UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Segurança Cibernética: Proposta de Implementação de uma Plataforma SIEM

Caso de Estudo:

Instituto Nacional de Tecnologias de Informação e Comunicação, IP

Autor:

MASSUNGUINE, Gilvaldo Pedro

Supervisor:

Eng.º Délcio Arnaldo Chadreca

Supervisor no INTIC:

Prof. Doutor Eng.º Lourino Alberto Chemane

Maputo, Agosto de 2022.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Segurança Cibernética: Proposta de Implementação de uma Plataforma SIEM

Caso de Estudo:

Instituto Nacional de Tecnologias de Informação e Comunicação, IP

Autor:

MASSUNGUINE, Gilvaldo Pedro

Supervisor:

_____

Eng.º Délcio Arnaldo Chadreca

Supervisor no INTIC:

_____

Prof. Doutor Eng.º Lourino Alberto Chemane

Maputo, Agosto de 2022.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTRÓTECNICA

TERMO DE ENTREGA DE RELATÓRIO DE ESTÁGIO PROFISSIONAL

Declaro que o estudante **Gilvaldo Pedro Massunguine** entregou no dia 15/08/2022, às 03 cópias do seu relatório de Estágio Profissional com referência **2021EIEPD217**, intitulado: Segurança Cibernética: Proposta de Implementação de uma Plataforma de SIEM. Caso de Estudo: INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação, IP.

Maputo, 15 de Agosto de 2022.

A Chefe da Secretaria do DEEL

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTRÓTECNICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, 15 de Agosto de 2022.

O Autor

_____

(Gilvaldo Pedro Massunguine)

Dedicatória

À todos que sempre acreditaram no meu potencial e investiram em mim, em especial aos meus pais, Rui Paulo Pedro Massunguine & Maria Helena Matola.

Agradecimentos

Em primeiro lugar, agradeço a Deus, pelo dom da vida, e por todas as outras coisas que me acrescentou para que eu pudesse realizar este sonho.

À minha querida Mãe, Maria Helena Matola que nunca mediu esforços e investiu tudo o que esteve ao seu alcance para me ver progredir na vida, sempre esteve ao meu lado apoiando e dando forças para que eu nunca perdesse o foco e que batalhasse para alcançar os meus objectivos.

Ao meu Pai, Rui Paulo Pedro Massunguine, por acreditar no meu potencial, pelo seu apoio e os seus sábios conselhos que conduziram durante este longo percurso.

Aos meus Avôs, Júlio Massunguine e Laura Massunguine (em memória), que juntos aos meus Pais fizeram de tudo para que nada me faltasse, serei eternamente grato.

À minha família, em especial aos meus irmãos Fernando e Yuran Massunguine, ao meu Tio Agostinho Matola, as minhas Tias Sara Matola (em memória) & Salda Matola e a minha Madrinha Amélia Munguambe pelo apoio que sempre deixaram ficar e pela disponibilidade em me ajudar nos momentos em que mais precisei.

À minha namorada Felayne Sitoe, pelo amor, por estar sempre comigo me ajudando a enfrentar vários obstáculos que têm surgido pelo caminho, transmitindo confiança e motivação para que eu siga em frente em busca dos meus sonhos!!

Ao meu supervisor Eng. Délcio Arnaldo Chadreca, que para além de ser um excelente profissional é também umas das minhas principais fontes de inspiração nesta área, agradeço por ter me orientado e partilhado as suas ideias durante a realização deste trabalho, e pela oportunidade de poder trabalhar consigo como Monitor nas cadeiras em que leciona.

Ao terminar esta etapa particularmente importante da minha vida, não poderia deixar de expressar o meu agradecimento à instituição Faculdade de Engenharia da UEM e aos docentes do Departamento de Engenharia Electrotécnica (DEEL), essenciais no meu processo de formação académico, pela dedicação e por todo conhecimento que partilharam durante o período em que estive vinculado à FENG.

Agradeço a todos os meus colegas do curso, com quem convivi intensamente durante os últimos anos, pelo companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando, espero que possamos trabalhar juntos novamente, nomeadamente: António João Cossa, Pedro Madabula, Tomás Mondlane, Hélio C. Chaúque, Luís Macuvele, Luís Cossa, Fátima Massicame, Rafael Stoner, Cany Mangue, Sara Tivana, Raimundo Dias Jr. e Carson Simbine.

Ao Instituto Nacional de Tecnologias de Informação e Comunicação, pelo acolhimento e excelente ambiente de trabalho no qual fui inserido, podendo desta forma, aprimorar os meus conhecimentos, um especial e profundo agradecimento ao meu supervisor nesta instituição o Prof. Doutor Eng. Lourino Alberto Chemane, pelos incentivos e apoio disponibilizado.

Ao Eng. Sérgio Henrique Guivala, que me propôs o título deste trabalho de pesquisa, ao Eng. Hélder Fernando, ao Eng. Jeremias Zunguza, e aos meus colegas do estágio, nomeadamente: à Catarina B. Maxaieie, o Carlos G. Mussa, à Maria Isabel Mucombo, o Sérgio Mussica Jr., o Kelvin Lukanga e a Esselina Magandane.

Um especial agradecimento ao Óscar Chissano “Rustóbe”, pelo suporte que sempre me tem prestado principalmente na área académica, não podia deixar de referir que a sua dedicação e genialidade me motivaram bastante, e isso foi crucial para o meu desenvolvimento!

Aos meus amigos, que apesar de todas as dificuldades enfrentadas sempre me acompanharam, motivaram e não deixaram desanimar durante este longo percurso, para não me estar a esquecer de ninguém, diria “vocês sabem quem são”, mas enfim, um abraço para eles: Alberto B. Senda, Domingos L. Vicente, Joaquim Mazanalo M., João Sérgio Dimande, Humberto Tandane Jr., Glenda Matilde Chalufo, Milton Cabral, Shelsea Massango, Margarida Libombo e ao Edson Panguana.

À todos que directa ou indirectamente contribuíram para a materialização do presente trabalho de pesquisa e que não foram referidos anteriormente.

Epígrafe

“Se você tem um objectivo e o mesmo não te tira o sono, certamente esse é o objectivo de qualquer um e não o seu!”

Edson Alberto Cossa *(In memoriam)*

Resumo

Hoje em dia, é inegável que um dos maiores desafios das empresas e instituições é o de garantir a segurança dos seus activos na sua infra-estrutura de rede corporativa. A monitorização e a detecção de padrões comportamentais indesejáveis em tempo útil é de crucial importância para criar uma defesa forte contra eventuais adversários, desta forma, os profissionais de TI, precisam aceder, monitorizar e analisar cada um dos logs gerados pelos mecanismos de segurança, aplicações e dispositivos de rede, o que é uma tarefa deveras lenta e custosa porque esses componentes geram uma enorme quantidade de logs. As plataformas SIEMs podem ajudar a ultrapassar os referidos desafios, pois estas soluções permitem aos seus utilizadores ter uma visão global sobre o que acontece em tempo real numa infra-estrutura de rede corporativa. Colectando e consolidando os logs gerados num único repositório central é possível monitorizar, automatizar o processo de análise e correlacionar eventos de forma a detectar automaticamente comportamentos indesejáveis para que rapidamente sejam eliminadas as hipóteses de um possível ataque bem-sucedido. Nesta perspectiva, o principal objectivo do trabalho é de propor a implementação de uma plataforma SIEM para detecção e mitigação de ataques cibernéticos sofisticados no INTIC. Para tal, foi feita uma análise da segurança cibernética na infra-estrutura de rede corporativa do INTIC e de seguida foi realizada uma pesquisa bibliográfica e documental sobre os principais mecanismos de segurança utilizados actualmente, eventos e incidentes de segurança, e por fim debruçou-se em torno das plataformas SIEM e as principais soluções de código fonte aberto/fechado, comercias ou grátis utilizadas actualmente. Tendo como base o relatório da Gartner 2020, foram recolhidos os dados sobre as soluções disponíveis e foram consideras para a análise comparativa as soluções IBM QRadar, Splunk e AlienVault OSSIM. A partir dessa análise comparativa, chegou-se a conclusão de que a solução que melhor se adequa as condições e realidade actual do INTIC é AlienVault OSSIM e de seguida propôs-se a sua implementação. Houve a necessidade de se criar uma infra-estrutura de rede corporativa virtualizada similar a do INTIC com recurso a ferramenta de virtualização VMware *Workstation* para testar a solução num ambiente próximo do “real”.

Palavras-chave: Segurança Cibernética, Infra-estrutura de Redes Corporativas, …, SIEM, Eventos (logs).

Abstract

Nowadays, it is undeniable that one of the biggest challenges for companies and institutions is to guarantee the security of their assets in their corporate network infrastructure. Timely monitoring and detection of undesirable behavioral patterns is of crucial importance to create a strong defense against possible adversaries, in this way, IT professionals need to access, monitor and analyze each of the logs generated by security mechanisms, applications and network devices, which is a very slow and costly task because these components generate a huge amount of logs. SIEMs platforms can help overcome these challenges, as these solutions allow users to have a global view of what happens in real time in a corporate network infrastructure. By collecting and consolidating the logs generated in a single central repository, it is possible to monitor, automate the analysis process and correlate events in order to automatically detect undesirable behavior so that the chances of a possible successful attack are quickly eliminated. In this perspective, the main objective of the work is to propose the implementation of a SIEM platform for detection and mitigation of sophisticated cyber-attacks in INTIC. To this end, an analysis was made of cybersecurity in INTIC's corporate network infrastructure and then a bibliographic and documentary research was carried out on the main security mechanisms currently used, security events and incidents, and finally around SIEM platforms and the main open/closed source, commercial or free source solutions used today. Based on the Gartner 2020 report, data on available solutions were collected and IBM QRadar, Splunk and AlienVault OSSIM solutions were considered for comparative analysis. From this comparative analysis, it was concluded that the solution that best suits the conditions and current reality of INTIC is AlienVault OSSIM and then its implementation was proposed. There was a need to create a virtualized corporate network infrastructure similar to that of INTIC using the VMware Workstation virtualization tool to test the solution in an environment close to the “real”.

Keywords: Cyber Security, Corporate Network Infrastructure, SIEM, Events (logs).

Índice

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e acrónimos

ACL	Access Lists Control
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
HIDS	Host-Based Intrusion Detection System
IDS	Sistema de Detecção de Intrusão
INTIC	Instituto Nacional de Tecnologias de informação e Comunicação
IP	Internet Protocol
IPS	Sistema de Prevenção de Intrusão
ISP	Internet Service Provider
NAT	Network Address Translation
NIDS	Network-Based Intrusion Detection System
OSSIM	Open-Source Security Information Management
PENSC	Plano Estratégico Nacional de Segurança Cibernética
SI	Sistemas de Informação
SIEM	Security Information and Event Management
SNAT	Source Network Address Translation
SOC	Security Operation Center
TI	Tecnologias de Informação
TICS	Tecnologias de Informação e Comunicação
USM	Unified Security Management
UEBA	User and Entity Behavior Analytics
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

Glossário de termos

- **Activo**

É um recurso corporativo que possui valor para a organização, deve ser protegido de acordo com práticas e políticas que garantam a sua confidencialidade, integridade e disponibilidade. Um activo pode ser lógico, como um *site*, informações ou dados; ou ainda, um activo pode ser físico, como uma pessoa, computador etc. Activos como as informações no formato digital são o foco dos esforços de segurança cibernética.

- **Ameaça**

Uma categoria de objectos, pessoas ou outras entidades que representam um perigo para os activos, ou seja, qualquer factor ou acção capaz de interferir ou causar danos aos pilares da segurança da informação de um activo. Em suma, as ameaças estão sempre presentes e podem ser intencionais ou não intencionais.

- **Ataque Cibernético**

Conjunto de acções ilícitas e deliberadas que podem ser manuais ou automáticas que tem como objectivo explorar as vulnerabilidades com a intenção de quebrar os pilares da segurança da informação de um activo no ambiente digital.

- **Continuidade de negócios**

Processo capaz de proporcionar a uma organização um nível de funcionamento operacional suficiente após interrupções ou incidentes de negócios.

- **Defesa de perímetro**

Consiste em proteger a rede da empresa ou instituição contra ameaças vindas do ambiente externo, ou seja, serve fundamentalmente para restringir as interações entre domínios de segurança.

- ***Exploit***

É um programa que se aproveita de uma vulnerabilidade de um sistema para desta forma tentar obter o controlo do sistema. Habitualmente essas vulnerabilidades são reportadas pela entidade criadora do software que consequentemente desenvolve um *patch* para a correcção, porém estas correcções nem sempre são instaladas.

