do suporte (Urgente: 4 horas; Alto: 1 dia; Normal: 2 dias úteis) 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Recursos avançados de segurança do Elastic Stack <input checked="" type="checkbox"/> Machine learning <input checked="" type="checkbox"/> Replicação entre clusters <p>SUPORTE</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Suporte 24 horas por dia, 7 dias por semana, 365 dias no ano <input checked="" type="checkbox"/> Suporte pela Web e por telefone <input checked="" type="checkbox"/> SLAs aprimorados de tempo de resposta do suporte (Urgente: 1 hora; Alto: 4 horas; Normal: 1 dia útil) 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Acesso ao Elastic Endgame <input checked="" type="checkbox"/> Snapshots buscáveis <input checked="" type="checkbox"/> Supor te para camadas cold (disponibilidade geral) e frozen (prévia técnica) buscáveis <input checked="" type="checkbox"/> Elastic Maps Server (beta) <p>SUPORTE</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Supor te 24 horas por dia, 7 dias por semana, 365 dias no ano <input checked="" type="checkbox"/> Supor te pela Web e por telefone <input checked="" type="checkbox"/> SLAs aprimorados de tempo de resposta do suporte (Urgente: 1 hora; Alto: 4 horas; Normal: 1 dia útil)
SUPORTE	SUPORTE	SUPORTE	SUPORTE
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Suporte pela Web, tempo de resposta pretendido de 3 dias úteis (somente Elastic Cloud) 			

Figura 8 - Várias Funcionalidades das Licenças do Elastic Stack

Vantagens e Desvantagens

Vantagens

- **Comunidade**- o *Elastic Stack* tem uma comunidade bastante ativa que disponibiliza tutoriais, cursos, ferramentas e nos fóruns do site do mesmo há tópicos novos e respostas muito frequentemente.
- **Recursos de registo centralizado** - oferece recursos de registo centralizado, permitindo ao utilizador agregar registos de ambientes da nuvem cada vez mais complexos em um único índice pesquisável. Esse recurso torna possível correlacionar dados dos *logs* e eventos de várias fontes, permitindo casos de uso como monitorização de segurança e análise de causa raiz.

- **Análise e visualização de dados em tempo real**- Com o *Kibana*, os utilizadores do *Elastic Stack* podem criar visualizações de dados e painéis personalizados dando uso aos dados em tempo real do *Elasticsearch*. A capacidade de visualizar dados em tempo real diminui o tempo para suposições, dando suporte a uma variedade de casos de uso e impulsionando a agilidade organizacional e tomar decisões mais adequadas.
- **Clientes com várias linguagens de programação**- JavaScript, Go, Python, .NET e Perl. O *Elastic Stack* fornece suporte para todos os seus clientes oficiais, corrigindo bugs e respondendo às consultas de suporte conforme necessário.

Desvantagens

Como o objetivo é analisar as soluções e funcionalidades *open source* uma desvantagem do *Elastic Stack* é que o utilizador terá de ter alguns conhecimentos e fazer algumas configurações tais como:

- Configurar a análise e tratamento de regtos;
- Construir um pipeline de dados (configurar o *Logstash*);
- Monitorização e lidar com exceções para evitar perda de dados;
- Configurar réplicas e fragmentação para otimizar o desempenho caso queira evitar a perda de dados;
- Testar as configurações de registo para garantir a consistência dos dados;
- Implementar monitorização e alertas de segurança

Outras desvantagens também são:

- Alto custo de propriedade;
- Problemas de estabilidade e tempo de atividade.

Importante referir que sendo uma desvantagem o utilizador ter que aprender sobre esta solução é difícil e requer uma gestão intensa, mas após ultrapassar essas dificuldades acaba por ser vantajoso ter este conhecimento e ter uma solução mais robusta (Tal, 2018).

2.3.2.3. SPLUNK

Splunk é uma plataforma que recolhe e armazena centralmente todos os *logs* do sistema informático de uma organização. Funciona através da recolha e indexação de *logs* em tempo real, permitindo a criação de gráficos, alertas, *dashboards* e gráficos através da *Search Processing Language* (SPL), tendo como principal objetivo auxiliar as atividades da organização através de diagnósticos de problemas, indicadores e padrões de opções comerciais. Máquina a aprendizagem também é usada.

Deve-se também observar que a solução Splunk possui quatro soluções de licenciamento: Splunk Cloud, Splunk Enterprise, Splunk Light e Splunk Free. As duas primeiras geralmente têm as mesmas funções porque Splunk Light e Splunk Free têm algumas limitações (Vazão, 2020).

No entanto iremos só falar do Splunk Free devido a este estudo comparativo ser relativamente a apenas SIEM *open source* e freeware.

Splunk free

O Splunk free permite indexar até 500MB cada dia sem expiração (Splunk, s.d.), a vantagem desta “funcionalidade” é que se pode ir adicionando 500MB por dia para sempre, o que eventualmente poderá dar vários *TeraBytes* e os dados ficam armazenados na plataforma vitaliciamente (Vazão, 2020) no entanto, suporta a definição de limites temporais na retenção dos dados (wiki.splunk, 2016) (wiki.splunk, 2016).

O Splunk Enterprise oferece visibilidade em tempo real, permitindo automatizar a recolha, indexação e alerta de dados (Splunk, s.d.). Através do *machine learning* a solução vai tornando-se cada vez mais inteligente. Splunk Enterprise é um programa de SIEM abrangente, embora o Splunk Free compartilhe muitos de seus recursos, ele não apresenta alerta ou *clustering* do indexador, por exemplo, entre outros utilizadores da organização.

Arquitetura

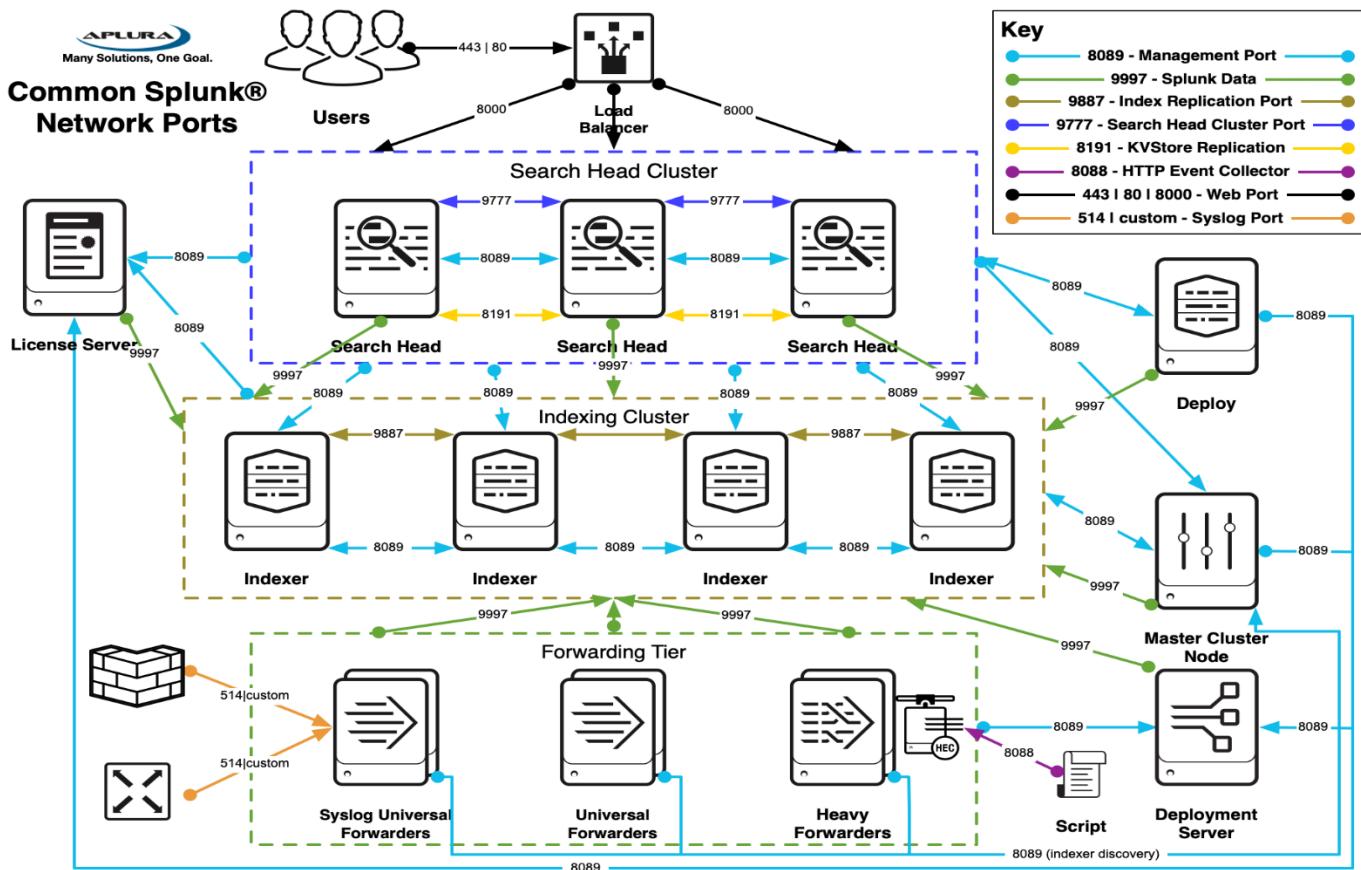


Figura 9 - Arquitetura do Splunk

Com o Slunk Free é apenas possível implementar o Splunk num único servidor, com apenas um utilizador e não permite configuração de alertas (Splunk, s.d.) no qual são processadas todas as funcionalidades, no entanto, o Splunk Free utiliza um indexador e um motor de pesquisa próprios (Vazão, 2020). Já num meio distribuído há uma divisão logica entre cabeçalhos de pesquisa e indexação tendo que haver no mínimo duas máquinas.

Numa implementação simples há um servidor indexador que recebe e indexa os dados e outra máquina separada onde estão os cabeçalhos de pesquisa. Estas duas máquinas comunicam entre si e realizam tarefas diferentes.

No caso de se criar um ambiente *cluster* haverá uma combinação de vários indexadores e cabeçalhos de pesquisa, e haverá mais redundância de dados.

Resumindo neste tipo de ambientes distribuídos a implementação de um *cluster* inclui haver um ambiente distribuído devido a vários indexadores e cabeçalhos trabalharem em funções isoladas.

Funcionalidades

A solução Splunk também permite pesquisar, analisar e visualizar um grande volume de dados (Splunk a. , 2021). De entre o elevado número de funcionalidades que o Splunk oferece, listamos as seguintes (Splunk, 2018b):

Dentro das várias funcionalidades que o Splunk oferece, foram listadas as seguintes (Splunk a. , 2021) (Vazão, 2020):

Dashboards - contém painéis de módulo tais como caixas de pesquisa, campos, gráficos, entre outros. Os painéis geralmente são ligados a pesquisas ou pivôs salvos. Eles mostram os resultados de pesquisas concluídas e dados de pesquisas em tempo real executados em segundo plano.

Pivô – refere-se a uma tabela, gráfico ou visualização de dados que se cria usando um editor dinâmico. O Pivot Editor permite que os utilizadores mapearem atributos definidos por objetos de modelo de dados para tabelas, gráficos ou visualizações de dados sem escrever consultas SPL para gerá-los. O pivô pode ser salvo como um relatório e adicionado ao painel.

Modelo de dados - Os modelos de dados codificam o conhecimento de domínio especializado sobre um ou mais conjuntos de dados indexados. Eles permitem que os utilizadores do Pivot Editor criem relatórios e painéis sem projetar as pesquisas que os geram.

- Recolher e Indexar – Recolher os dados de qualquer origem, formato ou local, em tempo real;
- Esquema Instantâneo – Pode ser efetuado qualquer filtro aos dados que estão na base de dados da plataforma;
- Cronologia de eventos baseada no tempo – É determinada automaticamente a data e hora de qualquer evento;
- Splunk Search Processing Language (SPL) – Esta linguagem avançada de consulta permite a realização de pesquisas avançadas sobre os dados. Esta também permite cinco tipos de correlação, a saber: tempo, transações, subpesquisas, consultas e uniões;
- Resultados interativos – Podem ser formatados gráficos e tabelas em tempo real;
- Amostragem de dados – Permite que seja possível otimizar os dados em tempo real;

- Machine Learning – Através do recurso à análise integrada do Splunk ou com modelos próprios, é possível otimizar os recursos da Organização. É também possível serem criados os modelos com recurso à linguagem Python;
- Monitorizar e Alertar – É possível criar alertas para sinalizar situações críticas que, por sua vez, podem desencadear automaticamente várias operações;
- Integridade dos dados – O Splunk permite criar hash dos dados indexados para que seja possível garantir a integridade ao longo do tempo;
- Escalável e alta disponibilidade – Esta opção tem como base uma arquitetura distribuída com ajuste horizontal, para que se possam processar grandes volumes de dados;
- Apps – Existem várias apps certificadas para auxiliar nas tarefas de monitorização e de criação de relatórios e de alertas.

Licenciamento

O Splunk contem várias licenças cada uma com características diferentes (devquora, 2020), segue-se então as várias licenças:

A licença Splunk Enterprise que inclui todos os recursos corporativos, como autenticação e pesquisa distribuída. Vários tipos de licença Splunk Enterprise incluem a licença Splunk Enterprise Trial e a licença Splunk for Industrial IoT.

A licença gratuita - alguns recursos estão desabilitados nesta licença gratuita, como o recurso de autenticação. Ele permite um volume de indexação limitado(500MB/dia).

A licença do encaminhador - é usada com os encaminhadores, pois permite apenas encaminhar e não indexar os dados.

A licença Beta - possui recursos corporativos, mas é restrita às versões Beta do software Splunk.

Vantagens e Desvantagens

Neste subcapítulo serão apenas descritas as vantagens e desvantagens das características do Splunk Free pois o objetivo desta análise é comparação das versões gratuitas.

Vantagens

Devido ao Splunk free ser muito limitado e não ter muitas funcionalidades na versão gratuita foram encontradas muito poucas vantagens, sendo que as que foram encontradas foram as seguintes:

Instalação e Configuração Simples – Existe bastante informação e documentação sobre a instalação e configuração do Splunk sendo que a mesma já é básica e não requer muitos conhecimentos (Zarzosa, 2017).

Acumular dados – caso não se pretenda receber grandes quantidades de informação ao início, dando uso aos 500MB diários, a longo prazo os dados ficam guardados para sempre.

Desvantagens

- Só permite a implementação de 1 servidor
- Suporta apenas um utilizador
- Não permite configuração de alertas
- Não permite configuração de definição de perfis de utilizador
- É preciso conhecimentos avançados de base de dados
- Não é uma solução viável a longo prazo devido a não ter muitos recursos
- suporta a definição de limites temporais na retenção dos dados (o que pode impactar negativamente o uso da “funcionalidade” dos 500MB diários)

2.3.2.4. MozDef

O Mozilla defense Platform (MozDef) são uma combinação de serviços que podem ser usados como um SIEM *open source*. Foi criado pela Mozilla Foundation em 2014 com o objetivo de automatizar o processo de tratamento de incidentes de segurança e facilitar as atividades em tempo real, de acordo com a MozDef (Mozilla, MozDef Documentation, 2021). O MozDef funciona em cima do *Elasticsearch* e utiliza o *Kibana* para a visualização.

Arquitetura

A arquitetura do MozDef é composta de várias ferramentas *open source*, como o Nginx, RabbitMQ, *Elasticsearch* já mencionado, entre outros (Mozilla, Overview, 2021).

O MozDef utiliza o processamento de frontend, que consiste em receber um log em formato JSON, fazendo de seguida a transformação de dados, adicionando metadata e enviando os dados para o *Elasticsearch*.

O MozDef usa o RabbitMQ para enfileirar os eventos ainda não processados. O diagrama seguinte mostra essas interações.

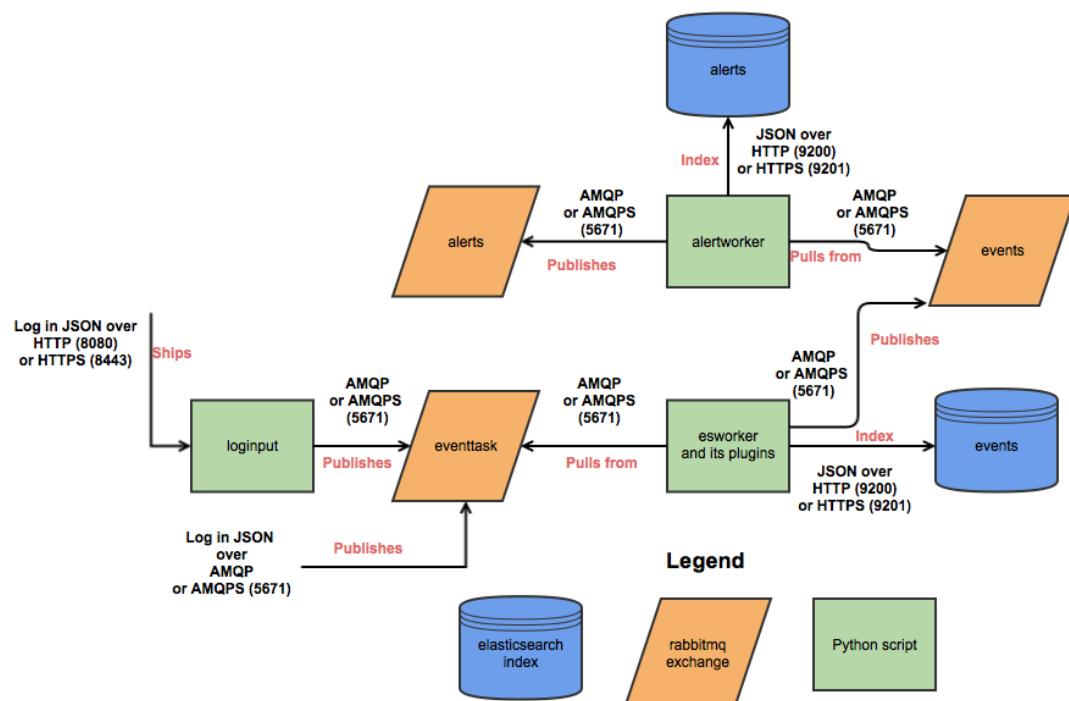


Figura 10 - Arquitetura do MozDef

Funcionalidades

O MozDef tem como objetivo oferecer micro-serviços que compõem uma gestão de eventos e informações de segurança SIEM *open source*, escalável, capaz de lidar com milhares de eventos por segundo, fornecer pesquisa rápida, alertas, correlação e lidar com interações entre trabalhadores responsáveis pelos incidentes.

MozDef visa fornecer as funcionalidades tradicionais de um SIEM como:

- Receber *logs* de vários sistemas;
- Armazenamento de eventos/*logs*;
- Facilitar as pesquisas;
- Criação de alertas;
- Facilitar a gestão de *logs*.

Por outro lado, esta solução difere-se das tradicionais pois:

- Apenas aceita entradas no formato JSON;
- Fornece acesso aberto aos dados;
- Integra-se com uma variedade de remetentes de log, como o *Logstash*, beaver, nxlog e qualquer outro que possa enviar JSON para rabbit-mq ou um *endpoint* HTTP;
- Fornece fácil integração com fontes de dados em *cloud*, como Cloudtrail e Gaurd Duty;
- Fornece plug-ins python fáceis para manipular dados em trânsito;
- Fornece acesso em tempo real aos trabalhadores responsáveis pelas respostas de incidentes para permitir que eles vejam o trabalho em simultâneo.

Licenciamento

O MozDef é uma solução inteiramente *open source*, portanto não existem versões pagas disponibilizadas pelo Mozilla.

Vantagens e Desvantagens

Tendo em conta as funcionalidades descritas pela Mozilla em relação à sua solução SIEM, pode-se concluir que é uma opção ideal para pequenas ou médias empresas, mas não recomendada para ambientes empresariais. Abaixo estão algumas vantagens e desvantagens da sua utilização (Heikamp, 2020).

Vantagens:

- Boas opções de painéis de visualização, pois utiliza o *Kibana*;
- Opções para teste de alerta, o que reduz erros humanos;
- Funcionalidade para rastrear incidentes e investigações;
- Alertas bem flexíveis.

Desvantagens:

- A criação de conteúdo não é direta, precisa de trabalho por parte da programação;
- Sem opções de alta disponibilidade ou *clustering*;
- Nenhum controle de utilizador ou separação de funções;
- A documentação é mínima.

2.3.2.5. SIEMonster

O SIEMonster é um software SIEM personalizável e escalonável, extraído de uma coleção das melhores ferramentas de segurança de *open source* e desenvolvidas internamente. SIEMonster é um SIEM relativamente recente, mas surpreendentemente popular na indústria. O SIEMonster foi inspirado pela necessidade de construir uma solução de SIEM que minimizasse as frustrações causadas pelos custos exorbitantes de licenciamento de produtos comerciais de SIEM.

O SIEMonster tem algo para todos - pequenas e médias empresas, grandes corporações, provedores de serviços gerenciados e a comunidade. A edição da comunidade é a edição de servidor único de código aberto gratuita para empresas com até 100 terminais. A edição da comunidade (gratuita) oferece suporte a recursos de relatórios e *Threat Intelligence* em tempo real. Ele pode ser implantado na nuvem usando containers Docker e em máquinas físicas e virtuais.

Arquitetura

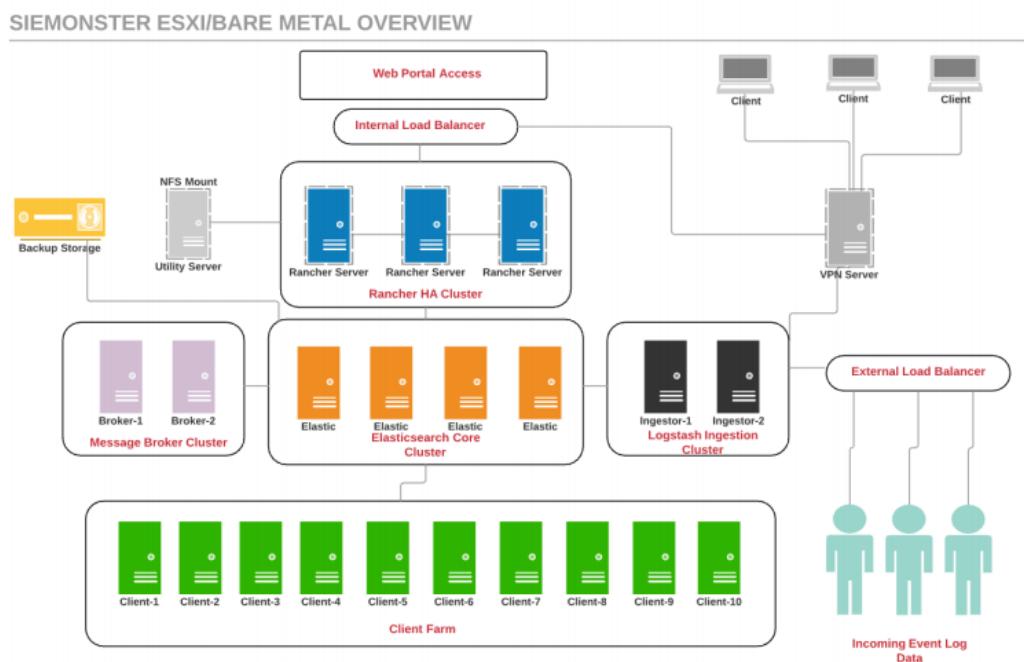


Figura 11 - Funcionamento do SIEMonster

A arquitetura do SIEMonster passa muito parecida com o *Elastic Stack* pois dá uso ao *Elasticsearch* e ao *Logstash*, ou seja, o *Logstash* recolhe os *logs* e transforma em mensagens JSON para mais tarde serem indexadas pelo *Elasticsearch* tal como mostrado na figura 12.

Mas em vez de usar o *Kibana* o Siemonster contém o seu próprio User Interface e em vez dos *Beats*, contém uma vasta quantidade de ferramentas fornecidas pela comunidade que serão descritas no próximo capítulo.

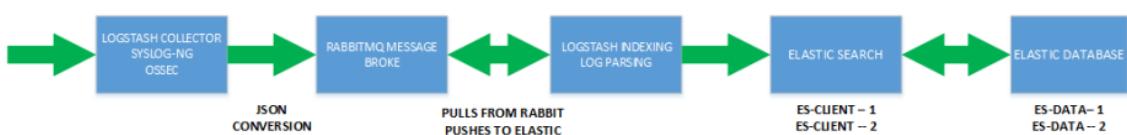


Figura 12 - Flow dos Logs no Siemonster

Funcionalidades



Figura 13 - Vários recursos do SIEMonster

O SIEMonster contém várias ferramentas e funcionalidades, algumas fornecidas pela comunidade, sendo estas as foram encontradas e descritas (SIEMonster a., 2021):

Open Distro - Open Distro for *Elasticsearch* fornece um sistema de alerta e monitorização de eventos poderoso e fácil de usar, permitindo a monitorização dos dados e envio de notificações automaticamente para as partes interessadas.

Shuffle SOAR - incluiu a tecnologia Shuffle SOAR de ponta que permitirá a criação de fluxos de trabalho que podem integrar-se com aplicações que fazem parte da stack SIEMonster, bem como produtos externos que são frequentemente encontrados como parte dos conjuntos de ferramentas de segurança cibernética implantados na empresa.

O Hive - TheHive é utilizado na plataforma SIEMonster como um sistema de resposta a incidentes / gerir de casos. Ele está integrado no Alerting, MISP, OpenCTI, Patrowl e Cortex para automatizar o processo de criação de incidentes. Todas as informações relativas a um incidente de segurança são apresentadas para revisão. Enquanto avalia e exclui falsos positivos, a equipa recebe uma indicação das próximas etapas a serem executadas.

Cortex - O Cortex pode analisar (e fazer a triagem) observáveis em escala com uso de mais de 100 analisadores. Pode ser respondido ativamente a ameaças e interagir com seu eleitorado e outras partes, graças aos respondentes da Cortex. Dentro da plataforma SIEMonster, o Cortex é pré-integrado com TheHive e MISP para colocá-lo em funcionamento.

MITER ATT & CK - MITER ATT & CK é uma base de conhecimento globalmente acessível de táticas e técnicas adversárias com base em observações do mundo real. A base de conhecimento da ATT & CK é usada como base para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética. A integração com a plataforma SIEMonster fornece informações detalhadas sobre ataques.

Framework MISP - A Malware Information and Sharing Platform (MISP) é uma plataforma de *Threat Intelligence* para partilhar, armazenar e correlacionar indicadores de comprometimento de ataques direcionados, *Threat Intelligence*, informações de fraude financeira, informações de vulnerabilidade ou mesmo informações de contraterrorismo.

Ni-FI - Na plataforma SIEMonster, o NiFi é usado para ingerir dados de log de eventos de entrada da fila de mensagens Kafka. Vários modelos foram fornecidos para diferentes tipos de terminais, incluindo, mas não se limitando a, Active Directory, firewall comum e dispositivos VPN, agentes HIDS e feeds IDS.

PatrOwl - PatrOwl é uma plataforma avançada para orquestrar operações de segurança como teste de penetração, avaliação de vulnerabilidade, revisão de código, verificações de conformidade, *Threat Intelligence* cibernéticas / caça e operações de SOC e DFIR, incluindo:

- Visão geral da segurança de stack completa (IP para dados)
- Definir *Threat Intelligence* e políticas de varredura de avaliação de vulnerabilidade
- Orquestrar varreduras usando mecanismos feitos sob medida
- Recolher e agregar descobertas
- Contextualizar, rastrear, priorizar descobertas
- Verifique a eficácia da remediação

OpenCTI - OpenCTI é uma plataforma de código aberto que permite às organizações gerenciar seu conhecimento e observáveis de inteligência contra ameaças cibernéticas. Foi criado com o objetivo de estruturar, armazenar, organizar e visualizar informações técnicas e não técnicas sobre ameaças cibernéticas.

A estruturação dos dados é realizada por meio de um esquema de conhecimento baseado nos padrões STIX2.

Alert - o alert é fornecido pela interface OpenDistro *Kibana*, Elastalert com interface GUI e via Apache Nifi dependendo do caso de uso. Mais de 30 tipos de alerta predefinidos são fornecidos para se começar a trabalhar. As consultas típicas incluem anomalias, agregações, correspondência de padrões e correlação de *Threat Intelligence* / Mitre, indicadores de comprometimento (IOCs), correspondência de assinaturas NIDS e vulnerabilidades de ativos. Os alertas podem ser configurados para criar tickets automaticamente no módulo de resposta a incidentes do TheHive e para notificar as partes interessadas por meio de *webhooks* mais comuns ou e-mail direto.

Reports - a ferramenta de relatórios internos SIEMonster oferece uma ferramenta abrangente com relatórios automatizados diretamente para sua caixa de entrada. Essa ferramenta permite que relatórios automatizados sejam gerados e enviados para a pessoa adequada, em qualquer evento, como o MacAfee Antivírus, detetou um vírus, mas não limpou e enviou esses itens de acompanhamento em um relatório. Os relatórios estão disponíveis em formato PDF ou XLS, incluindo instantâneos de painéis para visualização.

Suricata - Suricata é um mecanismo de deteção de ameaças de *open source* desenvolvido pela Open Information Security Foundation (OISF). Suricata pode atuar como um sistema de deteção de intrusão (IDS) e um sistema de prevenção de intrusão (IPS), ou ser usado para monitorização de segurança de rede. Ele foi desenvolvido junto com a comunidade para ajudar a simplificar os processos de segurança.

Licenciamento

EDITION:	COMMUNITY EDITION	PROFESSIONAL EDITION	ENTERPRISE EDITION	MSSP EDITION
	The Community Edition is a single server built by the community for the community.	The Professional Edition is a single appliance or Virtual machine, for small business.	The SiEMonster Enterprise Edition. Monitor network assets in an affordable scalable solution.	Want to run your own SOC? run our Multi-Tenant Edition for Managed Security Service Providers.
Server Requirements:	1 Server	1 Server	5+ Servers	7+ Servers
Endpoints:	1-100	1-200	1-100,000	Infinite
EPS:	5,000	13,000	500k+ (Cloud)	Infinite
Bare-Metal:	✓	✓	✓	✓
Virtual Machine:	✓	✓	✓	✓
Upgradeable:	✗	✓	✓	✓
Cloud:	✗	✓	✓	✓
Kubernetes Scalable:	✗	✓	✓	✓
Support:	✗	✓	✓	✓
Reporting:	2 Reports	✓	✓	✓
Threat Intelligence:	✓	✓	✓	✓
Human Based Behaviour:	✗	✗	✓	✓
Machine Learning:	✗	✗	✓	✓
	DOWNLOAD	CONTACT SALES	CONTACT SALES	CONTACT SALES

Figura 14 - Várias licenças do Siemonster (Siemonster, 2021)

A versão gratuita Community Edition contem ainda algumas funcionalidades tais como integração Threat Intelligence e acesso a todas as ferramentas disponibilizadas pela comunidade descritas no capítulo anterior.

O resto das versões já inclui mais características e retira certas limitações tais como poder ter apenas 1 servidor e aumenta significativamente os Endpoints e possibilita Cloud, upgrade, suporte e *machine learning* (exceto na versão Professional) entre as outras referenciadas na figura 14.

Vantagens & Desvantagens

Vantagens:

Comportamento de base humana: o SIEMonster, juntamente com a análise comportamental do ResponSight, é capaz de determinar quaisquer desvios na forma como qualquer utilizador interage com seu sistema que poderia levar a algum tipo de risco cibernético.

Threat Intelligence: Palo Alto MineMeld, uma das ferramentas do SIEMonster, basicamente coleta filtros de vários *feeds* de inteligência. Isso pode ser usado para filtrar domínios maliciosos.

Aprendizado profundo: este é provavelmente um dos recursos mais cruciais do SIEMonster, em que ele é capaz de absorver facilmente quaisquer dados e, em seguida, traçar paralelos com outros eventos e dados anteriores para procurar quaisquer discrepâncias.

Desvantagens:

- Difícil de atualizar
- Não tem análises comportamentais do utilizador
- Não tem suporte
- Capacidade de relatório limitada a 2

2.4. Comparações das soluções SIEM

Baseado na pesquisa (Canner, 2018) podemos tirar algumas das funcionalidades mais importantes a se verificar numa SIEM. Abaixo, na Tabela 1, será apresentado algumas dessas funcionalidades principais, para que possa ser feita uma comparação.

Tabela 1 - Características dos vários SIEMS

Recursos	Características do SIEM				
	OSSIM	Splunk Free	Elastic Stack	SIEMonster	MozDef
Implementação	<ul style="list-style-type: none"> • Local • Ambiente virtual 	<ul style="list-style-type: none"> • Local • Cloud 	<ul style="list-style-type: none"> • Local • Cloud(pago) • Ambiente virtual 	<ul style="list-style-type: none"> • Local • Cloud 	<ul style="list-style-type: none"> • Local • Cloud
Sistema Operativo	<ul style="list-style-type: none"> • Windows • Mac 	<ul style="list-style-type: none"> • Windows • Linux • Mac • Solaris 	<ul style="list-style-type: none"> • Windows • Linux • Mac 	<ul style="list-style-type: none"> • Windows • Linux 	<ul style="list-style-type: none"> • Linux
Escalabilidade	Não	Não	Sim	Não	Sim
Gerir de logs	Não	Sim	Sim	Sim	Sim
Correlação de eventos de segurança	Sim	Sim	Sim	Sim	Sim
Alertas de segurança	Sim	Não	Sim (limitado)	Sim	Sim
Conexões de Threat Intelligence	Sim	Não (Stoner, 2020)	Sim	Sim	Não
Apresentação de Relatório	Sim	Sim	Sim (limitado)	Sim	Não
Machine Learning	Não	Não	Não	Não	Não

Em termos de hardware, este pode variar muito dependendo da quantidade de dados que se quer tratar. No na Tabela 2 é apresentado um resumo do hardware necessário para o funcionamento de cada solução SIEM discutida nos tópicos anteriores.

De referir que os requisitos apresentados na tabela foram dados como requisitos mínimos para o funcionamento correto de cada solução, no entanto como não foram testadas as restantes soluções não é possível afirmar se estão 100% corretas, além da Elastic Stack. Com a Ealstic Stack foi verificado que é possível utilizar com menos de 16 GB de RAM e menos de 8 vCPU. No entanto como é de se esperar, ao realizar a ingestão de logs e ao depender da quantidade de informação a ser analisada, torna-a muito lenta.

Como o cenário de testes era bastante simples para acomodar todos os recursos disponíveis, a mesma conseguiu-se utilizar com 6 a 8GB RAM e 6 vCPU.