- **Exploração**

É uma técnica usada para comprometer um sistema. Ou seja, uma exploração pode ser um processo documentado para tomar vantagem de uma vulnerabilidade ou exposição, geralmente em *software*, que é inerente ao *software* ou é criado pelo invasor. *Exploits* fazem uso de ferramentas de *software* existentes ou componentes de *software* personalizados.

- **Informação no formato/meio digital**

Compreende um ambiente de troca de informações em formato electrónico (números, letras, caracteres), onde são inseridos e compartilhados diferentes tipos de conteúdo, que proporcionam interacção entre as pessoas localmente ou a distância.

- **Infra-estrutura de Rede Corporativa**

Compreende o conjunto de componentes (dispositivos de rede, sistemas, servidores, mecanismos de segurança, entre outros) necessários para a operação e gestão de serviços de TI em ambientes corporativos.

- **Internet**

Sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos TCP/IP com o propósito de servir progressivamente usuários no mundo inteiro.

- **Mecanismos de Segurança**

Conjunto de ferramentas, técnicas e métodos que são utilizados para implementar os serviços de segurança.

- **Mitigação**

São um conjunto de estratégias adoptadas por uma organização para identificar potenciais riscos e ameaças para actuar de forma a minimizar seus impactos nas operações do negócio.

- **Open-source**

Software cujo código fonte está disponível para todos, não só o código fonte, mas o *software* em si, isto é, completamente livre para todos, no qual o direito autoral fornece o direito de estudar, modificar e distribuir de graça independentemente da finalidade.

- **Perímetro de segurança ou rede**

É a linha virtual que separa a infra-estrutura de rede interna de uma organização, tão segura e controlada quanto possível, do exterior, de redes inseguras e sobre as quais não temos qualquer tipo de controlo.

- **Sistemas Computacionais**

Consiste num conjunto de dispositivos electrónicos (*hardware*) capazes de processar informações de acordo com um programa (*software*).

- **Tecnologias de Informação**

Conjunto de todas as actividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

- **Vírus**

São programas maliciosos que infectam os sistemas modificando e corrompendo os ficheiros. A contaminação dos sistemas ocorre habitualmente pela acção do utilizador que executa um determinado programa que à partida pode parecer inofensivo. A sua detecção é feita pelos Antivírus que contêm uma base de dados de assinaturas e pedaços de código de vírus podendo desta forma reconhecê-los e em alguns casos até corrigir os ficheiros infectados.

- **Vulnerabilidade**

É uma característica de um activo (por exemplo um sistema) que o torna susceptível a certos ataques, é uma fraqueza que pode ser explorada com intenções maliciosas. Alguns exemplos de vulnerabilidades são uma falha em um pacote de *software*, uma porta de sistema desprotegida ou uma porta destrancada.

1. Capítulo I – Introdução

1.1. Contextualização

Nas empresas e instituições, activos como informações no formato digital são um dos bens mais importantes. Com a tendência desses activos encontrarem-se num meio digital, a segurança cibernética surge da necessidade de garantir a confidencialidade, integridade e disponibilidade dos mesmos, tornando-se desta forma, indispensável para a continuidade de negócios.

Preocupados em proteger as suas informações no ambiente digital, empresas e instituições, dispõem de profissionais, mecanismos de segurança, técnicas etc., para defender a sua infra-estrutura de rede corporativa contra ataques cibernéticos.

Para Conceição (2017), acerca de mecanismos de segurança disponíveis, o mercado oferece uma imensa quantidade de proteção que vai desde *Firewalls* dedicados, passando por Sistemas de Detecção de Intrusão (IDS), Sistemas de Prevenção de Intrusão (IPS), *Proxies*, servidores de antivírus, entre outros.

Esses mecanismos de segurança têm sido adquiridos por empresas e instituições, que por sua vez são incorporados à infra-estrutura de rede corporativa. Entretanto, segundo Conceição (2017), cada uma dessas tecnologias, tem a sua própria *interface* de gestão, apresentação de dados, relatórios e geram um grande volume de *logs*.

No âmbito da segurança em infra-estrutura de redes corporativas, a monitorização e a detecção de padrões comportamentais indesejáveis em tempo útil é de crucial importância para criar uma defesa forte contra eventuais adversários, para tal, os profissionais de TI, precisam aceder, monitorizar e analisar cada um dos *logs* gerados por cada uma das suas aplicações, sistemas ou mecanismos segurança.

Nessa perspectiva, o presente trabalho pretende estudar e mostrar os benefícios das plataformas SIEM – *Security Information and Event Management,* que de acordo com Cruz (2012), centralizando em si um conjunto de registos de actividade (*logs*), estas soluções permitem aos seus utilizadores monitorizar a segurança da infra-estrutura em tempo real, bem como automatizar o processo de análise.

Cruz (2012) salienta que, com estas ferramentas não só é possível monitorizar os elementos já referidos da periferia da rede, mas também outros elementos internos críticos da organização como servidores de autenticação, servidores *Web*, antivírus,

sistemas operativos, acessos físicos, aplicações, entre outros exemplos. Com esta informação recolhida e consolidada num repositório central é possível correlacionar os registos de actividade dos activos e aplicações da infra-estrutura rede corporativa, detectando e mitigando atempadamente ataques que ponham em causa a segurança do nosso perímetro.

Elementos como relatórios de actividade, *dashboards* que permitem visualização gráfica de eventos e notificações (alertas) podem também ser criados para auxiliar este processo de monitorização (Cruz, 2012).

Neste presente trabalho de pesquisa, a primeira fase consistira em fazer uma análise da segurança cibernética em infra-estrutura de redes corporativas, onde será feito um estudo com intuito de descrever e explicar detalhadamente sobre o funcionamento de alguns dos principais mecanismos de segurança usados actualmente.

Depois desta fase, iremos estudar os eventos (l*ogs*) e incidentes de segurança com objectivo de poder diferencia-los, pois é comum ter dezenas, centenas ou até milhares de eventos (*logs*) num único dia provenientes de várias fontes de uma infra-estrutura de rede corporativa, entretanto um evento por si só não significa absolutamente, desta forma, devemos colectá-los e investiga-los, onde a partir disso podemos ter dois potenciais resultados a saber:

- Nada (evento normal ou de operação não usual); ou
- Incidente de segurança – O que indica que alguma coisa aconteceu e deve ser tratada de forma apropriada de acordo com as metodologias de resposta a incidentes estabelecidas.

Na última fase, iremos estudar as plataformas SIEM, nomeadamente: a sua origem, conceitos básicos, apresentando a arquitectura geral e as principais soluções mais usadas actualmente no mercado.

Desta forma, com base no estudo que será realizado em torno das plataformas SIEM, pretende-se realizar uma análise comparativa entre principais soluções SIEM que serão identificadas, onde através desta análise, será proposta e desenvolvida como solução do problema deste trabalho de pesquisa, a plataforma SIEM que melhor se adeque as condições e a realidade da infra-estrutura de rede corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação.

1.2. Descrição do problema

Actualmente, as principais actividades de vários negócios, sejam estes de pequeno ou grande porte, dependem nalgum momento de tecnologias de informação e no que concerne ao meio onde se inserem, lidam diariamente com sistemas computacionais ou outros meios que gerem informações críticas e sensíveis como bases de dados que podem conter informações pessoais de clientes, servidor de ficheiros, servidor de aplicações, entre outros.

Segundo a República de Moçambique (2021) – PENSC, à medida que o uso das TICs aumenta, cresce também a exposição do país a ataques e outro tipo de incidentes cibernéticos, tais como: crimes contra infra-estruturas críticas, sistemas, pessoas, espionagem política e empresarial, ciberguerra entre outros.

Ataques cibernéticos que coloquem em causa a confidencialidade, disponibilidade ou integridade de uma infra-estrutura de rede corporativa de empresas ou instituições, fará com que as mesmas deixem de funcionar devidamente, e mediante a gravidade da situação, poderá causar danos como: perdas financeiras de grandes proporções ou até terem a sua reputação afectada.

A República de Moçambique (2021) – PENSC afirma que, a tendência internacional mostra o aumento de incidentes e ataques cibernéticos, em frequência, grau, número, qualidade e sofisticação dos ataques.

Hoje em dia, as empresas e instituições para protegerem a sua infra-estrutura de rede corporativa contra ataques cibernéticos têm investido na segurança em perímetro usando mecanismos de segurança, tais como: *Firewalls*, DMZ, *Proxies*, IDS, IPS, Antivírus, *Network Address Translation* (NAT), entre outros.

Apesar de implementados esses mecanismos de segurança, com a sofisticação dos ataques cibernéticos a aumentar, empresas e instituições continuam a sofrer com os incidentes causados por esses ataques.

Portanto, esses mecanismos de segurança em perímetro, por si só são essenciais, mas já não são suficientes, pois não permitem ter uma visão global sobre o que acontece em tempo real numa infra-estrutura de rede corporativa, o que melhoraria bastante o processo de detecção e mitigação de ataques cibernéticos cada vez mais sofisticados.

1.3. Motivação

A Internet tem facilitado as actividades de negócio de várias empresas e instituições, promovendo produtos e serviços, aumentando a produtividade e a rentabilidade do mesmo. Apesar disso, a internet também traz consigo alguns pontos negativos, e um deles é a exposição a ataques cibernéticos.

A realização do presente trabalho é, primordialmente, impulsionada pelo interesse do autor na área de segurança cibernética. Sob outra perspectiva, o que motiva o autor a realizar o presente trabalho é que actualmente, com a crescente sofisticação dos ataques cibernéticos e capacidade de reinvenção dos atacantes, tem emergido a necessidade de exploração de novos mecanismos e técnicas que visam uma deteção mais precoce e precisa de ocorrências anómalas e indesejadas.

É nesse âmbito que o presente trabalho pretende abordar sobre um mecanismo de segurança relativamente recente, que são as plataformas SIEM – Security Information and Event Management. Em suma, os SIEMs têm a capacidade de colectar, agregar, armazenar, correlacionar e monitorizar eventos gerados por uma infra-estrutura de rede corporativa. Hoje, eles constituem a plataforma central dos modernos centros de operações de segurança (SOCs), pois reúnem eventos de diversos sensores de segurança. Correlaciona esses eventos (*logs*) e fornecem visualizações sintéticas dos alertas para tratamento de ameaças e relatórios de segurança.

1.4. Objectivos

1.4.1. Geral

- Propor a implementação de uma plataforma SIEM para deteção e mitigação de ataques cibernéticos no Instituto Nacional de Tecnologias de Informação e Comunicação.

1.4.2. Específicos

- Analisar a Segurança Cibernética na Infra-estrutura de Rede Corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação;
- Fazer uma análise comparativa entre diferentes soluções de plataformas SIEM e escolher a que melhor se adeque as condições e a realidade do Instituto Nacional de Tecnologias de Informação e Comunicação;
- Implementar a solução de plataforma SIEM escolhida numa infra-estrutura de rede corporativa virtualizada para efeito de testes.

1.5. Metodologia

1.5.1. Pergunta de Pesquisa

O presente trabalho de pesquisa propõe responder a seguinte pergunta:

De que forma as empresas e instituições moçambicanas podem ter uma visão global sobre o que acontece em tempo real na sua infra-estrutura de rede corporativa de modo a detectar e/ou mitigar ataques cibernéticos cada vez mais sofisticados?

1.5.2. Classificação da metodologia

Em relação a metodologia, o presente trabalho de pesquisa pode ser classificado:

a) Quanto à abordagem

Este trabalho de pesquisa segue uma abordagem tanto quanto qualitativa assim como quantitativa, que segundo Martins (2006) citado por Beúla (2017), o trabalho não se resume somente em empregar técnicas estatísticas para o tratamento de informações numéricas mas também, em uma análise dos dados recolhidos de forma a se chegar a um profundo entendimento do problema e com isso poder-se selecionar a solução mais adequada para a resolução do mesmo.

b) Quanto à natureza

O presente trabalho classifica-se como pesquisa aplicada, porque o presente trabalho tem como principal finalidade produzir conhecimento para aplicação prática e imediata na resolução de um problema.

c) Quanto aos objectivos

Os objectivos do presente trabalho classificam como exploratórios, porque de acordo com Gil (1991) citado por Nascimento (s/d), pesquisas exploratórias objetivam facilitar familiaridade do pesquisador com o problema objecto da pesquisa, para possibilitar a construção de hipóteses ou tornar a questão mais clara. Gil (1991) refere ainda que os exemplos mais conhecidos de pesquisas que possuem objectivos exploratórios são as pesquisas bibliográficas e os casos de estudo, que são as pesquisas utilizadas no presente trabalho.

d) Quanto aos procedimentos

Os procedimentos do presente trabalho classificam-se como: Pesquisa bibliográfica, pesquisa documental e Caso de estudo. A seguir será feita a descrição de cada um dos procedimentos segundo Gerhardt e Silveira (2009) citados por Michaque (2017).

- **Pesquisa bibliográfica**

É feita a partir do levantamento de referências teóricas já analisadas e publicadas por meios escritos e electrónicos como livros, artigos científicos, páginas web. Assim, em qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, portanto tem como principais objectivos descobrir se alguém já respondeu as perguntas propostas pela pesquisa, analisar se vale a pena repetir uma pesquisa cujos objetivos já foram esclarecidos em outro estudo ou avaliar os métodos utilizados em estudos parecidos para empregar na busca por novas soluções.

- **Pesquisa documental**

É similar à pesquisa bibliográfica, diferem pelo facto da pesquisa bibliográfica utilizar material já elaborado, ou seja, livros e artigos, enquanto que, a pesquisa documental recorre a fontes mais diversificadas e dispersas sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, documentos oficiais, cartas, filmes, fotografias, relatórios, etc.

- **Caso de estudo**

Caracteriza-se como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa ou uma unidade social. Tem como finalidade conhecer em profundidade o como e o porquê duma determinada situação que se supõe ser única em muitos aspectos, procurando descobrir o que há de mais essencial e característico. O presente trabalho de pesquisa teve como caso de estudo o Instituto Nacional de Tecnologias de Informação e Comunicação.

1.5.3. Técnicas de colecta de dados

Na realização do presente trabalho de pesquisa foram consideradas duas técnicas de colecta de dados, nomeadamente: Entrevista e Questionário.

- **Entrevista**

É uma técnica de instigação em que o investigador elabora perguntas e as apresenta de forma oral ao investigado com o intuito de obter dados que interessem à pesquisa.

Foi realizada uma e única entrevista aos responsáveis pela infra-estrutura de rede corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação, com o objectivo de se ter um profundo conhecimento sobre a real situação da instituição, para tal, foram elaboradas perguntas de resposta aberta. (*Vide o anexo – 1*).

- **Questionário**

Também é uma técnica de instigação, contudo, diferencia-se da entrevista pelo facto das questões elaboradas pelo investigador serem apresentadas de forma escrita ao investigado, normalmente apresentam um número de questões relativamente maior em relação as apresentadas numa entrevista e podem ser respondidas na ausência do investigador.

Foi elaborado um e único questionário contendo apenas perguntas de resposta única (Sim/Não), e foi dirigido aos responsáveis pela infra-estrutura de rede corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação. (*Vide o anexo – 2*)

1.6. Estrutura do trabalho

Este trabalho de pesquisa esta organizado da seguinte forma:

- **Capítulo I – Introdução**

Neste capítulo apresenta-se a contextualização, a descrição do problema, motivação, os objectivos que se pretendem alcançar, são identificadas e descritas as técnicas metodológicas usadas para atender aos objectivos traçados e por fim apresenta-se a estrutura do trabalho.

- **Capítulo II – Revisão da literatura**

Neste capítulo são descritas e apresentadas as definições mais relevantes em torno do tema deste trabalho, nomeadamente a segurança cibernética em infra-estruturas de Redes Corporativas (dando-se ênfase a mecanismos de segurança), Eventos & Incidentes de segurança, e por fim debruça-se em torno das plataformas SIEM e as principais soluções *open-source* e comercias mais usadas actualmente.

- **Capítulo III – Caso de estudo**

Neste capítulo é feita apresentação do INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação, a descrição da situação actual e os constrangimentos que advém da situação actual.

- **Capítulo IV – Proposta de solução**

Após a apresentação clara e precisa do problema, neste caso, os constrangimentos anteriormente identificados no INTIC, neste capítulo propõe-se e desenvolve-se uma solução para resolver o referido problema.

- **Capítulo V – Apresentação e Discussão de Resultados**

Neste capítulo, apresenta-se e discute-se em torno dos resultados apresentados no presente trabalho de pesquisa.

- **Capítulo VI – Considerações Finais**

Neste último capítulo são sumarizadas as principais conclusões deste trabalho de pesquisa, bem como é analisado o cumprimento dos objetivos propostos no início deste trabalho. Também são apresentados os constrangimentos (isto é, limitações encontradas durante a realização do trabalho) e são dadas recomendações para futuros pesquisadores e/ou entidades com interesse nessa área de estudo.

- **Bibliografia**

Nesta secção são indicadas todas as fontes (obras) consultadas para materializar o presente trabalho de pesquisa assim como para alcançar os objectivos traçados.

- **Anexos**

Nesta secção são apresentados os elementos adicionais que facilitam à compreensão do presente trabalho de pesquisa.

2. Capítulo II – Revisão da Literatura

2.1. Segurança cibernética em Infra-estruturas de Redes Corporativas

2.1.1. Segurança cibernética

Para Lima (s/d), com o advento da era da Informação, também conhecida como era Digital, e sua sucedânea, a era do Conhecimento, a informação foi alçada à categoria de activo estratégico para organizações e Estados-Nação, conferindo àqueles que a detém e dela se utilizam, efectiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais.

Ainda segundo Lima (s/d), a Internet, proporcionando conectividade em tempo real e abrangência mundial, trouxe consigo um crescimento sem precedentes no volume de informações disponíveis aos modernos decisores, entretanto, por outro lado, sua grande vulnerabilidade, aliada à existência de novos actores conduzidos por funestas intenções no cenário internacional, fez crescer a preocupação com a proteção da informação que por ela trafega.

O meio através do qual essas informações trafegam, ou seja, a internet, também é conhecido como espaço cibernético, de acordo com Barros *et al.* (2011) em Desafios Estratégicos para Segurança e Defesa Cibernética do Brasil, espaço cibernético é um ambiente virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.

Para República de Moçambique (2021) – Plano Estratégico Nacional de Segurança Cibernética, o espaço cibernético compreende um ambiente complexo, de valores e interesses, materializado numa única área de responsabilidade colectiva, que resulta da interacção entre pessoas, redes e sistemas de informação.

Assim, no entendimento do autor, espaço cibernético é um conjunto de meios pelos quais são necessários para a troca e partilha da informação em meios digitais.

Actualmente, como salienta Teixeira (2021), o avanço tecnológico e a quantidade de sistemas e redes conectadas à Internet estão a crescer rapidamente, além de sofrerem repentinas mudanças, entendidas por actualizações e/ou ainda evoluções à tecnologia já existente. Portanto, aumenta a preocupação quanto a segurança desses sistemas "conectados" e requer-se mecanismos que possam garantir a segurança e mitigar vulnerabilidades deles.

Para Schultz (2020a) citado por Teixeira (2021), a segurança cibernética é um ramo da segurança da informação que tem como objetivo prevenir os ataques realizados por sistemas maliciosos que se aproveitam de falhas sistêmicas para invadir dispositivos, roubando, manipulando e tornando indisponível uma série de dados ou arquivos.

Ainda segundo os autores supracitados, a segurança cibernética envolve a prevenção e proteção no que tange ao espaço cibernético e a segurança da informação envolve a prevenção e proteção contra todo tipo de risco, seja físico ou digital, controlando acessos de pessoas a locais, permissões para acessos de arquivos, entre outros.

De acordo com República de Moçambique (2021) – Plano Estratégico Nacional de Segurança Cibernética, a segurança cibernética compreende o conjunto de medidas e acções de prevenção, monitorização, detecção, reacção, análise e correcção que visam manter o estado de segurança desejado, ou seja, garantir a confidencialidade, disponibilidade, integridade, e não repúdio da informação, das redes e sistemas de informação no espaço cibernético, e das pessoas que nele interagem.

A segurança cibernética engloba todas as medidas legais, tecnológicas e processos que visam proteger pessoas, colectivas e singulares, e bens, com destaque para as infra-estruturas críticas de informação, no espaço cibernético.

A seguir são descritas as referidas propriedades para manter um estado de segurança desejado com base em (Fernandes, 2015):

- Confidencialidade é a propriedade que limita o acesso à informação apenas às entidades legítimas, isto é, apenas às entidades autorizadas pelo proprietário da informação.
- Integridade é a propriedade que garante que a informação não sofreu qualquer modificação indevida ao longo do processo de transmissão da mesma.
- Disponibilidade é a propriedade que garante que a informação estará sempre disponível para uso legítimo, ou seja, para uso dos utilizadores autorizados pelo proprietário da informação.
- Não repúdio é a propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

2.1.2. Firewalls

Segundo Mamede (2006), quando se cria uma forma de ligação da nossa rede interna à *internet*, abre-se um canal de troca de tráfego entre estes dois ambientes. Pode se controlar a rede interna de uma organização (ambiente privado), mas é impossível controlar a *internet* (ambiente público). A zona onde termina a rede interna e começa a rede não controlada chama-se perímetro ou fronteira.

Há o desafio de ter que se implementar mecanismos de segurança, que incluem medidas e tecnologias, que permitam criar segurança ao nível de perímetro de forma a garantir que todo o tráfego desconhecido não consiga acesso à rede interna. O dispositivo que se utiliza para este fim toma o nome de antepara de proteção ou firewall no original em Inglês (Mamede, 2006).

Para Scussiatto (2017), uma *firewall* pode ser descrita como um componente de *hardware* ou *software* que separa uma rede segura de uma outra não segura. A *firewall* é constituída por diversas componentes funcionais a saber:

- Hardware (computadores, redes e equipamentos de interligação como *hubs*, *switches*, *gateways*, routers, etc.); e
- Software (sistemas operativos, aplicações especificas para filtrar, controlar e modificar fluxos de comunicação).

Aos sistemas de firewall são assim atribuídas as diferentes responsabilidades, como a implementação da política de segurança da empresa no interior da rede protegida, o controlo de acesso, o assegurar a manutenção da privacidade e disponibilizar meios de auditoria. E tudo isto com dois pressupostos básicos que são (Mamede, 2006):

- Aquilo que não é expressamente permitido, é proibido;
- Aquilo que não é expressamente proibido, é permitido.

De acordo com Mamede (2006), o enfoque primário de uma *firewall* é o controlo de acesso, a diferentes níveis abaixo indicados:

- O controlo de serviços, com a definição de que serviços podem ser acedidos.
- O controlo de redireccionamento, com a definição em que direção pode o serviço ser iniciado e permitido o fluxo.
- O controlo de acessos, com a especificação de que serviços pode um utilizador específico aceder; e

- O controlo de comportamento, definindo como são usados determinados serviços particulares, como o controlo de e-mail para eliminação de *spam*.

Portanto, uma *firewall* é um mecanismo de segurança que funciona com base num conjunto bem definido de regras[1] de filtragem de pacotes, que controlam e filtram todas as ligações entre duas ou mais redes, através de um único ponto de acesso, como pode ser visto na figura abaixo. O controlo e a filtragem são feitos com base no tipo de pacote, endereço origem e destino, porta de origem e destino, entre outros parâmetros.

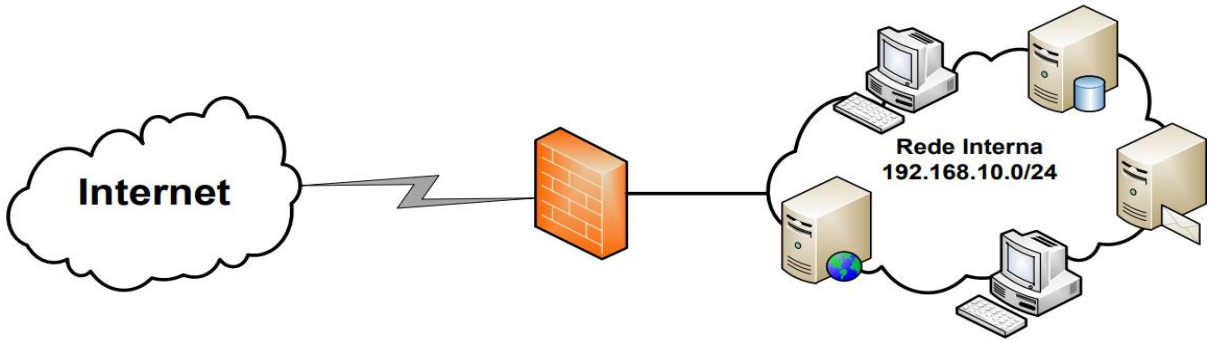

Figura 1: Estrutura básica de um Firewall.
Fonte: Elaborado pelo autor.