Tabela 2 - Requisitos de Hardware das soluções SIEM

	Requisitos do SIEM				
	OSSIM	Elastic Stack	Splunk	MozDef	SIEMONster
Recursos	<ul style="list-style-type: none"> • 2 CPU • 4 a 8GB de RAM • 250GB HDD 	<ul style="list-style-type: none"> • 2 a 8 CPU • 16 a 32 GB de RAM • Disco SSD 	<ul style="list-style-type: none"> • 12 CPU • 16 a 32 GB RAM • SSD 1 TB 	<ul style="list-style-type: none"> • 2 CPU • 4 GB RAM 	<ul style="list-style-type: none"> • 8 CPU • 32 GB RAM

Após esta análise documental destas soluções, apenas com as informações descobertas e sem testes e implementações, é possível fazer um resumo comparativo entre estas soluções.

Com base na documentação dos SIEM referidos foi possível fazer a tabela 2 que contem os requisitos necessários para a implementação de cada um dos SIEM (Or, 2020).

2.5.Características mais relevantes num SIEM

Conforme foi explicado nos tópicos anteriores, é inegável que as implementações de uma SIEM sejam uma componente chave para melhorar a prática de segurança de uma empresa. No entanto a escolha da ferramenta correta tem de ser decidida com bastante planeamento, de seguida estão algumas características e dicas úteis na escolha de uma SIEM:

- **Escalabilidade** - certificar-se de que a solução tem a capacidade de acomodar o crescimento atual e projetado;

- **Compatibilidade de registos** - certificar-se de que a solução seja compatível com seus registos;
- **Mecanismo de correlação** - a solução tem a capacidade de pesquisar em vários dispositivos e registos;
- **Capacidades forenses** - A solução oferece capacidades de análise forense da fonte do evento;
- **Painéis** - A solução deve fornecer a capacidade de criar facilmente painéis e relatórios;
- **Threat Intelligence** - Descubra se a solução tem a capacidade de se integrar com fontes de inteligência internas / externas;
- **Implementação local ou na cloud** - determine se um SIEM como serviço baseado em nuvem é a solução certa para a organização;
- **Armazenamento** – sendo que as funções de um SIEM é armazenar *logs* para análise, o custo para lidar com esse armazenamento pode ser muito elevado se não houver boa gestão.

Tendo estes pontos em consideração, e após o estudo das diferentes soluções anteriores, conseguimos ter uma boa base para nos ajudar a tomar uma decisão na escolha do SIEM mais adequado.

2.6.Threat Intelligence

O *Threat Intelligence* pode identificar e analisar ameaças cibernéticas.

A palavra-chave para a compreensão deste termo é "análise". A *Threat Intelligence* trata de minar grandes quantidades de dados. O Threat Intelligence examina no contexto para descobrir o problema ou possível ameaça e implementar uma solução específica para o problema. A definição de *Threat Intelligence* geralmente é simplificada ou confundida com outros termos de segurança cibernética. Maioria das vezes, o termo "dados de ameaças" é confundido com "inteligência de ameaças". Os dados de ameaças são uma lista de possíveis ameaças.

Pensemos no *feed* do Facebook, é uma lista continua de possíveis problemas, e esses dados são ameaças, as postagens não significam nada até que sejam lidas ou sejam combinados esses conhecimentos com outras postagens de amigos, isto é a *Threat Intelligence*.

De início, especialistas na área ou ferramentas sofisticadas irão ler a ameaça e analisá-la. Em seguida, aplicar o conhecimento histórico para ver se a ameaça é real e, em caso afirmativo, como lidar com a mesma (kaspersky, 2021).

Mesmo assim, o termo Threat Intelligence não tem uma definição específica oficial, elas divergem de acordo com a visão de cada um.

Mais e mais organizações começaram a estabelecer ou expandir seus programas e práticas de *Threat Intelligence*. O processo de implementação de programas de *Threat Intelligence* permite que as organizações recolham, analisam, geram e integram a sua própria inteligência interna e externa. O objetivo final de qualquer programa de *Threat Intelligence* é criar inteligência que será incorporada ao fluxo de trabalho da organização.

A *Threat Intelligence* é útil para todas as organizações de segurança. As companhias enfrentam cada vez mais uma quantidade maior de ameaças. Deixamos de questionar se um ataque irá acontecer, mas sim quando. As companhias e seus *Security Operations Center* (SOC) requerem mais informações, mais consistência e mais inteligência nos dados obtidos.

2.6.1. Threat Intelligence Platform (TIP)

O Threat Intelligence Platform (TIP) é tal como o nome diz uma Plataforma de Threat Intelligence, ou seja, uma solução que recolhe, junta e organiza os dados de Threat Intelligence de várias fontes.

O TIP fornece informações sobre o malware conhecido e outras ameaças como listas negras de IP's, domínios, ficheiros duvidosos entre outros, com isto, garante a identificação, investigação e respostas eficientes e precisas às ameaças apresentadas. O TIP permite que se analise dados e investir em ameaças de segurança em vez de perder tempo a gerir e recolher dados. Além disso um TIP permite que as equipas de segurança e Threat Intelligence partilhem com facilidade os dados de Threat Intelligence com outras partes interessadas e sistemas de segurança. Um TIP pode ser implantado como um software como serviço (SaaS) ou como uma solução local (paloaltoNetworks, 2019).

2.6.2. Como os TIP podem complementar um SIEM

Quando as organizações integram um sistema existente de gerir de eventos e informações de segurança (SIEM) com uma plataforma de *Threat Intelligence*, elas podem priorizar alertas, agregando valor ao seu SIEM.

Atualmente cada vez mais organizações pensam na implementação de segurança dos seus sistemas, no entanto, muitas falham numa etapa inicial (Varonis).

Com a utilização de uma ferramenta de *Threat Intelligence* conseguimos resolver alguns que nos deparamos com soluções SIEM, mencionadas abaixo ((TIP), 2019).

Algumas das dificuldades encontradas inicialmente são:

- Grandes quantidades de *logs*;
- Análise dos *logs* e saber reconhecer o que pode ser uma ameaça;
- Falta de contexto dos *logs* analisados;
- Dificuldade de identificar o contexto de eventos únicos;

Um SIEM correlaciona os *logs*, dando uso à análise do comportamento dos utilizadores e entidades para identificar as ameaças e enviar alertas e, devido à sua eficácia, pode gerar demasiados alertas, sendo que poderá haver alertas em excesso.

2.6.3. Como funciona a integração TIP no SIEM

A implementação de um TIP dentro do SIEM de uma organização de segurança fornece uma visão da comunidade global de segurança cibernética e fornece recursos valiosos de conscientização sobre ameaças que podem melhorar a postura de segurança de qualquer corporação. Estas integrações atribuem valor aos alertas, dando prioridade de acordo com seu nível de gravidade.

Partilha de informação e colaboração

Os SIEM têm ferramentas capazes de agregar informações e compartilhá-las. Os TIP foram desenvolvidos para permitir esse tipo de compartilhamento, permitindo que os analistas e outros especialistas colaborem sem serem sobrecarregados pelas informações contidas nos *logs*.

A realidade é que, se nós descobrirmos pela primeira vez uma ameaça em um *feed*, provavelmente será tarde demais. O objetivo é fornecer à nossa equipe de segurança ferramentas para monitorar e rastrear ameaças antes que se tornem um ataque bem-sucedido.

Um bom TIP ajuda um profissional de segurança a compilar e monitorar as informações para que ele possa ser identificado e imediatamente atendido.

O seguinte exemplo, a organização está a utilizar o Umbrella¹ e Investigate² em conjunto com o SIEM e o TIP, e através da API disponibilizada pela Cisco para criar um ciclo de *feedback*.

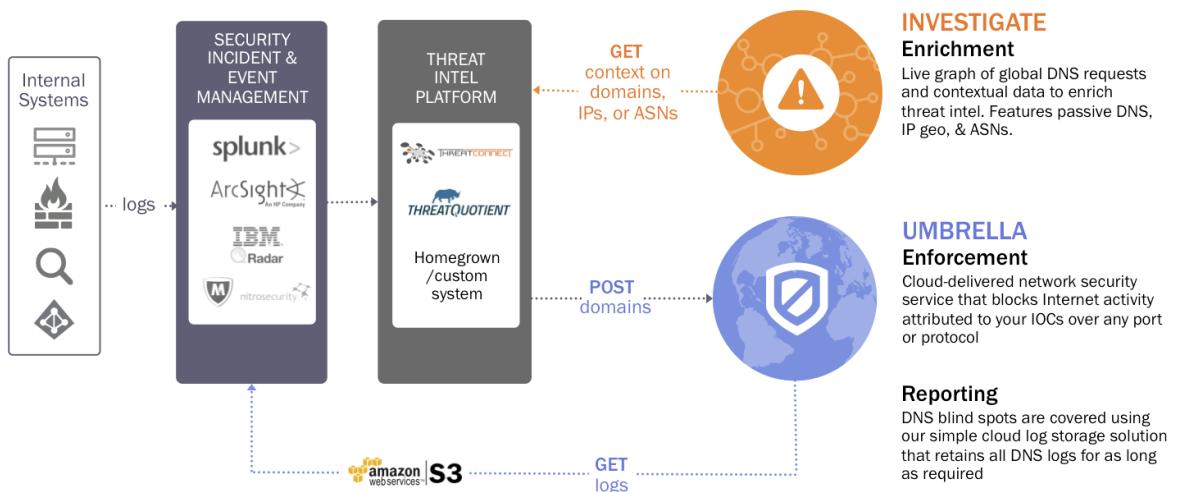


Figura 15 - Diagrama do funcionamento de um SIEM com TIP, (Prytuluk, 2021)

¹ <https://umbrella.cisco.com/>

² <https://umbrella.cisco.com/products/umbrella-investigate>

2.6.4. Soluções TIP

As soluções TIP existentes são imensas e algumas delas apresentam custos de utilização e outras são gratuitas. De seguida são apresentadas na Tabela 3 as soluções TIP gratuitas mais utilizadas.

Tabela 3 - Soluções TIP mais utilizadas

Nome	Tipo	Ano criado	Dono
GOSINT	<i>Open source</i>	2017	Cisco
CRITs	<i>Open source</i>	2014	MITRE
CIF	<i>Open source</i>	2012	CSIRT Gadgets Foundation
MANTIS	<i>Open source</i>	2013	SIEMENS
MISP	<i>Open source / Community</i>	2012	CIRCL
MineMeld	<i>Open source</i>	2016	Palo Alto
Yeti	<i>Open source</i>	2017	Yeti
Threat Central	<i>Community</i>	2015	Micro Focus
OTX	<i>Community</i>	2012	AlienVault
ThreatExchange	<i>Community</i>	2015	Facebook
X-Force Exchange	<i>Community</i>	2015	IBM
ThreatStream	<i>Commercial</i>	2013	Anomali
EclecticIQ Platform	<i>Commercial</i>	2014	EclecticIQ
LookingGlass	<i>Commercial</i>	2015	LookingGlass
Soltra Edge	<i>Commercial</i>	2014	NC4
ThreatConnect	<i>Commercial</i>	2013	ThreatConnect
ThreatQ Platform	<i>Commercial</i>	2015	ThreatQuotient
TruSTAR	<i>Commercial</i>	2014	TruSTAR Technologies

Tanto as versões *Open source* como *community* são gratuitas, sendo que no caso das comerciais não é possível receber *feeds* (além das funcionalidades pagas) a partir de outras TIP, por exemplo é possível aderir a *feeds* fornecidos por utilizadores independentes ou comunidades como no caso do OTX e MISP onde é possível receber *feeds* de outros TIP gratuitos.

Há muitos motivos pelos quais escolhemos uma solução gratuita de TIP, mas normalmente se planejamos incluir alguns recursos pagos no futuro, pode ser mais caro do que um TIP comercial.

Com referência ao artigo da Enisa, será feita uma descrição de cada um dos TIP que achamos mais relevantes descritos na tabela 3 (Enisa.europa, 2017)

Open source

GOSINT – *framework* usada para recolher, processar e exportar IOC de grande qualidade.

CRIT (Collaborative Research Into Threats) – O CRIT aproveita outros software *open source* para a criação de uma ferramenta unificada na defesa contra ameaças. O modelo de segurança para CRIT é atualmente baseado no que chamamos de "Acesso à Fonte". É bastante restritivo, pois cada utilizador só tem acesso para ler e gravar conteúdo para as fontes as quais tem acesso.

Collective Intelligence Framework – É um sistema para gerir *threat intelligence open source* sendo que as informações mais comuns são endereços IP, domínios e URL. O CIF permite combinar informações de ameaças conhecidas por muitas fontes e usar as mesmas para as identificar, detetar e mitigar.

MANTIS Cyber Threat Intelligence Management Framework – estrutura para gerir *threat intelligence* sobre ciberataques que expressa em padrões como STIX, CybOX, IODEF e mais linguagens estruturadas para *cyber threat intelligence*. É um repositório de informações de ameaças que também possui navegação, filtragem e recursos de pesquisa.

Malware Information Sharing Platform (MISP) – solução para recolher, armazenar, distribuir e partilhar indicadores de segurança cibernética e informações sobre as ameaças, análise de incidentes de segurança e análise de *malware*. O MISP é projetado por e para analistas de incidentes, profissionais de segurança para apoiar suas operações do dia-a-dia para partilhar informações de forma eficiente. Finalmente, existem várias comunidades MISP às quais uma organização pode aderir tais como CIRCL OSINT Feed que é a comunidade standard ao qual é aderida ao inicializar o MISP, mas existem muitas outras.

MineMeld – É uma estrutura de processo de indicadores *open source*. Com uma arquitetura modular e facilita a agregação, aplicação e partilha de indicares de ameaças.

Yeti – Estrutura destinada a organizar observáveis, IOC, TTP (táticas, técnicas e procedimentos), e conhecimento sobre as ameaças em um repositório único e unificado. O Yeti também enriquece automaticamente os observáveis e fornece uma interface para utilizadores e outra para máquinas (via API) para que outras ferramentas possam falar com ele.

Community

Anomali ThreatStream é uma solução comercial que permite às organizações de recolher, otimizar, integrar e disseminar *feeds* de *threat intelligence*. IOC são mapeados com modelos de ameaças estratégicas para que os analistas sejam capazes de identificar, investigar e reagir rapidamente a ameaças à segurança.

EclecticIQ Platform é uma plataforma comercial de *threat intelligence* que oferece soluções centradas na análise tecnológica para consolidar, analisar, gerir, agir e disseminar inteligência e relatórios. Esta plataforma fornece fluxos de trabalho amigáveis para analistas, bem como integração com os principais provedores de *threat intelligence*.

LookingGlass fornece soluções comerciais para gerir inteligência e ameaças. ScoutPrime e o ScoutVision (ferramentas integradas no LookingGlass) fornecem a capacidade de recolher, priorizar e orquestrar a resposta à ameaça conforme além de fornecer ferramentas de análise, colaboração e partilha de ameaças.

NC4 Soltra Edge é uma plataforma comercial que automatiza processos para partilhar, receber, validar e atuar com base nos *feeds* recebidos do *threat intelligence*.

A Central de Ameaças da Micro Focus é uma plataforma de partilha de inteligência de segurança fornecida pela comunidade. A plataforma aglomera informações de *feeds* públicos, fornecedores de segurança e membros da comunidade que são analisados e posteriormente disseminados para os membros da comunidade.

ThreatConnect é uma solução TIP comercial que ajuda as organizações a orquestrar a segurança e processa, analisa dados, responde a ameaças. Também pode integrar-se com as ferramentas de segurança existentes e partilhar inteligência com outras entidades internas e externas.

A plataforma ThreatQuotient ThreatQ é uma solução comercial que se concentra em ameaças cibernéticas operações e gestão. Ele fornece recursos de agrupamento de dados das ameaças, dinamização de inteligência, fluxos de trabalho personalizados, bem como recursos de orquestração e automação.

A plataforma TruSTAR é uma solução comercial de software como serviço. O foco principal é colocado na operacionalização de *feeds* ISAC e OSINT, agilizando processos internos e partilha, bem como partilha flexível de informações com as partes interessadas.

2.7.Síntese

Tendo em conta o tema deste trabalho, foi necessário de início, desenvolver alguns conceitos sobre eventos de segurança, isto incluiu como funcionam ataques informáticos e os tipos de ataques realizados. Também foi mencionado o que são *logs*, e como funciona o seu processamento, pois é uma parte essencial na análise de ameaças.

O capítulo seguinte teve como objetivo fazer o estudo do SIEM e um comparativo entre as seguintes soluções: OSSIM, *Elastic Stack*, Splunk Free, MozDef e SIEMONster.

Primeiro para que fosse possível perceber melhor cada SIEM, foi realizada uma breve explicação sobre como surgiu o SIEM e suas características gerais que se encontram em cada um. Seguindo de um subcapítulo descrevendo as funções importantes tais como arquitetura, funcionalidades e vantagens e desvantagens, que julgamos ser características relevantes ter cada SIEM para a sua implementação mais tarde.

Logo é feita a descrição geral do SIEM em si, depois é descrita a arquitetura do mesmo e suas funcionalidades, devido a no fim ser feita a comparação entre os mesmos para percebermos e nos influenciar a escolha da arquitetura proposta, é feito um capítulo com as vantagens e desvantagens de cada SIEM.

Neste capítulo também é dado uma introdução ao que é o Threat Intelligence, ajudando a perceber o que significa, visto que ainda não há uma definição específica para o termo.

Com o termo Threat Intelligence explicado, facilita a percepção de o que é um TIP.

Por alto TIP é uma Plataforma de Threat Intelligence, que recolhe, junta e organiza os dados de Threat Intelligence de várias fontes.

Dando seguimento ao como funciona um TIP é explicado como é ele pode complementar um SIEM e como funciona a sua integração em SIEM.

Como o objetivo do projeto é que através desta análise comparativa dos vários SIEM *open source* e que nessa versão seja possível implementar um SIEM já com alguma robustez, portanto, é importante avaliar as funcionalidades chave que se pretende implementar em uma PME. Dito isto, consideramos importante que seja possível para que uma PME seja capaz de implementar o SIEM escolhido desde a instalação do SIEM até à sua configuração.

A solução Splunk Free foi ponderada devido à sua instalação básica (Zarzosa, 2017), mesmo com uso dos 500MB diários existe uma grande falha que é a definição de limites temporais na retenção dos dados, o que impossibilita o utilizador que queira analisar dados com alguma longevidade, por isso decidimos descartar esta funcionalidade.

O SIEMonster cativou-nos bastante devido a ter bastante documentação e à sua popularidade ganha em tão pouco tempo, contudo, pareceu um SIEM já bastante robusto e pouco ajustável (Bycroft, 2018) pois por exemplo como monitoração possui apenas o Prometheus e o nosso objetivo é que esse tipo de funcionalidades seja implementado e configurado de raiz.

Apesar do OSSIM parecer uma solução relativamente fácil de implementar e utilizar, requeria a partida, alguns conhecimentos para aproveitar das suas funcionalidades, como a correlação e análise de *logs*.

O MozDef tem algumas funcionalidades atrativas como a utilização do *Kibana* para a visualização, no entanto, foi encontrada muito pouca documentação sobre sua implementação e, portanto, requereria algum esforço extra para ter um protótipo funcional.

Considerando todos estes fatos anteriormente referidos foi decidido que o SIEM mais interessante para implementação da nossa solução é o *Elastic Stack* pois apesar de conter uma curva de aprendizagem maior, com estes conhecimentos será possível já configurar uma SIEM já bastante robusto e com as funcionalidades que são fundamentais para a implementação do nosso projeto tais como recolha e processamento de *logs*, o armazenamento é feito logo no *Elasticsearch* que é escalável e tolerante a falhas (Berman, 2018) (Vazão, 2020) o que é bastante importante pois é muito raro nas PME existir qualquer redundância no que toca a armazenamento, as *Dashboards* exigem já algum conhecimento mas assim que configuradas torna-se numa ferramenta bastante útil e poderosa, e claro a possibilidade de integração TIP que é um fator chave no nosso projeto.

Todos estas características são importantes, mas algo que tornou a decisão final foi o facto de o *Elastic Stack* estar sempre a disponibilizar melhorias e novas funcionalidades pois cada versão disponibiliza gratuitamente sempre alguma funcionalidade que em outros SIEM são pagas como por exemplo agora parte do *X-PACK* é gratuito o que disponibiliza alertas (com algumas limitações). Com isto, torna que a implementação desta solução possa estar sempre sujeita a melhorias e sempre cada vez mais funcionalidades.

3. Arquitetura e *Elastic Stack*

O objetivo deste capítulo é mostrar de uma maneira mais abstrata o funcionamento do SIEM desde os inputs do sistema até aos outputs e aprofundar um pouco algumas características sobre o *Elastic Stack* pois como foi falado no capítulo anterior será esse o SIEM que será implementado e testado nesta solução.

3.1. Arquitetura lógica

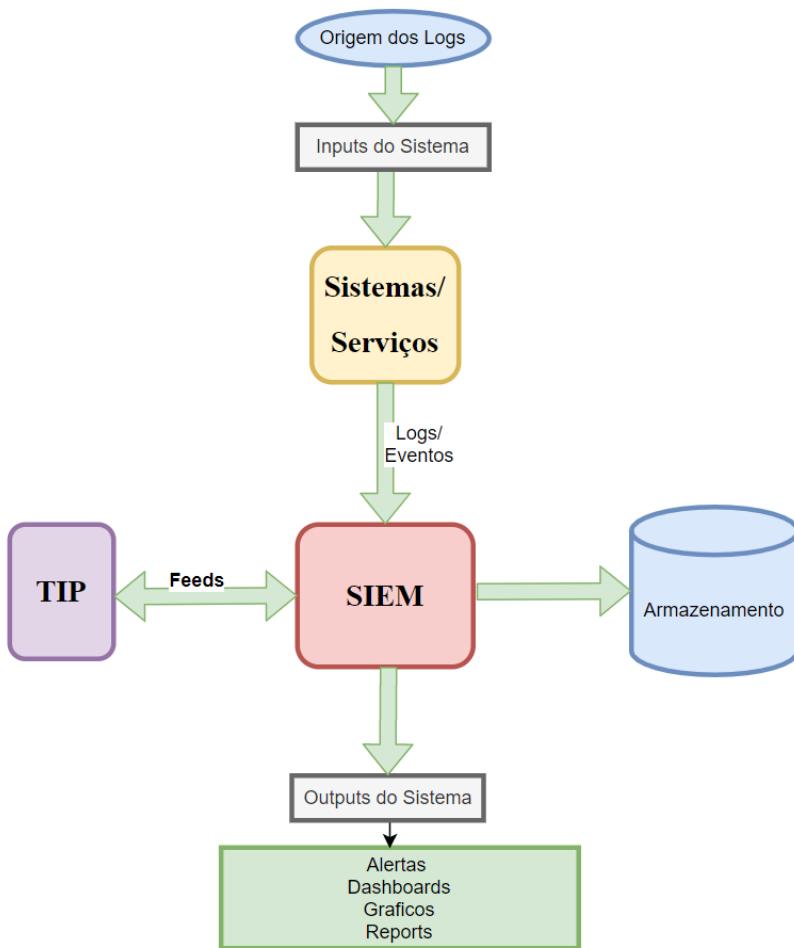


Figura 16 - Arquitetura abstrata do funcionamento de um SIEM com integração TIP

Como existe pouca documentação e não foram encontrados quaisquer esquemas que expliquem bem o funcionamento do SIEM com Integração a TIP foi criado o esquema da figura acima. Como se pode visualizar neste esquema, o bloco Sistemas/Serviços será referente ao sistema ou serviço que se pretende monitorização onde os *logs* ou outro tipo de

informação são gerados e enviados para o SIEM através de serviços, agentes instalados na máquina ou configuração do sistema de *logs* para encaminhar par ao SIEM.

No bloco do SIEM vai armazenar, analisar, tratar esses dados para que possam ser gerados outputs, os outputs podem ser *Reports*, Alertas, *dashboards*, gráficos entre outros.

No bloco TIP são enviados os *feeds*, que contem informação sobre possíveis ameaças tais como listas de IP's e domínios malignos, ficheiros com nomes suspeitos e possíveis ameaças.

3.2. *Elastic Stack*

Seguindo o que foi explicado anteriormente no capítulo sobre o *ELASTIC STACK*, é constituído por 4 ferramentas, *Logstash*, *Kibana*, *Elasticsearch* e *Beats*, que serão descritas nos próximos capítulos e mostrado como as mesmas funcionam.

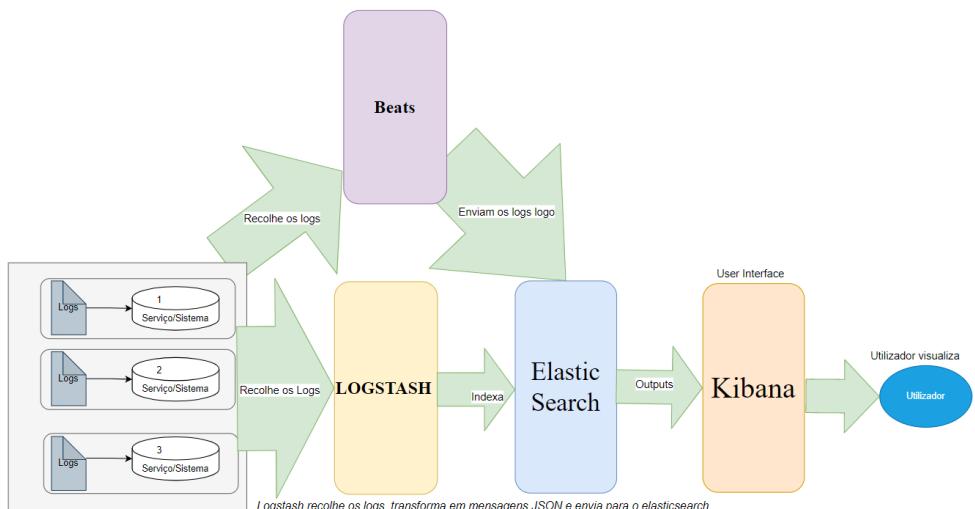


Figura 17 - Funcionamento lógico do *Elastic Stack*

O que é pretendido com este esquema da Figura é que se perceba o *flow* dos *logs* até ao utilizador sendo que a recolha dos *Logs* é diferente do *Logstash* e nos *Beats*, a diferença é o que *Logstash* recolhe e envia os *Logs* logo sendo que nos *beats* são tratados consoante o que foi configurado e depende do beat por exemplo o *Packetbeat* trata apenas dos *logs* referentes à rede.

O resto do funcionamento do *Elastic Stack* será descrito nos próximos subcapítulos.

3.2.1.1. Elasticsearch

O *Elasticsearch* é um mecanismo de pesquisa e análise de dados distribuídos e aberto a todo o tipo de dados () e é conhecido pela sua REST API's simples, natureza distribuída, velocidade e escalabilidade sendo que este possui um agregado de ferramentas gratuitas para tratamento, enriquecimento, armazenamento análise e visualização de dados ().

Como o *Elasticsearch* é o núcleo do *Elastic Stack*, armazena os dados centralmente para garantir rapidez de pesquisa e analítica poderosa que pode ser ampliada.

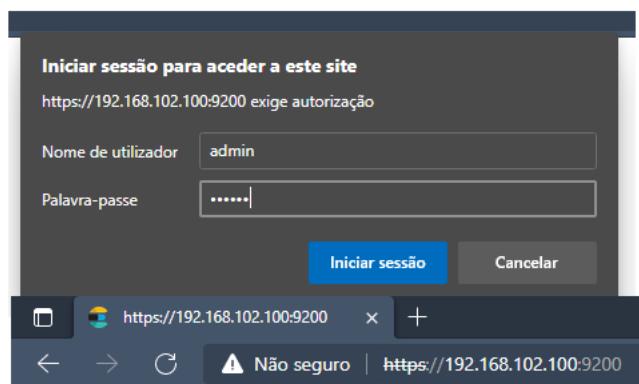
O *Elasticsearch* é um mecanismo de análise de dados e busca RESTful distribuído, capaz de atender a um número crescente de casos de uso (elastic, 2021).

Implementação na Solução

Na solução foi feita a instalação do *Elasticsearch*

e há pouca interação direta do utilizador com o *Elasticsearch* devido ao *Kibana* ser a ferramenta de visualização e onde é feito todo o gerir dos dados fornecidos pelo *Elasticsearch*.

O *Elasticsearch* encontra-se na porta 9200 que pode ser acedida através do browser como *https://<ip da máquina>:9200*.



```
{
  "name" : "elk-1",
  "cluster_name" : "demo-elk",
  "cluster_uuid" : "3FGb4VjbTTGU8FZysr-cPg",
  "version" : {
    "number" : "7.13.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "4d960a0733be83dd2543ca018aa4ddc42e956800",
    "build_date" : "2021-06-10T21:01:55.251515791Z",
    "build_snapshot" : false,
    "lucene_version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Figura 18 - aceder à porta 9200 (Elasticsearch)

3.2.1.2. Logstash

O *Logstash* é um pipeline de processamento de dados que permite fazer a tratamento de dados de várias fontes diferentes juntamente e enriquecer e transformar os dados antes de serem indexados no *Elasticsearch*.

O *Logstash* vai recolher os *logs*, transformar em mensagens JSON e agrupar e processar dados e enviar para o *Elasticsearch* para indexação (elastic a. , 2021).

Implementação na Solução

Na solução foi feita a instalação e configurações do Anexo – A Instalação *Logstash*.

3.2.1.3. Kibana

O *Kibana* é uma ferramenta de visualização, ou seja, a interface do utilizador onde é feita a visualização e gerir de dados para o *Elasticsearch* fornecer histogramas, gráficos e mapas.

O *Kibana* é a ferramenta que trata da visualização dos dados indexados pelo *Elasticsearch* e também atua como interface para o utilizador monitorar, gerenciar e proteger o *cluster* do ElasticStack.

Pode-se ver todos estes elementos anteriormente falados em *dashboard* em tempo real as suas analíticas de grandes volumes de dados tais como (elastic b. , 2021):

- Logging e análise de *logs*;
- Métricas de infraestrutura e monitorização de *containers*;
- Monitorização de performance de aplicação (APM);
- Análise e visualização de dados geoespaciais;
- Analítica de segurança;
- Análise de dados empresarial;
- Monitorização, gerir e proteção de uma instância do *Elastic Stack* via interface Web;
- Centralização do acesso para soluções integradas desenvolvidas no *Elastic Stack* para aplicações de observabilidade, segurança e busca empresarial.

Funcionamento do *Kibana* na busca e visualização de dados

Possibilitando a análise visual de dados de um índice do *Elasticsearch* ou de vários índices, os mesmos são criados quando o *Logstash* ou os *Beats* ingerem dados não estruturados de *logs* e os converte em um formato estruturado para as funcionalidades de armazenamento e busca do *Elasticsearch*.

Implementação na Solução

Na solução implementada foi instalado o *Kibana* no Anexo-A e após todas as configurações tem-se acesso ao *Kibana* na porta 5601.

https://<ip da máquina>:5601

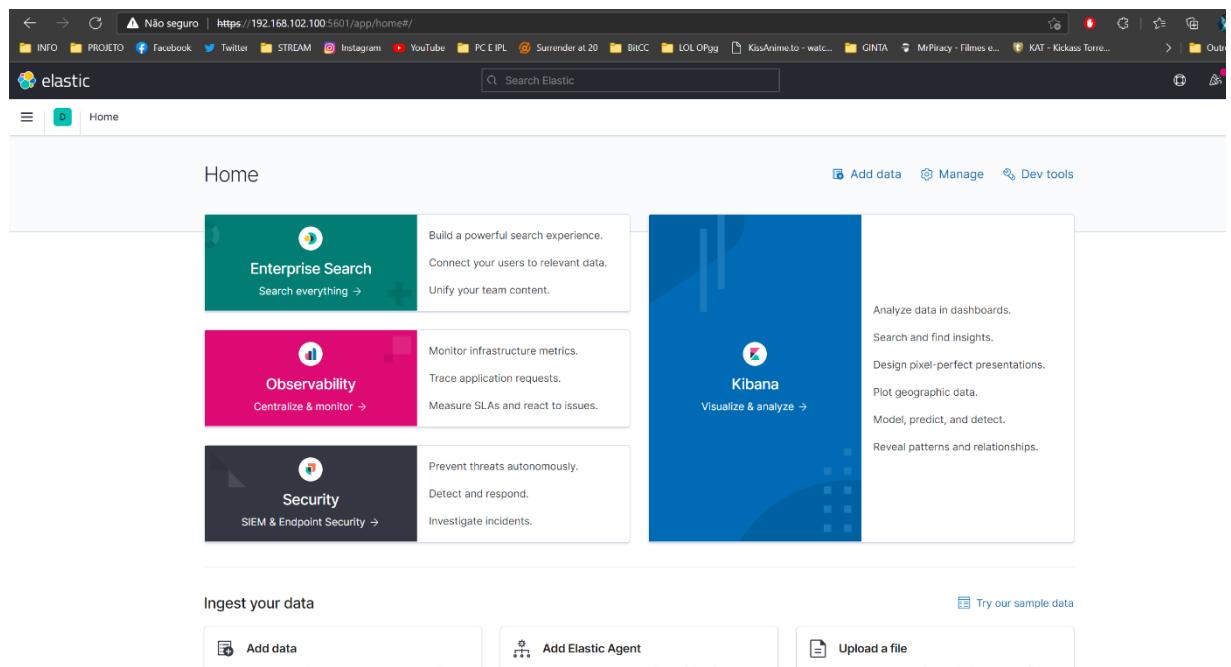


Figura 19 - Menu Principal do *Kibana*

Criação de um utilizador

Para facilitar o acesso ao *Kibana*, foi criado um novo utilizador **Admin** com todas as permissões.

The screenshot shows the 'Create user' interface in Kibana. It is divided into several sections:

- Profile**:
Provide personal details.
 - Username**: admin
 - Full name**: admin user
 - Email address**: admin.demoelk@gmail.com
- Password**:
Protect your data with a strong password.
 - Password**: (redacted)
 - Confirm password**: (redacted)
 - Message: Password must be at least 6 characters.
- Privileges**:
Assign roles to manage access and permissions.
 - Roles**: superuser
 - Link: Learn what privileges individual roles grant.
- Buttons**:
 - Create user (blue button)
 - Cancel

Figura 20 - Criar um user no Kibana

3.2.1.4. Beats

Auditbeat

Auditbeat serve para verificar atividades dos utilizadores e processos nos sistemas. Por exemplo pode-se usar para recolher e centralizar eventos de auditoria do Linux Audit Framework, sendo que também é possível detetar alterações em ficheiros especiais, como por exemplo ficheiros de configuração e identificar violações nas políticas de segurança (elastic b. , 2021).

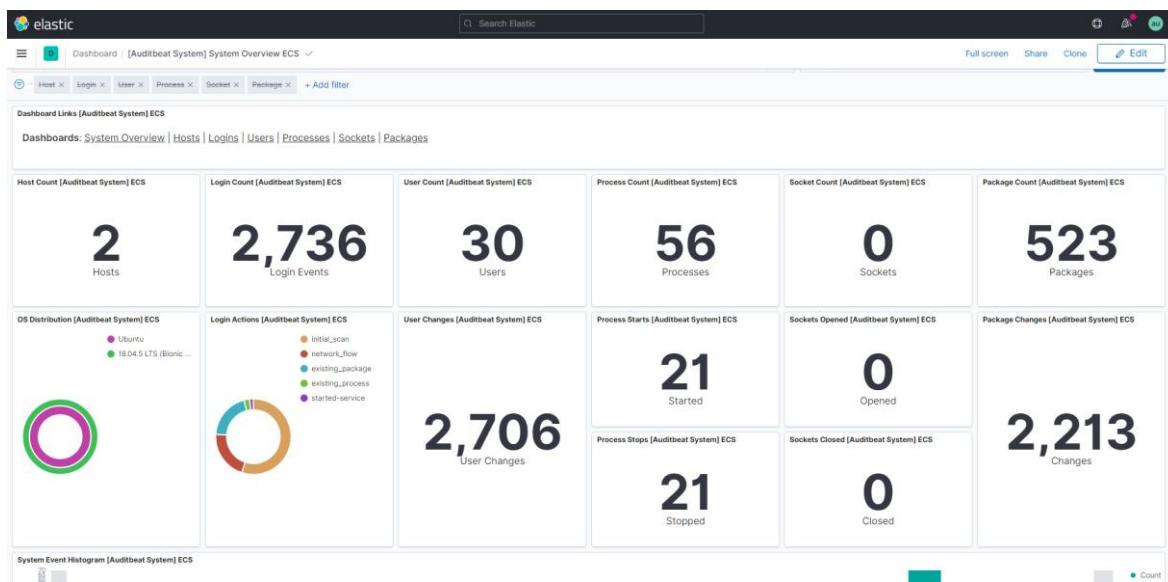


Figura 21 - Dashboard do Auditbeat

Filebeat

O Filebeat serve para encaminhar e centralizar dados dos *logs* e monitorizar os *logs*. Uma pasta pode ser especificada no ficheiro de configuração do mesmo, encaminhando os *logs* para o *Elasticsearch* ou *Logstash* (elastic b. , 2021).

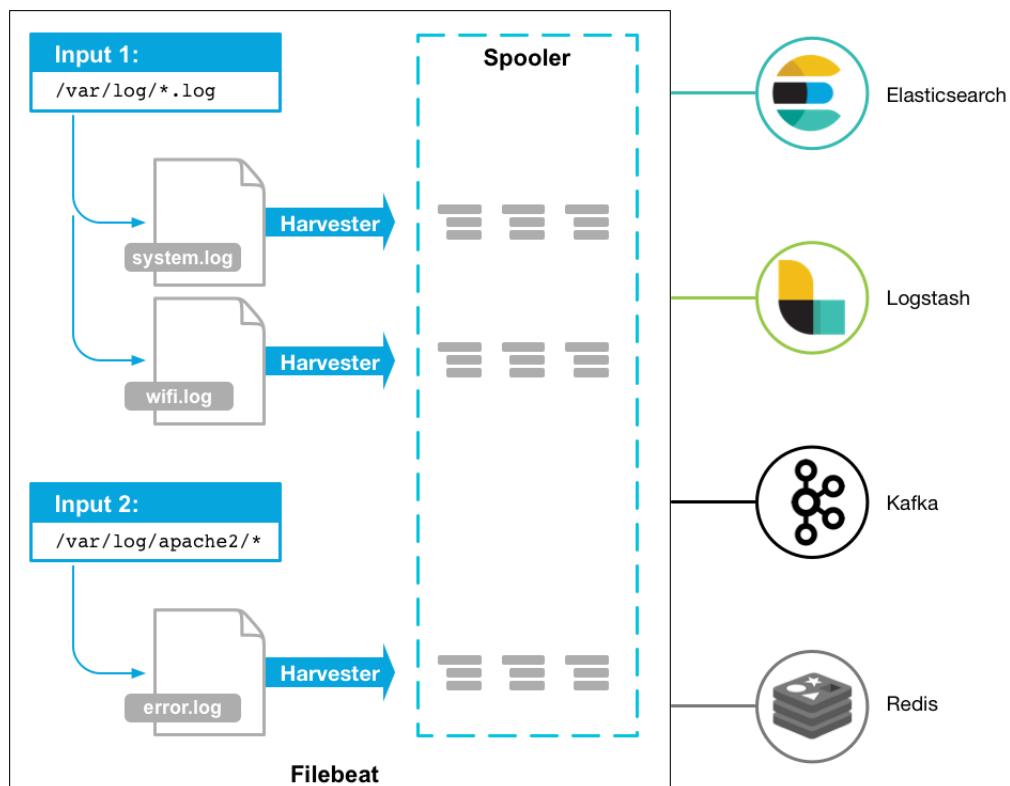


Figura 22- Como os dados são recolhidos no Filebeat (elastic f. , 2021)

O *harvester* é responsável por ler o conteúdo de um ficheiro, e de seguida envia o conteúdo lido para a saída, por exemplo, para o *Elasticsearch*, que de seguida é enviado para o *Kibana*, permitindo criar e visualizar *dashboards* (elastic b. , 2021).

No contexto do nosso projeto, o Filebeat foi utilizado para detetar diversas anomalias, como por exemplo excesso de tentativas de login ao servidor web 4.3.1 Ataques simulados.

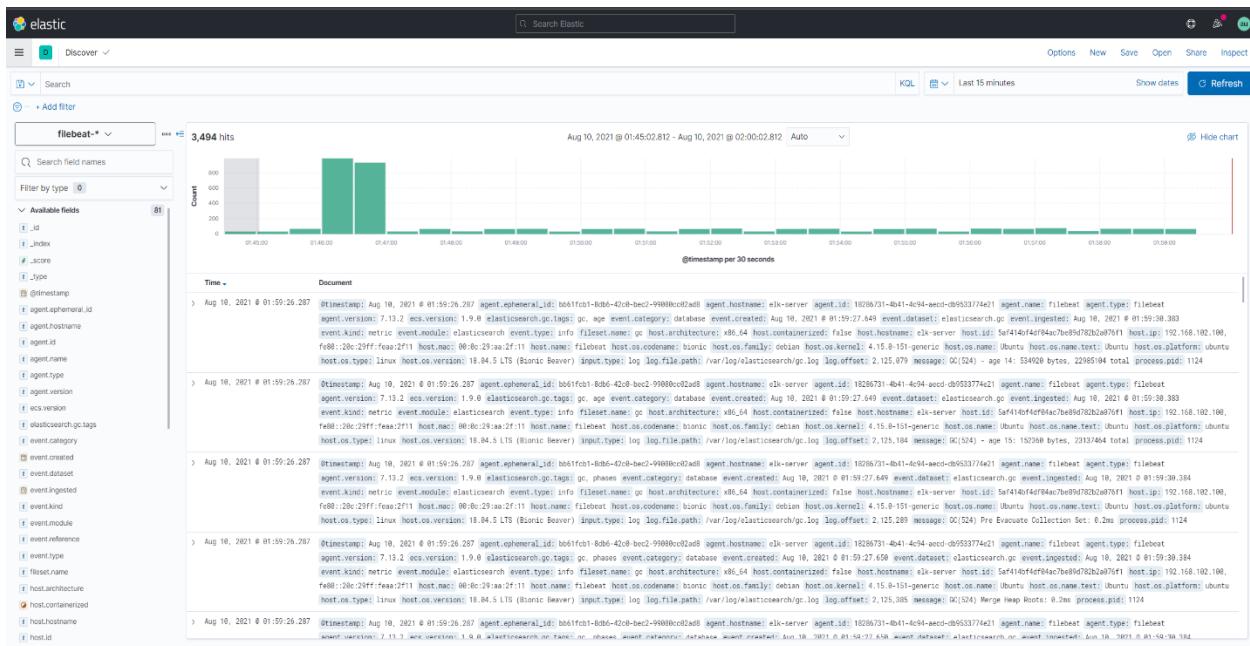


Figura 23 - Menu Discover do Kibana onde se pode visualizar os logs do Filebeat com as tags

Heartbeat

Heartbeat serve para verificar periodicamente a condição dos serviços e determinar se estão acessíveis. Serve também para verificar se um serviço está a cumprir o seu tempo ativo e verificar se de fora pode aceder aos serviços fornecidos pelo servidor (elastic b. , 2021).

O Heartbeat pode ser configurado para mandar *ping* a todos os endereços IP resolvidos por DNS para um nome de *host* especificado podendo assim verificar todos os serviços com balanceamento de carga para ver se estão disponíveis.

Sendo que também é possível especificar *hosts* para serem monitorizados que são conhecidos como “monitor” que podem ser verificados a tempos específicos para cada monitor (elastic b. , 2021).

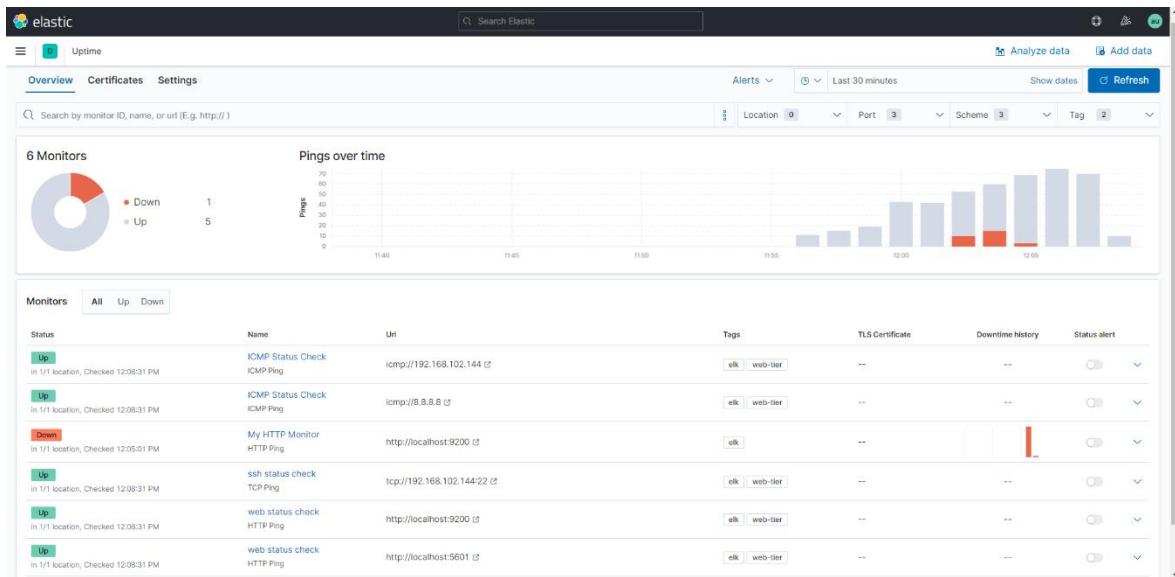


Figura 24 – Verificação dos vários monitors no Heartbeat

Metricbeat

Metricbeat consiste em módulos e conjuntos de métricas, um módulo pode definir para recolher dados de um serviço específico, especificando detalhes do serviço e como se ligar ao mesmo, e com que frequência recolhe as métricas e quais recolhe. Em vez de recolher cada métrica como um evento separado, os conjuntos de métricas recuperam uma lista de várias métricas relacionadas em uma única solicitação para o sistema remoto (elastic b. , 2021).

A maior vantagem do Metricbeat é que sua instalação é muito fácil e não requer nenhuma dependência. É apenas preciso ligar os módulos desejados no ficheiro de configuração, e referenciar corretamente o *Elasticsearch* e o *Kibana*.

O Metricbeat é ideal na monitorização de soluções dentro de Dockers, no entanto, como a arquitetura do nosso projeto é baseada em máquinas virtuais num ambiente local, por isso procuramos por explorar outras ferramentas de monitorização, mencionadas em **Erro! A origem da referência não foi encontrada. Erro! A origem da referência não foi encontrada..**

Packetbeat

Packetbeat serve para analisar pacotes da rede em tempo real garantido visibilidade entre os servidores da rede em que está. Funciona recolhendo o tráfego da rede entre servidores das aplicações e descodificando os protocolos da camada das aplicações (Ex: HTTP).

Oferecendo suporte a vários protocolos, deteta o tráfego entre os servidores da rede e analisa os protocolos das aplicações em tempo real correlacionando as mensagens (elastic b., 2021).

Na nossa solução usamos o Packetbeat para detetar um número enorme de pacotes quando é feito um ataque *SYN Flood*, demonstrado nos 4.3.1 Ataques simulados.

Winlogbeat e Sysmon

Winlogbeat envia *logs* dos eventos do Windows para o *Elasticsearch*, onde são processados e enviados para o *Kibana*, onde podemos visualizar diferentes *dashboard* (Elastic, Winlogbeat: Analyse Windows Event Logs | Elastic, 2021).

O Sysmon é um serviço do Windows, que complementa o envio dos *logs*, pois este serviço fornece informações detalhadas sobre o sistema, permitindo uma visão mais detalhada de atividades maliciosas (Mark Russinovich, 2021)..

Na nossa solução, estes serviços vão ser utilizados para detetar e enviar informações sobre potencial *malware* ao ser executado remotamente, 4.3.1 Ataques simulados.

3.3.Síntese

Este capítulo visa a esclarecer o funcionamento genérico de um sistema com integração TIP num SIEM através de uma arquitetura mais abstrata explicando o caminho dos logs desde a sua criação até aos outputs, gerando assim as Dashboards, Graficos e os outros mencionados.

Como segunda parte do capítulo é feito um aprofundamento do funcionamento do Elastic Stack e as suas ferramentas, vendo as diferenças do flow dos logs quando passa pelo Logstash ou pelos beats.

Dando seguimento ao esclarecimento do Elastic Stack é feita uma descrição mais detalhada das suas ferramentas e como estão implementadas no nosso projeto.

4. Implementação e testes

As implementações de um SIEM envolve vários passos a seguir para o seu funcionamento correto. Sendo que neste trabalho o foco era a implementação de uma solução SIEM *open source*, que funcione em conjunto com um TIP.

Pretendeu-se que o protótipo fosse capaz de assegurar a ingestão de *logs* de diferentes sistemas, incluindo os próprios *feeds* do TIP, e garantir que seja possível realizar pesquisas desses mesmos *logs* dentro da plataforma.

Foi também tomado em consideração a necessidade de enviar alertas relativamente a diferentes tipos de eventos, sejam estes ameaças a alguma máquina local, ou informações recolhidas pelo TIP.

4.1. Protótipo

Como é referido no próximo subtópico, a implementação de um protótipo deste tipo é exigente a nível de hardware, por esse motivo numa fase inicial tivemos de simplificar o cenário de forma a conseguirmos ter os recursos suficientes para o funcionamento do SIEM assim como as restantes máquinas virtuais que compõe a rede de testes.

De forma a conseguir demonstrar o funcionamento em diferentes sistemas operativos, foi criado o seguinte cenário de testes, representado pela Figura 23.

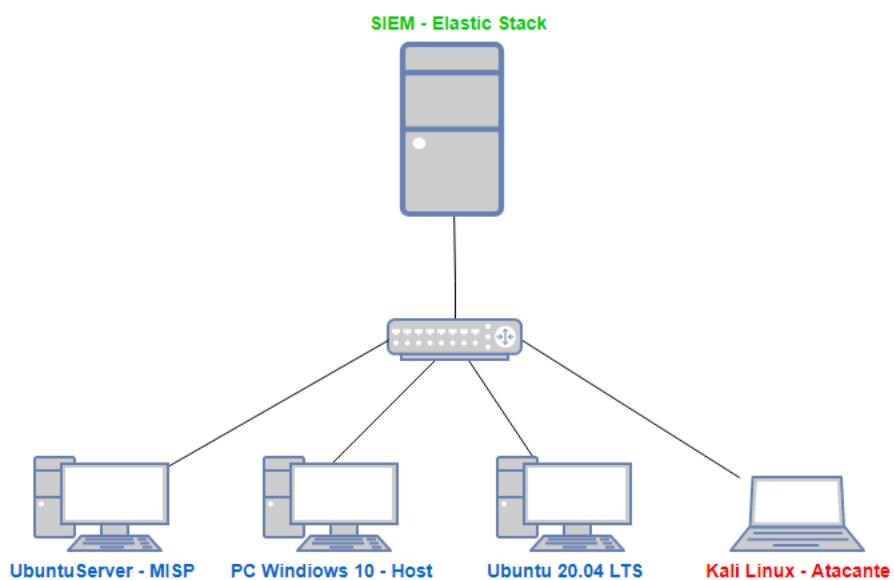


Figura 25 - Arquitetura da solução

Cada máquina virtual neste cenário tem o seu propósito e software instalados, que vão ser detalhados seguidamente.

4.1.1. Especificações técnicas do protótipo

A criação deste cenário foi feita somente num computador com as seguintes especificações:

- CPU: AMD Ryzen 5 2600, 3.90 GHz
- RAM: 16GB
- HDD: 1 TB

As máquinas virtuais do cenário foram criadas com o VMware Workstation 16 Pro, cada uma com a quantidade de recursos necessários para o correto funcionamento. No entanto como pela falta de recursos foi impossível conseguir ter todas as máquinas ligadas em simultâneo, algumas especificações, como a quantidade de memória RAM, tiveram de ser alteradas com o decorrer dos testes.

A Tabela 4 resume as especificações de cada máquina virtual assim como o seu software.

Tabela 4 - Descrição das várias máquinas da solução

Máquina Virtual	Hardware	Sistema Operativo	Software
ELK Server	6 vCPU 8 GB RAM HDD 200 GB	Ubuntu Server 18.04 LTS	<i>Elasticsearch</i> <i>Logstash</i> <i>Kibana</i> Auditbeat Filebeat Metricbeat Packetbeat Heartbeat Netdata
Webserver	2 vCPU 2 GB RAM HDD 100 GB	Ubuntu Desktop 20.04 LTS	Auditbeat Filebeat Metricbeat Packetbeat Heartbeat Netdata Prometheus Elastalert

Windows 10 - Host	Ryzen 5 2600 16 GB RAM HDD 1 TB	Windows 10 Home	Winlogbeat Sysmon
MISP	1 vCPU 3 GB RAM HDD 25 GB	Ubuntu Server 18.04 LTS	MISP – Threat Intel
Kali Linux - Atacante	2 vCPU 2 GB RAM HDD 80 GB	Kali Linux 2021.2	Hydra

O servidor ELK tem grande parte dos recursos, pois é onde será feito todo o processamento dos *logs*, envio de alertas e monitorização da rede.

O Webserver foi criado para ser feita a sua monitorização, enviar alertas e ser alvo de ataques. Nesta máquina foi instalado o Apache, o Elastalert e todos os *Beats* para enviar toda informação para o servidor ELK.

A máquina MISP foi obtida a partir do repositório³ onde é possível obter imagens atualizadas para o VMware e VirtualBox. Optou-se por utilizar esta opção pois é ideal para a realização de testes, e num caso de produção, seria melhor a sua implementação de raiz.

Por fim foi adicionado a máquina Kali Linux. Esta distribuição Linux é voltada para tarefas que envolvam segurança informática, como testes de penetração, o que foi muito útil para a realização dos vários testes ao cenário.

De seguida é explicado como foi feita a instalação do protótipo.

³ <https://vm.misp-project.org/>

4.1.2. Instalação do *Elastic Stack*

A instalação do *Elastic Stack* envolve a instalação do *Elasticsearch*, *Kibana* e do *Logstash*. Adicionalmente, para o funcionamento de certas funcionalidades, foi preciso realizar configurações dentro dos componentes do *Elastic Stack*, como a configuração de TLS e HTTPS. Estas configurações foram descritas no Anexo A – Instalação do *Elastic Stack*.

4.1.3. Instalação e configurações dos *Beats*

A instalação dos *Beats* e respetiva configuração também está incluído no Anexo A – Instalação do *Elastic Stack*.

Para este cenário de teste, temos o seguinte exemplo do funcionamento, representado pela Figura 24. É instalado o Metricbeat no servidor web, que por sua vez vai recolher, monitorar informações do sistema, onde de seguida, vai alimentar o *Elasticsearch* para obtermos por exemplo os *dashboards* no *Kibana*.

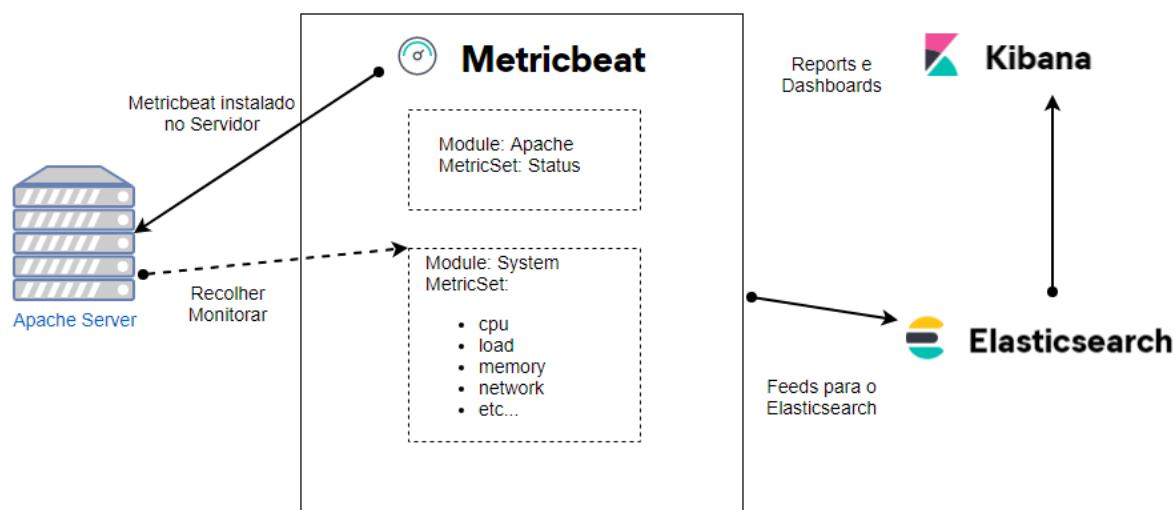


Figura 26 - Esquema da recolha de métricas do servidor Apache

O esquema acima representa o funcionamento do cenário de testes, no entanto, num cenário de produção o esquema seria diferente, de forma que o cenário esteja preparado para falhas. Isto pode ser representado de uma forma simples, como na Figura 25, onde é representado um cenário de funcionamento do *Elasticsearch* a enviar informações para o Metricbeat para serem feitas monitorizações.

No caso de falha do *cluster* de monitorização, podemos ainda ter os serviços de produção a serem monitorados a partir do *cluster* de produção, e no caso do *cluster* de produção falhar, podemos fazer um *troubleshoot* do porque ter falhado, utilizando o *cluster* de monitorização.

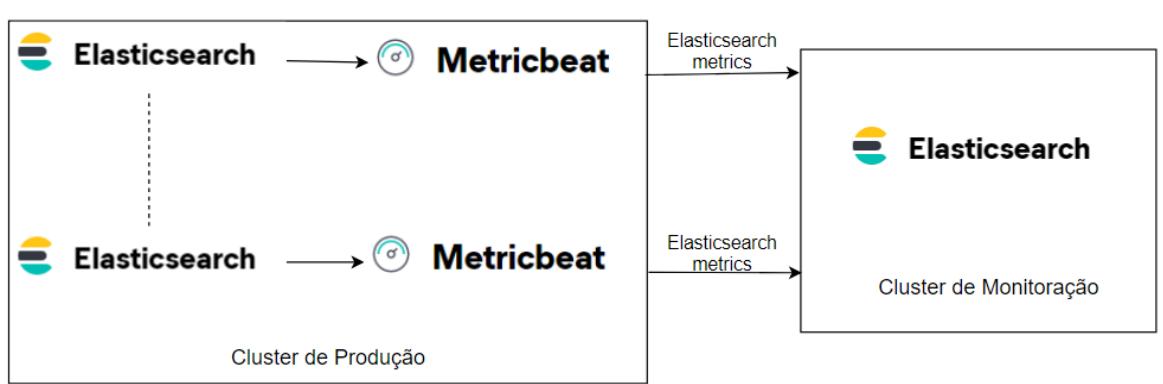


Figura 27 - Esquema Lógico da recolha de métricas com redundância

4.1.4. Instalação e configuração do Elastalert

Numa primeira parte, ao procurar uma solução *open source* para o envio de alertas, chegou-se a conclusão de que a melhor solução para isso foi o Elastalert. A sua instalação está documentada no Anexo E – Instalação do Elastalert, que foi feita no servidor web, com objetivo de enviar alertas para o Slack, ao comunicar com o servidor ELK.

O funcionamento do Elastalert é explicado pela Figura 26. O servidor web envia as métricas obtidas pelos Beats para o *Elasticsearch* no servidor ELK, que por sua vez, envia essas métricas para o serviço Elastalert, que assim que encontrar alguma correspondência, vai enviar o respetivo alerta para a plataforma configurada, neste caso o Slack.

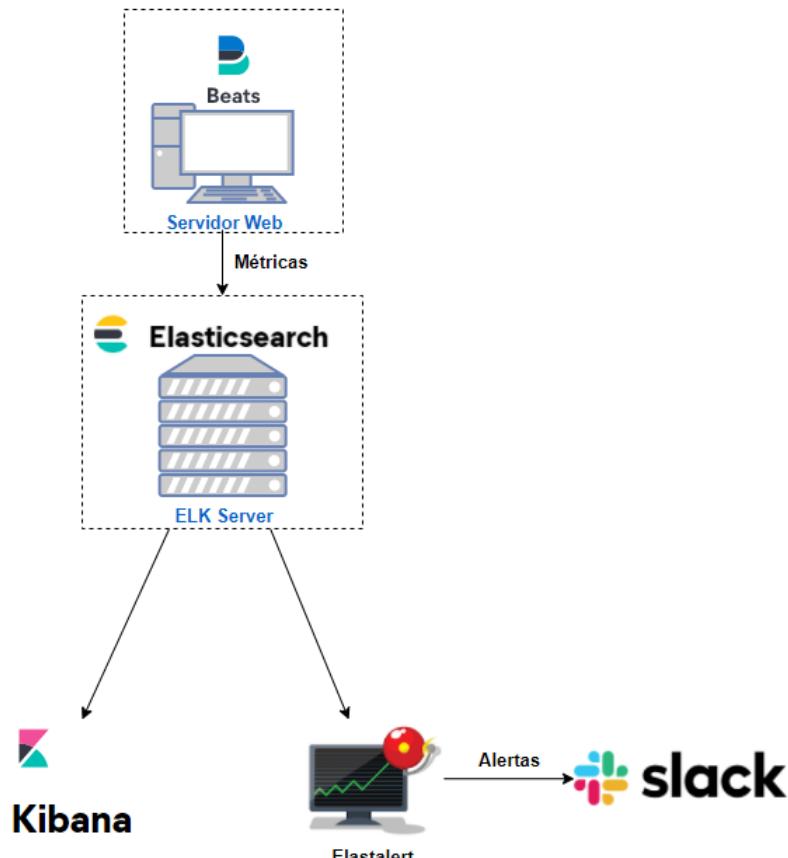


Figura 28 - Esquema do funcionamento de um alerta do Elastalert

4.2. Integração do TIP no SIEM

Como foi falado nos capítulos anteriores, a informação dos TIP's é recebida através de *feeds*, sendo que há sempre uma Instância Intermedia que trata de cuidar da informação para enviar ao SIEM como está representado na figura seguinte.

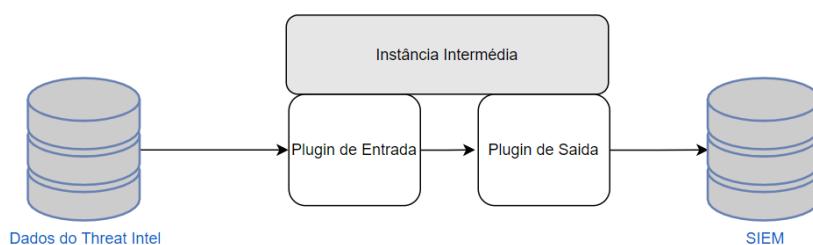


Figura 29 - Esquema Genérico do *flow* dos Feeds do TIP

Na nossa solução a informação é recebida através do plugin ThreatIntel do Filebeat onde é automaticamente adicionada à pasta especificada para colheita de *logs*, cuidado assim da informação e enviada para o Elasticsearch onde mais tarde será visualizado nas *dashboards* do Kibana.

4.2.1. TIP MISP

O Threat Intelligence plugin do MISP é uma plataforma de partilha de ameaças que recolhe, partilha e correlaciona os indicadores fornecidos que podem comprometer o sistema tais como ataques direcionados, *Threat Intelligence*, informações de fraude financeira, informações de vulnerabilidade ou mesmo informações de contraterrorismo (vanimpe, 2021).

O seu objetivo do MISP é produzir uma plataforma fiável que armazena localmente as informações relativas às ameaças aperfeiçoando a deteção de *malware* para ajudar na troca de informação entre organizações.

Como funciona

Eventos, utilizadores, *feeds* e grupos estão dentro da estrutura do MISP.

O seu funcionamento passa por um acontecimento ser uma entrada de ameaça que inclui os detalhes sobre a mesma e IOC's. Ao ser criado um evento o utilizador pode atribuir a um *feed* específico que age como uma lista de eventos de uma determinada organização e inclui eventos específicos.

Consistindo em utilizadores independentes e de confiança e informação gerada das ameaças a organizações sempre gerada pela base de utilizadores do MISP.

Integração do MISP na Solução

No cenário de testes, a máquina MISP foi configurada de forma a enviar os seus *feeds* para o módulo Filebeat do servidor ELK, que por sua vez, nos permite visualizar os *feeds* no *Kibana* e criar alertas com essas informações (elastic e. , 2021).

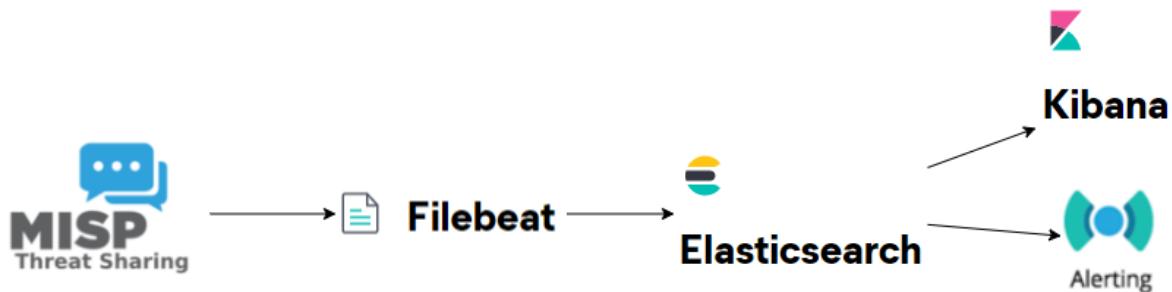


Figura 30 - Esquema do flow dos *feeds* do Misp

Para que essa comunicação fosse possível, primeiro é preciso obter a chave API do utilizador do MISP. Para ter acesso à chave, no menu do MISP acedemos a Administration – List Users – Admin – My Profile – Auth keys.

A captura de tela mostra a interface do usuário do MISP. No topo, há uma barra com links para Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs e API. No topo direito, há uma barra com o nome do usuário (Admin), o nome do sistema (MISP) e links para Logout.

O menu lateral esquerdo está aberto para "My Profile". As opções visíveis são: My Settings, Set Setting, Dashboard, List Organisations, Role Permissions, List Sharing Groups, Add Sharing Group, User Guide, Terms & Conditions e Statistics.

O formulário "User admin@admin.test" mostra os seguintes detalhes:

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
Event alert enabled	No
Contact alert enabled	No
Invited By	N/A
NIDS Start SID	4000000
PGP key	N/A
Created	N/A

Há um botão "Download user profile for data portability".

A seção "Auth keys" contém uma lista com uma única chave:

#	User	Auth Key	Expiration	Last used	Comment	Allowed IPs	Actions
1	admin@admin.test	kGQ*****7EB8	Indefinite	2021-07-16 16:49:26			

Um campo de busca "Enter value to search" e um botão "Filter" estão disponíveis para filtrar as chaves.

Figura 31 - Localização da Auth Key no MISP

Esta chave é então adicionada ao ficheiro de configuração do módulo threatintel do Filebeat, o que vai permitir o envio dos *feeds* para o Elasticsearch e Kibana.

As organizações podem se inscrever em *feeds* vinculados a riscos em seus respetivos setores, entrando em grupos MISP.

Os *feeds* do MISP são recebidos através de um modulo no Filebeat THREATINTEL onde é colocado a key do mesmo e a informação poderá ser visualizada no *Kibana* através do Filebeat como *logs* ou JSON e através das várias Tags é possível criar alertas como por exemplo IP's malignos enviados pelos *feeds* sem esse IP alguma vez ter feito qualquer contato com o servidor.

Segue-se um esquema de como o *flow* dos Feeds Funciona.

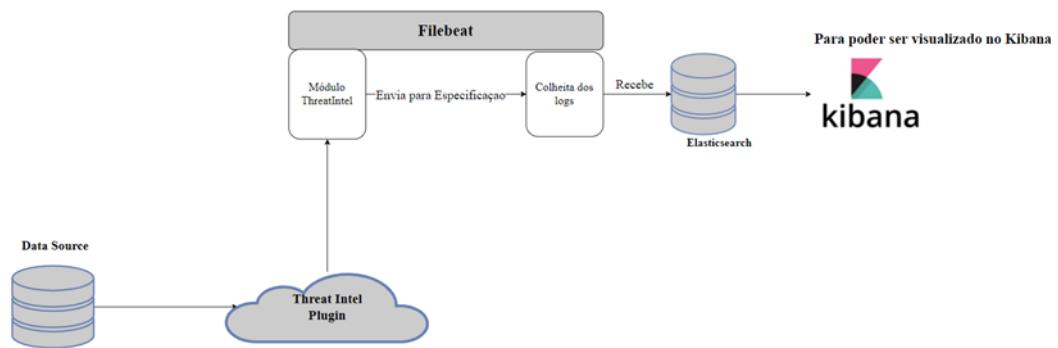


Figura 32 -- Flow dos feeds do TIP na solução

4.2.2. TIP OTX

O Open Threat Exchange (OTX) da AlienVault garante bastante informação sobre as ameaças mais recentes relatadas pela comunidade.

Dando uso à plataforma Unified Security Management (USM) causa a inteligência contra ameaças bastante fácil de subscrever aos pulsos. Pulsos são o envio dos *feeds* ao qual foram subscritos, estes pulsos integram sempre cinco recursos essenciais de segurança - descoberta de ativos, avaliação de vulnerabilidades, deteção de intrusão, monitorização comportamental e SIEM.

Figura 33 - Subscrição de feeds no OTX

Apos fazer subscrição do *feed* desejado a *AlienVault USM Threat Intelligence* regula os cinco controlos essenciais de segurança para manter os recursos de deteção de ameaças do USM atualizados com as informações mais recentes e detalhes sobre o que é a ameaça, origem e os ativos do seu ambiente que estão em risco e como responder.

Beneficiando destas informações do OTX e melhorando-as com os dados da AlienVault, a equipa AlienVault Labs atualiza continuamente oito regras coordenadas pela plataforma USM, tais como:

- Diretivas de correlação - o USM é fornecido com mais de 3.000 regras predefinidas que traduzem padrões de comportamento em informações de ameaças específicas e acionáveis, vinculando eventos distintos em sua rede
- Assinaturas de IDS de rede - deteta o tráfego malicioso mais recente em sua rede
- Assinaturas de IDS de *host* - identifique as ameaças mais recentes que visam seus sistemas críticos
- Asset Discovery Signatures - deteta os mais recentes sistemas operacionais, aplicativos e informações do dispositivo
- Assinaturas de avaliação de vulnerabilidade - descubra as vulnerabilidades mais recentes em seus sistemas
- Módulos de relatório - receba novas visualizações de dados críticos sobre o seu ambiente para gerenciar e atender às solicitações do auditor
- Modelos dinâmicos de resposta a incidentes - orientação personalizada sobre como responder a cada alerta
- Plug-ins de fonte de dados com suporte recente - expanda sua pegada de monitorização integrando dados de dispositivos e aplicativos de segurança legados

Estes conjuntos de regras, juntamente com os controlos integrados de segurança do USM, garantem a deteção de ameaças bastante eficaz, poupando tempo pessoal a fazer pesquisas próprias sobre as ameaças e ajudar sistemas para a deteção das mesmas.

Integração do OTX na Solução

A integração TIP do OTX é feita através do site da AlienVault onde os *feeds* são recebidos no plugin do Filebeat diretamente através de um servidor.

Após criar conta no site da AlienVault basta ir ao listar os “pulsos” que são os *feeds* específicos que nos subscrevemos.

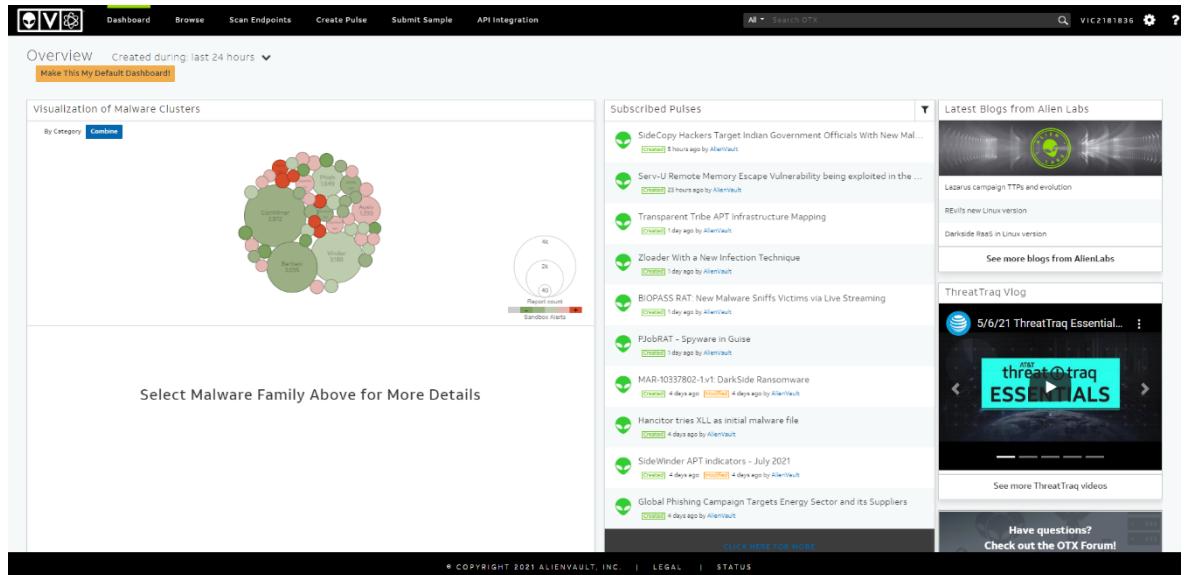


Figura 34 - Dashboard do OTX

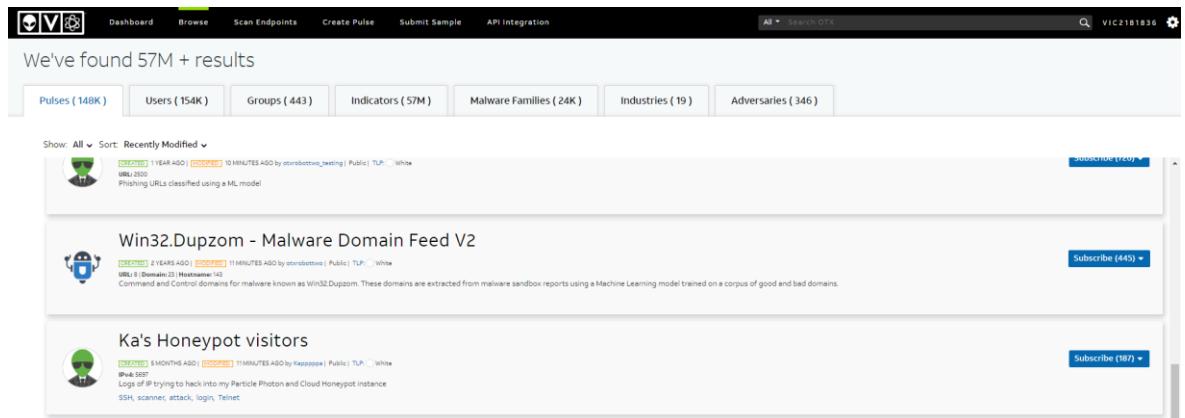


Figura 35 - Vários feeds para subscrever no OTX

Seguindo a subscrição dos pulsos, basta pegar na API KEY fornecida no menu de utilizador e adicionar no ficheiro de configuração do Filebeat.

The screenshot shows the 'Settings' section of the OTX Key configuration. It includes an 'Email Notifications' section with various checkboxes for receiving alerts about new pulses, follows, comments, subscribers, and other activity. Below this is the 'OTX Key' section, which displays a long API key value: '94bd1cd07a053d761167b90885e15424bd50218402479d1508c58d0f9fb'. A red box highlights this key. To the right of the key is a 'Regenerate OTX API Key' button. At the bottom is the 'Account Settings' section, showing email addresses associated with the account and a field to enter a new email address.

Figura 36 - OTX key para receber os feeds

De seguida na *dashboard* do Filebeat foi feita uma pesquisa com a tag “otx” para ver se estava a receber os *feeds* que foram subscritos e feito uma comparação (foi feito a comparação através de um IP maligno fornecido pelo pulso específico).

The screenshot shows the search results for the tag 'otx'. The top section displays basic information about the search: 'Visibilities (192) +', 'Add To Group', 'Download', 'Embed', 'Close', 'Suggest Edit', and 'Report Issue'. Below this is a summary bar with social media sharing options. The main content area shows a chart titled 'Ka's Honeypot visitors' with data from 'Filebeat (400)' and 'MULTIPE ADD by Kassiopeia | Public | TLP: White'. The chart indicates that the IP trying to hack into the Particle Photon and Cloud Honeypot instance is from Vietnam (256). Other countries listed include Brazil (256), Russia (257), China (1624), United States (504), and Other (2487). Below the chart is a section titled 'INDICATORS OF COMPROMISE (5390)' with tabs for 'Related Pulses (7069)', 'Comments (0)', and 'History (0)'. A sub-section titled 'TYPES OF INDICATORS' shows a single entry for 'IPv4 (536)'. The detailed view for this entry shows the following information:

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
IPv4	43.245.216.102	bruteforce	Telnet Login attempt	Apr 19, 2021, 11:33:11 PM	0	6

Details for this entry include: Title: Telnet Login attempt, Description: , Role: bruteforce, Expiration: 5/18/21, and Related Pulses: 6. There is also a 'More Details' button.

Figura 37 - Informação que irá ser enviada pelos feeds do OTX

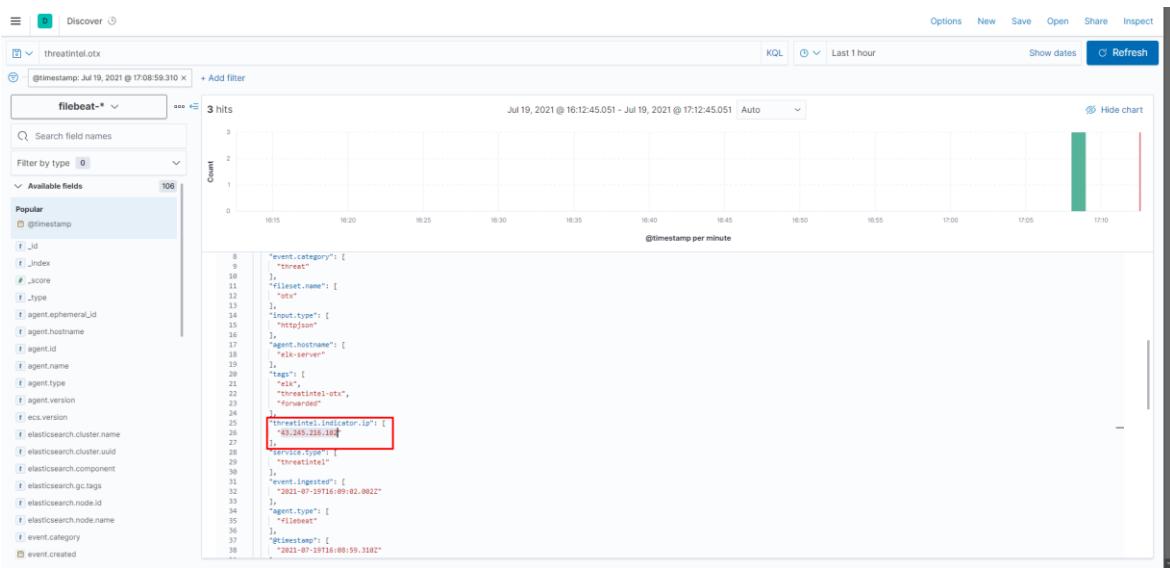


Figura 38 - Log recebido no Filebeat com IP recebido pelos feeds do OTX

4.3. Testes

O objetivo deste tópico, é validar o funcionamento do protótipo recorrendo a diferentes tipos de testes que irão ser mencionados, e com isto poder afirmar ou não se o funcionamento foi como desejado.

Tendo realizado a instalação dos componentes que formam o cenário de testes, neste ponto iremos apresentar alguns testes que foram realizados e demonstrar a sua utilidade. Estes incluem, ataques de *brute-force* para tentar obter a palavra-passe do servidor, sobre carregamento na rede através de ataques *SYN Flood*, transferência de ficheiros maliciosos e a monitorização do desempenho das máquinas.

4.3.1. Ataques simulados

Como dito anteriormente, como forma de provar o funcionamento das ferramentas, foram realizados alguns ataques com ajuda de ferramentas existentes do Kali Linux.

Hydra

Com esta ferramenta, foi possível realizar um ataque de força bruta de SSH ao servidor Web. O objetivo deste ataque, é conseguir ter acesso remoto ao servidor Web pelo serviço SSH, ao utilizar uma longa lista de passwords, até que eventualmente uma seja a correspondente (Congleton, 2018).

A Figura 39 representa graficamente o decorrer deste ataque. É feito pelo atacante (Kali Linux) que tenta obter acesso remoto ao Servidor Web numa rede interna.

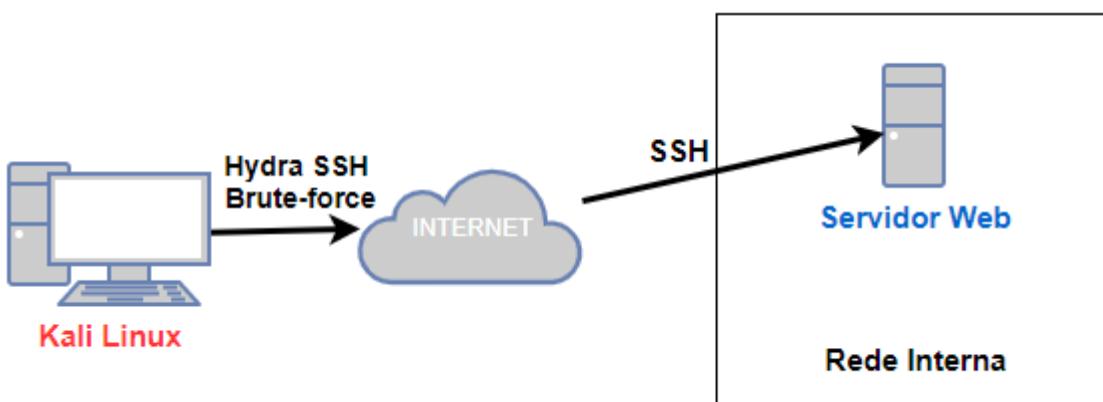


Figura 39 - Esquema de ataque *Brute-force*

Ao realizar este ataque, é especificado o ficheiro de texto com uma lista de passwords aleatórias, e o IP da máquina, como se pode ver na Figura 40.