Os principais benefícios que se podem ter pelo recurso a este de dispositivos são a proteção contra tráfego indesejado proveniente do exterior da rede e proteção contra a violação da privacidade da rede interna. No entanto, Mamede (2006) afirma que, os *firewalls* não constituem, só por si, a pedra filosofal[2] da segurança de perímetro, até porque eles apresentam alguns riscos, tais como:

- Impacto no desempenho, já que aumentam a latência ao tráfego entre a rede controlada e a *internet*, na medida em que o mesmo tem de ser analisado;
- Por outro lado, como constituem, ou devem constituir, o único ponto de entrada na rede controlada, se a *firewall* for comprometida por um atacante, então, toda a rede interna pode ser comprometida;
- Também, dadas as suas atribuições, não protegem contra ataques de *software* malicioso, como vírus, apesar do tráfego destes passar pela *firewall*.

[1] *São implementadas de acordo com a política de segurança em perímetro definida pelas empresas ou instituições.*
[2] *No contexto, refere-se a um mecanismo de segurança que seja capaz de resolver todos os problemas de segurança em perímetro numa empresa ou instituição.*

Mamede (2006) considera que, por vezes é necessário considerar a possibilidade da existência de segmentos na rede com um menor grau de segurança ou proteção para, por exemplo, disponibilizar serviços que pretendemos assegurar ao exterior do perímetro de segurança, mas de forma controlada. Esses segmentos tomam o nome de zonas desmilitarizadas, do inglês *demilitarized zone (DMZ).* Uma DMZ reside entre uma rede pública como *internet* e a rede privada, protegida. Todo tráfego que entra ou sai da DMZ é inspecionado pelas regras da firewall, de forma a determinar se o mesmo é ou não permitido.

2.1.2.1. Arquitecturas de implementação de *firewalls*

Em termos de arquitectura, Mamede (2006) afirma que, existem quatro configurações básicas que podem ser utilizadas como modelos de implementação para a solução de *firewall*. Entretanto, antes de debruçar-se sobre arquitecturas é necessário vermos o conceito de bastião de segurança (no original em inglês *Bastion Host).*

Para Mamede (2006), o bastião de segurança constitui um ponto crítico muito forte na segurança de rede, pois nele se inclui o sistema de firewall e os demais sistemas que garantem a defesa por perímetro. Normalmente, serve como plataforma de *gateways* a nível de aplicação ou circuito, apresentando várias características, de entre as quais se destacam: Existir uma exigência para autenticação adicional para permitir acesso a *proxy*, adicionalmente cada *proxy* poderá exigir a sua própria autenticação.

As quatro arquitecturas de implementação de *firewalls* são a seguir disseminadas segundo (Mamede, 2006):

1) **Filtro de pacotes (Packet-Filtering Boundary Router)**

O filtro de pacotes constitui a forma mais antiga de implementação de um sistema de firewall. Na figura abaixo, está representada esta arquitectura, com *router,* que possui capacidades de filtro de pacotes, posicionado entre a rede segura e a rede publica ou não protegida.

Dada a sua posição, este *router* é também, por vezes, designado de *router* de perímetro. Um *router* com estás funções recorre à utilização de ACL ou listas de controlo de acesso para encaminhar ou descartar os pacotes que chegam até si, garantindo de forma genérica proteção contra ataques provenientes da rede não segura. Esta forma de implementação possui algumas deficiências que são:

- Falta de mecanismos de autenticação forte;
- Complexidade da manutenção da ACL no *router*;
- Criação de registos de jornal bastante limitados, dificultando a auditoria;
- Se o *router* for comprometido, o tráfego pode fluir directamente através deste, vindo da Internet, para máquinas da rede interna;

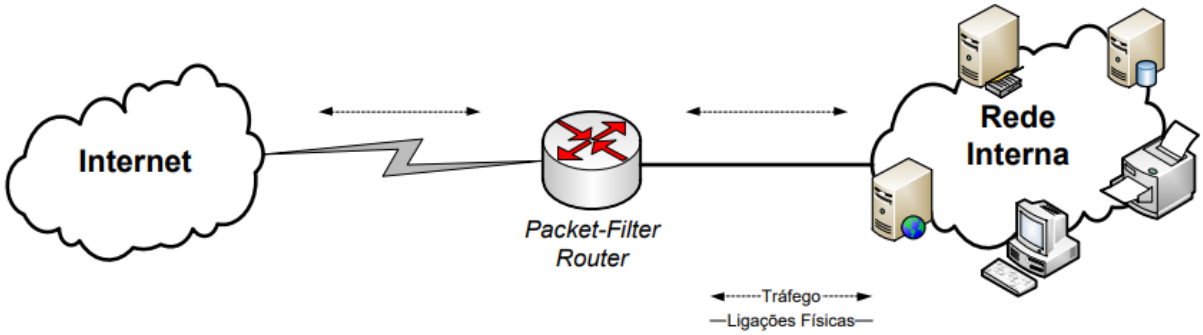

Figura 2: Filtro de pacotes.
Fonte: Adaptado de Mamede (2006).

2) Screened Host Firewall (Singled, Dual e Multi home):

Esta arquitectura de *firewall* utiliza um *router* filtro de pacotes e um *host* bastião. É uma arquitectura com um desenho um pouco mais complexo que a outra já referida porque oferece um nível de segurança superior, disponibilizando serviços no nível de rede, com filtro de pacotes, e ao nível aplicacional, como servidor *proxy*.

Assim, este tipo de sistema *firewall* é considerado bastante seguro porque exige a um atacante a intrusão em dois sistemas separados antes de conseguir comprometer a rede protegida.

a) Singled-home Bastion Host

Esta arquitectura recorre à utilização de dois sistemas distintos: Um *router,* que é configurado de forma a seguir duas regras básicas:

1. Para tráfego proveniente da Internet, apenas pacotes destinados ao bastião são permitidos; e
2. Para tráfego proveniente da rede interna, apenas pacotes originados pelo bastião podem passar.

O bastião preenche algumas lacunas apresentadas na arquitectura anterior, com funcionalidades que lhe permitem garantir mecanismos de autenticação forte e de *proxy*.

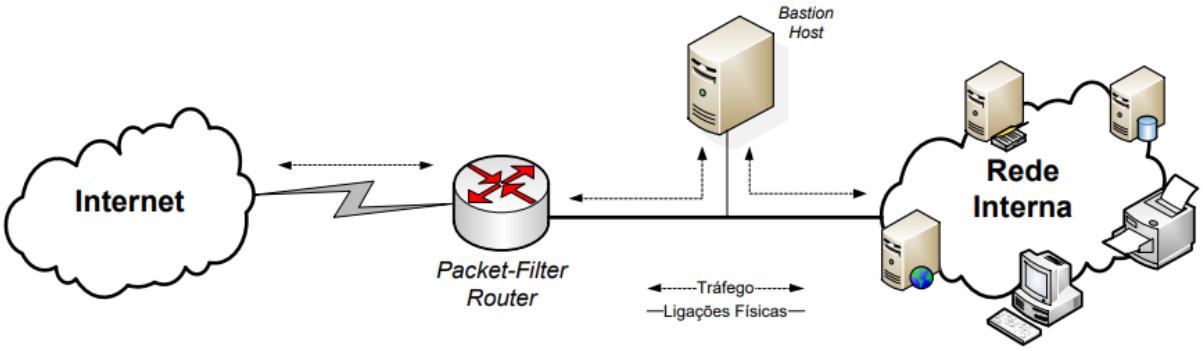

Figura 3: Bastion Host Singled-home.
Fonte: Adaptado de Mamede (2006).

A figura anterior apresenta a arquitectura referida. Salienta-se a possibilidade de definição de uma zona desmilitarizada, com o acesso controlado pelo bastião, como se pode ver na figura abaixo, de forma a possibilitar acessos públicos a determinados serviços como, por exemplo, um servidor *web*.

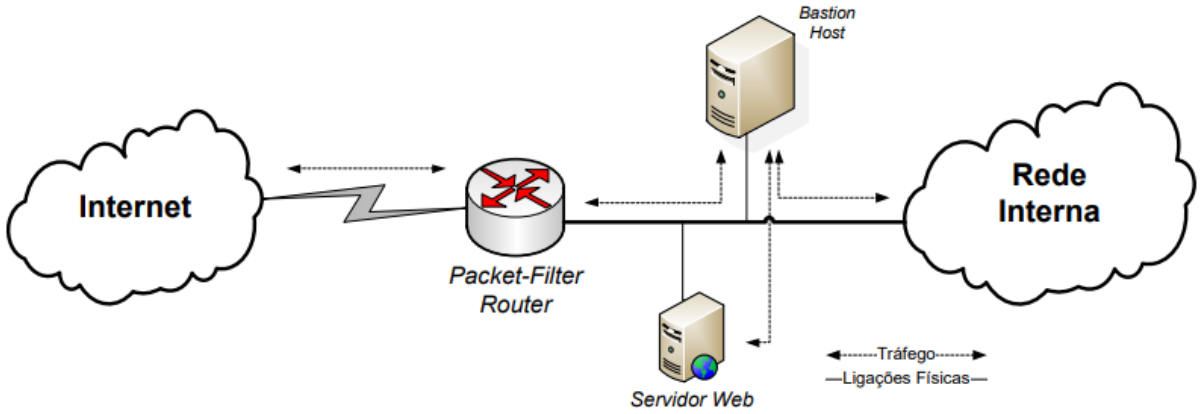

Figura 4: Bastion Host Singled-home com DMZ.
Fonte: Adaptado de Mamede (2006).

b) Dual e Multi-home Bastion Host.

A implementação de uma arquitectura *screened host firewall* com um bastião a definir a separação física de redes (*dual-home bastion host*) permite preencher lacunas deixadas pela arquitectura anterior (filtro de pacotes). O sistema *dual-home* pretende preencher esta lacuna de segurança, pelo isolamento físico da rede *Internet* e da rede interna da empresa, como se pode ver na figura abaixo. Esta arquitectura também é muitas vezes denominada por *multi-homed bastion host*.

Um computador *multi-homed* constitui um dispositivo que possui mais do que uma interface de rede. A implementação mais vulgar recorre a sistemas *dual-homed*, que possui apenas duas *interfaces*. Uma *firewall dual-homed* é um sistema de *firewall* com duas interfaces de rede (NIC) com cada uma delas ligadas numa rede diferente.

Por exemplo, uma das interfaces estará ligada à rede externa não protegida e a outra estará ligada à rede interna, protegida. Nesta configuração existe um ponto crucial que temos de respeitar, que basicamente consiste em não permitir o roteamento do tráfego proveniente do exterior directamente para a rede interior, ou seja, a *firewall* tem de actuar como intermediário entre duas redes.

NB: O roteamento pela *firewall* deve ser restringido para que pacotes IP de uma rede não sejam directamente encaminhados.

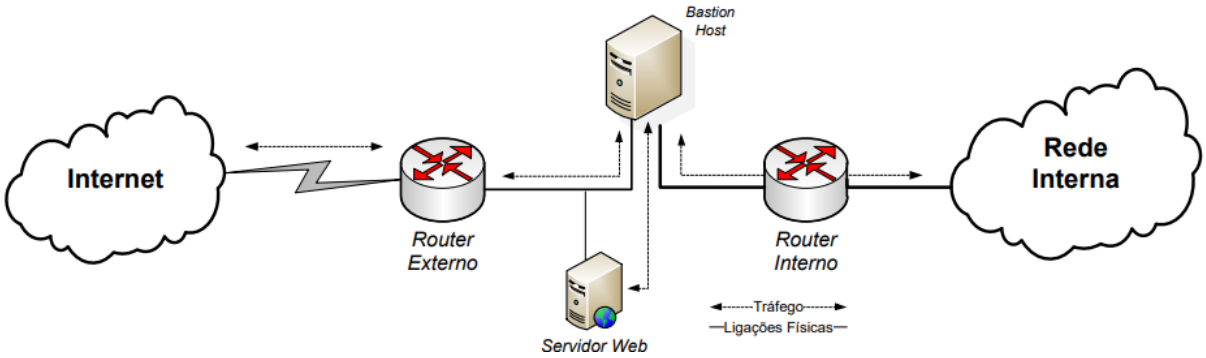

Figura 5: Bastion Host dual-home.
Fonte: Adaptado de Mamede (2006).

3) Screened Subnet Firewall

Esta arquitectura constitui-se como o sistema de firewall mais seguro. Nesta é criada uma sub-rede isolada, entre a rede protegida e a rede não protegida, onde existe um bastião e onde podem existir *servers* de informação e *modems* para acesso remotos. Para tal, recorre-se à utilização de dois *routers* com funções de filtragem de pacotes, ficando o bastião localizado entre os mesmos. O princípio básico é que todo tráfego através da sub-rede está bloqueado.