```

-(kali㉿kali)-[~]
└─$ hydra -i root -P unix_pass.txt -t 6 192.168.102.146 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-22 14:41:13
[DATA] max 6 tasks per 1 server, overall 6 tasks, 1009 login tries (l:1/p:1009), -169 tries per task
[DATA] attacking ssh://192.168.102.146:22/
  
```

Figura 40 - Comando hydra para ataque *brute-force*

Ao realizar o ataque, podemos ver na Figura 41 que houve um grande pico de tentativas falhadas de autenticação

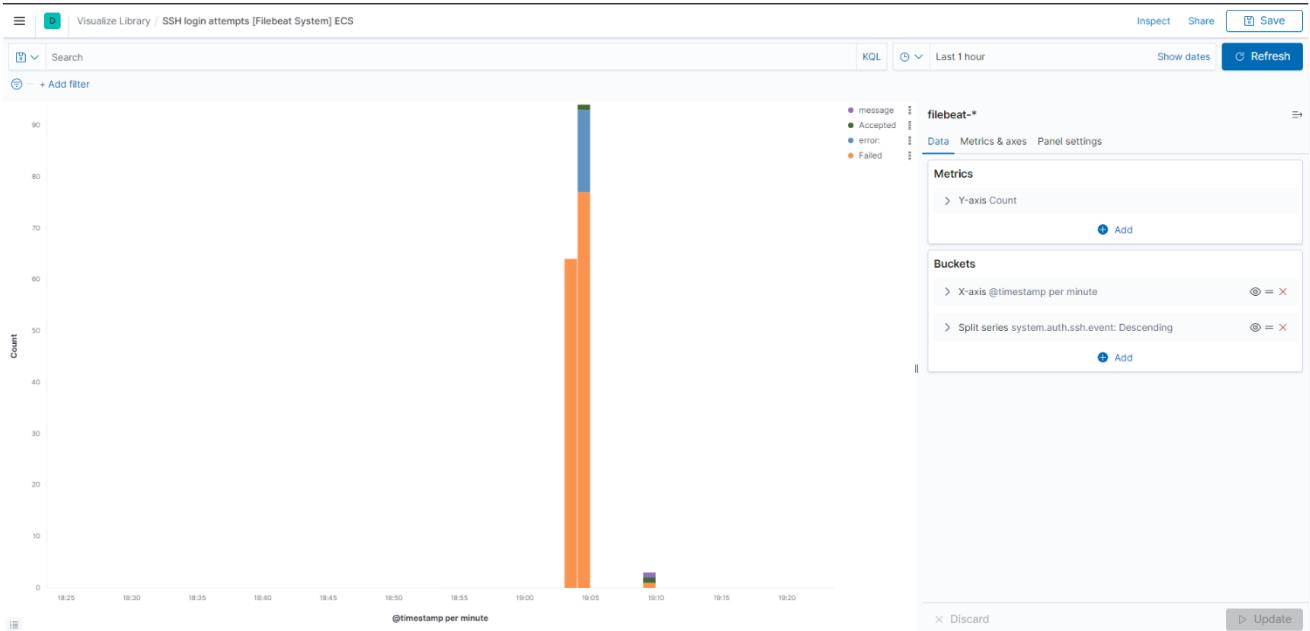


Figura 41 - várias tentativas de autenticação no menu SSH Login Attempts

Ataque DDoS – Slowloris

Neste ataque, o objetivo é tornar os recursos do servidor Web indisponíveis. Não se trata de uma invasão do sistema, mas uma sobrecarga nos recursos.

Para este teste, foi utilizado o programa Slowloris (Cloudflare, 2021), que vai abrir e manter várias conexões HTTP entre o invasor e o alvo, como se pode ver na Figura 42.

De forma resumida, esta ferramenta permite que uma única máquina consiga interromper os serviços de um servidor sem usar muita largura de banda, onde são feitas ligações parciais de HTTP, que faz com que o servidor fique sobrecarregado.

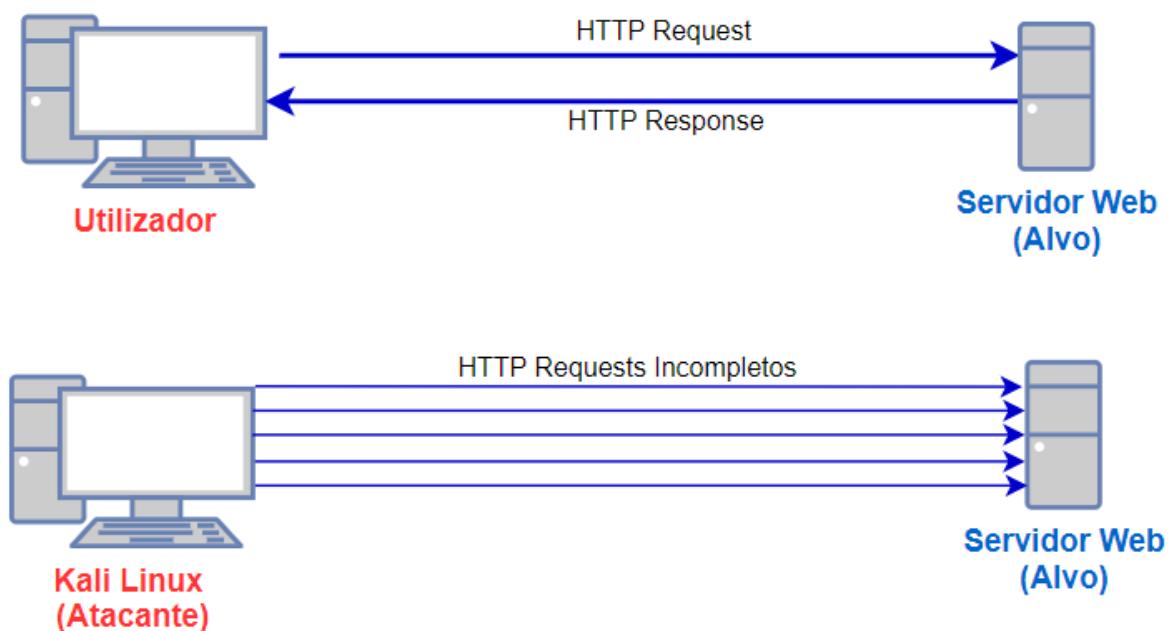


Figura 42 – Esquema ataque DDoS

Para realizar este ataque, é descarregada a ferramenta Slowloris, de seguida é executado o comando indicado na Figura 43, especificando o IP da máquina a ser atacada.

A captura de tela mostra o terminal Kali Linux com duas janelas abertas. A janela esquerda exibe o resultado da execução do comando `python3 slowloris.py 192.168.102.146 -s 500`. O log mostra a criação de 500 sockets e a envio de cabeçalhos de manutenção. A janela direita exibe o resultado do comando `ifconfig`, mostrando as interfaces docker0 e eth0 com suas respectivas estatísticas de rede.

```
(kali㉿kali)-[~/Desktop/Slowloris/slowloris]
$ python3 slowloris.py 192.168.102.146 -s 500
[11-08-2021 10:50:14] Attacking 192.168.102.146 with 500 sockets.
[11-08-2021 10:50:14] Creating sockets ...
[11-08-2021 10:50:15] Sending keep-alive headers ... Socket count: 500

(kali㉿kali)-[~/Desktop]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:34:6c:ef:7e txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.102.141 netmask 255.255.255.0 broadcast 192.168.102.255
inet6 fe80::20c:29ff:feaa:9e42 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:ea:9e:42 txqueuelen 1000 (Ethernet)
RX packets 82 bytes 40565 (39.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 92 bytes 24799 (24.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 43 - Comando ataque DDoS

Após ser executado o comando, conseguimos verificar que o serviço Apache deixa de responder e no *dashboard* de acessos do Apache, podemos verificar esse aumento de pedidos, exemplificado na Figura 44.

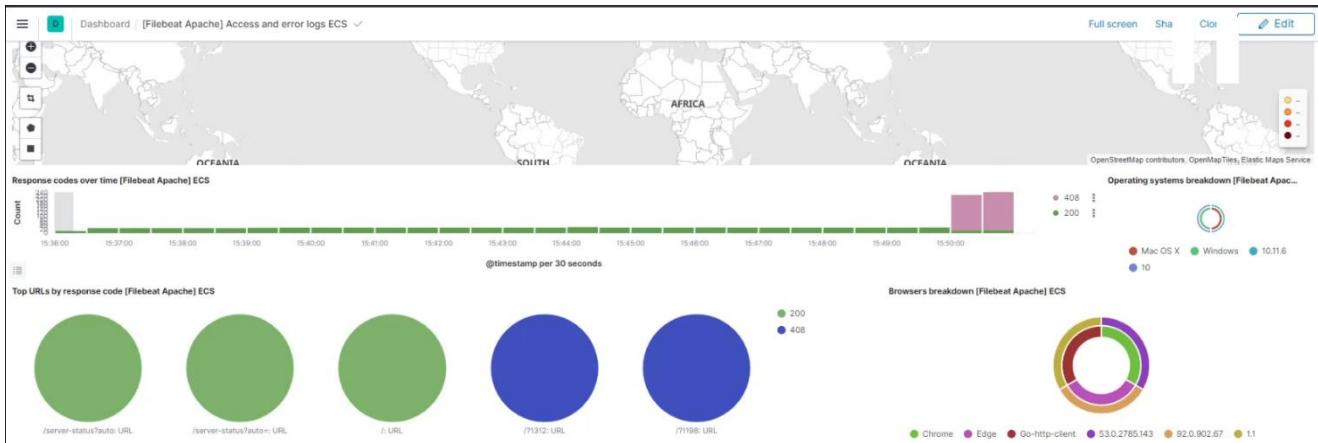


Figura 44 - Dashboard Access and error logs

Ataque *SYN Flood*

Assim como o ataque DDoS, um ataque *SYN Flood* é um ataque de negação de serviço, com o objetivo de sobrecarregar o sistema. Como diz no nome do ataque, um *SYN Flood* consiste no atacante enviar constantemente pacotes SYN para os portos do servidor, que por sua vez vai responder com pacotes SYN-ACK (Administrator, 2021).

Como podemos ver na Figura 45, o atacante envia vários pacotes SYN, mas não envia o pacote “ACK” de volta ao servidor, tornando assim a conexão aberta a consumir recursos ao servidor. Quando um utilizador legitimo, tentar aceder aos recursos, o servidor recusa-se a abrir a conexão, causando assim uma negação de serviço.

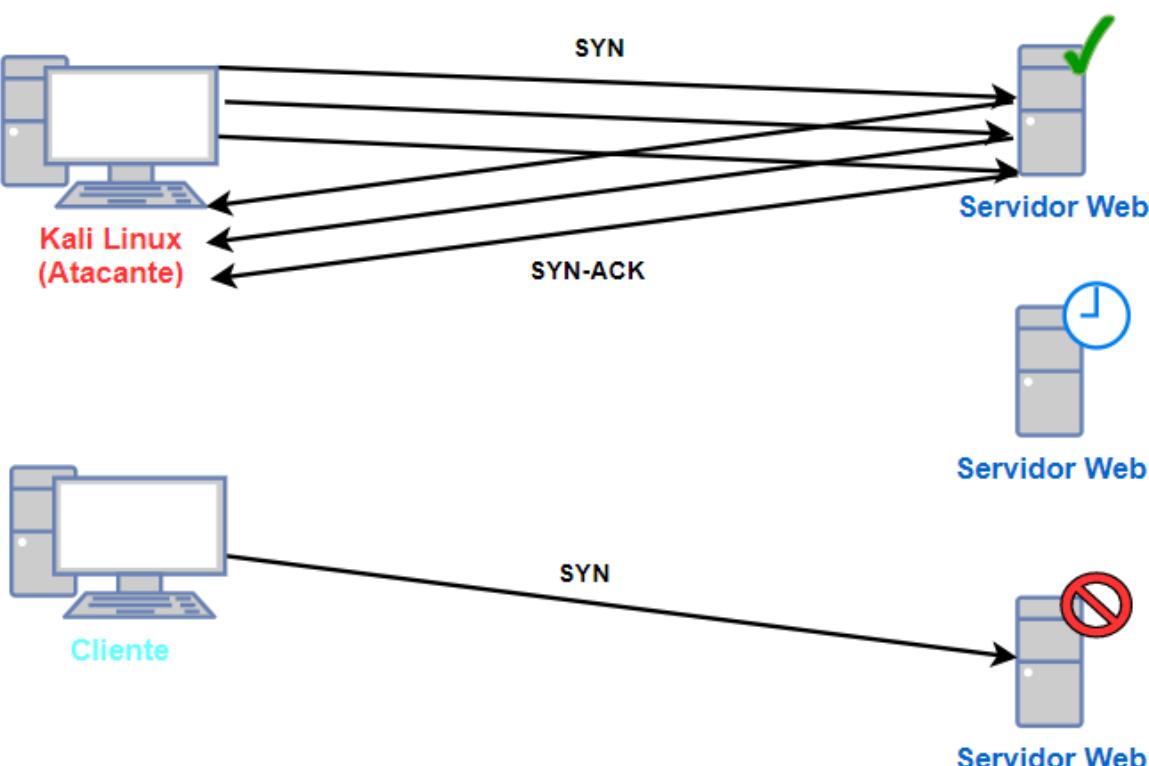


Figura 45 - Esquema de ataque SynFlood

O ataque foi realizado utilizando o comando hping3, como se pode ver na Figura 46. Vão ser enviados 15000 pacotes, cada um com 120 bytes, especificados pelo -c 15000 e -d 120.

```
(kali㉿kali)-[~]
$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.102.146
HPING 192.168.102.146 (eth0 192.168.102.146): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Figura 46 - Comando ataque Synflood

Ao ser realizado o ataque, podemos verificar no *dashboard* do *Kibana*, o tráfego obtido pelo Packetbeat, sendo possível identificar o momento em que o ataque começou e terminou, Figura 48 e Figura 49.

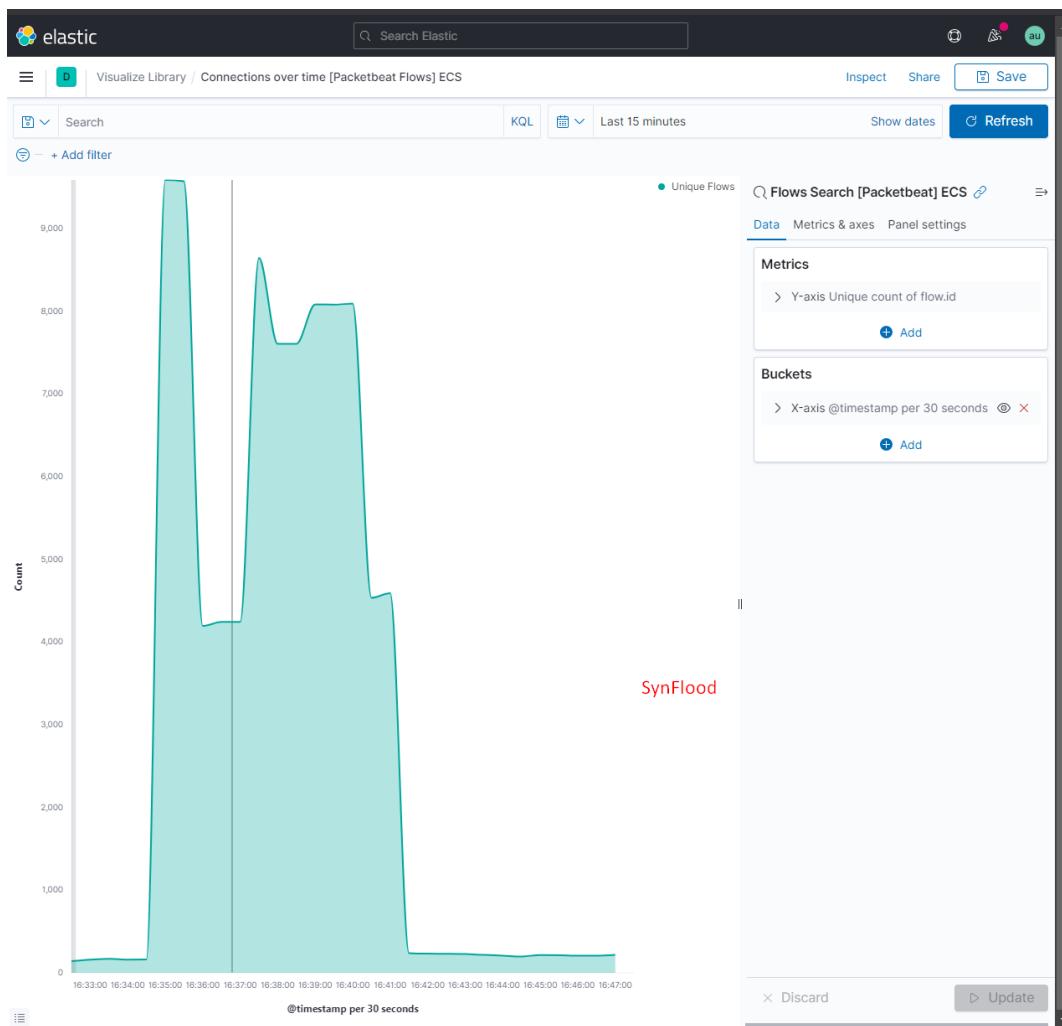


Figura 48 - Pico de Pacotes recebidos pelo ataque SY flood

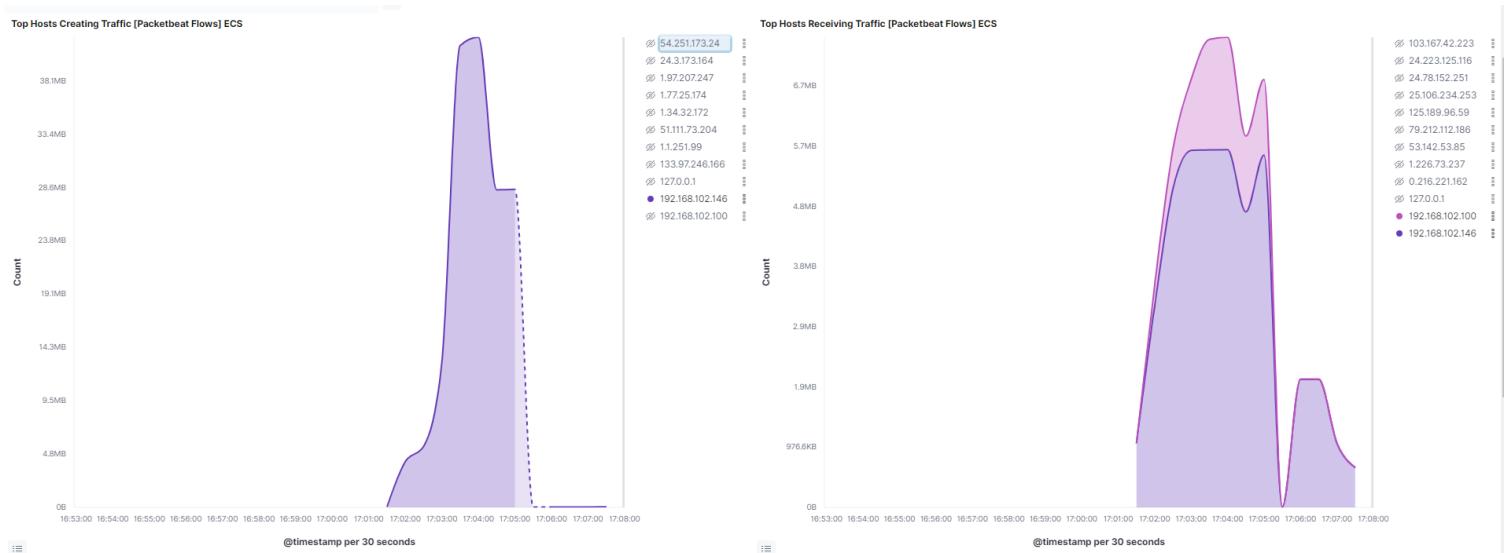


Figura 47 - Picos de pacotes recebidos (Por IP)

PsExec

Com este ataque, vamos executar um programa remotamente no sistema Windows *host*, e com isso verificar se o ELK consegue detetar essa atividade maliciosa e enviar o devido alerta (Russinovich, 2021).

Ao executar este ataque, assumimos já que o atacante tem acesso às credenciais do alvo. Neste caso o ataque foi direcionado para o sistema Windows correspondente ao *host*, e através da Figura 49 pode-se ver o nome do ficheiro ao ser executado no windows.

```
(kali㉿kali)-[~]
└─$ sudo /usr/bin/python3 /usr/share/doc/python3-impacket/examples/psexec.py victorba@192.168.1.79 ipconfig
[sudo] password for kali:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.1.79.....
[*] Found writable share ADMIN$.
[*] Uploading file SNaNLRPg.exe
[*] Opening SVCManager on 192.168.1.79.....
[*] Creating service yVzY on 192.168.1.79.....
[*] Starting service yVzY.....
[!] Press help for extra shell commands
```

Figura 49 – Comando para execução do PsExec

Tendo realizado o ataque, podemos verificar a sua deteção de diferentes formas. Através do discover do winlogbeat, Figura 50, conseguimos realizar uma pesquisa e verificar que o ficheiro foi detetado no sistema.

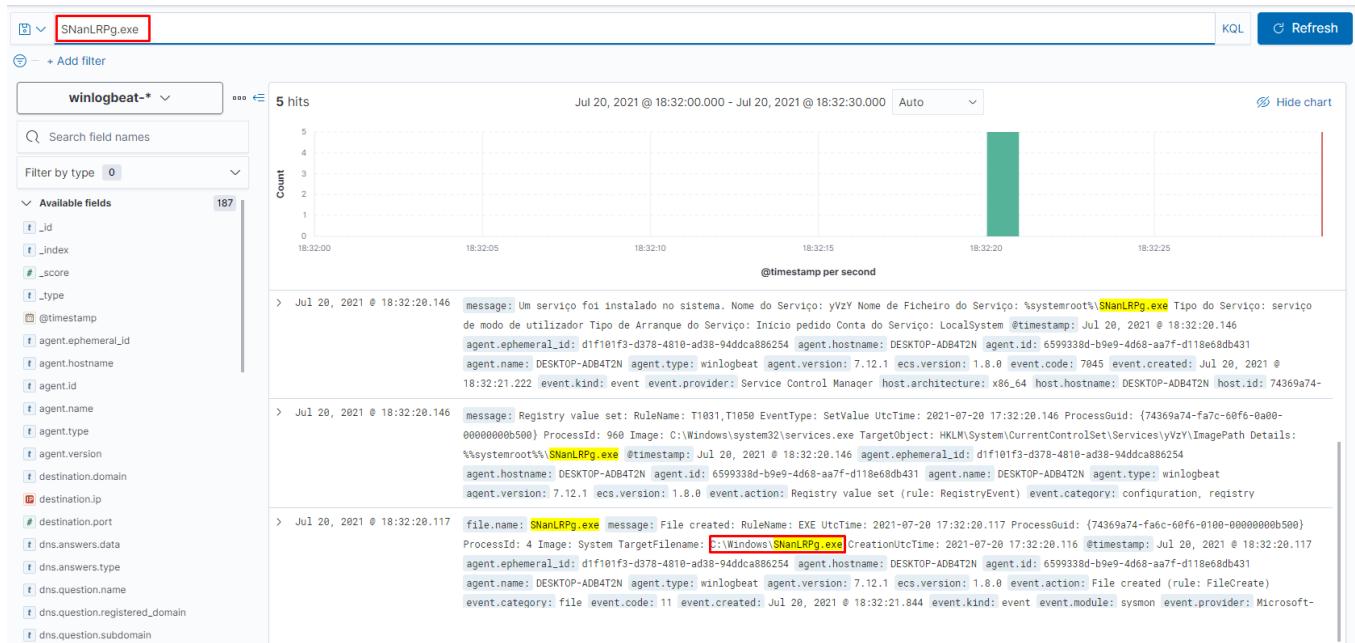


Figura 50 - Verificação do ataque Psexec pelo Winlogbeat

O próprio sistema antivírus do Windows é capaz de detetar a ameaça, assim como o módulo Security, indicado na Figura 51, anteriormente chamado de módulo SIEM, onde é possível ligar várias regras pré-definidas, sendo que a execução de ficheiros remotos é uma delas.

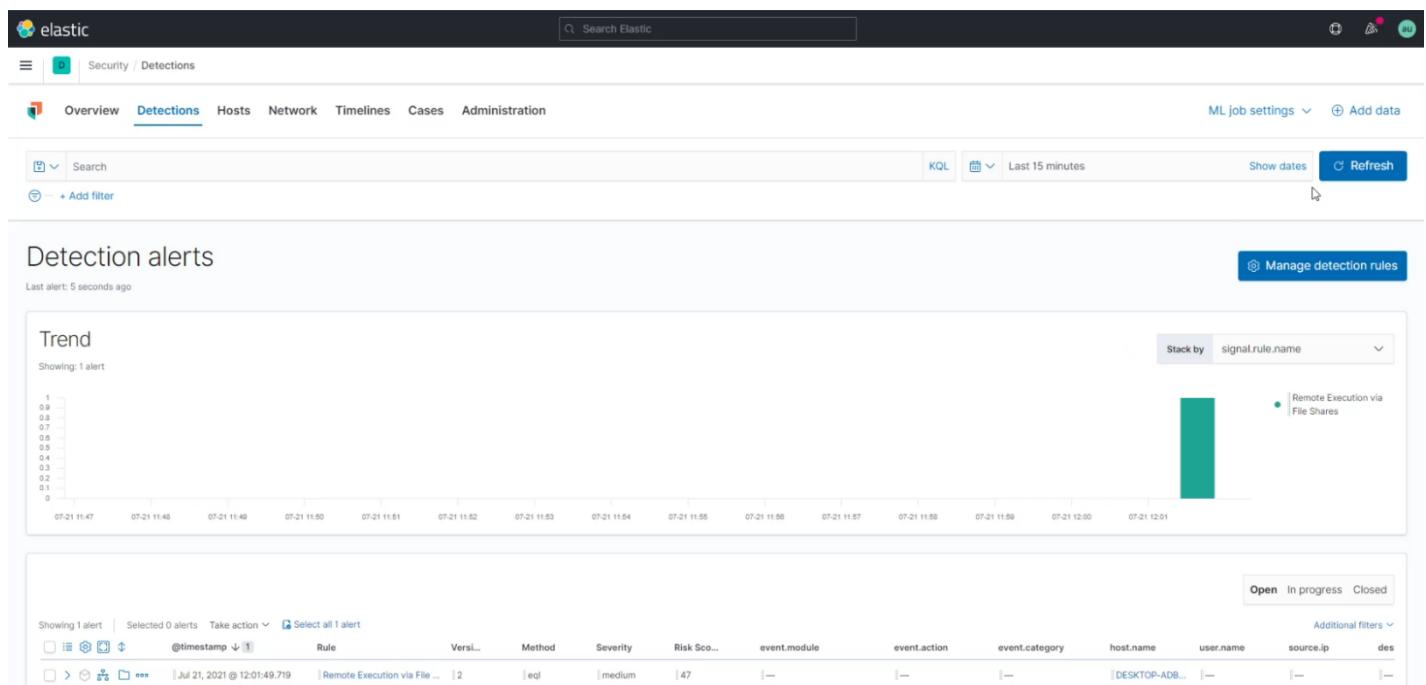


Figura 51 - Verificação do ataque PsExec através do menu Detections do Kibana

Também foi possível testar o alerta criado com o *Kibana*, baseando da pesquisa feita no discover mencionado anteriormente. Na Figura 52 podemos ver a confirmação do envio do alerta para a plataforma Slack.

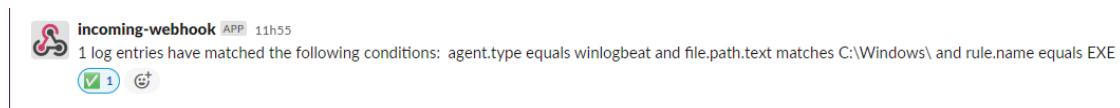


Figura 52 - Alerta no Slack do Ataque PsExec

A criação deste alerta é explicada no Anexo F – Alertas *Kibana*.

4.3.2. Monitorização e recolha de métricas

Metricbeat

Como foi referido (ref *Beats 5.1.4*), o Metricbeat permite recolher métricas dos sistemas, e através dos seus módulos podemos especificar aquilo que queremos monitorar. Para este teste ligou-se o módulo do system e do apache.

Como simples teste ao seu funcionamento, o Metricbeat foi instalado e configurado no servidor web, para enviar as métricas ao servidor Elastic. Dentro da secção das Metrics, é possível visualizar que o servidor envia informações básicas sobre a sua utilização de CPU, memória e network, indicado na Figura 53.

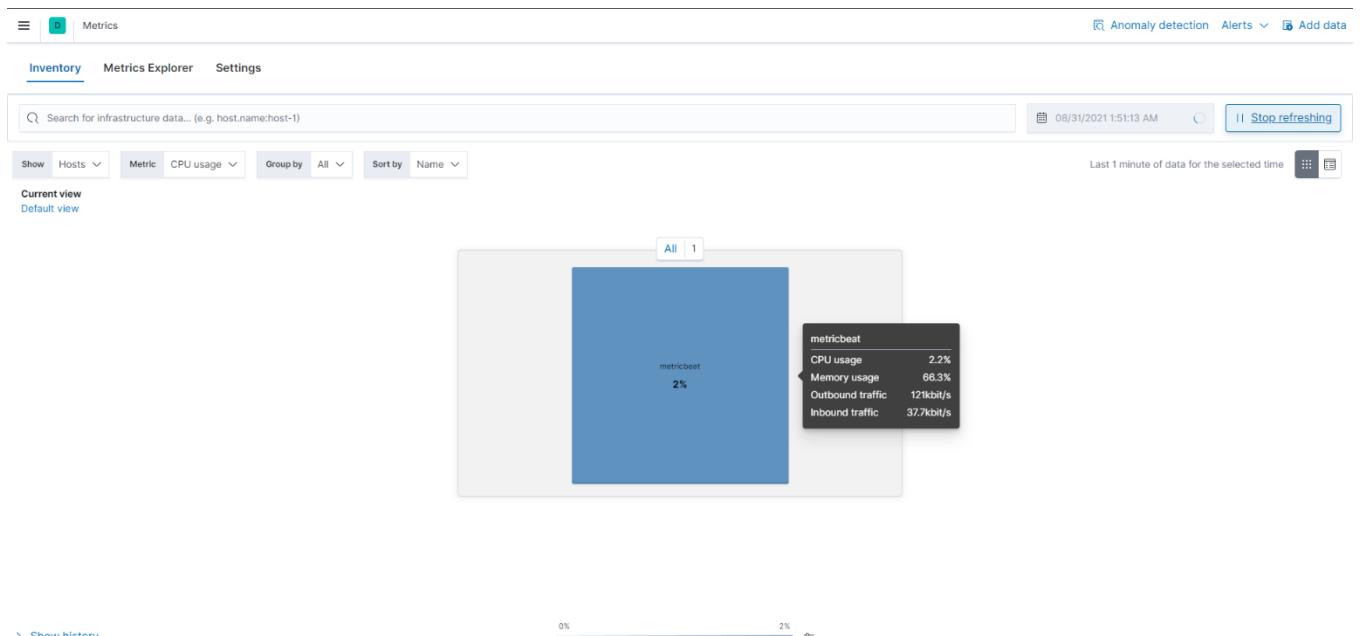


Figura 53 - Métricas mostradas no Metricbeat

Na opção "Metrics Explorer" é onde podemos especificar aquilo que queremos monitorar do sistema, indicado na Figura 54.



Figura 54 - Metricas mostradas no Metricbeat por tags

Devido á limitações deste tipo de monitorização, foi-nos proposto o uso de outras ferramentas de recolha de métricas dos sistemas, estas ferramentas sendo o Netdata, Grafana e Prometheus, conforme referido no Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus,. Sendo que o objetivo principal é utilizar estas três ferramentas em simultâneo e dar uso às mesmas para fins diferentes.

Netdata

O NetData é uma ferramenta *open source* que permite a visualização e monitorização de métricas tais como utilização de RAM, utilização do CPU, atividade do disco e muito mais em tempo real. Importante referir que esta ferramenta permite guardar os dados na Cloud Netdata sem custos.

A ferramenta de monitorização distribuído do Netdata recolhe milhares de métricas de sistemas, hardware e aplicações com nenhuma configuração. Ele é executado

permanentemente em todos os seus servidores físicos e virtuais, containers, implantações na cloud e IoT (Netdata, 2021).

A ferramenta de monitorização distribuído do Netdata recolhe milhares de métricas de sistemas, hardware e aplicações com nenhuma configuração. Ele é executado permanentemente em todos os seus servidores físicos e virtuais, containers, implantações na cloud e IoT (Netdata, 2021).

O netdata foi instalado no servidor web e no *Elastic Stack*, sua instalação é explicada no (ref anexo B). Após sua instalação pode-se aceder sem quaisquer configurações adicionais, o seu *dashboard*, com informações em tempo real da utilização dos recursos, visível na figura 55.

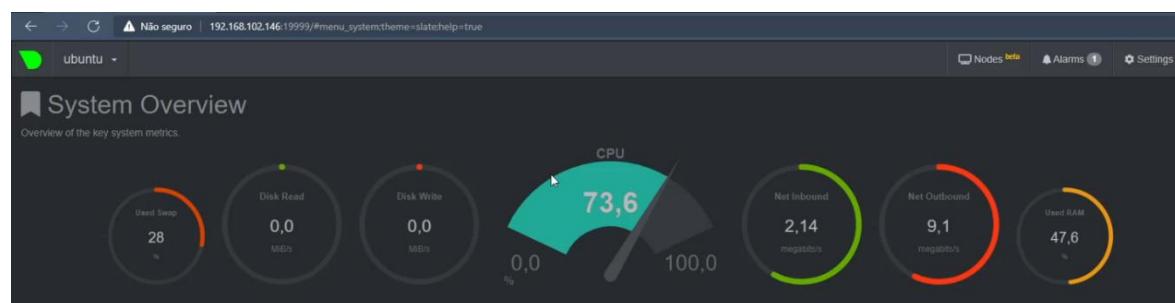


Figura 55 - Visão Global do Sistema no Netdata

Prometheus

Prometheus é uma plataforma de monitorização *open source* de recolha de dados, baseado em texto e independente de fornecedor (Elastic, Analise suas métricas do Prometheus em escala, 2021).

Na implementação deste trabalho, será o Netdata a enviar as métricas diretamente ao Prometheus e ainda será possível fazer a monitorização de várias máquinas ao mesmo tempo e aceder as métricas individuais de cada máquina ao mesmo tempo.

No seu ficheiro de configuração, é adicionado os targets, Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus.

De seguida pode-se escolher os parâmetros que queremos monitorar no Graph e visualizar o gráfico, como é exemplificado na Figura 56.

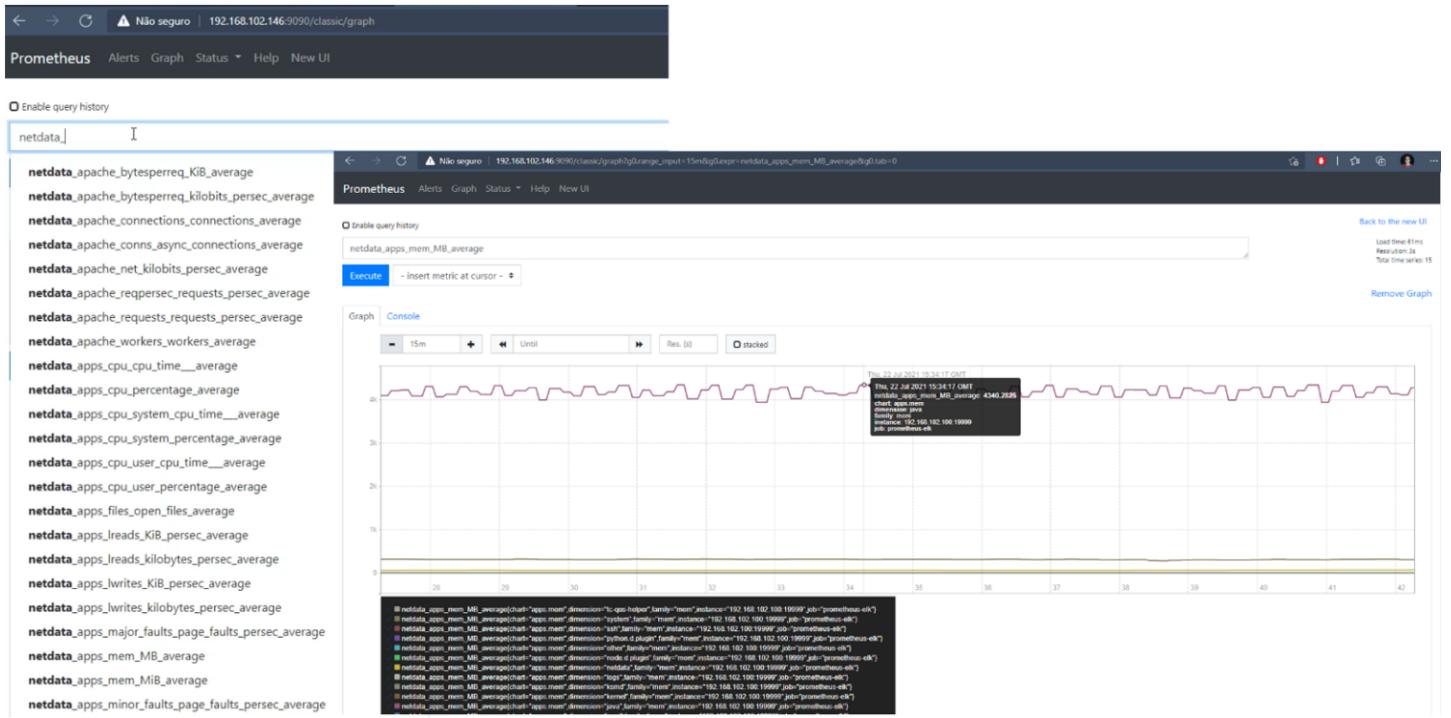


Figura 56 - Métricas no Prometheus pelas várias tags

Grafana

Grafana é uma solução *open source* para executar análises de dados, obtendo métricas que fazem sentido à enorme quantidade de dados recebidos e para monitorar as aplicações com ajuda das *dashboards* que são personalizáveis. O Grafana liga-se a todas as fontes de dados possíveis, nomeadamente bases de dados como Graphite, Prometheus, Influx DB, Elasticsearch, MySQL, PostgreSQL, etc (Shivang, s.d.).

Uma qualidade bastante interessante do Grafana é que ao ser *open source* permite aos utilizadores escrever plugins do zero para integrar as várias fontes de dados diferentes.

Uma vez que esta ferramenta ajuda a estudar analisar e monitorar dados ao longo de um período de tempo ajuda a investigar o comportamento do utilizador ou da aplicação, e também a frequência de erros que aparecem e os cenários contextuais, fornecendo dados relativos ao mesmo.

Monitorização e recolha de métricas

O Netdata permite guardar as métricas na cloud mas como o objetivo desta recolha de métricas é para pequenas empresas queríamos também garantir a confidencialidade das mesmas caso elas decidam a manter. Dito isto, foi escolhido a instalação do Prometheus e o Grafana para recolher os *logs* das próprias máquinas. Mesmo que o prometheus permita recolha de uma grande variedade de métricas e independente do sistema operativo ou aplicação foi optado por usar as métricas fornecidas pelo Netdata, usando as mesmas também no Grafana onde será permitido visualizá-las em *Dashboards*.

Dando uso as três ferramentas e apos a instalação dos mesmo no Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus e indo por passos:

Podemos aceder a qualquer máquina no *cluster* ao netdata e ver as suas métricas, mas apenas cada máquina tem acesso à sua informação, Figura 55.

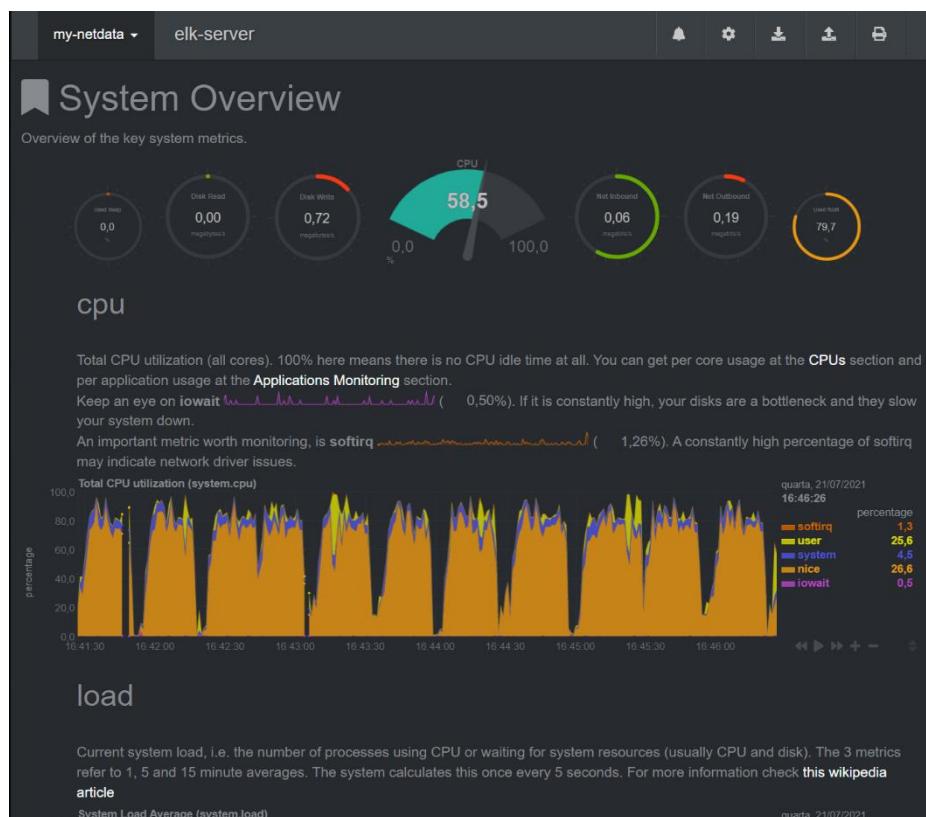


Figura 57 - Visão inicial do Netdata

Mais tarde através do ficheiro de configuração do Prometheus, /etc/prometheus/prometheus.yml, conforme é mostrado no Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus, temos acesso aos targets (cada máquina que tenha acesso ao netdata) onde o Prometheus recebe a informação de todos os Targets, Figura 56.

Targets					
All Unhealthy Collapse All					
prometheus (1/1 up) Show less					
Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://192.168.102.146:19999/api/v1/allmetrics?format=prometheus	UP	instance="192.168.102.146:19999" job="prometheus"	8.72s ago	118.5ms	

prometheus-elk (1/1 up) Show less					
Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://192.168.102.100:19999/api/v1/allmetrics?format=prometheus	UP	instance="192.168.102.100:19999" job="prometheus-elk"	9.174s ago	111.7ms	

Figura 58 - Targets no Prometheus

Aqui o Prometheus poderá aceder às várias métricas de cada PC e por exemplo ver percentagem de utilização do CPU em cada serviço de todos as máquinas do *cluster*, Figura 57.

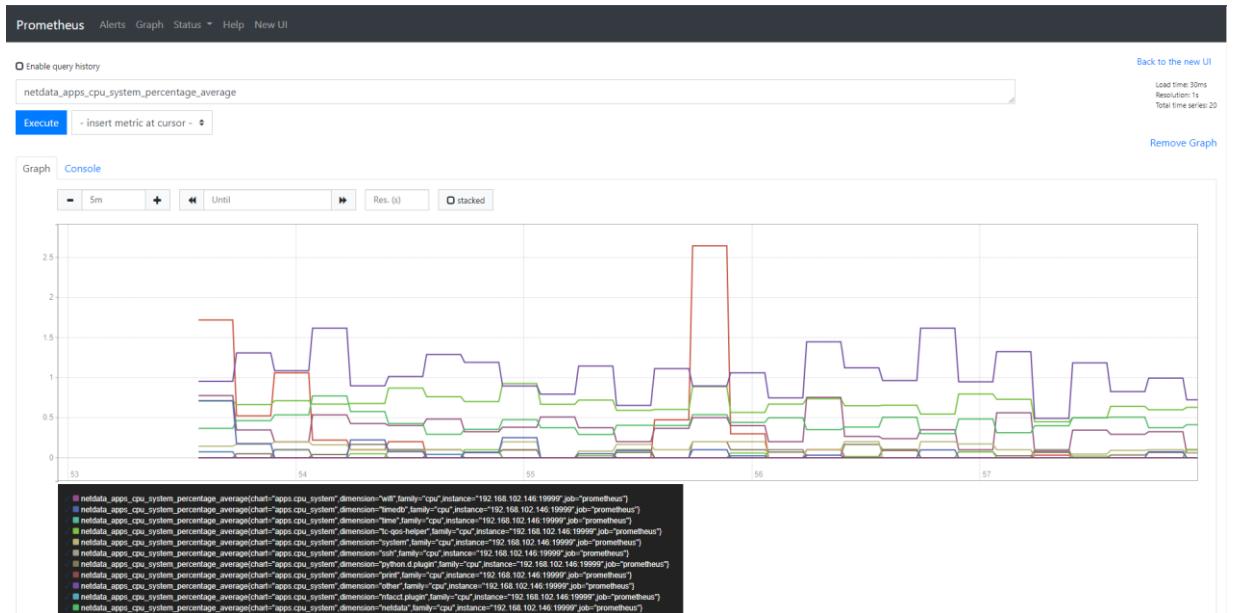


Figura 59 - Grafico com o uso do cpu das diferentes máquinas

Visto que no Prometheus a informação as vezes pode ficar um pouco confusa sem as devidas configurações e especificações no gráfico, decidiu-se por utilizar o Grafana, pois facilita bastante a visualização das várias métricas e tem uma interface mais intuitiva.

Apos a instalação e configurações necessárias no Grafana demonstradas no Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus, temos acesso a toda a informação com o seguinte formato.

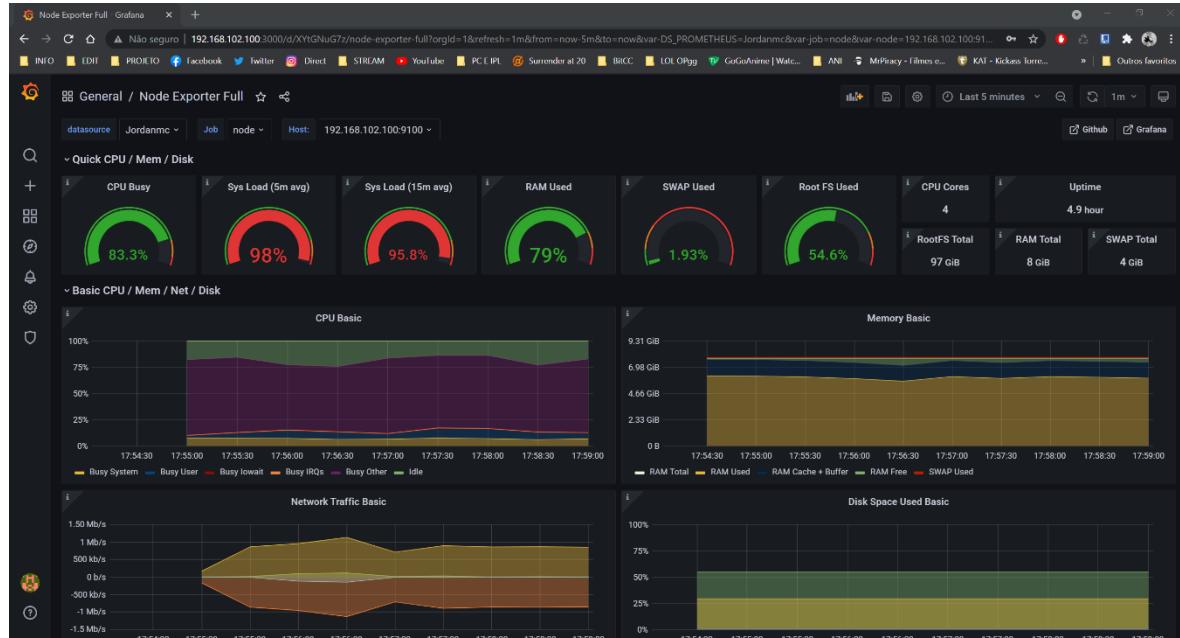


Figura 60 - Dashboard com as métricas no Grafana

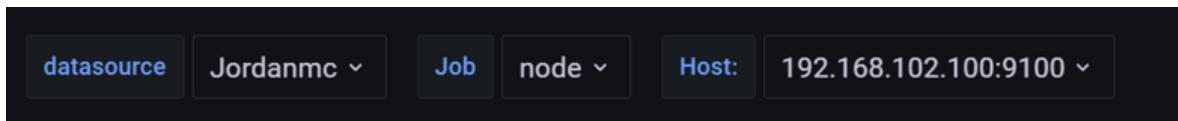


Figura 61 - Datasource / Job/ Host no Grafana

Datasource → Representa a Instância do Prometheus adicionada anteriormente.

Job → seria para os vários nós em caso de vários *clusters* como por exemplo em Kubernetes.

Host → São os vários targets representados no ficheiro de configuração do Prometheus.

Após esta explicação fica um esquema de como funciona estas três ferramentas ao mesmo tempo na nossa solução.

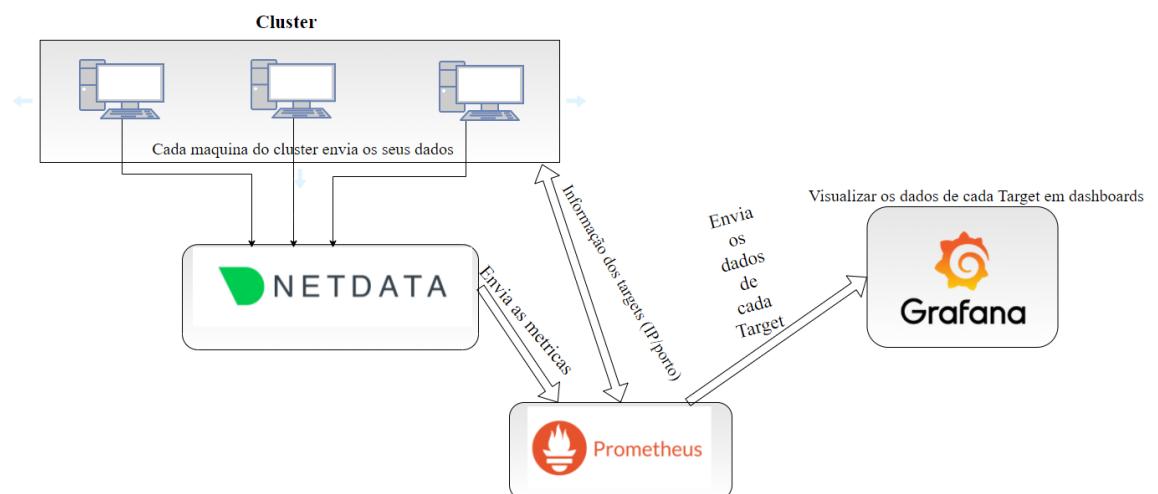


Figura 62 - Esquema do Funcionamento logico entre o Netdata/Prometheus/Grafana

De seguida será visualizado as várias diferenças de métricas em caso de ataques *SYN Flood* e poderá se visualizar um número elevado de pacotes enviados a cada máquina.

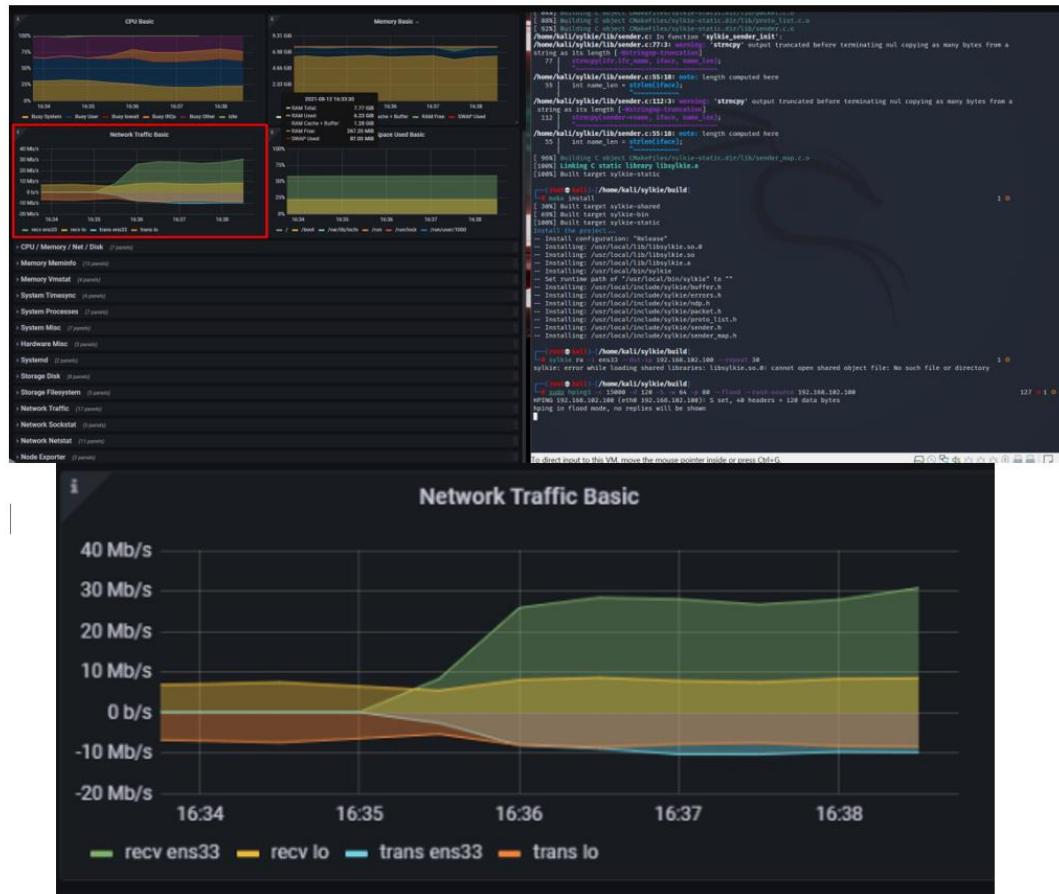


Figura 63 - Aumento nas métricas do tráfego da rede quando um ataque 'SYN Flood' é feito

Como se pode verificar na figura anterior, existe um número elevado de tráfego na rede quando é iniciado o ataque *SYN Flood*.

4.3.3. TIP

Foram realizados testes com as plataformas MISP e OTX. Com o MISP, começamos por aceder a página inicial do MISP, com as credenciais fornecidas.

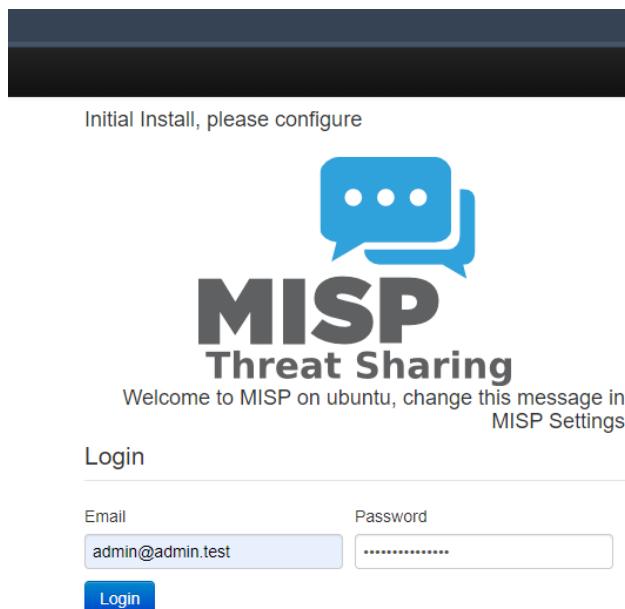


Figura 64 - Menu de login do MISP

Estando autenticado, começamos por adicionar *feeds* de ameaças disponíveis no repositório dos *feeds*⁴, que contém uma lista de default *feeds* para o MISP. Para adicionar um novo *feed*, accedemos em Sync Actions – List Feeds.

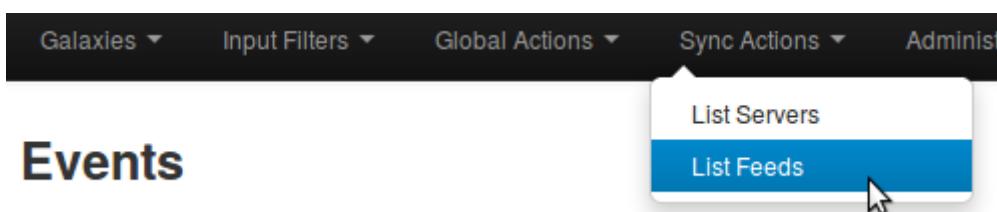


Figura 65 - Listar feeds no Misp

⁴ <https://www.misp-project.org/feeds/>

É preenchido com a informação disponibilizada na página dos *feeds*.

Figura 66 - Adicionar Feeds para o Misp

Os *feeds* adicionados são gerados em List Feeds. Para começarmos a receber os *feeds*, é preciso verificar que este está ativo e de seguida carregar no botão “Fetch and store all feed data” para buscar os dados de todos os *feeds* e inseri-los na base de dados do MISP.

Figura 67 - Feeds adicionados ao MISP

De seguida é possível verificar os eventos que foram “buscados” na lista de atributos em Event Actions – List Attributes.

Attributes																		
	Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	ID\$	Distribution	Sightings	Activity	Actions	
Search Attributes	2021-07-16	1443	●	Network activity	url	80.248.206.162:8080/pony/admin.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View Proposals	2021-07-16	1443	●	Network activity	url	176.31.255.41:81/pony/admin.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View delegation requests	2021-07-16	1443	●	Network activity	url	194.146.227.48:8080/pony/admin.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
List Attributes	2021-07-16	1443	●	Network activity	url	85.95.247.26/~estacion/PanelWeb-Panel/prv8/	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
Export Automation	2021-07-16	1443	●	Network activity	url	streeloftancy.com/viewweb/control.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
Search Attributes	2021-07-16	1443	●	Network activity	url	195.88.74.88/badmin.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View Proposals	2021-07-16	1443	●	Network activity	url	top30news.comeze.com/img/index.php?p=Login	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View delegation requests	2021-07-16	1443	●	Network activity	url	stopwell.org/cp.php?m=login	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
Search Attributes	2021-07-16	1443	●	Network activity	url	mmmoney1.com/panel/	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View Proposals	2021-07-16	1443	●	Network activity	url	mmmoney1.com/www/	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
View delegation requests	2021-07-16	1443	●	Network activity	url	virusmafia.in/stat.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	
Search Attributes	2021-07-16	1443	●	Network activity	url	policebrave.info/cp.php	🕒👤🕒🕒🕒	🕒🕒🕒		14371440 1442	3	☒	All	🕒👤🕒	●	🕒	🕒	

Figura 68 - Lista de Atributos no Misp

Estes atributos são então enviados para o Elasticsearch através do módulo threatintel, mencionado anteriormente na integração, permitindo assim visualizar os indicadores no Kibana através de uma dashboard.

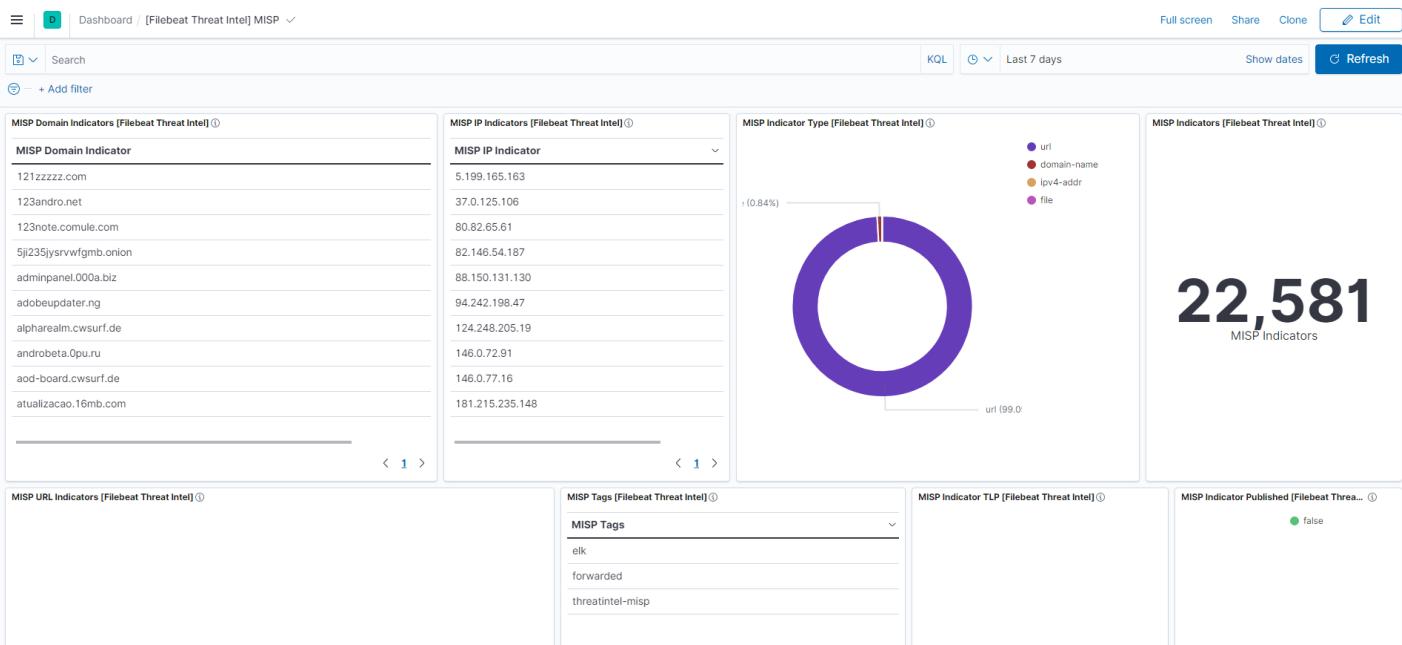


Figura 69 - Dashboard no Kibana com a informação recebida pelos feeds

Com isto é possível criar alertas com o *Kibana*. Neste exemplo foi criado uma regra para enviar alertas quando é obtido uma ameaça classificada com nível 4. (Os níveis de ameaça variam entre 5 a 1, sendo 1 o mais critico) (Elastic, threatintel fields, 2021).

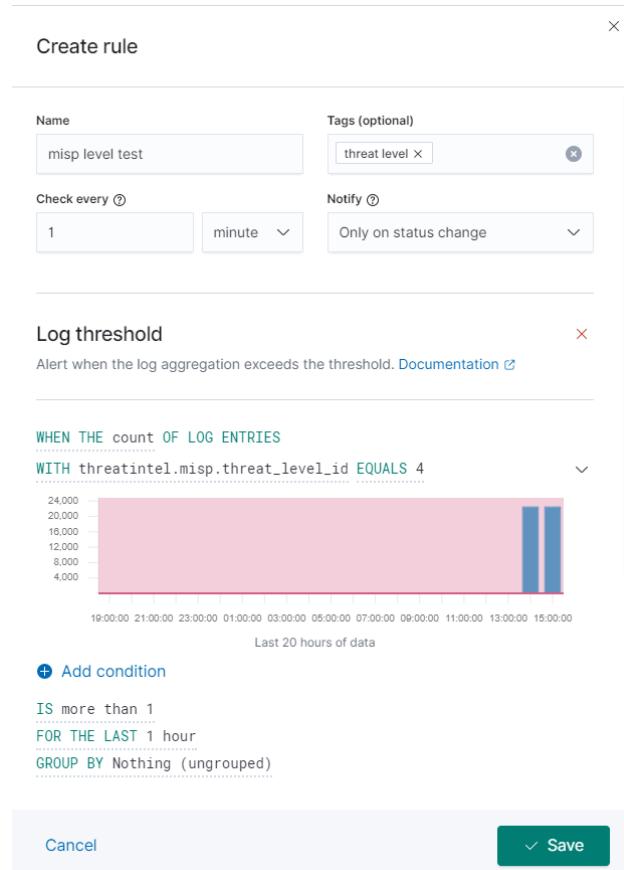


Figura 70 - Criar regra no Kibana

Ao ligar a regra, recebemos de imediato as correspondências da última hora no Slack.

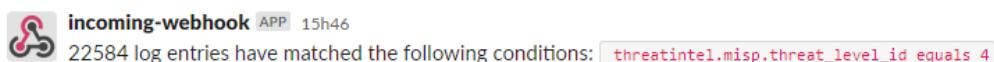


Figura 71 - Alerta no Slack descrevendo as condições

No caso do OTX, como já foi explicado sua implementação no tópico “Integração do TIP no SIEM”, também é possível criar regras para alertas do *Kibana*, especificando o seu indicador. Neste exemplo exibimos todos os *logs* com a tag *otx*, e a medida que novos *feeds* são carregados, é enviado um alerta para o slack.

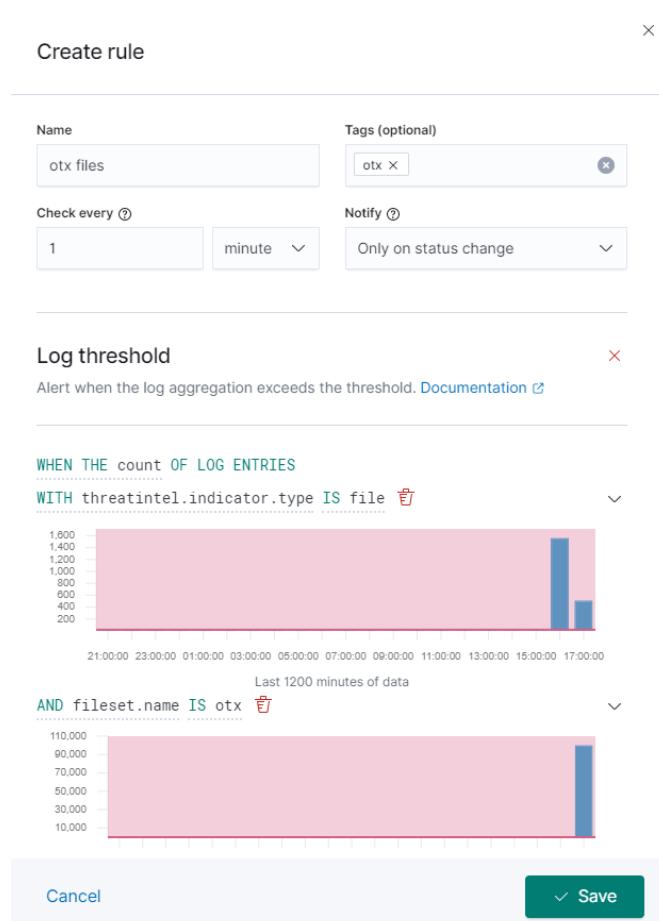


Figura 72 - Criar Regra com os tags recebidas pelos feeds do OTX



Figura 73 - Alerta no Slack coicidindo as tags do OTX

4.3.4. Relatórios

Para utilizarmos os relatórios do *Kibana*, é primeiro preciso realizar um diagnóstico para verificar se todas as funcionalidades necessárias estão em funcionamento.

The screenshot shows the Kibana navigation bar at the top with 'Stack Management' and 'Reporting' selected. On the left, there's a sidebar with sections for Ingest, Data, Alerts and Insights, Security, Kibana, and Stack. The main area is titled 'Reports' with the sub-section 'Reporting Diagnostics'. It contains three items: 'Verify Kibana configuration' (with a 'Verify configuration' button), 'Check browser' (with a 'Check browser' button), and 'Check screen capture' (with a 'Capture screenshot' button). A final message says 'All set!' with the note 'Everything looks good for reporting to function.'

Figura 74 - Criar Relatório

De seguida podemos então criar relatórios das pesquisas que realizamos. Neste teste realizamos uma pesquisa ao Winlogbeat para descobrir os ficheiros executáveis dentro da pasta C:\Windows\.

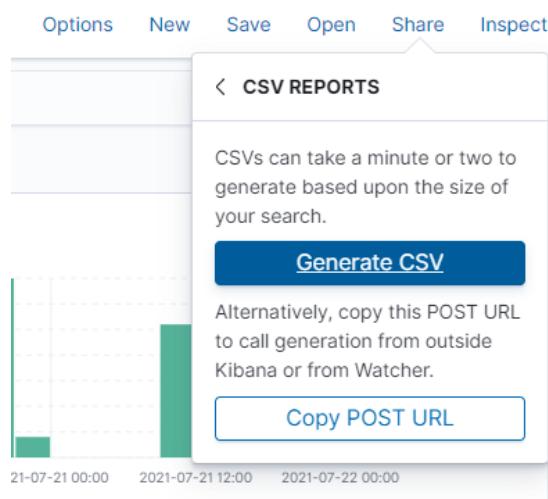


Figura 75 - Gerar relatório em formato CSV com as pesquisas realizadas

O relatório pode ser guardado no formato de PDF, PNG e CSV.

Reports			
Get reports generated in Kibana applications.			
Report	Created at	Status	Actions
<input type="checkbox"/> windows EXEcs search	2021-07-22 @ 11:19 AM admin	Completed at 2021-07-22 @ 11:19 AM	
			< 1 >

Figura 76 - Relatórios Listados

4.4.Síntese

Neste capítulo, a proposta de implementação do protótipo SIEM foi apresentada, juntamente com um TIP. Sendo importante referir que foi utilizada o *Elastic Stack* por ser uma solução *open source* como um dos requerimentos, no entanto, fez-se uso de uma licença de avaliação para ser possível realizar testes mais detalhados das suas funcionalidades.

Foi detalhada a sua instalação e dos seus componentes. Refere-se que em várias partes da sua implementação tivemos algumas dificuldades, como por exemplo na instalação do Elastalert, que provou ser um pouco instável e foi necessário correr certos comandos em determinada ordem para que tudo funcionasse.

Tendo o cenário em funcionamento, foram realizadas algumas simulações de ataques, com ajuda das ferramentas do Kali Linux, como o Hydra, que permitiu realizar ataques *SYN Flood* e brute force SSH. Estes ataques foram então observados dentro do *Kibana* a partir dos seus *dashboards* e ao realizar pesquisas diretas nos *logs*.

Outro requerimento deste trabalho foi o envio de alertas após a deteção de anomalias. De referir que com o Elastalert apenas foi realizado um teste com comando logger da máquina onde este estava instalado, e verificado o envio do alerta para a plataforma configurada, o Slack. Os restantes dos alertas foram realizados utilizando o alerta do *Kibana*, que na sua versão gratuita, não permite enviar para outras plataformas, por isso fez uso da licença de avaliação para enviar alertas para a plataforma Slack.

Outro ponto importante de referir foi a tentativa de explorar o Watcher, no entanto não se obteve grandes resultados no mesmo. Outros tipos de alertas que também foi explorado foram na secção Security (antigamente conhecida como módulo SIEM), no entanto não se conseguiu apesar de apresentar resultados significantes.

Foram também exploradas outras funcionalidades do *Elastic Stack*, como a exportação de dados em CSV

Outra parte do trabalho foi a implementação de um TIP. Neste caso foi implementada a plataforma MISP, com objetivo de enviar os *feeds* obtidos para a plataforma SIEM para que pudessem ser analisados de forma mais detalhada. Foram exploradas outras soluções TIP, como OTX, que também foi possível configurar para enviar informações publicadas pela comunidade. No entanto não foram implementadas mais soluções, pois não foi considerado relevante, apesar de ser possível ter diversas fontes diferentes em simultâneo.

Em síntese, consideramos que o protótipo implementado, realiza as tarefas básicas que se pretende, como a análise em tempo real de *logs* e deteção de ameaças, no entanto o funcionamento em conjunto com um TIP provou ser mais desafiante no sentido de conseguir realizar tarefas automatizadas com os *feeds* recebidos.

5. Conclusão

Este projeto acabou por ficar repartido em quatro partes que passa por explicar os conceitos fundamentais da temática em questão, clarificar e fazer uma análise comparativa de vários SIEMS escolhidos, implementar uma solução SIEM *open source* e por último realizar vários testes e configurações para garantir a segurança da Entidade.

No segundo capítulo é feito um esclarecimento sobre os conceitos fundamentais que serão mais tarde a base do projeto, tais como o funcionamento de um ataque Informático e o *flow* dos *logs*.

De seguida é esclarecido as bases do que é um SIEM e suas funções, mais tarde descrevendo cada SIEM e suas características relevantes tais como Arquitetura, funcionalidades e as suas Vantagens e desvantagens. No fim do capítulo é feita um estudo comparativo baseado na informação descrita de cada SIEM.

Continuando o capítulo, é feita introdução do que é Threat Intelligence para que se possa perceber a ideia geral do que é um TIP e como podem complementar um SIEM, mostrando várias soluções e os fatores que podem influenciar o custo, sendo que um TIP *open source* com várias funcionalidades pagas pode ser mais caro que um TIP comercial.

O objetivo da análise comparativa feita, é escolher um SIEM para implementar na solução respondendo ao requisito que possa ser implementado em uma PME e correspondendo às características que decidimos ser críticas para a escolha, dito isto, o SIEM que foi escolhido foi o *Elastic Stack*.

No capítulo três é feito um esclarecimento abstrato de como funciona a recolha de *logs* até aos outputs mostrando uma arquitetura lógica e explicando o seu funcionamento.

Como já tinha sido explicado no capítulo dois a arquitetura do *Elastic Stack*, foi aprofundado neste capítulo as suas funcionalidades tanto como os quatro produtos principais (*Elasticsearch*, *Logstash*, *Kibana* e *Beats*).

O capítulo quatro trata da implementação e testes da solução, de início é mostrada a arquitetura do protótipo que foi planeada para a implementação da solução, esta teve de permanecer um pouco simplificada devido às limitações de hardware proporcionadas pelo

covid-19, mas para a ideia principal de ser implantada em uma situação de PME deve satisfazer os requisitos que foram propostos. De seguida são mostrados os requisitos e especificações técnicas de cada Máquina implementada na solução.

Dando seguimento ao mesmo capítulo é mostrado os passos iniciais da implementação da solução onde é explicado a instalação dos vários componentes do *Elastic Stack* remetendo para os anexos com os passos tomados e configurações feitas na instalação dos produtos.

Continuando o mesmo capítulo, é apresentado como foram integrados os TIP e uma breve explicação de o que são e como funcionam, sendo estas o TIP MISP e o TIP OTX. Similarmente é mostrado no fim do capítulo como o *Elastic Stack* interage com a informação recebida pelos TIP.

O fim do capítulo serve para mostrar os vários testes realizados com a solução. Foram feitos vários ataques a sistemas que o *Elastic Stack* monitora e por vezes mesmo ao servidor *Elastic Stack*, os ataques passam por ataques *Brute-force*, *Synflood* e colocar um ficheiro que possa ser maligno nas máquinas fazendo com que o Elastic alerte através de várias Plataformas sendo que as que decidimos usar foi o Slack e o Telegram.

Também como adenda do projeto foi nos proposto o uso de outras ferramentas de recolha de métricas sendo que o metricbeat sem configurações específicas possa ser um pouco confuso, dito isto decidimos usufruir de uma junção de Netdata/Prometheus/Grafana para recolha de métricas mais específicas podendo assim monitorizar todas as máquinas da solução. São também mostrados vários testes realizados sobre como são afetadas as métricas do sistema por exemplo em caso de ataque SynFlood.

Analizado o projeto podemos dizer que o principal objetivo do projeto foi conseguido, sendo que foi feita a análise de vários SIEMs e implementado um SIEM com integração TIP.

Algumas dificuldades que tivemos:

- Houve algumas dificuldades na instalação do *Elastic Stack* pois maioria dos tutoriais existentes falta por vezes um passo ou uma configuração importante para prosseguir com a instalação e muitas vezes começar de novo e criar uma VM nova
- A instalação e configuração do Elastalert pois bastantes dos tutoriais existentes também tinham passos e configurações em falta.

- Na instalação do Prometheus e adicionar Prometheus como serviço do Ubuntu, pois o ficheiro de configuração é bastante rigoroso até mesmo com um espaço a mais ou o nome dos targets muitas vezes dar erro e não conseguindo iniciar o serviço
- Na configuração do Grafana foi preciso actualizar o gerenciador de pacotes através do node_exporter ao actualizar as tags das métricas enviadas pelo porto 19999
- Para colocar o certificado SSL no *Elastic Stack* foi bastante complicado pois a documentação fornecida pelo próprio elastic era muito confusa, e também gerar as keys e certificado não estava na documentação do elastic e colocar nos ficheiros de configuração do *Elasticsearch* e *Kibana*
- Para gerar keys do certificado TLS era preciso aceder a um gerador de keys do *Elasticsearch* e todos os tutoriais apenas diziam onde colocar a key no ficheiro de configuração do *Elasticsearch*.
- Bastante informação sobre os TIP no que toca ao seu funcionamento e dados enviados são escassos, portanto maioria do que foi descrito neste projeto é a nossa interação e o que foi visto através da sua integração e funcionamento.

Dito isto a comunidade do elastic ajudou bastante em fóruns e chats, e muitas vezes mesmo por era possível complementar e ajustar aos nossos problemas e conseguimos resolver todos os problemas que tivemos.

Também tivemos algumas dificuldades proporcionadas pelas limitações impostas pelo covid-19 tais como uso de hardware limitado tais como armazenamento ou CPU e RAM, por exemplo por vezes pretendíamos configurar o Filebeat ou o *Logstash* para grande tratamento de *Logs* e a máquina ia abaixo.

Cada um teve que usar o *Elastic Stack* no seu computador pessoal e ir complementando um ao outro as configurações feitas,

Mas esta dificuldade também nos fez encontrar outros caminhos e influenciar a nossa arquitetura da solução para ajustar as condições e resolver estas advertências.

De relembrar que nesta temática existe muito pouca informação quando os tópicos já são um pouco aprofundados e foi encontrado poucos documentos com esta temática em análise.

É entendido que o presente projeto concretiza os objetivos propostos, mas como referido no capítulo anterior, há bastantes funcionalidades que ainda podem ser mais bem exploradas para o melhor funcionamento desta solução.

Dito isto, os objetivos do projeto era estudar os SIEM e perceber melhor a sua importância no mundo, e fazer a comparação de vários SIEM e sua análise o que foi conseguido. Com base nessa comparação selecionou-se uma arquitetura que foi definida e baseada em um sistema gratuito e implementação do protótipo com base em *Elastic Stack* e integração de TIP MISP e OTX. Importante referir que não foi decidido integrar mais TIP devido ao MISP e OTX fornecer já uma grande “pegada” de informação tanto se pode aceder a informação recebida por outros TIP através da subscrição às comunidades de outros TIP.

Podendo dizer que o sistema foi validado e testado com resultados positivos, no entanto gostaríamos de ter conseguido interagir mais com o TIP e automatizar processos.

5.1. Análise crítica e proposta de melhorias

Vimos a realizar um projeto que visa a corresponder às várias características faladas ao longo do documento, mas há sempre aspetos que se poderia melhorar tais como:

- Aprofundar as funcionalidades do *Logstash* pois na nossa solução está com as configurações básicas (transformar os *Logs* em mensagens JSON e enviar para o *Elasticsearch*)
- Explorar melhor algumas funcionalidades pagas tais como os Alertas, Machine Learning, Watcher e fleets mas devido ao tempo limitado da licença não foi possível aprofundar essas funcionalidades.
- Aprofundar melhor cada funcionalidade dos *Beats* restantes pois só foi mais estudado e explorado as configurações e módulos do Filbeat.

- Explorar melhor a relação SIEM-TIP pois só foi mais trabalhado na automação com IP's malignos quando também era possível automatizar o bloqueio de sites e ficheiros malignos recebidos pelos *feeds* dos Tips.

No entanto, concluímos que o projeto tirou bom proveito das características e funcionalidades anteriormente mencionadas, e como o *Elastic Stack* é um SIEM com um enorme dinamismo e são adicionadas melhores e mais ferramentas para a sua robustez torna este projeto sempre sujeito a melhorias.

6. Bibliografia

- (TIP), T. I. (28 de Agosto de 2019). *How Threat Intelligence Can Solve 3 Common SIEM Problems.* Obtido de CircleID: https://circleid.com/posts/20190828_how_threat_intelligence_can_solve_3_common_siem_problems/
- Or, A. (5 de Junho de 2020). *LEARN SIEM FOR FREE.* Obtido de Blue Team Blog: <https://blueteamblog.com/learn-siem-for-free>
- Administrator. (7 de Setembro de 2021). *HOW TO PERFORM TCP SYN FLOOD DOS ATTACK & DETECT IT WITH WIRESHARK - KALI LINUX HPING3.* Obtido de Firewall.cx: <https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html>
- AlienVault. (25 de 5 de 2021). *AT&T Cybersecurity.* Obtido de Compare OSSIM to USM: <https://cybersecurity.att.com/products/ossim/compare>
- AT&T. (15 de Abril de 2021). *About USM Appliance System Architecture and Components.* Obtido de AT&T Cybersecurity: <https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm>
- Banon, S. (2021). *Apresentamos a Elastic License v2, simplificada e mais permissiva; a SSPL continua sendo uma opção.* Obtido de elastic: <https://www.elastic.co/pt/blog/elastic-license-v2>
- Barajas, E. (4 de Fevereiro de 2020). *Tripwire.* Obtido de What Is Log Management, and Why Is It Important?: <https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/log-management-why-important/>
- Berman, D. (Junho de 2018). *Using the ELK Stack for SIEM.* Obtido de logz: <https://logz.io/blog/elk-siem/>
- Bhattacharya, A. (6 de Março de 2021). *Encryption Consulting.* Obtido de Cyber Security Attack Types - Active and Passive Attacks: <https://www.encryptionconsulting.com/active-and-passive-attacks/>

- Bisson, D. (26 de Novembro de 2017). *What Is Log Management?* Obtido de Tripwire: <https://www.tripwire.com/state-of-security/security-data-protection/security-controls/what-is-log-management/>
- Borkar, P. (26 de julho de 2018). *Security Data Lakes: Comparing the “Do It Yourself” Deployments Versus Commercial Solutions.* Obtido de exabeam: <https://www.exabeam.com/siem/data-lakes/>
- Bycroft, C. R. (15 de Janeiro de 2018). *SIEMONSTER VERSION 3 HIGH LEVEL DESIGN.* Obtido de pdfslide: <https://pdfslide.net/documents/siemonster-version-3-high-level-design-table-of-contents-1-authors-preface-.html>
- Canner, B. (9 de Maio de 2018). *7 Key SIEM Capabilities to Look For in Your Solution.* Obtido em 5 de Abril de 2021, de Solutions Review: <https://solutionsreview.com/security-information-event-management/7-key-siem-capabilities-look-solution/>
- Carstensen, N. (29 de Novembro de 2019). *What is Log Management? A Complete Logging Guide.* Obtido de Graylog: <https://www.graylog.org/post/what-is-log-management-a-complete-logging-guide>
- Cisco. (s.d.). *What Is a Cyberattack?* Obtido de Cisco: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
- Cloudflare. (2021). *Slowloris DDoS attack.* Obtido de <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/>
- Congleton, N. (22 de Setembro de 2018). *SSH Password Testing With Hydra on Kali Linux.* Obtido de LinuxConfig.org: <https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux>
- Cybersecurity, A. (2021). *AlienVault Pricing - Affordable Plans to Fit Any Budget.* Obtido de AT&T Cybersecurity: <https://cybersecurity.att.com/pricing>
- Cybersecurity, A. (2021). *Compare AlienVault Products.* Obtido de AT&T Cybersecurity: <https://cybersecurity.att.com/products/ossim/compare>

Cybersecurity, A. (2021). *OSSIM: The Open Source SIEM / AlienVault*. Obtido de AT&T Cybersecurity: <https://cybersecurity.att.com/products/ossim>

devquora. (12 de Março de 2020). *List different types of Splunk Licenses? - Online...* Obtido de List different types of Splunk Licenses?: <https://www.onlineinterviewquestions.com/list-different-types-of-splunk-licenses/>

Elastic. (2021). *Analise suas métricas do Prometheus em escala*. Obtido de <https://www.elastic.co/pt/what-is/prometheus-monitoring>

Elastic. (2021). *threatintel fields*. Obtido de <https://www.elastic.co/guide/en/beats/filebeat/7.14/exported-fields-threatintel.html>

elastic. (2021). *What is elasticsearch*. Obtido de elastic: <https://www.elastic.co/pt/what-is/elasticsearch>

Elastic. (2021). *Winlogbeat: Analyse Windows Event Logs / Elastic*. Obtido de <https://www.elastic.co/pt/beats/winlogbeat>

elastic, a. (2021). *Logstash*. Obtido de elastic: <https://www.elastic.co/pt/logstash>

elastic, b. (2021). *beats*. Obtido de elastic/beats: [https://www.elastic.co/pt/beats/](https://www.elastic.co/pt/beats)

elastic, b. (2021). *o que é o kibana*. Obtido de Elastic: [https://www.elastic.co/pt/kibana/](https://www.elastic.co/pt/kibana)

elastic, e. (2021). *MISP MODULE*. Obtido de elastic: <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-misp.html>

elastic, f. (2021). *Filebeat Overview*. Obtido de Elastic Filebeat: <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html>

Enisa.europa. (2017). Exploring the opportunities and limitations of current Threat Intelligence Platforms. 2017, p. 42.

Gartner. (2021). *Security Information and Event Management (SIEM) Reviews and Ratings*. Obtido de Gartner: <https://www.gartner.com/reviews/market/security-information-event-management>

- Grustniy, L. (24 de Março de 2021). *The great lockdown: How COVID-19 has affected cybersecurity.* Obtido de Kaspersky daily: <https://www.kaspersky.com/blog/pandemic-year-in-infosec/39123/>
- Heikamp, F. (18 de Junho de 2020). *Opensource SIEM: MozDef.* Obtido de <https://folmer.info/blog/opensource-siem-mozdef>
- Help, S. T. (27 de Agosto de 2021). *Top 11 Best SIEM Tools In 2021 For Real-Time Incident Response And Security.* Obtido de Software Testing Help: <https://www.softwaretestinghelp.com/siem-tools/>
- kaspersky. (2021). *Threat Intelligence Definition. Why Threat Intelligence Is Important for Your Business and How to Evaluate a Threat Intelligence Program.* Obtido de kaspersky: <https://www.kaspersky.com/resource-center/definitions/threat-intelligence>
- Mark Russinovich, T. G. (18 de Agosto de 2021). *Sysmon - Windows Sysinternals / Microsoft Docs.* Obtido de <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
- Mozilla. (16 de Junho de 2021). *MozDef Documentation.* Obtido de MozDef Documentation: https://mozdef.readthedocs.io/_/downloads/en/latest/pdf/
- Mozilla. (2021). *Overview.* Obtido de Mozilla Enterprise defense Platform: <https://mozdef.readthedocs.io/en/latest/overview.html#architecture>
- Netdata. (24 de Agosto de 2021). *What is Netdata? / Learn Netdata.* (2021). Obtido de Netdata Learn: <https://learn.netdata.cloud/docs/overview/what-is-netdata>
- oliveira, W. (16 de Abril de 2021). *Princípios Básicos Da Segurança Da Informação.* Obtido de Techtem: <https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao/>
- OSSIM: *The Open Source SIEM / AlienVault.* (s.d.). Obtido de AlienVault OSSIM: <https://cybersecurity.att.com/products/ossim>

paloaltoNetworks. (2019). *What is a Threat Intelligence Platform.* Obtido de paloaltoNetworks: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform>

Petters, J. (15 de Junho de 2020). *What is SIEM? A Beginner's Guide.* Obtido de Varonis: <https://www.varonis.com/blog/what-is-siem/>

Prytuluk, M. (Junho de 2021). *Cisco Umbrella: The Umbrella Enforcement API for Custom Integrations.* Obtido de <https://support.umbrella.com/hc/en-us/articles/231248748-Cisco-Umbrella-TheUmbrella-Enforcement-API-for-Custom-Integrations>

Research, 4. (2015). *Information Security.* New York: 451 Research.

Russinovich, M. (25 de Maio de 2021). *PsExec v2.34.* Obtido de Microsoft: <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>

S., L. (4 de Março de 2020). *[SIEM] Introdução ao OSSIM.* Obtido de <https://lucxs.medium.com/siem-introdu%C3%A7%C3%A3o-ao-ossim-98a45fffeb19>

Santos, P. I. (2016). *Segurança Informática: A Importância para a Segurança Interna.* Lisboa.

Security_guest. (12 de Junho de 2019). *SIM, SEM, and SIEM: Definitions and Choosing the Right Enterprise Solution.* Obtido de CyberRes Community: <https://community.microfocus.com/cyberres/b/sws-22/posts/sim-sem-and-siem-definitions-and-choosing-the-right-enterprise-solution>

Shivang. (s.d.). *What is Grafana? Why Use It? Everything You Should Know About It.* Obtido de 8bitmen: <https://www.8bitmen.com/what-is-grafana-why-use-it-everything-you-should-know-about-it/>

Siemonster. (2021). *Pricing SIEM Pricing for any budget.* Obtido de Siemonster.com: <https://siemonster.com/pricing/>

Siemonster, a. (2021). *Siemonster Community Edition .* Obtido de Siemonster: <https://siemonster.com/community-edition/>

- Splunk. (s.d.). *Free vs. Enterprise.* Obtido de Splunk: https://www.splunk.com/pt_br/view/SP-CAAAE8W
- Splunk, a. (11 de Janeiro de 2021). *About Splunk Enterprise - Splunk Documentation.* Obtido de docs.Splunk: <https://docs.splunk.com/Documentation/Splunk/8.2.2/Overview/AboutSplunkEnterprise>
- Srivastava, A. (2019). *Kibana 7 Quick Start Guide.* Obtido de https://books.google.pt/books?id=ZGSGDwAAQBAJ&printsec=frontcover&hl=pt-PT&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Stoner, J. (29 de Abril de 2020). *Integrating COVID (or Any) Threat Indicators with MISP and Splunk Enterprise Security.* Obtido de splunk: https://www.splunk.com/en_us/blog/security/integrating-covid-or-any-threat-indicators-with-misp-and-enterprise-security.html
- Tal, L. (3 de Junho de 2018). *Log Management Comparison: ELK vs Graylog.* Obtido de coralogix: <https://coralogix.com/blog/log-management-comparison-elk-vs-graylog/>
- Team, L. (23 de Outubro de 2020). *Must-Have Features of a Modern SIEM.* Obtido de Logsign: <https://www.logsign.com/blog/must-have-features-of-a-modern-siem/>
- Torres, A. F. (2014). *Os referenciais de segurança da informação e a melhoria contínua: um caso exploratório.* Porto.
- TrustRadius. (s.d.). *AlienVault OSSIM vs Elasticsearch.* Obtido de TrustRadius: <https://www.trustradius.com/compare-products/alienvault-ossim-vs-elasticsearch>
- vanimpe. (2021). *Use Elastic to represent MISP threat data.* Obtido de vanimpe.eu: <https://www.vanimpe.eu/2021/01/13/use-elastic-to-represent-misp-threat-data/>
- Varonis. (s.d.). *5 Ways Your SIEM is Failing You and What to do About It.* Obtido de https://info.varonis.com/hubfs/docs/whitepapers/en/5%20Ways%20Your%20SIEM%20is%20Failing%20You%20and%20What%20to%20do%20About%20It.pdf?utm_medium=email&_hs_mi=89538557&_hsenc=p2ANqtz-_woJ1m1AnUYeMwpDsixMafq0g44E2nHxV0IuyQ4ab1F956W3MovB9_a8f3XXZWqdFzqPWgkg6

Vazão, A. (2020). *Implementação de sistema SIEM open-source em conformidade com o RGPD*. Leiria.

Watts, S. (16 de Janeiro de 2018). *SIEM vs Log Management: What's the difference?* Obtido de bmc: <https://www.bmc.com/blogs/siem-vs-log-management-whats-the-difference/>

wiki.splunk. (11 de Março de 2016). *Deploy: SplunkBucketRetentionTimestampsAndYou*. Obtido de wiki.splunk: <https://wiki.splunk.com/Deploy:SplunkBucketRetentionTimestampsAndYou>

Zarzosa, S. G. (28 de 02 de 2017). In-depth analysis of SIEMs . *DiSIEM – Diversity-enhancements for SIEMs*, p. 148.

Anexo A – Instalação do *Elastic Stack*

A implementação do *Elastic Stack* foi feita numa máquina com sistema operativo Ubuntu 20.04.2 LTS.