Existem assim três níveis de defesa contra intrusos. O *router* externo fornece proteção contra ataques provenientes do exterior, enquanto que o *router* interno gere o acesso do tráfego proveniente da rede protegida à DMZ, passando também através do bastião.

Desta forma, esta separação assegura que em caso de ataque com sucesso ao bastião, o atacante ficará restringido a rede de perímetro pelo *router* que faz a ligação entre esta rede e a interior. A principal desvantagem deste sistema é a complexidade da configuração e manutenção da mesma.

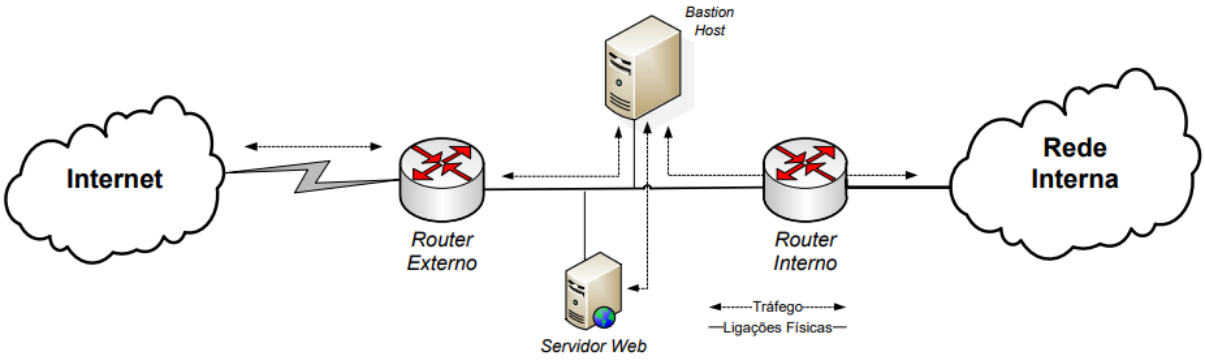

Figura 6: Screened subnet firewall.
Fonte: Adaptado de Mamede (2006).

2.1.2.2. Network Address Translation (NAT)

Para Mamede (2006), o NAT é um conceito muito importante para redes informáticas, especialmente para os sistemas de *firewall*.

Com este serviço, os sistemas de *firewall* podem promover o mascaramento[3] dos esquemas de endereçamento utilizados nas empresas e instituições modificando o tráfego IP à entrada ou à saída da *firewall*. Permitindo assim, manter a privacidade dos clientes, que não se expõem na *Internet*.

Uma das funcionalidades deste serviço é de converter um endereço IP privado para um endereço IP público, com efeito, segundo Mamede (2006), com NAT, um único dispositivo pode funcionar como intermediário entre a *Internet* e uma rede local, o que significa que apenas um único endereço público é necessário para representar um grupo de computadores. Tipos e alguns cenários em que interessa utilizar o NAT são:

- **Source NAT (SNAT)**

Consiste em modificar o endereço IP de origem das máquinas da rede interna antes dos pacotes serem enviados para rede externa (Russell *et al*., 2002).

Esses pacotes, terão na firewall o seu endereço de origem alterado para o endereço externo da *firewall (eth0)*. Para lembrar dos pacotes modificados, a *firewall* reescreve os endereços assim que obtém a resposta da máquina de destino, direcionando os pacotes ao destino correto.

[3] *Ocultar os verdadeiros endereços IP dos equipamentos no interior de uma rede protegida.*

Desta forma, para Russell *et al.* (2002), o objectivo do SNAT é de ocultar a origem e garantir que nenhuma máquina da internet possa ter acesso directo as máquinas de sua rede interna via SNAT.

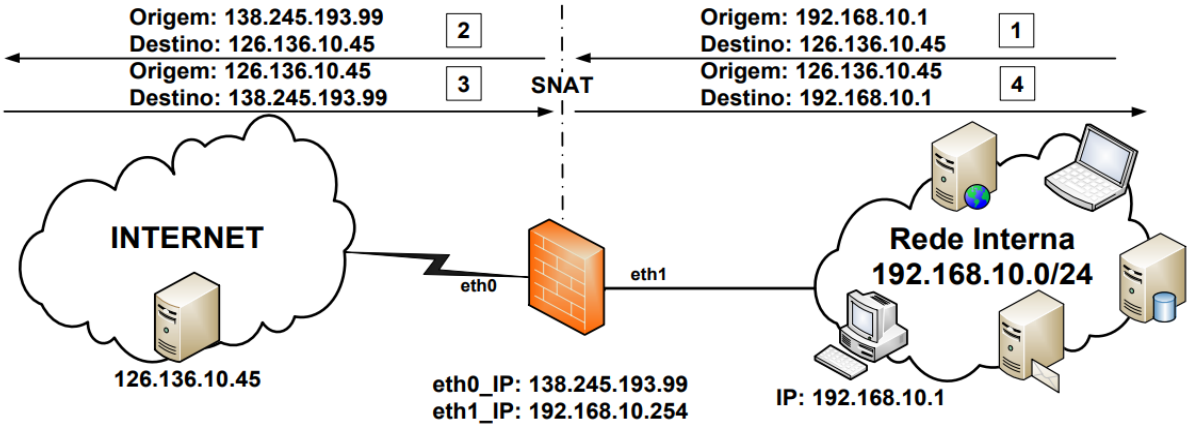

Figura 7: Source NAT (SNAT).
Fonte: Elaborado pelo autor.

- **Destination NAT (DNAT)**

Segundo Russell *et al.* (2002), consiste em modificar o endereço IP de destino do tráfego das máquinas com origem na rede externa com destino ao endereço externo da *firewall*. Umas das aplicações do DNAT é de disponibilizar o acesso a serviços mantidos em máquinas da rede interna, geralmente quando essas máquinas utilizam endereços IPs privados.

Nessa perspectiva, os serviços são disponibilizados na *internet* com o endereço IP externo da *firewall (eth0),* e os pacotes de comunicações destinadas a esses serviços têm o seu endereço de destino alterado para o endereço da máquina da rede interna onde reside o serviço “real”.

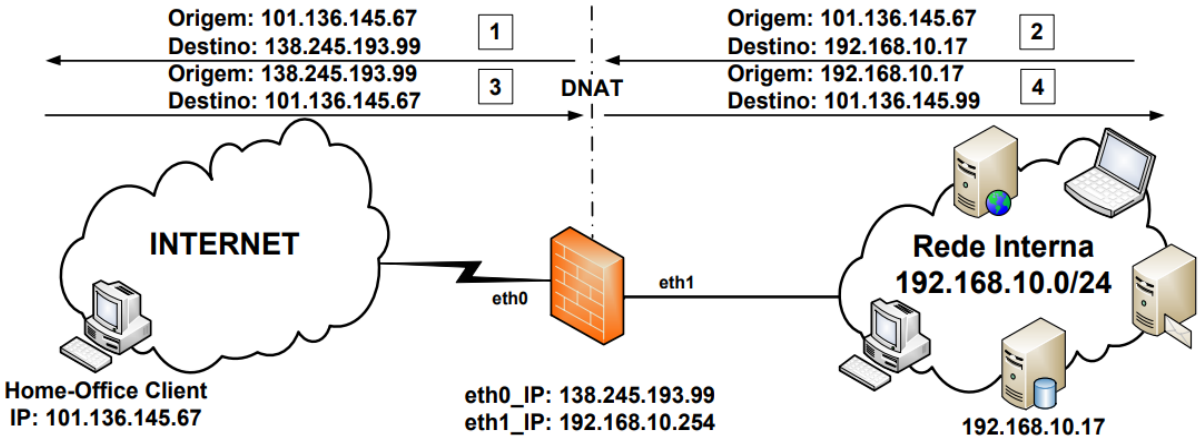

Figura 8: Destination NAT (DNAT).
Fonte: Elaborado pelo autor.

2.1.3. Sistemas de Detecção de Intrusão (IDS)

Segundo Gonçalves Sobrinho Júnior (2016), todo sistema, programa ou pessoa que tenta ou consegue acessar informações de alheios ou realizar actividades ilegais em *software* de terceiros pode ser considerado um intruso. Ainda segundo o autor citado, Intrusão é um conjunto de ações que buscam comprometer os pilares da segurança da informação de recurso computacional enquanto que o acto de detectar ações que podem comprometer a segurança da informação de um recurso computacional pode ser denominado detecção de intrusão.

Para Kumar *et al.* (2013), um IDS pode ser um *software* ou um dispositivo físico que monitoriza o tráfego de rede ao longo da rede interna ou num computador, para detectar actividades intrusivas e/ou eventos indesejados, como por exemplo tráfego ilegal e malicioso, tráfego que viole as políticas de segurança.

Existem vários tipos de tecnologias IDS devido à variação das configurações de rede, e cada tipo tem as suas vantagens e desvantagens. A seguir serão referidos alguns tipos de sistemas IDS (Kumar *et al.*, 2013):

- **Network Based Intrusion Detection System (NIDS)**

Em português IDS Baseado em Rede, segundo Gonçalves Sobrinho Júnior (2016), estes sistemas processam informações capturadas, analisando o fluxo de pacotes que trafegam pela rede, eles são geralmente posicionados em locais estratégicos da infra-estrutura da rede. O NIDS pode capturar e analisar dados para detectar ataques conhecidos pela comparação de padrões e assinaturas em um banco de dados ou pela detecção de actividades ilegais. O NIDS é normalmente referenciado como *packet-sniffers,* pois esta categoria de IDS captura todos os pacotes que trafegam na rede.

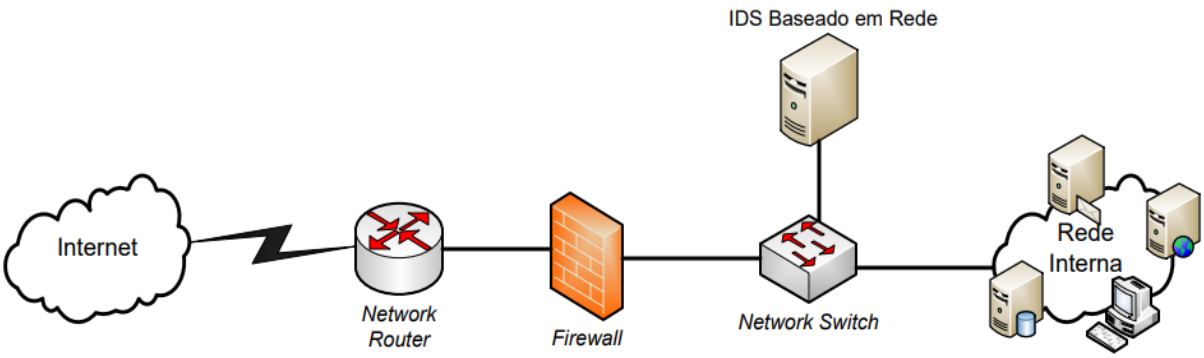

Figura 9: IDS Baseado em Rede.
Fonte: Elaborado pelo autor.

Os NIDS também são chamados de IDS passivos porque caso um ataque seja detectado, este emite uma notificação (alerta) para o administrador informando que um ataque ocorreu, e este por sua vez toma medidas adequadas para garantir a segurança desse recurso computacional (Kumar *et al*., 2013).

- **Host Based Intrusion Detection System (HIDS)**

Neste caso, segundo Claro (2015), o IDS encontra-se instalado em cada máquina monitorada, como mostra a figura abaixo, a fim de analisar os eventos gravados nos arquivos de *log* ou pelos agentes de auditoria. Funcionam como a última linha de defesa, no caso de o ataque ter sido bem-sucedido e ter conseguido atravessar a *firewall* e o NIDS. Os HIDS são comumente implantados em máquinas críticas, como servidores acessíveis publicamente e em servidores que contêm informações confidenciais (Kumar *et al*., 2013).

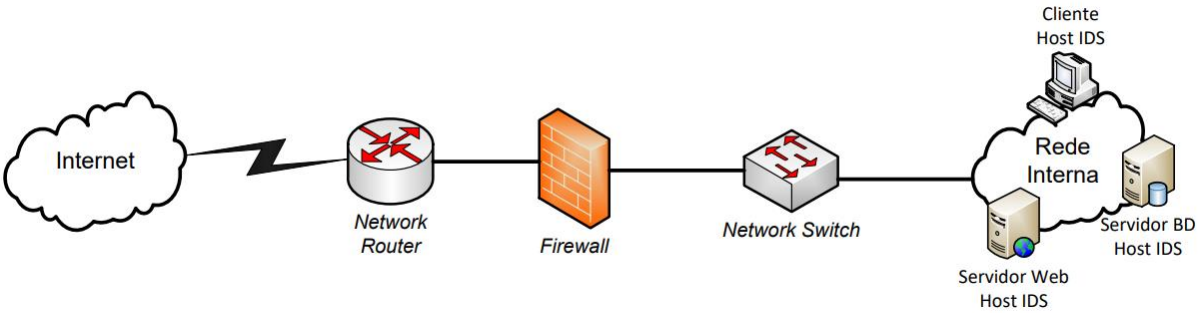

Figura 10: IDS Baseado em Host.
Fonte: Elaborado pelo autor.