```
ubuntu@ubuntu:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.2 LTS
Release:        20.04
Codename:       focal
```

Seguindo a ordem de instalação recomendada pela Elastic⁵, começou-se por instalar o *Elasticsearch*, seguido pelo *Kibana*, *Logstash*, *Beats*...:

Instalação do *Elasticsearch*

Primeiramente é necessário a chave PGP do *Elasticsearch*, seguido pela instalação do repositório APT e finalmente a instalação do Elasticsearch.

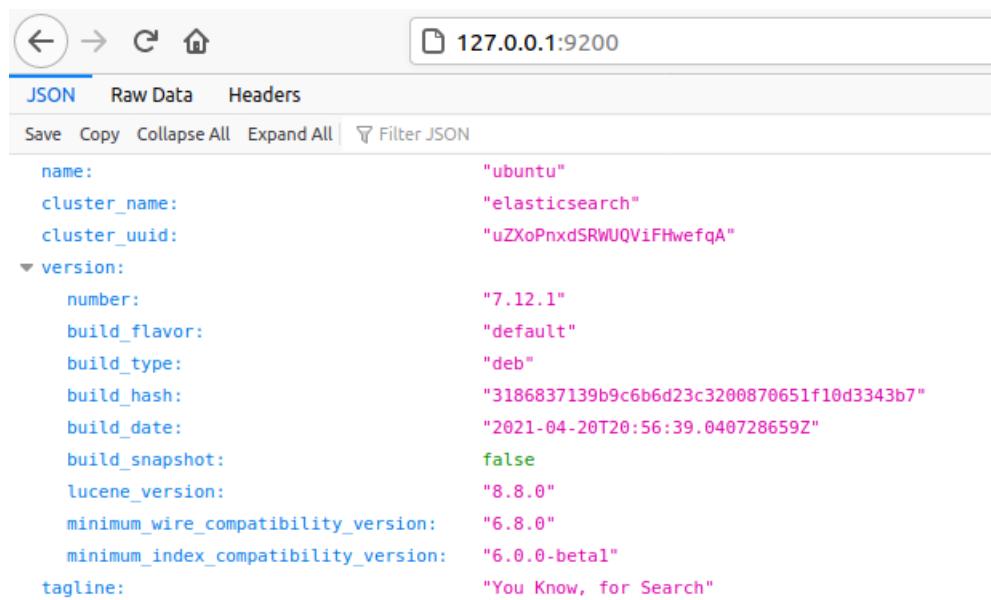
```
ubuntu@ubuntu:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
ubuntu@ubuntu:~$ sudo apt-get install apt-transport-https
ubuntu@ubuntu:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install elasticsearch
```

Após instalado é preciso configurar o *Elasticsearch* para iniciar automaticamente quando o sistema é iniciado.