Apontam-se a seguir os componentes de um Sistema de Detecção de Intrusão, segundo Gonçalves Sobrinho Júnior (2016), em geral, consiste de três componentes funcionais que são abaixo disseminados:

Figura 11: Principais componentes de um IDS.
Fonte: Gonçalves Sobrinho Júnior (2016).

– Fontes de dados: São as referências que o IDS possui para achar vulnerabilidades. Em geral, elas podem ser classificadas em duas categorias que são: Host-based monitors e Network-based monitors.

- **Host-based monitors**

Coleta as informações de fontes internas de um computador, geralmente a nível de sistema operacional. As fontes incluem pista de auditoria do sistema operacional e *logs* do sistema.

- **Network-based monitors**

A fonte de dados são os pacotes da rede. Isto é usualmente alcançado usando dispositivos que são configurados para capturar todo o tráfego acessível da rede.

– Motor de detecção: Este componente usa as informações da fonte de dados para detectar actividades maliciosas e pode funcionar em uma das seguintes formas de abordagens:

- **Detecção baseada em Assinaturas:** Segundo Claro (2015), compara os pacotes recebidos com um conjunto de assinaturas previamente definidas. Neste caso, o IDS compara um padrão apresentado pelo possível ataque a uma base de dados de padrões de ataques (assinaturas). Se o padrão suspeito for confirmado na base de dados, o ataque é detectado.
- **Detecção baseada em Anomalias:** Analisa o comportamento do tráfego de rede, comparando-o a um modelo de comportamento considerado normal para o ambiente. Quando o tráfego de rede se desvia do comportamento considerado normal, ocorre uma anomalia, o IDS considera como um possível ataque, gerando o alerta (Miguel, s.d.) citado por (Claro, 2015).

– Gerenciador de Reposta: Ele é responsável por armazenar e informar ao usuário ou administrador quando um possível ataque for identificado.

2.1.3.1. Incidência de alertas em IDS/IPS

De acordo com Stiawan *et al.* (2011) citado por Tavares (2015) existem quatro tipos de alertas em IDS/IPS a saber:

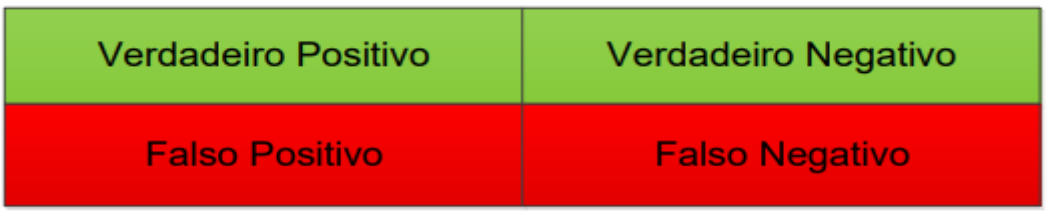

Figura 12: Tipologia de alertas em IDS/IPS.
Fonte: Elaborado pelo autor.

– Verdadeiro Positivo:

- **IDS:** Seria a geração de um alerta devido a uma ocorrência suspeita no tráfego.
- **IPS:** Corresponderia a geração de um alerta e o bloqueio do tráfego devido a uma ocorrência suspeita.

– Verdadeiro Negativo: Tanto para IDS ou IPS, corresponderia ao próprio tráfego do utilizador sem qualquer alerta gerado e/ou bloqueio do tráfego.

– Falso Positivo:

- **IDS:** Acontece quando é gerado um alerta com tráfego normal e legítimo.
- **IPS:** Acontece quando tráfego normal e legítimo é bloqueado, e de seguida gerado um alerta.

– Falso Negativo: Tanto para IDS ou IPS, ocorre quando tráfego malicioso entra na rede interna, entretanto não é gerado nenhum alerta e/ou bloqueio do tráfego.

Em suma, a incidência de Verdadeiro ou Falso é referente a decisão que o IDS/IPS toma em relação ao tráfego, se ele toma a decisão certa, i.e, se ele detectou/bloqueou o que realmente tinha de detectar/bloquear ou se não detectou/bloqueou o que não tinha de detectar/bloquear então teremos um alerta do tipo “Verdadeiro”.

Entretanto, se o IDS/IPS detectou/bloqueou o que não devia detectar/bloquear ou se não detectou/bloqueou o que realmente tinha de detectar/bloquear então teremos um alerta do tipo “Falso”, certamente que este tipo de alerta, é o que não desejamos nas nossas soluções IDS/IPS.

A questão de positivo ou negativo, é referente ao conteúdo do pacote, que pode assumir duas possibilidades a saber: pacote legítimo, que corresponde a positivo e pacote ilegítimo (malicioso) que corresponde a negativo.

Nas empresas e instituições, a incidência de falsos positivos nos IPS é altamente prejudicial à produtividade, na medida em que trafego legítimo é bloqueado devido a uma falsa suspeita de ataque, enquanto nos IDS, segundo Mamede (2006), fazem com que os *admins* tenham de investigar cada um dos alertas de falsa intrusão, o que pode levar o(s) *admins* do sistema a desligar o alerta, ou ainda pior, a desligar todo o IDS, com um resultado que pode ser desastroso.

No geral, tanto nos IDS ou IPS, os falsos negativos representam um sério problema de segurança, visto que nesse tipo de alerta, um pacote com conteúdo malicioso entra na rede interna da organização.

2.1.4. Sistemas de Prevenção de Intrusão (IPS)

Para Kumar *et al.* (2013), ao longo de muitos anos, a filosofia da detecção de intrusões na rede consistiu em detectar o maior número possível de ataques e possíveis intrusões e consigná-los para que outros tomassem as medidas necessárias.

Pelo contrário, os sistemas de prevenção das intrusões na rede foram desenvolvidos numa nova filosofia "tomando as medidas necessárias para combater com precisão os ataques ou intrusões detectáveis" (Kumar *et al.*, 2013).

Claro (2015) afirma que, O IPS é um complemento do IDS, ele acrescenta à detecção de ataques, a possibilidade de prevenção. Ambos IDS e IPS necessitam de uma base de dados de assinaturas conhecidas para realizar a comparação com possíveis ataques.

Ainda segundo Claro (2015), o IDS se restringe a detectar tentativas de intrusão, registrá-las e enviá-las ao administrador da rede, enquanto que o IPS opera "*inline*[4]" na rede, adoptando medidas adicionais para bloquear as intrusões em tempo real.

Um dos problemas da operação *inline* do IPS é que impacta no desempenho da rede, devido ao aumento da latência ao tráfego entre a rede interna e a rede externa, na medida em que o mesmo tem de ser analisado.

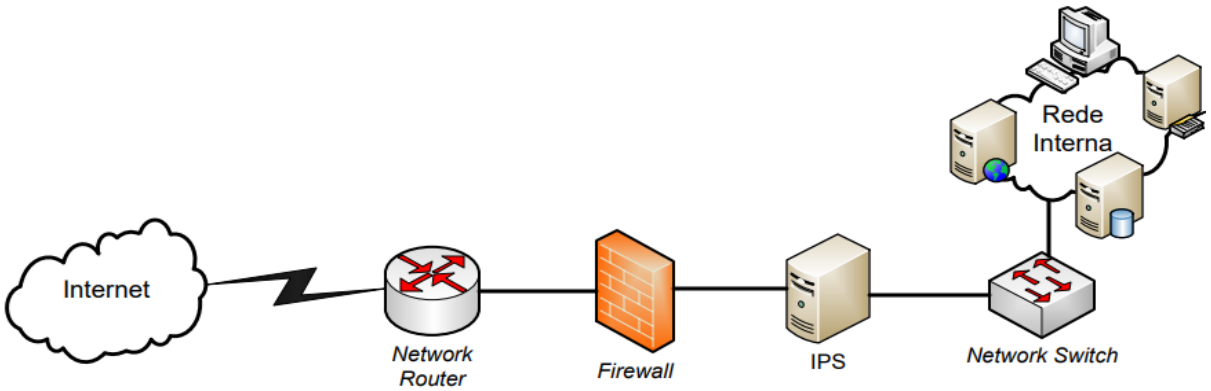

Figura 13: Posição do IPS na topologia da rede.
Fonte: Adaptado de Mamede (2006).

[4] *O IPS está no meio do fluxo da rede, fazendo com que tráfego entre a rede interna e rede externa (internet) passe directamente por ele.*

2.2. Eventos, *Logs* e Incidentes de Segurança

2.2.1. Eventos

Para Filho (2012), um evento pode ser descrito como qualquer ocorrência detectável ou discernível que seja significativa para a gestão da infra-estrutura de TI ou para a entrega do serviço de TI. Eventos são notificações criadas por um serviço de TI, item de configuração ou ferramenta de monitorização.

Desta forma, Filho (2012) afirma que, a operação de serviço eficiente depende do conhecimento da situação da infra-estrutura e da detecção de qualquer desvio da operação normal ou esperada. Isto ocorre com bons sistemas de monitorização e controle, baseados em dois tipos de ferramenta, a saber:

- **Ferramentas activas de monitorização:** Avaliam *itens* chave de configuração para determinar sua situação e disponibilidade;
- **Ferramentas passivas de monitorização:** Detectam e correlacionam alertas operacionais ou comunicações geradas por itens de configuração.

Os eventos podem ser tipificados em (Filho, 2012):

- **Eventos que indicam uma operação normal:** Indicam que o serviço está funcionando. Como por exemplo: Um usuário conectou-se à aplicação e o *job* agendado foi executado.
- **Eventos que indicam uma operação anormal:** Como quando o usuário tenta entrar na aplicação e não consegue e um *log* é registrado com esta informação. Por exemplo, o *software* de coleta identificou um *software* não autorizado e ocorreu uma situação não usual no processo.
- **Eventos que sinalizam uma operação não usual:** Fornecem uma indicação de que a situação requer um pouco mais de supervisão, como no caso da memória do servidor estar acima do nível estabelecido como limite.

Ainda segundo Filho (2012), eventos ocorrem continuamente, mas nem todos devem ser detectados ou registrados. Com isso, durante o projecto, desenvolvimento, gestão e suporte da infra-estrutura e dos serviços de Tecnologias de Informação é importante ter clareza da necessidade ou importância do evento para o seu registro.

2.2.2. *Logs*

Kent & Souppaya (2006) e Rouse (2012) *apud* Vazão (2020), definem os *logs* como os registros de eventos que ocorrem nos sistemas operativos, nas aplicações e nos equipamentos de uma organização, possibilitando também o acesso à hora, à data e a outras informações relacionadas com o evento que o gerou.

Segundo Dionísio (2019), os *logs* são indicadores cruciais para se identificar o que está a acontecer numa infra-estrutura de rede corporativa de uma organização. São os *logs* que ajudam os analistas a correlacionar por exemplo comportamentos de rede, fornecendo informações muito valiosas sobre diferentes tipos de problemas de segurança numa infra-estrutura.

Assim, estes *logs* para além de ajudarem a evitar que uma organização possua uma visão limitada sobre o que está a acontecer na sua infra-estrutura, permitem também aos especialistas de segurança a verificarem comportamentos maliciosos com intuito de prejudicar a mesma (Dionísio, 2019).

Actualmente, para Dionísio (2019), os SIEMs funcionam correlacionando estes *logs* de diferentes fontes de modo a evitar ou a identificar incidentes de segurança. Um SIEM usufruindo desta vasta coleção de *logs*, pode correlaciona-los para por exemplo alertar uma equipa do SOC avisando de que um utilizador específico está a realizar actividade incomum na sua organização.

Para Vazão (2020), de uma forma geral, uma mensagem de *log* possui três elementos fundamentais a saber:

- ***Timestamp*** – Registo da data e da hora em que a mensagem de *log* foi gerada;
- **Origem** – Sistema que gerou a mensagem de *log*, pode, por exemplo, ser um endereço IP ou o nome da máquina;
- **Dados** – Informação sobre o evento gerado.

Em relação a tipologia, os *logs* podem ser categorizados em quatro tipos segundo (Chuvakin et al., 2012; Q. Li & Clark, 2015) citados por Vazão (2020), nomeadamente *logs* operacionais, de *debugging*, de conformidade e de segurança, este último tipo de *logs* contém informações relacionadas com a segurança, e tem como principal objectivo a deteção e/ou mitigação de ataques cibernéticos, a tentativas de roubo de dados, assim como outros problemas relacionados com a segurança dos dados.