```
ubuntu@ubuntu:~$ sudo /bin/systemctl daemon-reload
ubuntu@ubuntu:~$ sudo /bin/systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service →
/lib/systemd/system/elasticsearch.service.
```

⁵ <https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html>

Por fim é iniciado o serviço e verificado o seu funcionamento, através de um pedido HTTP pelo porto 9200 do *localhost*.



```

{
  "name": "ubuntu",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "uZXoPnxdsRwUQViFHwefqA",
  "version": {
    "number": "7.12.1",
    "build_flavor": "default",
    "build_type": "deb",
    "build_hash": "3186837139b9c6b6d23c3200870651f10d3343b7",
    "build_date": "2021-04-20T20:56:39.040Z",
    "build_snapshot": false,
    "lucene_version": "8.8.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}

```

Verificada o funcionamento do *Elasticsearch*, é necessário realizar algumas configurações no ficheiro */etc/Elasticsearch/Elasticsearch.yml*. De notar que a diretoria */etc/Elasticsearch* tem propriedades do tipo *root:Elasticsearch*.

Neste caso foi apenas definido um nome ao *cluster* e ao *node*.

```

# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: elasticsearch-siem
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#

```

Para verificar as alterações, reinicia-se o serviço *sudo systemctl restart Elasticsearch.service*.

```

{
  "name": "node-1",
  "cluster_name": "elasticsearch-siem",
  "cluster_uuid": "uZXoPnxdSRWUQViFHwefqA",
  "version": {
    "number": "7.12.1",
    "build_flavor": "default",
    "build_type": "deb",
    "build_hash": "3186837139b9c6b6d23c3200870651f10d3343b7",
    "build_date": "2021-04-20T20:56:39.040Z",
    "build_snapshot": false,
    "lucene_version": "8.8.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}

```

Instalação do *Kibana*

Instalação do *Kibana* e configuração para iniciar automaticamente.

```

ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install kibana
ubuntu@ubuntu:~$ sudo /bin/systemctl daemon-reload
ubuntu@ubuntu:~$ sudo /bin/systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service →
/etc/systemd/system/kibana.service.
ubuntu@ubuntu:~$ sudo systemctl start kibana.service

```

Após instalado o serviço *Kibana*, é necessário realizar algumas configurações iniciais no ficheiro */etc/Kibana/Kibana.yml*. Como os serviços vão estar na mesma máquina, o parâmetro **Elasticsearch.hosts** é o próprio *localhost*.

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.102.130"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

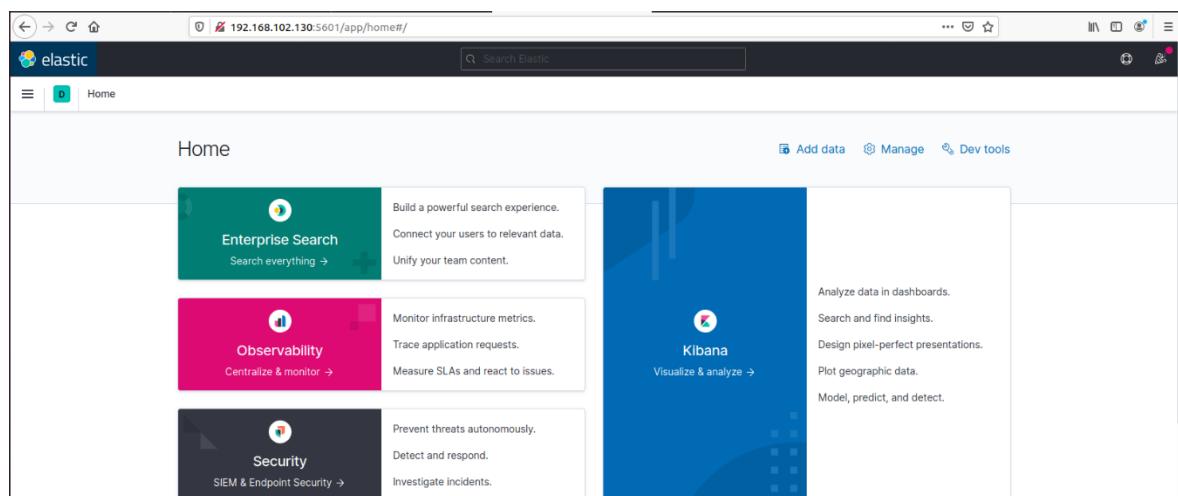
# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.
server.name: "Kibana-SIEM"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]
```

Feita estas configurações é verificado o funcionamento do serviço, através do endereço <http://localhost:5601/>.



Instalação Logstash

É instalado o logstash e de seguida configurado o serviço, com nome do node.

```
ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install logstash
root@ubuntu:/home/ubuntu# nano /etc/logstash/logstash.yml

# ----- Node identity -----
#
# Use a descriptive name for the node:
#
node.name: no_teste
#
```

De seguida é testado o funcionamento do serviço.

```
ubuntu@ubuntu:/usr/share/logstash$ sudo bin/logstash -e 'input { stdin { } } output { stdout { } }'
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console
[INFO ] 2021-05-03 10:39:24.780 [main] runner - Starting Logstash {"logstash.version"=>"7.12.1", "jruby.version"=>"jruby 9.2.13.0 (2.5.7) 2020-08-03 9a89c94bcc OpenJDK 64-Bit Server VM 11.0.10+9 on 11.0.10+9 +indy +jit [linux-x86_64]"}
[WARN ] 2021-05-03 10:39:25.212 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2021-05-03 10:39:25.885 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600}
[INFO ] 2021-05-03 10:39:26.536 [Converge PipelineAction::Create<main>] Reflections - Reflections took 34 ms to scan 1 urls, producing 23 keys and 47 values
[INFO ] 2021-05-03 10:39:27.006 [[main]-pipeline-manager] javapipeline - Starting pipeline {:pipeline.id=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50, "pipeline.max_inflight"=>500, "pipeline.sources"=>["config string"], :thread=>"#<Thread:0x1c9b3e16 run>"}
[INFO ] 2021-05-03 10:39:27.670 [[main]-pipeline-manager] javapipeline - Pipeline Java execution initialization time {"seconds"=>0.66}
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by com.jrubystdinchannel.StdinChannelLibrary$Reader (file:/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/jruby-stdin-channel-0.2.0-java/lib/jruby_stdin_channel/jruby_stdin_channel.jar) to field java.io.FilterInputStream.in
WARNING: Please consider reporting this to the maintainers of com.jrubystdinchannel.StdinChannelLibrary$Reader
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
[INFO ] 2021-05-03 10:39:27.712 [[main]-pipeline-manager] javapipeline - Pipeline started {"pipeline.id"=>"main"}
The stdin plugin is now waiting for input:
[INFO ] 2021-05-03 10:39:27.766 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
teste123
{
    "@version" => "1",
    "@timestamp" => 2021-05-03T17:39:59.415Z,
    "message" => "teste123",
    "host" => "ubuntu"
}
```

Após a verificação do funcionamento, configurou-se o Logstash para iniciar automaticamente com o sistema.

```
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl daemon-reload
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service →
/etc/systemd/system/logstash.service.
```

Instalação do *Beats*

Iremos descrever o procedimento de instalação dos *Beats*. Merecido da sua complexidade decidimos fazer um manual da instalação dos mesmos, baseado no manual disponibilizado pela elastic.⁶

Auditbeat

O auditbeat é instalado e de seguida configurado para iniciar com o sistema.

```
ubuntu@ubuntu:/usr/share/logstash$ sudo apt-get update && sudo apt-get install auditbeat
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl enable auditbeat
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl start auditbeat.service
```

Podemos de seguida ver o funcionamento do serviço.

```
ubuntu@ubuntu:~$ sudo systemctl status auditbeat.service
● auditbeat.service - Audit the activities of users and processes on your system.
   Loaded: loaded (/lib/systemd/system/auditbeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-05-03 11:00:51 PDT; 22min ago
     Docs: https://www.elastic.co/products/beats/auditbeat
      Main PID: 14654 (auditbeat)
        Tasks: 14 (limit: 4618)
       Memory: 90.4M
      CGroup: /system.slice/auditbeat.service
              └─14654 /usr/share/auditbeat/bin/auditbeat --environment systemd -c /etc/auditbeat/auditbeat.yml --path.ho>
mai 03 11:18:25 ubuntu auditbeat[14654]: 2021-05-03T11:18:25.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:18:55 ubuntu auditbeat[14654]: 2021-05-03T11:18:55.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:19:25 ubuntu auditbeat[14654]: 2021-05-03T11:19:25.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:19:55 ubuntu auditbeat[14654]: 2021-05-03T11:19:55.397-0700      INFO      [monitoring]      log/log.go>
mai 03 11:20:25 ubuntu auditbeat[14654]: 2021-05-03T11:20:25.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:20:55 ubuntu auditbeat[14654]: 2021-05-03T11:20:55.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:21:25 ubuntu auditbeat[14654]: 2021-05-03T11:21:25.397-0700      INFO      [monitoring]      log/log.go>
mai 03 11:21:55 ubuntu auditbeat[14654]: 2021-05-03T11:21:55.396-0700      INFO      [monitoring]      log/log.go>
mai 03 11:22:25 ubuntu auditbeat[14654]: 2021-05-03T11:22:25.397-0700      INFO      [monitoring]      log/log.go>
mai 03 11:22:55 ubuntu auditbeat[14654]: 2021-05-03T11:22:55.396-0700      INFO      [monitoring]      log/log.go>
lines 1-20/20 (END)
```

Filebeat

A instalação do Filebeat é bastante simples basta executar os seguintes comandos:

```
ubuntu@ubuntu:/usr/share/logstash$ sudo apt-get update && sudo apt-get install filebeat
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl enable filebeat
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl start filebeat.service
```

Depois de estar instalado é preciso editar o ficheiro Filebeat.yml.

⁶ <https://www.elastic.co/guide/en/beats/libbeat/7.12/getting-started.html>

```
filebeat.inputs:
```

```
- type: log
```

```
enabled: true
```

```
paths:
```

```
- /var/log/*.log
```

Para testar as configurações do Filebeat executa-se o seguinte comando:

Para iniciar o serviço executa se o seguinte comando:

- sudo systemctl start Filebeat

Para ver o status do Filebeat executa se o seguinte comando:

- sudo systemctl status Filebeat.service

```
ubuntu@ubuntu:/usr/share/logstash$ sudo systemctl status filebeat.service
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enable>
   Active: active (running) since Mon 2021-05-03 11:12:46 PDT; 1s ago
     Docs: https://www.elastic.co/products/beats/filebeat
 Main PID: 15500 (filebeat)
    Tasks: 9 (limit: 4618)
   Memory: 27.4M
      CGroup: /system.slice/filebeat.service
              └─15500 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebea>

mai 03 11:12:46 ubuntu filebeat[15500]: 2021-05-03T11:12:46.876-0700      INFO  >
mai 03 11:12:46 ubuntu filebeat[15500]: 2021-05-03T11:12:46.877-0700      INFO  >
mai 03 11:12:46 ubuntu filebeat[15500]: 2021-05-03T11:12:46.877-0700      INFO  >
mai 03 11:12:46 ubuntu filebeat[15500]: 2021-05-03T11:12:46.879-0700      INFO  >
```

Heartbeat

Instalar e Iniciar heartbeat:

```
ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install heartbeat-elastic
ubuntu@ubuntu:~$ sudo systemctl enable heartbeat-elastic
```

Configurar no ficheiro **heartbeat.yml** o seguinte:

```
#####
# Define a directory to load monitor definitions from. Definitions take the form
# of individual yaml files.
heartbeat.config.monitors:
  # Directory + glob pattern to search for configuration files
  path: ${path.config}/monitors.d/*.yml
  # If enabled, heartbeat will periodically check the config.monitors path for changes
  reload.enabled: true
  # How often to check for changes
  reload.period: 5s
```

Para ver o status do Heartbeat executar:

```
ubuntu@ubuntu:~$ sudo systemctl status heartbeat-elastic.service
● heartbeat-elastic.service - Ping remote services for availability and log results to Elasticsearch or send to Logstash
   Loaded: loaded (/lib/systemd/system/heartbeat-elastic.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-05-03 11:30:50 PDT; 8s ago
     Docs: https://www.elastic.co/products/beats/heartbeat
     Main PID: 16501 (heartbeat)
        Tasks: 9 (limit: 4618)
       Memory: 39.7M
      CGroup: /system.slice/heartbeat-elastic.service
              └─16501 /usr/share/heartbeat/bin/heartbeat --environment systemd -c /etc/heartbeat/heartbeat.yml --path.ho

mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.635-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.635-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.635-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.635-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.637-0700      INFO      template/load.go:183      Ex>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.696-0700      INFO      template/load.go:117      Tr>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.761-0700      INFO      template/load.go:109      te>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.761-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.880-0700      INFO      [index-management]      idxm>
mai 03 11:30:51 ubuntu heartbeat[16501]: 2021-05-03T11:30:51.882-0700      INFO      [publisher_pipeline_output] >
```

Metricbeat

*monitorar com o Metricbeat:⁷

Para Instalação e Iniciar o Metricbeat executar o seguinte comando:

```
ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install metricbeat
ubuntu@ubuntu:~$ sudo systemctl enable metricbeat
```

⁷ <https://www.elastic.co/guide/en/elasticsearch/reference/current/configuring-metricbeat.html>

Configurar no ficheiro **Metricbeat.yml** o seguinte:

```
# ===== Modules configuration =====

metricbeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: true

  # Period on which files under path should be checked for changes
  #reload.period: 10s
```

O Metricbeat permite ativar vários módulos **através dos seguintes comandos:**

Para ver a lista dos módulos:

```
./metricbeat modules list
```

Para ativar os módulos:

```
./metricbeat modules enable apache mysql
```

Para ver o status do serviço:

```
ubuntu@ubuntu:~$ sudo systemctl start metricbeat.service
ubuntu@ubuntu:~$ sudo systemctl status metricbeat.service
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
   Loaded: loaded (/lib/systemd/system/metricbeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-05-03 11:56:23 PDT; 1s ago
     Docs: https://www.elastic.co/products/beats/metricbeat
 Main PID: 17603 (metricbeat)
    Tasks: 9 (limit: 4618)
   Memory: 91.9M
      CGroup: /system.slice/metricbeat.service
              └─17603 /usr/share/metricbeat/bin/metricbeat --environment systemd -c /etc/metricbeat/metricbeat.yml --path.h

mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.681-0700      INFO      [beat]      instance/beat.go:1
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.681-0700      INFO      [beat]      instance/beat.go:1
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.682-0700      INFO      [beat]      instance/beat.go:1
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.682-0700      INFO      instance/beat.go:304      Setup
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.682-0700      INFO      [index-management]      idxmgm>
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.682-0700      INFO      eslegclient/connection.go:99      >
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.682-0700      INFO      [publisher]      pipeline/modu>
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.713-0700      INFO      [monitoring]      log/log.go:1
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.713-0700      INFO      instance/beat.go:468      metr>
mai 03 11:56:23 ubuntu metricbeat[17603]: 2021-05-03T11:56:23.713-0700      INFO      cfgfile/reload.go:164      Con>
[lines 1-20/20 (END)]
```

Packetbeat

Para Instalação e Iniciar o Packetbeat executar o seguinte comando:

```
ubuntu@ubuntu:~$ sudo apt-get update && sudo apt-get install packetbeat
ubuntu@ubuntu:~$ sudo systemctl enable packetbeat
```

Para ver o status do serviço:

```
ubuntu@ubuntu:~$ sudo systemctl start packetbeat.service
ubuntu@ubuntu:~$ sudo systemctl status packetbeat.service
● packetbeat.service - Packetbeat analyzes network traffic and sends the data to Elasticsearch.
  Loaded: loaded (/lib/systemd/system/packetbeat.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2021-05-03 12:40:42 PDT; 5s ago
    Docs: https://www.elastic.co/products/beats/packetbeat
 Main PID: 18495 (packetbeat)
   Tasks: 10 (limit: 4618)
  Memory: 78.4M
     CGroup: /system.slice/packetbeat.service
             └─18495 /usr/share/packetbeat/bin/packetbeat --environment systemd -c /etc/packetbeat/packetbeat.yml --path.h

mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.251-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.251-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.251-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.251-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.253-0700      INFO      template/load.go:183      Exist>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.337-0700      INFO      template/load.go:117      Try >
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.411-0700      INFO      template/load.go:109      temp>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.412-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.494-0700      INFO      [index-management]      idxmgm>
mai 03 12:40:47 ubuntu packetbeat[18495]: 2021-05-03T12:40:47.495-0700      INFO      [publisher_pipeline_output]  >
lines 1-20/20 (END)
```

Winlogbeat e Sysmon

A instalação do Winlogbeat foi feita no Windows *host* com a Powershell. Primeiramente fez-se o download do Winlogbeat através da página oficial da elastic⁸. De seguida seguiu-se os passos descritos na documentação do Winlogbeat⁹.

O ficheiro de configuração fica localizado em C:\Program Files\Winlogbeat\winlogbeat.yml, e nele foram alteradas as seguintes linhas a negrito.

Para que seja possível carregar os *dashboards* do Winlogbeat, é preciso adicionar o endereço IP da máquina *Elastic Stack*, e foram também importados os certificados para que a comunicação de forma segura funcionasse.

⁸ <https://www.elastic.co/pt/downloads/beats/winlogbeat>

⁹ <https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation-configuration.html>

```

# ===== General =====
tags: ["windows-10"]

# ===== Kibana =====
setup.kibana:

    # Kibana Host
    host: "https://192.168.102.100:5601"

    ssl.enabled: true
    ssl.certificateAuthorities: "certs/client-ca.cer"
    ssl.certificate: "certs/client.cer"
    ssl.key: "certs/client.key"

# ===== Outputs =====
# ----- Elasticsearch Output -----
output.elasticsearch:
    # Array of hosts to connect to.
    hosts: ["192.168.102.100:9200"]

    # Protocol - either `http` (default) or `https`.
    protocol: "https"

    # Authentication credentials - either API key or username/password.
    #api_key: "id:api_key"
    username: "elastic"
    password: "owAVlTEEp4jI6a6hZ2GQ"

    ssl.verification_mode: none

# ===== Logging =====
# Available log levels are: error, warning, info, debug
logging.level: debug
logging.selectors: ["*"]

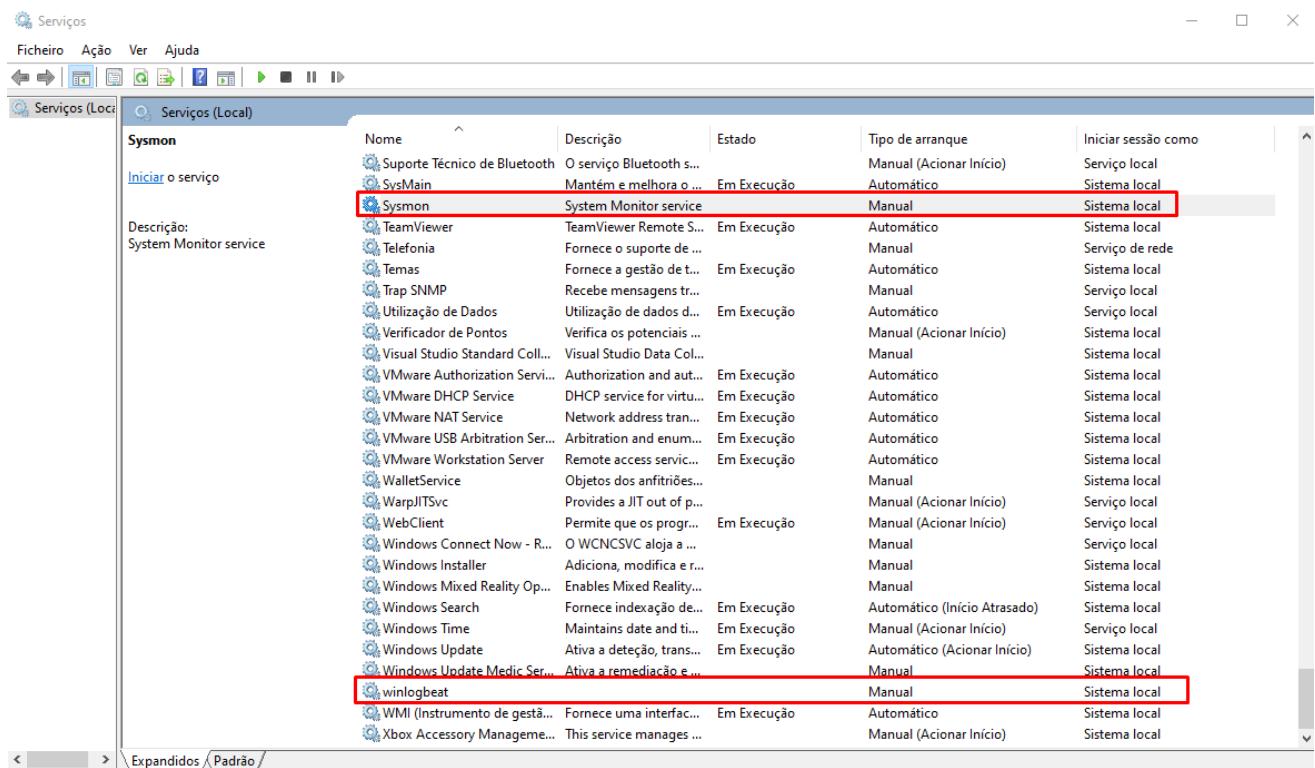
#Escrever os logs para um ficheiro
logging.to_files: true
logging.files:
    path: C:\Program Files\Winlogbeat\Logs
logging.level: info

```

Para a instalação do Sysmon, fez-se o download na página do Sysmon da Microsoft, de seguida é colocado os conteúdos do ficheiro para a pasta C:\Program Files\Sysmon. Por fim, a instalação é feita pela linha de comandos realizando os seguintes comandos.

```
C:\Program Files\Sysmon>sysmon -i sysmonconfig.xml -accepteula -h sha256 -l -n
```

Por fim, para verificar a instalação e funcionamento dos serviços, acedemos aos serviços, que pode ser acedido ao fazer Windows+R e escrever *services.msc*, e encontrar os serviços na lista.



Resumo dos *Beats*

A máquina em que o serviço vai estar instalado, não envia *logs* para o *Logstash* (não existem utilizadores a aceder às mesmas só os administradores), mas sim diretamente para o *Elasticsearch*.

Para iniciar, parar ou verificar o estado dos *Beats* podemos utilizar o comando *systemctl* e o nome do beat que enumeramos: auditbeat, heartbeat-elastic, Filebeat, Metricbeat, packetbeat

```
#iniciar o auditbeat automaticamente  
$sudo systemctl enable "beat name"  
  
#iniciar o serviço  
$sudo systemctl start "beat name"  
  
#parar o serviço  
$sudo systemctl stop "beat name"  
  
#verificar o estado do serviço  
$sudo systemctl status "beat name"
```

Instalação do APM server

Instalação e verificação:

```
curl -L -O https://artifacts.elastic.co/downloads/apm-server/apm-server-7.12.1-linux-x86_64.tar.gz  
tar xzvf apm-server-7.12.1-linux-x86_64.tar.gz
```

```
ubuntu@ubuntu:~$ sudo systemctl status apm-server.service
● apm-server.service - Elastic APM Server
   Loaded: loaded (/lib/systemd/system/apm-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-05-03 13:21:49 PDT; 14s ago
     Docs: https://www.elastic.co/solutions/apm
    Main PID: 5325 (apm-server)
      Tasks: 9 (limit: 9450)
     Memory: 13.0M
        CGroup: /system.slice/apm-server.service
                  └─5325 /usr/share/apm-server/bin/apm-server --environment systemd -c /etc/apm-server/apm-ser

mai 03 13:21:52 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:21:52.097-0700">>
mai 03 13:21:52 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:21:52.097-0700">>
mai 03 13:21:56 ubuntu apm-server[5325]: {"log.level":"error","@timestamp":"2021-05-03T13:21:56.070-0700">>
mai 03 13:21:56 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:21:56.070-0700">>
mai 03 13:22:02 ubuntu apm-server[5325]: {"log.level":"error","@timestamp":"2021-05-03T13:22:02.744-0700">>
mai 03 13:22:02 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:22:02.744-0700">>
mai 03 13:22:02 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:22:02.744-0700">>
mai 03 13:22:02 ubuntu apm-server[5325]: {"log.level":"info","@timestamp":"2021-05-03T13:22:02.744-0700">>
lines 1-20/20 (END)
```

Anexo B – Instalação e configuração do Grafana, Netdata e Prometheus

Sendo que de precisávamos de outras ferramentas para recolha de métricas diferentes do *Elastic Stack*, recorreu -se às seguintes ferramentas: Grafana, NetData e Prometheus.

A seguir é descrito por passos a instalação das três soluções referidas anteriormente.

Instalação do NetData¹⁰

Como o ubuntu 20.04 tem por defeito os pacotes NetData nos seus repositórios a instalação foi bastante simples é só fazer os seguintes passos.

```
$ sudo apt update
$ sudo apt install netdata
```

Fazer sudo nano /etc/netdata/netdata.conf e alterar o seguinte no ficheiro de configuração do NetData

```
[global]
run as user = netdata
web files owner = root
web files group = root
bind socket to IP = <ip da máquina>
```

De seguida reiniciar o serviço com o seguinte comando:

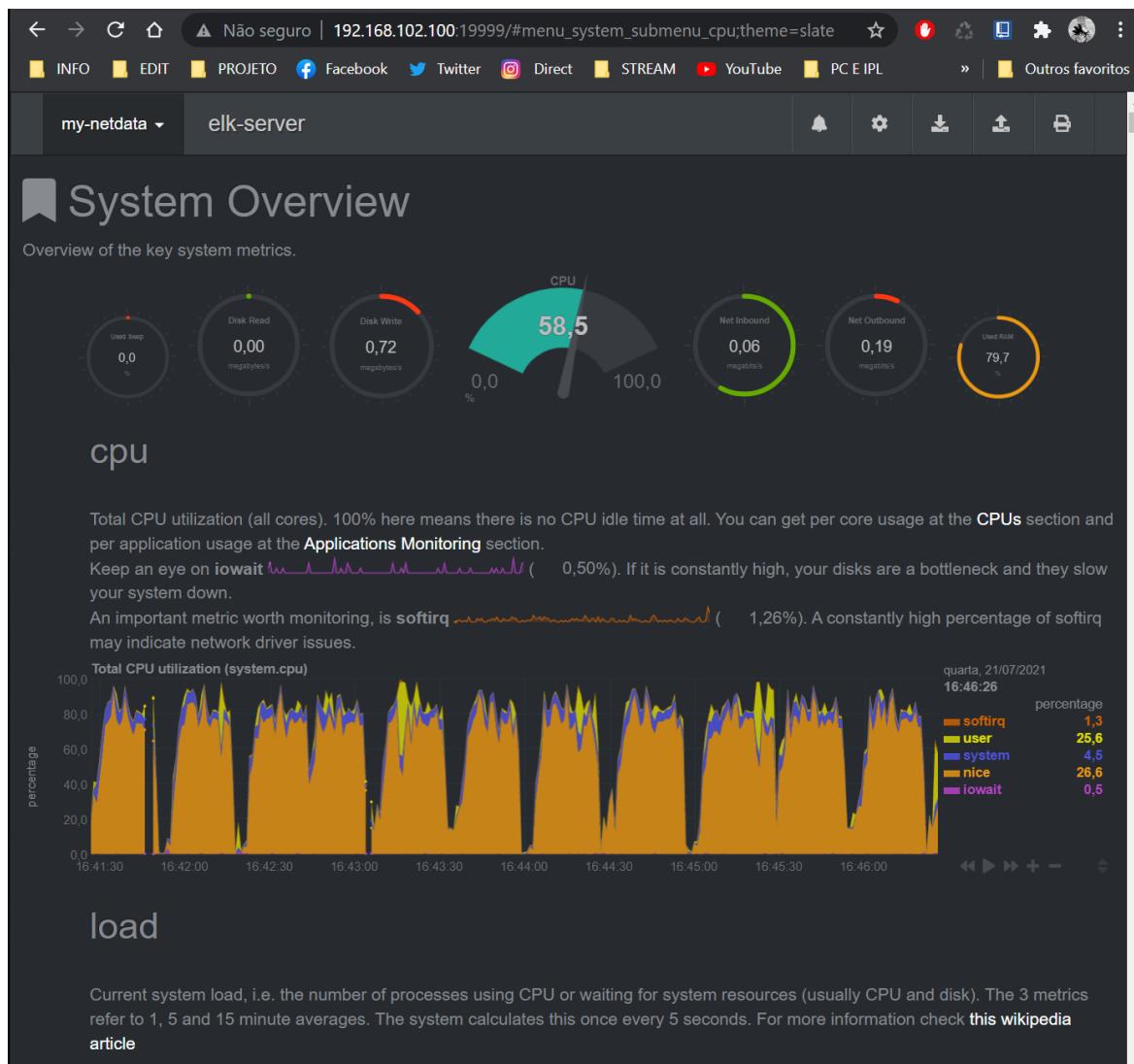
```
sudo systemctl restart netdata
```

Agora é só aceder à porta 19999 do IP do sistema onde foi instalado

```
http://< ip do sistema>:19999
```

¹⁰ <https://tecadmin.net/how-to-install-netdata-on-ubuntu-20-04/>

Foi instalado o NetData no servidor principal onde está o *ELASTIC STACK* e pode se visualizar na imagem seguinte.