No geral, os *logs* podem ter várias finalidades, apesar disso, neste presente trabalho pretende-se colectar, analisar, fazer a gestão e a correlação de *logs* que possuam relevância para segurança de infra-estrutura de redes corporativas.

2.2.3. Incidentes de segurança

Segundo Brownlee & Guttman (1998) – RFC 2350, incidente de segurança é qualquer evento adverso que comprometa algum aspecto da segurança do computador ou da rede. A definição de um incidente pode variar entre as organizações, mas pelo menos as seguintes categorias são geralmente aplicáveis:

- Indisponibilidade das informações;
- Perda de confidencialidade das informações;
- Comprometimento da integridade das informações;
- Uso indevido de serviço, sistemas ou informações; e
- Danos aos sistemas.

Numa abordagem mais ampla, um incidente de segurança é uma interrupção não planejada de qualquer serviço de Tecnologia da Informação, i.e., é algo que tem como objectivo comprometer os pilares da segurança da informação de um recurso de TI.

De qualquer forma, os incidentes de segurança são problemáticos e perigosos, idealmente é o que se pretende evitar, mas seguramente eles irão acontecer e a partir desse momento devemos fazer o correcto e o devido tratamento para reduzir o impacto desse incidente.

2.3. Security Information and Event Management (SIEM)

Nesta sessão iremos estudar as plataformas SIEM, definindo os conceitos básicos que norteiam estas ferramentas, apresentando a arquitectura geral e as principais soluções existentes no mercado.

Segundo Rodrigues (2015), as plataformas SIEM são uma tendência relativamente recente no sector empresarial das TI, tendo a sua definição sido cunhada em 2005, pelos investigadores Mark Nicolett e Amrit Williams da Gartner.

Cruz (2012) afirma que, estes investigadores descreveram as plataformas SIEM como sistemas que recolhem, analisam e apresentam a informação dos dispositivos de segurança tais como *Firewalls*, IDS, IPS, entre outros, bem como outras informações de segurança de outros activos (como bases de dados, sistemas operativos, etc.).

De acordo com Dionísio (2019), estes eventos são então coletados, normalizados, armazenados e correlacionados pelo SIEM. Nessa perspectiva, os inúmeros eventos armazenados possibilitam uma rápida identificação e resposta aos incidentes, nalguns casos esta resposta até pode ser automática por parte do sistema. Mantendo um histórico de todas as interações com a infra-estrutura, sendo também bastante útil para investigações forenses.

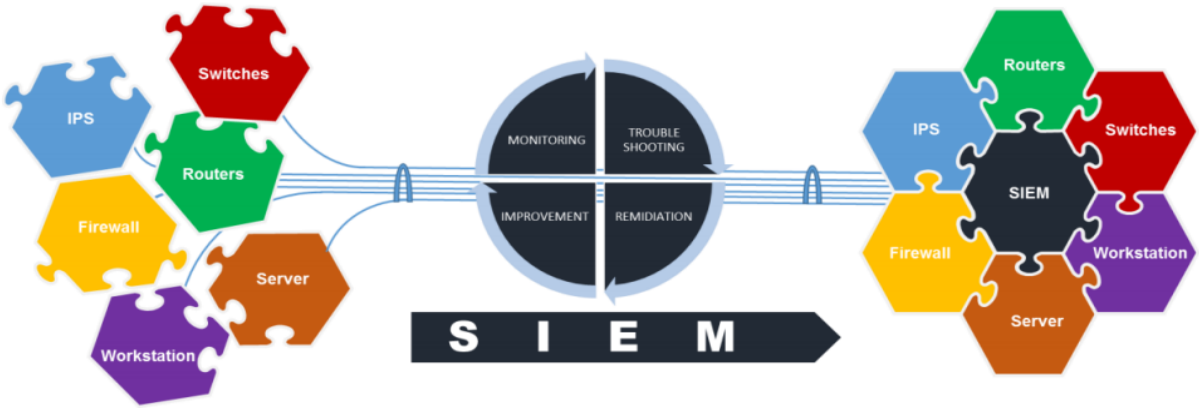

Figura 14*: Security Information and Event Management.*
Fonte: Kreeyaa citado por *(Santos, 2018)*.

Historicamente, segundo Jamil (2015) citado por Mendonça (2015), o conceito SIEM surgiu a partir de outros dois paradigmas:

- **Plataformas SEM – Security Event Management:**

Segundo Cruz (2012), efectuam a monitorização de dados em tempo real, correlação de eventos, notificações (alertas), etc., para suportar actividades de segurança, tais como a resposta "automatizada" a incidentes de segurança (Mendonça, 2015).

- **Plataformas SIM – Security Information Management):**

Segundo Cruz (2012), centralizam *logs* por largos períodos temporais. A partir daí, de acordo com (Mendonça, 2015), podem conduzir-se vários tipos de análises, tais como investigações forenses ou auditorias de conformidade.

Surgiu desta forma o termo SIEM (Security information and event management), que é considerada uma solução híbrida pois suporta propriedades de ambos, SIM e SEM.

Em suma, para SearchSecurity (s.d) citado por Mendonça (2015), a tecnologia SIEM permite detectar ameaças e responder a incidentes, através da monitorização, análise e correlação de eventos em tempo real, combinada com a análise histórica de eventos recolhidos de uma variedade de fontes de dados.

2.3.1. Arquitectura geral de uma plataforma SIEM

Segundo Miller *et al.* (2011), existem variações na estrutura de uma plataforma SIEM, com componentes específicos adicionais, contudo um SIEM simples pode ser dividido em seis partes como pode ser visto na figura abaixo.

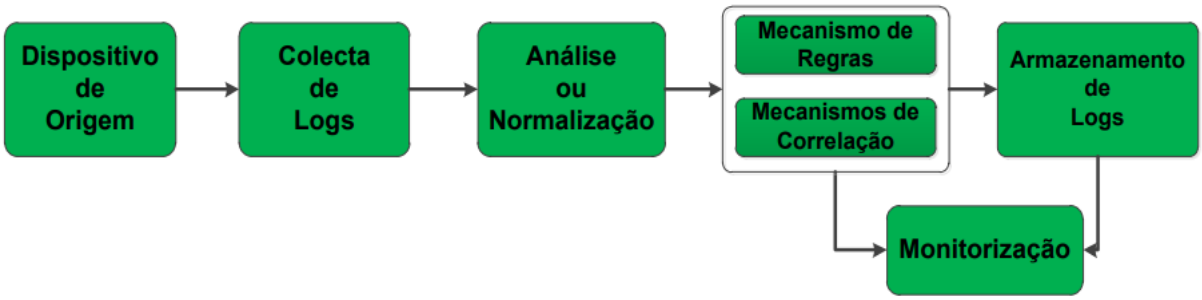

Figura 15: Arquitectura geral de uma plataforma SIEM.
Fonte: Adaptado de Miller et al. (2011).

a) Dispositivo de origem

Para Miller et al. (2011), a primeira parte de um SIEM são os activos, i.e., o dispositivo de origem que alimenta as informações no SIEM, que pode ser um dispositivo real na rede, como roteadores, *switches,* ou algum tipo de sistema, servidor ou qualquer outra fonte de informação geradas para o SIEM.

b) Colecta de *logs*

Conforme Cruz (2012), o processo de recolha de registos baseia-se num agente que colecta os *logs* de um ou mais activos, sendo configurado para enviá-los para um servidor central, alimentando assim o sistema SIEM. Segundo Miller *et al.* (2011), existem basicamente dois métodos para conseguir as informações de um dispositivo de origem, nomeadamente:

- **Método *Push:*** O dispositivo de origem envia seus *logs* para o SIEM.
- **Método *Pull:*** O SIEM vai atrás do dispositivo de origem e colecta os *logs*.

A principal diferença entre esses dois métodos é que para o caso do *pull*, é importante notar que os *logs* podem não chegar a tempo real no SIEM, enquanto que para o caso do *push,* os *logs* são enviados directamente para o SIEM assim que são gerados nos dispositivos de origem.

c) Análise/Normalização de *logs*

Depois da colecta de *logs,* a normalização deverá ser executada sobre cada um dos *logs* recolhidos.

Segundo Cruz (2012), esta normalização é imprescindível na medida em que, por entre todos os dispositivos, sistemas e aplicações que podem ser auditados numa infra-estrutura de rede corporativa, existe uma grande disparidade quanto ao formato em que os seus registos de actividade (*logs*) são escritos.

Portanto, para Cruz (2012) e Miller *et al.* (2011), o objectivo desta actividade é de padronizar os diversos formatos de *logs* para um formato conhecido pela plataforma de maneira a facilitar a correlação de eventos de diferentes activos. Cruz (2012) enfatiza que, esta normalização tanto pode ser feita quer nos agentes colectores, quer no repositório que centraliza os eventos, normalizando-os antes de os guardar.

d) Mecanismos de Regras e Correlação

***(*)* Regras:** Para Miller *et al.* (2011), esse mecanismo aciona alertas (notificações) na plataforma SIEM, a medida que regras especificas e pré-definidas são encontradas nos *logs.* Geralmente as regras começam simples e dependendo do que se quer de um certo dispositivo de origem, podem tornar-se complexas.

***(*)* Correlação:** Segundo Cruz (2012), a correlação tem como objectivo tentar definir uma relação coerente entre um conjunto de eventos registados, apresentando aos utilizadores da plataforma apenas um único evento, geralmente denominado "evento de correlação". Para tal, são definidas várias regras de correlação de forma a detectar estes padrões comportamentais. Vide o *anexo 5* – para exemplo de correlação!

e) Armazenamento de *logs*

Segundo Miller *et al.* (2011), há três formas de armazenamento para os *logs* que são gerados, nomeadamente: Base de dados, Arquivo de texto e Arquivo Binário.

f) Monitorização

Finalmente, segundo Cruz (2012), a fase de monitorização tem o objectivo de interagir activamente com os eventos recolhidos e guardados.

Para Miller *et al.* (2011), geralmente todo SEM usa uma interface *web* como console para interagir e entender melhor o que está acontecendo com os *logs*. Na *console* de gestão e monitorização do SIEM, podemos desenvolver as regras que serão usadas para extrair as informações dos eventos que serão processados.

Desta forma, a administração do SIEM ficará mais fácil, pois todo ambiente será visto trabalhando em conjunto em um único lugar.

2.3.2. Soluções de plataformas SIEM

Segundo Tavares (2015), actualmente a solução SIEM é muito utilizada por diversas empresas, instituições e centros académicos no âmbito de pesquisas.

A Gartner disponibiliza um leque considerável de análises feitas sobre diversas áreas e tecnologias existentes no mercado, análise das potencialidades de cada sistema e coloca à disposição no seu site. É interessante salientar que o Quadrante Mágico da Gartner é considerado como sendo umas das principais fontes de informação para as organizações. Para que uma solução SIEM esteja no Quadrante Mágico ela tem de possuir diversos méritos (Tavares, 2015).

Figura 16: Quadrante Mágico da Gartner.
Fonte: Gartner (2020).

De acordo com Gartner (2014) citado por Tavares (2015), os elementos e posições do quadrante mágico da SIEM podem ser classificados da seguinte forma:

Tipologia	Características
Challengers	Boa capacidade de execução, mas não agrega tanto na inovação.
Leaders	Boa em inovação e entregam o que prometem.
Niche Players	Não tem uma grande expressão no mercado actual como um todo e possuem produtos específicos comumente.
Visionaries	Tem extrema inovação, mas não possuem tanta capacidade para entregar o que prometem.

Tabela 1: Interpretação do quadrante Mágico da Gartner.
Fonte: Gartner (2014) citado por Tavares (2015).

Desta forma, de acordo com o relatório da Gartner de Fevereiro de 2020, as soluções líderes de mercado são as seguintes: Splunk, IBM, Exabeam, Securonix, LogRhythm, Rapid7, Dell Tecnologies (RSA). O relatório não apresenta soluções desafiadoras as líderes do mercado. Em relação a *niche players* encontram-se no mercado FireEye, AT&T Cybersecurity (OSSIM e USM Anywhere), McAfee, Micro Focus, Fortinet, HangSight, ManageEngine e SolarWinds. Finalmente, o referido documento identifica apenas como solução visionária o LogPoint.

No entanto, existem diversas soluções SIEM que não foram consideradas no relatório da Gartner por não possuir certos méritos, nomeadamente: GrayLog, Elastic Stack, BlackStatus, EventTracker, Trustwave, Venustech, entre outras.