Instalação do Prometheus¹¹

```
sudo apt-get update
```

Ir à página oficial do prometheus e fazer download da versão do Linux.

¹¹ <https://devopscube.com/install-configure-prometheus-linux/>

prometheus

The Prometheus monitoring system and time series database. [prometheus/prometheus](#)

2.3.2 / 2018-07-12 Release notes				
File name	OS	Arch	Size	SHA256 Checksum
prometheus-2.3.2.darwin-amd64.tar.gz	darwin	amd64	26.10 MiB	4c7475892eac1c94e4f2b91fdef3e8ba1835ece7d292d394db8eeda23ba45e48
prometheus-2.3.2.linux-amd64.tar.gz	linux	amd64	26.13 MiB	351931fe9bb252849b7d37183099047fbe6d7b79dcba013fb6ae19cc1bbd8552
prometheus-2.3.2.windows-amd64.tar.gz	windows	amd64	25.91 MiB	6eaefc996a1f6820b782a608f916c36725887a6f1dac604a3fe007cd6f8c4005

Ou fazer download da origem usando o curl e descomprimir através dos seguintes comandos.

```
curl -LO url -LO
https://github.com/prometheus/prometheus/releases/download/v2.22.0/prometheus-2.22.0.linux-amd64.tar.gz
```

```
### Se o download foi feito pelo site começar por aqui.
tar -xvf prometheus-2.22.0.linux-amd64.tar.gz
mv prometheus-2.22.0.linux-amd64 prometheus-files
```

Criar um user e as pastas onde o prometheus e outras ferramentas complementares para o seu funcionamento irão estar e dar permissões as pastas através dos seguintes comandos.

```
sudo useradd --no-create-home --shell /bin/false prometheus
sudo mkdir /etc/prometheus
sudo mkdir /var/lib/prometheus
sudo chown prometheus:prometheus /etc/prometheus
sudo chown prometheus:prometheus /var/lib/prometheus
```

Mover alguns ficheiros e dar permissão ao user prometheus.

```
sudo cp prometheus-files/prometheus /usr/local/bin/  
sudo cp prometheus-files/promtool /usr/local/bin/  
sudo chown prometheus:prometheus /usr/local/bin/prometheus  
sudo chown prometheus:prometheus /usr/local/bin/promtool  
sudo cp -r prometheus-files/consoles /etc/prometheus  
sudo cp -r prometheus-files/console_libraries /etc/prometheus  
sudo chown -R prometheus:prometheus /etc/prometheus/consoles  
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

Criar o ficheiro de configuração do prometheus.

```
sudo nano /etc/prometheus/prometheus.yml
```

Fazer as seguintes configurações:

```

global:
  scrape_interval:      10s
  evaluation_interval: 15s
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
        # - alertmanager:9093

rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

scrape_configs:
  - job_name: 'prometheus'
    metrics_path: '/api/v1/allmetrics?format=prometheus'
    static_configs:
      - targets: ['192.168.102.146:19999']

  - job_name: 'prometheus-elk'
    metrics_path: '/api/v1/allmetrics?format=prometheus'
    static_configs:
      - targets: ['192.168.102.100:19999']

```

Dar autorização ao user prometheus.

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

Criar o serviço prometheus.

```
sudo nano /etc/systemd/system/prometheus.service
```

Colocar o seguinte no ficheiro.

```
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
    --config.file /etc/prometheus/prometheus.yml \
    --storage.tsdb.path /var/lib/prometheus/ \
    --web.console.templates=/etc/prometheus/consoles \
    --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

Recarregar o serviço systemd para registar o prometheus como serviço e ligar o prometheus.

```
sudo systemctl daemon-reload
sudo systemctl start prometheus
```

Aceder ao prometheus na porta 9090.

```
http://<ip do servidor>:9090/graph
```

E assim será possível ter acesso ao prometheus no browser como mostrado na seguinte figura.

The screenshot shows the Prometheus web interface. At the top, there's a navigation bar with links for Prometheus, Alerts, Graph, Status, and Help. Below the navigation bar is a checkbox labeled "Enable query history". A search bar contains the placeholder "Expression (press Shift+Enter for newlines)". Below the search bar are two buttons: "Execute" (highlighted in blue) and "- insert metric at cursor -". Underneath these buttons are two tabs: "Graph" (selected) and "Console". A table below the tabs has columns for "Element" and "Value". The table displays the message "no data". At the bottom left, there's a button labeled "Add Graph".

Instalação do Grafana¹²

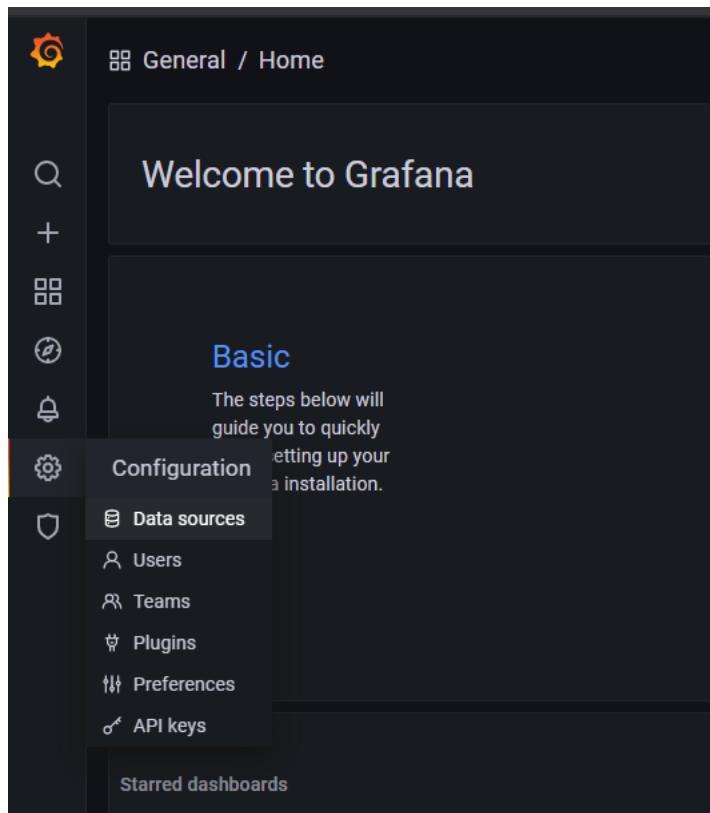
A instalação do grafana tem como referência a própria documentação do mesmo, mas como pode ser confuso, segue-se os comandos para a instalação do grafana.

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
echo "deb https://packages.grafana.com/enterprise/deb stable main" | 
sudo tee -a /etc/apt/sources.list.d/grafana.list
sudo apt-get update
sudo apt-get install grafana
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl status grafana-server
```

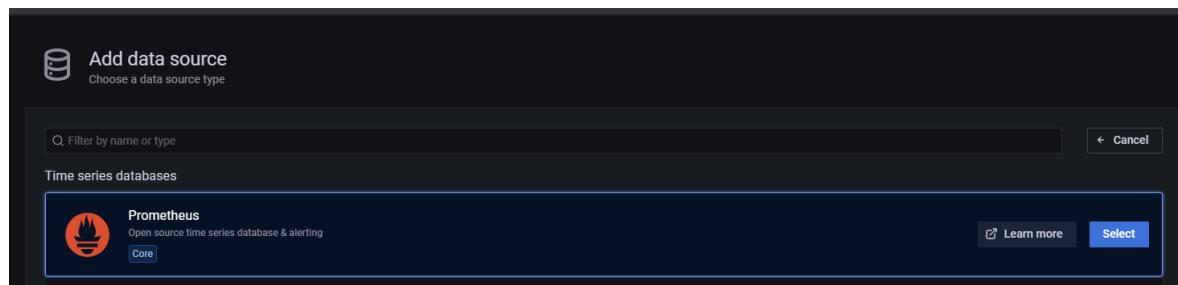
Após estes comandos aceder ao *https://<ip da máquina>:3000*.

No Grafana aceder ao menu Configuration -> Data sources (FIGURA)

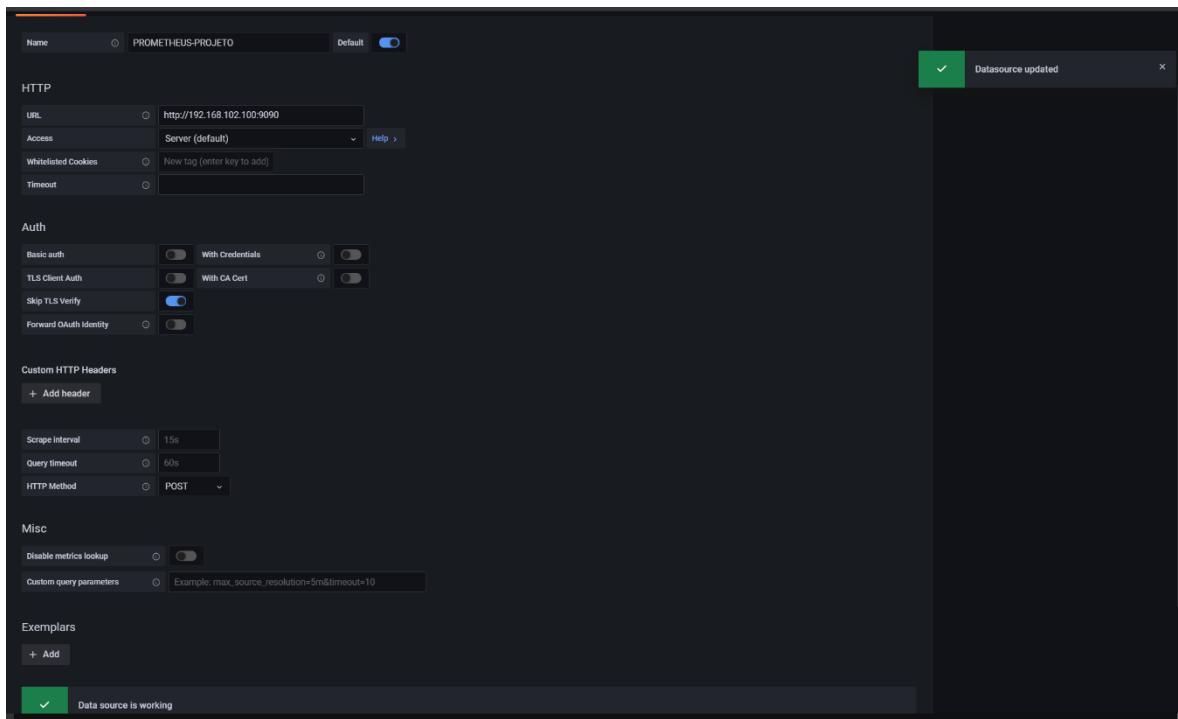
¹² <https://devconnected.com/how-to-install-grafana-on-ubuntu-20-04/>



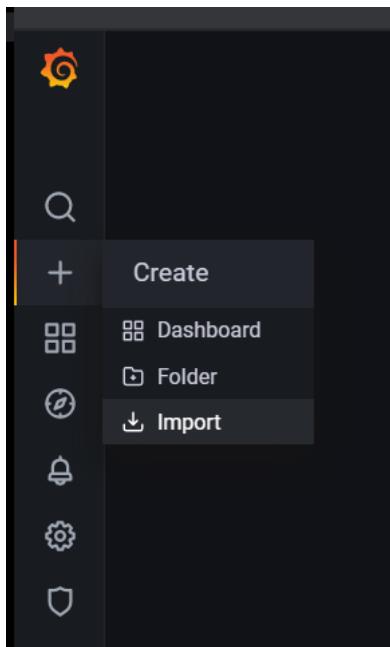
Adicionar Prometheus como Data Source.

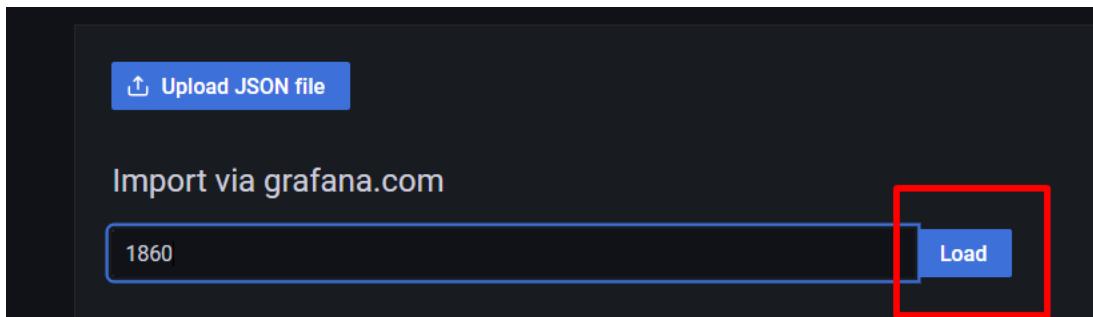


Adicionar o IP e porta e guardar (FIGURA).

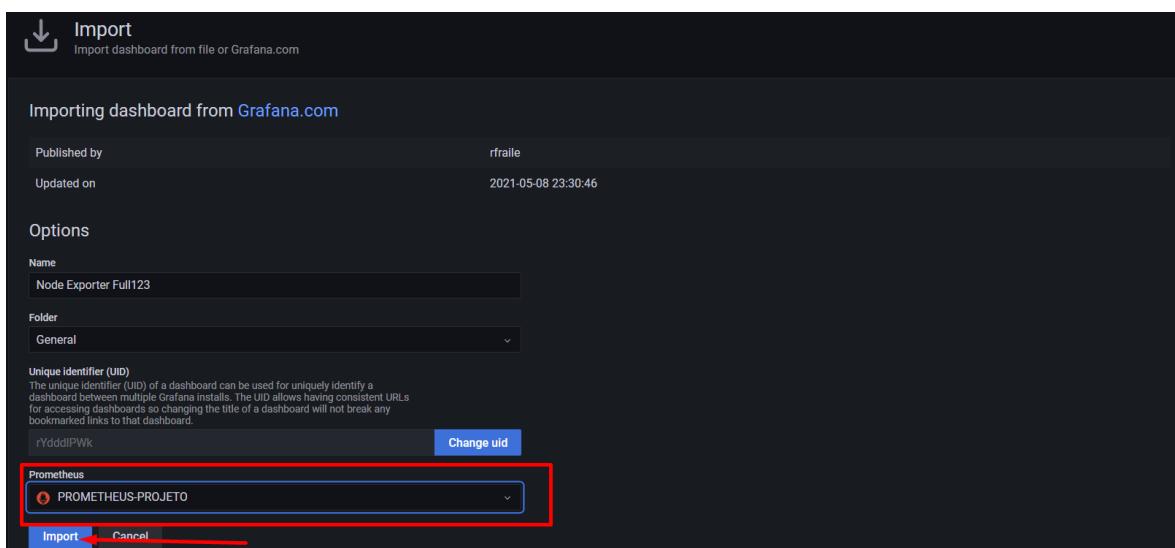


Adicionar uma *Dashboard* como esta representado nas seguintes Figuras.

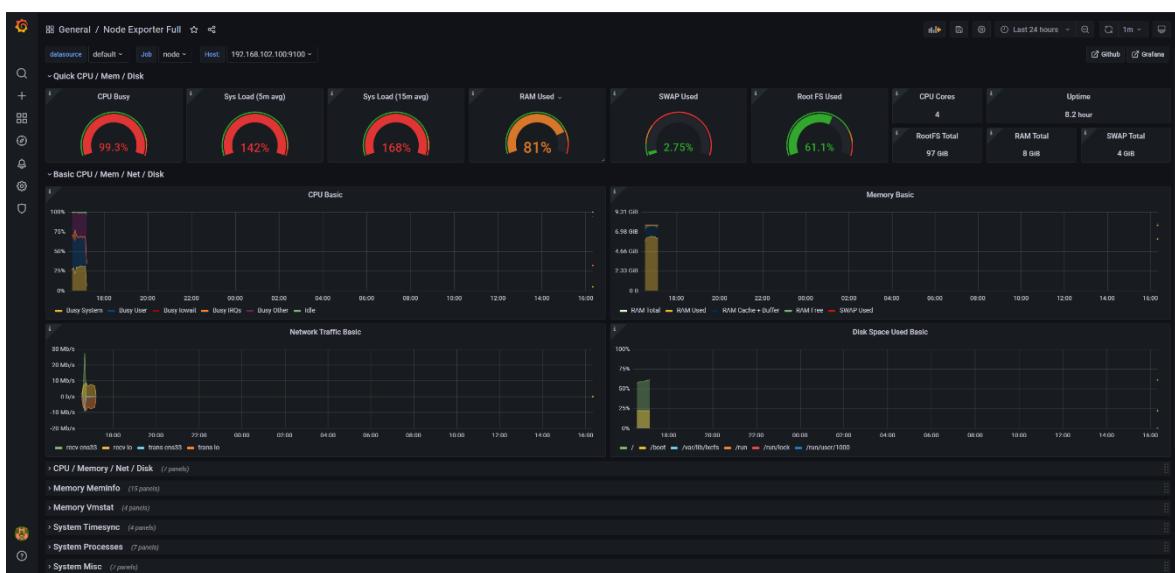




No menu do import da *dashboard* adicionar a data source que foi feita anteriormente.



Quando aceder a *dashboard* o resultado deverá ser o seguinte.



Anexo C – Certificado SSL

Para poder usufruir de uma licença no *Elasticsearch* (mesmo a versão gratuita) é obrigatório o uso de TLS/SSL para comunicação de transporte e tem de ser configurado manualmente e corretamente. Não esquecendo o fato que uma vez que temos o modulo de segurança ativo, todas as comunicações entre o *Kibana/Elasticsearch* e as outras aplicações são autenticadas.

A configuração de segurança TLS/SSL ainda é longa, portanto, este anexo contém todos os passos que se devem tomar tais como: habilitar a segurança; configurar TLS / SSL.

De seguida estão passo a passo os comandos e configurações necessárias.

No ficheiro de configuração do *Elasticsearch* adicionar a seguinte linha:

NOTA: Caso estiver em *cluster* tem de adicionar a linha em cada node

```
xpack.security.enabled: true
```

O protocolo de transporte é usado para a comunicação entre cliente e servidor, todos os certificados de transporte devem ser certificados de cliente e servidor

O *Elasticsearch* vem com uma ferramenta chamada de *Elasticsearch-certutil* que é usado para gerar certificados autoassinados que criptografam as comunicações internas do *Elasticsearch*

Segue-se então os passos de como gerar os certificados.

Aceder à pasta do *Elasticsearch* e no /bin usar o gerador de certificados com os seguintes comandos:

```
bin/elasticsearch-certutil ca
ENTER ENTER
bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12
ENTER ENTER ENTER
```

Assim que os comandos forem executados, teremos certificados TLS / SSL.

Os certificados criados deveram ser postos numa subdiretoria /certs na pasta do *Elasticsearch* para mais tarde serem especificados.

Os certificados serão então especificados no ficheiro de configuração *Elasticsearch.yml* da seguinte forma:

```
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: certs/elastic-certificates.p12
```

Normalmente, os certificados seriam assinados por um CA oficial dentro de uma organização. No entanto, como já usamos uma CA autoassinada, também assinamos os nossos certificados de cliente http com a mesma CA autoassinada que salvamos anteriormente como elastic-stack-ca.p12.

Podemos criar um certificado para autenticação de cliente da seguinte maneira:

```
bin/elasticsearch-certutil cert --ca \
config/certs/elastic-stack-ca.p12 \
-name
ENTER
client.p12 ENTER
ENTER
```

Para usar este certificado cliente.p12, é necessário dividi-lo em 3 chaves: chave privada, certificado público e certificado CA.

Isto é feito através dos seguintes comandos:

Private Key

```
openssl pkcs12 -in client.p12 -nocerts -nodes > client.key
```

Public Certificate

```
openssl pkcs12 -in client.p12 -clcerts -nokeys > client.cer
```

CA Certificate

```
openssl pkcs12 -in client.p12 -cacerts -nokeys -chain > client-ca.cer
```

Apos ter estes certificados criados, coloca los na pasta do *Kibana* numa pasta chamada /certs para mais tarde no ficheiro de configuração do *Kibana*

Configure *Kibana* para autenticar para *Elasticsearch*

Agora as comunicações devem ser autenticadas, ou seja, deve se ativar para a autenticação como user ser em https.

Itso pode ser feito com as seguintes linhas no arquivo *Kibana.yml*:

```
elasticsearch.url: "https://localhost:9200"
xpack.security.enabled: true
elasticsearch.username: "<utilizador do elastic >"
elasticsearch.password: "Password do elastic"
elasticsearch.ssl.certificateAuthorities: config/certs/client-ca.cer
elasticsearch.ssl.verifyMode: certificate
```

Certificar de alterar *localhost* para o nome do *Elasticsearch* e de que os certificados estão disponíveis na diretoria config / certs dentro da pasta *Kibana*.

O user *Kibana* é como uma conta de serviço que funciona nos bastidores para autenticar o aplicativo *Kibana* no cluster *Elasticsearch*.

Agora é só reiniciar o *Kibana* para que seja autenticado no *Elasticsearch* como user *Kibana*. Agora é possível fazer login pelo UI do *Kibana* como superuser (https).

Anexo D – TLS

Para poder ter acesso a algumas funcionalidades do *ELASTIC STACK* como por exemplo o alerting, foi necessário realizar a autenticação TLS entre o *Kibana* e o *Elasticsearch*, que passa por criar alguns certificados através do *Kibana* encryption key generator e colocar as keys geradas no ficheiro de configuração do *Kibana*.

Este anexo tem como objetivo mostrar como foram geradas as keys e como é feita a autenticação TLS entre o *Kibana* e o *Elasticsearch*.

Segue então os passos para o mesmo:

1º passo – Através da pasta do *Kibana* (/usr/share/Kibana) executar o seguinte comando para gerar as keys:

```
kibana-encryption-keys generate -l
```

Apos fazer este comando ira aparecer o processo para as definições das keys é só fazer yes em todos como na figura seguinte.

```
root@ubuntu:/usr/share/kibana# bin/kibana-encryption-keys generate -l
## Kibana Encryption Key Generation Utility
The 'generate' command guides you through the process of setting encryption keys for:
xpack.encryptedSavedObjects.encryptionKey
  Used to encrypt stored objects such as dashboards and visualizations
  https://www.elastic.co/guide/en/kibana/current/xpack-security-secure-saved-objects.html#xpack-security-secure-saved-objects

xpack.reporting.encryptionKey
  Used to encrypt saved reports
  https://www.elastic.co/guide/en/kibana/current/reporting-settings-kb.html#general-reporting-settings

xpack.security.encryptionKey
  Used to encrypt session information
  https://www.elastic.co/guide/en/kibana/current/security-settings-kb.html#security-session-and-cookie-settings

Already defined settings are ignored and can be regenerated using the --force flag. Check the documentation links for instructions on how to rotate encryption keys.
Definitions should be set in the kibana.yml used configure Kibana.

This tool will ask you a number of questions in order to generate the right set of keys for your needs.

Set xpack.encryptedSavedObjects.encryptionKey? [y/N] y
Set xpack.reporting.encryptionKey? [y/N] y
Set xpack.security.encryptionKey? [y/N] y

The following keys were generated:
xpack.encryptedSavedObjects.encryptionKey
xpack.reporting.encryptionKey
xpack.security.encryptionKey

Save generated keys to a sample Kibana configuration file? [y/N] y
What filename should be used for the sample Kibana config file? [/etc/kibana/kibana.sample.yml]
Write configuration to /etc/kibana/kibana.sample.yml
```

Depois é pegar no que esta no ficheiro *Kibana.sample.yml* e colocar no ficheiro de configuração do *Kibana*.

```
-----kibana.yml-----
xpack.encryptedSavedObjects.encryptionKey: 2d90ee929402f3997d498bed2cb6d7c8
xpack.reporting.encryptionKey: 3179628c55f585a9cde8ba3857a070df
xpack.security.encryptionKey: 06c13231461388862b1b24ce6cbb10c5
```

Depois destas configurações poderá se verificar no *Kibana* se existe a possibilidade de criar um alerta (FIGURA).

Alerts and Actions  Documentation

Detect conditions using alerts, and take actions using connectors.

[Alerts](#) [Connectors](#)

 Create your first alert

Receive an alert through email, Slack, or another connector when a condition is met.

[Create alert](#)

Anexo E – Instalação do Elastalert

Previamente a instalação do Elastalert é necessário instalar o Python 3.8, pip3 e todos os componentes num ficheiro contido na pasta do Elastalert, a seguir estão os comandos necessários a fazer:

```
sudo apt-get install python3
sudo apt-get install pip3
git clone https://github.com/jertel/elastalert2.git
cd elastalert/
pip3 install "setuptools>=11.3"
python3 setup.py install
pip3 install "elasticsearch>=5.0.0"
pip3 install -r requirements.txt
cp config.yaml.example config.yaml
sudo elastalert-create index
```

No ficheiro config.yaml adicionar as seguintes linhas:

```
# Connect with TLS to Elasticsearch
use_ssl: True
# Verify TLS certificates
verify_certs: False
# GET request with body is the default option for Elasticsearch.
# If it fails for some reason, you can pass 'GET', 'POST' or 'source'.
# See
http://elasticsearchpy.readthedocs.io/en/master/connection.html?highlight=send_get_body_as#transport
# for details
#es_send_get_body_as: GET
# Option basic-auth username and password for Elasticsearch
es_username: <user do elasticsearch>
es_password: <password do elasticsearch>
# Use SSL authentication with client certificates client_cert must be
# a pem file containing both cert and key for client
#verify_certs: True
client_cert: /etc/elasticsearch/certs/client.cer
client_key: /etc/elasticsearch/certs/client.key
```

Configurações Slack

Foi criada uma conta no Slack para testar o envio dos alertas para a plataforma. O motivo de ter sido escolhido esta plataforma, foi pela opção de adicionar diferentes apps, tendo sido adicionado a App Incoming WebHooks e Slagram.

Adicionar apps para # projeto-de-curso

[Ver Diretório de apps](#)

Pesquisar por nome ou categoria (por exemplo, produtividade, vendas)


Slagram

Slack <-> Telegram

[Ver](#)

Incoming WebHooks
[Ver](#)

Configurações de integração

Postar no canal

As mensagens enviadas ao webhook de entrada serão postadas aqui.

▼
[ou crie um novo canal](#)

URL do webhook

Enviar cargas JSON para este URL.
[Mostrar instruções de instalação](#)

[Copiar URL](#) • [Gerar novamente](#)

Foi também adicionado ao canal do Slack, a App do Slagram, que nos permite receber os alertas na aplicação do Telegram no telemóvel.

De mencionar que esta aplicação é paga com um pequeno período de testes gratuitos.

Testes de alertas

Para testar o funcionamento do Elastalert, foi criado uma regra chamada de frequency.yaml, baseando numa regra exemplo já disponibilizada.

```
frequency.yaml

name: slack-demo

type: frequency

index: filebeat-*

num_events: 3

timeframe:
  hours: 1

filter:
- term:
    process.name: "TESTE"

alert:
- "slack"
slack:
slack_webhook_url:
"https://hooks.slack.com/services/T026QN4AGAZ/B0276DS120Z/3j4LI7YYbMM6
qn9Nosa1hWRo"
alert_text_type: exclude_fields
slack_emoji_override: ":alert:"
slack_msg_color: "warning"
```

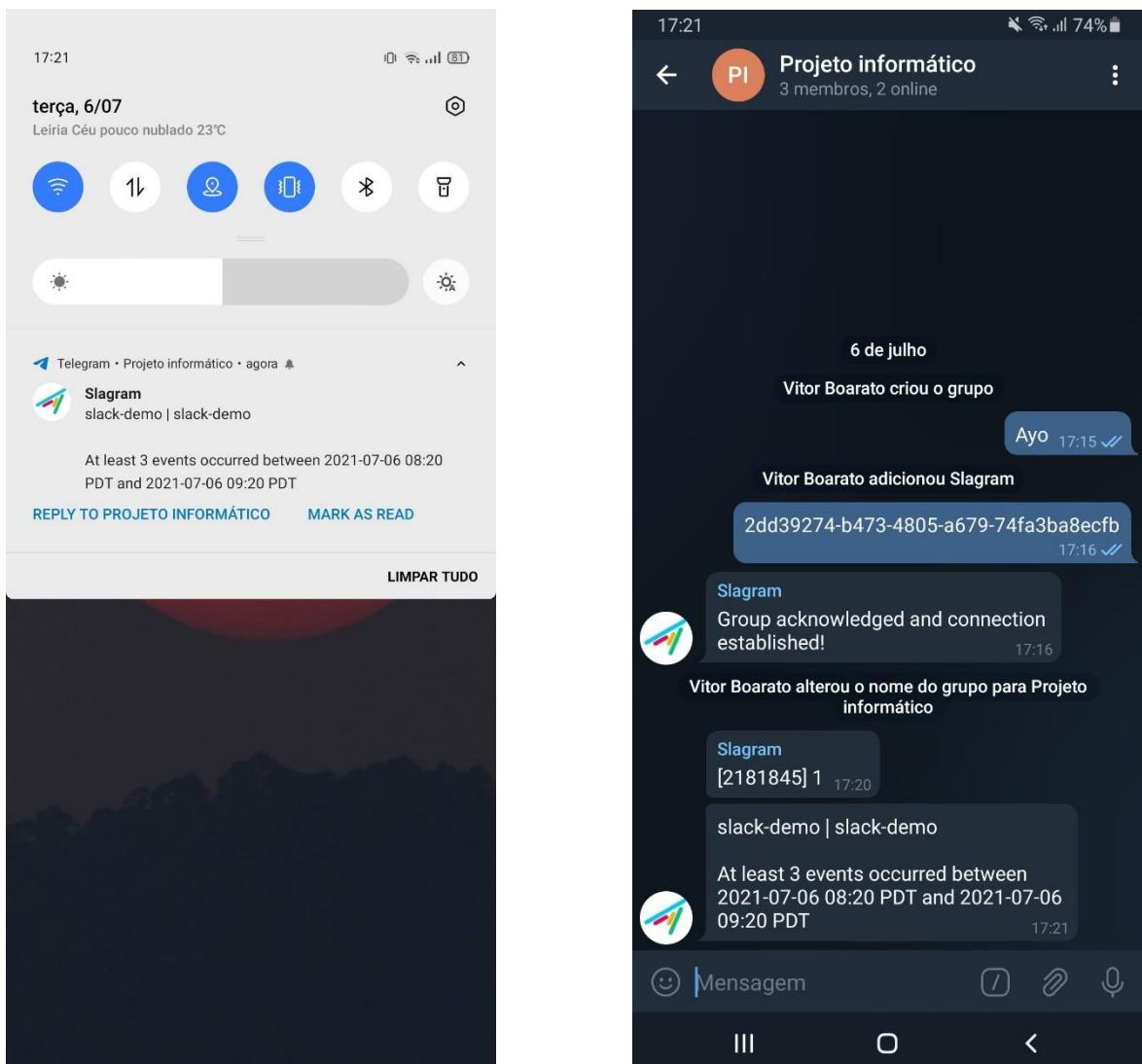
A regra foi testada através de um logger.

```
ubuntu@ubuntu:~$ sudo logger -t TESTE "mensagem teste"
ubuntu@ubuntu:~$ frequency.yaml
frequency.yaml

0 / 0 hits
its (0 already seen), 0 matches, 0 alerts sent

7 / 7 hits
ified HTTPS request is being made to host 'hooks.slack.com'.
nings

INFO:elastalert:Alert 'slack-demo' sent to Slack
INFO:elastalert:Ignoring match for silenced rule slack-demo
INFO:elastalert:Ran slack-demo from 2021-07-06 08:21 PDT to 2021-07-06 08:23 PDT: 7 query hits (0 already seen), 2 matches, 1 alerts sent
^CINFO:elastalert:SIGINT received, stopping ElastAlert...
ubuntu@ubuntu:~/Desktop/elastalerts
```



Anexo F - Alertas do Kibana

Para que fosse possível criar alertas com o *Kibana*, foi primeiro necessário ativar o TLS entre o *Kibana* e *Elasticsearch*, que também está documentado no anexo D -TLS.

As regras podem ser criadas e alteradas em Stack Management / Rules and Connectors.

Criação de uma regra

Create rule

Name: Windows Malware Detection

Tags (optional): windows

Check every: 1 minute

Notify: Only on status change

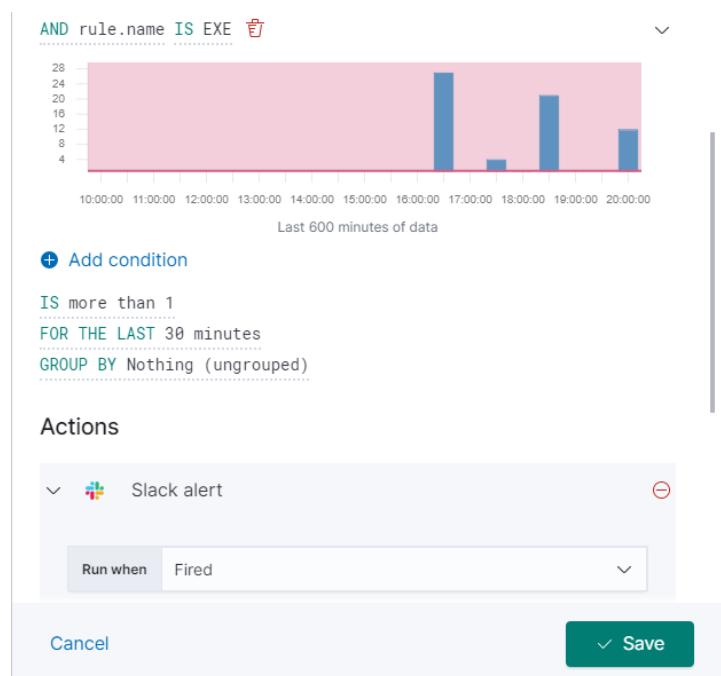
Log threshold: Alert when the log aggregation exceeds the threshold. Documentation

WHEN THE count OF LOG ENTRIES

WITH agent.type IS winlogbeat

Last 40 hours of data

AND file.path.text MATCHES C:\Windows



A regra demonstrada, foi referida no teste do ataque de PsExec no capítulo 7.1.1.