Para fundamentar a escolha das soluções SIEM que serão utilizadas na análise comparativa, foi efectuada uma pesquisa tendo em conta se a solução é *open-source* ou não, e o preço/licença, ou seja, se a solução é grátis ou comercial.

Assim, foram escolhidas três soluções SIEMs com base no relatório da Gartner 2020, sendo duas delas: Splunk e IBM QRadar que são soluções comercias e de código fonte fechado (não open-source). A outra solução escolhida foi AlienVault OSSIM da AT&T Cybersecurity que é grátis e de código fonte aberto (*open-source)*. Sendo esta a única que possui tais características entre as soluções apresentadas no relatório da Gartner 2020.

A seguir far-se-á uma descrição básica em torno das soluções escolhidas de modo a contextualizar a análise que será feita ao longo do trabalho.

a) AlienVault OSSIM

Para Bowling (2010) citado por Tavares (2015), o OSSIM é o futuro da SIEM, quando fez a seguinte declaração “Conheça AlienVault OSSIM, um sistema de segurança complexo concebido para tornar a sua vida mais simples”.

De acordo com Tavares (2015), a AlienVault oferece SIEM em dois tipos de produto, sendo um deles o Open Source (OSSIM) e outro comercial (USM) Unified Security Management, que estende o OSSIM com melhorias de escala, gestão, administração consolidada e relatórios. AlienVault Labs proporciona uma alimentação integrada de inteligência relativamente à análise de ameaças para seus produtos comerciais, que inclui atualizações para assinatura, vulnerabilidade, correlação, relatórios e resposta a incidentes.

b) Splunk

Segundo Dionísio (2019), Esta plataforma e capaz de receber vários tipos de dados estruturados e não estruturados, normalizá-los, indexá-los e correlacionar os eventos em tempo-real. Assim, com estes dados é possível gerar gráficos, relatórios, alertas, dashboards e diferentes tipos de visualizações.

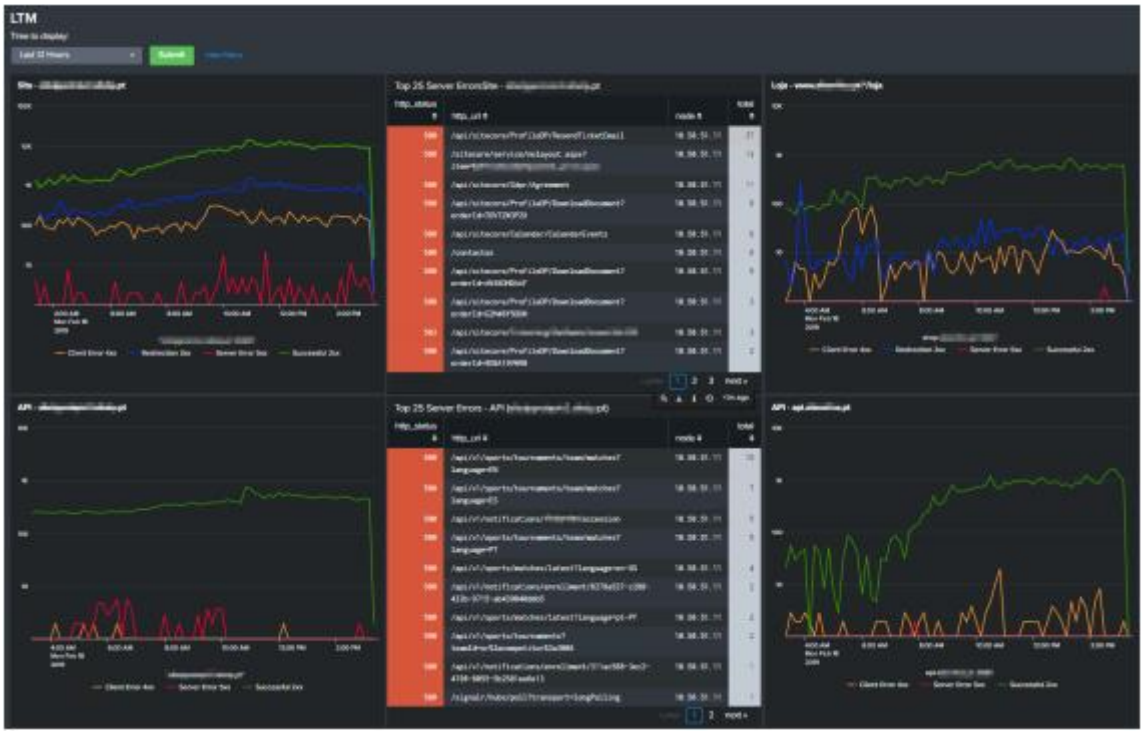

Figura 17: *Dashboards* de monitorização no Splunk.
Fonte: Dionísio (2019).

Ainda de acordo com Dionísio (2019):

- Esta plataforma é muito versátil, deixando de ser apenas uma plataforma para pesquisar dados num certo intervalo de tempo passando a ser uma aplicação que sustenta o negócio das empresas;
- As aplicações e integrações estão no centro da utilidade do Splunk sendo também bastante rápido e flexível a realizar as suas pesquisas. O Splunk e uma ferramenta muito completa para a monitorização operacional, segurança e analise do comportamento do cliente.
- A monitorização operacional é possível devido a automação dos alertas e a investigação de incidentes pelos logs da infra-estrutura. A nível de segurança devido a ser possível analisar todos os padrões de logs que não correspondem a padrões bons conhecidos.
- Com a junção de vários logs de vários sistemas é possível assim compreender os padrões de cada cliente, por exemplo, saber que um certo utilizador costuma ligar-se a infraestrutura da organização via VPN por um certo país.

c) IBM QRadar

Segundo Filipe (2020), a IBM QRadar Security Intelligence Platform é responsável por fornecer uma arquitetura unificada, a qual integra um sistema para gestão de eventos e informação de segurança (SIEM), gestão de logs, deteção de anomalias, análise forense de incidentes e configuração e gestão de vulnerabilidades.

Para além destes módulos, existem também aplicações, como é o caso da User Behavior Analytics (UBA), que criam ou estendem funcionalidades no QRadar, sendo geralmente desenvolvidas pela comunidade. O IBM Security QRadar, traduz-se numa arquitectura modular que disponibiliza em tempo-real, visibilidade sobre uma rede ou infra-estrutura das TIC, a qual pode ser utilizada para deteção e priorização de ameaças. É sobre esta arquitetura que é definida a operação do QRadar, a qual consiste na utilização de três camadas.

Desta forma, o QRadar recolhe, processa, agrega e armazena dados de diferentes fontes existentes na rede, em tempo real, permitindo-se depois fazer a gestão da segurança através da monitorização, geração de alertas e ofensas, bem como da resposta às diferentes ameaças. Para além do referido, o QRadar permite também a realização de pesquisas e produção de relatórios (Filipe, 2020).

3. Capítulo III – Caso de estudo

3.1. Instituto Nacional de Tecnologias de Informação e Comunicação

O INTIC é o órgão responsável por regular, supervisionar e fiscalizar o sector das Tecnologias de Informação e Comunicação (TIC) no nosso país. Sua génese foi a Unidade Técnica de Implementação da Política de Informática (UTIC), criada em 2002 para assessorar o Governo na introdução de TIC, tendo este estatuto vigorado até 2014, quando foi transformado no actual figurino de instituto público.

Inicialmente, tratou-se de um órgão bicéfalo, exercendo funções implementadoras e regulatórias ao mesmo tempo. Mas a Lei no 3/2017, de 9 de Janeiro, que estabelece os princípios, as normas gerais e o regime jurídico das transacções electrónicas em geral, do comércio electrónico e do governo electrónico em particular, acabaria com o regime bicéfalo ao designar o INTIC como a Entidade Reguladora da referida lei e remeter ao executivo a tarefa de criar uma autoridade de governo electrónico, que é o Instituto Nacional do Governo Electrónico (INAGE).

Assim, o INTIC passou a ocupar-se, entre outras funções, exclusivamente de:

- Garantir um ambiente seguro para Sociedade de Informação;
- Registar e licenciar provedores de serviços de TIC;
- Estabelecer regras de funcionamento do sector das TIC;
- Fiscalizar o cumprimento da legislação e outras normas do sector das TIC;
- Aplicar as penalizações;
- Promover políticas e boas práticas para o uso das TIC.

Como corolário da implementação da referida lei, a organização e funcionamento do INTIC foram revistos pelo Decreto no 90/2020, de 9 de Outubro, que materializa a vontade estatal de um maior controlo sobre a Sociedade de Informação, pela via da administração indirecta, em conformidade com o novo regime jurídico dos institutos, fundações e fundos públicos, aprovado pelo Decreto no 41/2018, de 23 de Julho.

A nova estrutura orgânica do INTIC integra um conselho de administração executivo, composto por três membros, incluindo o presidente, cobrindo as áreas operacionais e de apoio. Para o cumprimento das novas atribuições e funções, a estrutura operativa compreende as seguintes áreas:

- Divisão de Regulação e Fiscalização;

- Divisão de Licenciamento e Certificação;
- Divisão de Segurança Cibernética e Protecção de Dados; e
- Divisão de Governação Digital.

Com apenas cerca de quatro anos de existência, o processo de estruturação do INTIC ainda está por finalizar, a condição "*sine qua non*" para levar adiante a sua missão. Entretanto, são de destacar alguns projectos de impacto executados neste período, que actuou como regulador:

- Elaboração da Lei das Transacção Electrónicas e sua regulamentação através do Regulamento da Interoperabilidade do Governo Electrónico e do Regulamento do Sistema de Certificação Digital, este último ainda na fase de aprovação;
- Elaboração da Política para a Sociedade de Informação e a corresponde estratégia de implementação;
- Elaboração de Política de Segurança Cibernética e sua estratégia de implementação;
- Elaboração de Regulamento de Registo do Domínio "*.mz*";
- Elaboração de Regulamento de Provedores de Serviços de Internet;
- Adopção da Norma ISO das TIC pelo nosso país;
- Ratificação das convenções internacionais sobre a Segurança Cibernética pelo nosso país.

O processo de regulamentação da Lei das Transacções Electrónicas vai abarcar vários aspectos de regulação da Sociedade de Informação e está a ser conduzido de forma faseada em função das demandas administrativas, como foi o caso da interoperabilidade do governo electrónico, gestão do domínio "*.mz*" e uso da *Internet*.

3.1.1. Visão, Missão, Objectivos, Valores e Serviços

3.1.1.1. Visão

Ser referência em matérias de regulação, políticas, estratégias, modelos e padrões de uso das tecnologias de informação e comunicação, concorrendo para posições de destaque a nível regional e internacional.

3.1.1.2. Missão

Regular e fiscalizar o uso de TIC nos sectores público e privado, sociedade civil, instituições académicas e de pesquisa, como instrumento de melhoria de governação e desenvolvimento nacional.

3.1.1.3. Objectivos

- Regular e disciplinar o sector das tecnologias de informação e comunicação;
- Contribuir para a modernização dos serviços públicos e a elevação dos índices da competitividade do país em todas as esferas económicas e sociais;
- Contribuir para a integração do país na Sociedade Global de Informação e do Conhecimento, através de elaboração de políticas e estratégias alinhadas com os principais instrumentos programáticos de governação.
- Contribuir para a redução da pobreza e geração da riqueza através das TICs, promovendo a inovação tecnológica e a modernização para um desenvolvimento acelerado;
- Contribuir para a aceleração da reforma da administração pública, transparência e governação participativa e melhoria de prestação dos serviços públicos;
- Contribuir para a massificação de ensino, acesso e uso das TICs no país como instrumento de melhoria do desempenho social, da qualidade de vida e do bem-estar da população através da optimização dos serviços de saúde e da educação, em especial nas zonas rurais, com recurso às TICs;
- Contribuir para a garantia de elevados padrões de qualidade e segurança na implementação e uso das TICs, em ambiente de Convergência Tecnológica.

3.1.1.4. Valores

- Inovação na busca e criação de um ecossistema para facilitar o cumprimento da missão da instituição;
- Dinamismo no desempenho das funções e na regulação de serviços e relacionamento com a Sociedade da Informação; e
- Excelência nos resultados alcançados no âmbito da regulação de serviços de TIC.

3.1.1.5. Serviços

No cumprimento da sua missão, o INTIC implementa os seguintes serviços:

- Fiscalizar o sector das TIC;
- Registo de provedores de serviços de TIC;
- Registo e gestão de domínio "*.mz*";
- Credenciar Entidades de Certificação Digital;
- Realizar auditorias sobre o funcionamento, conformidade, segurança, qualidade de SI e TIC;
- Emitir parecer sobre o licenciamento comercial das organizações comerciais na área das tecnologias de informação e comunicação.

3.1.2. Estrutura orgânica

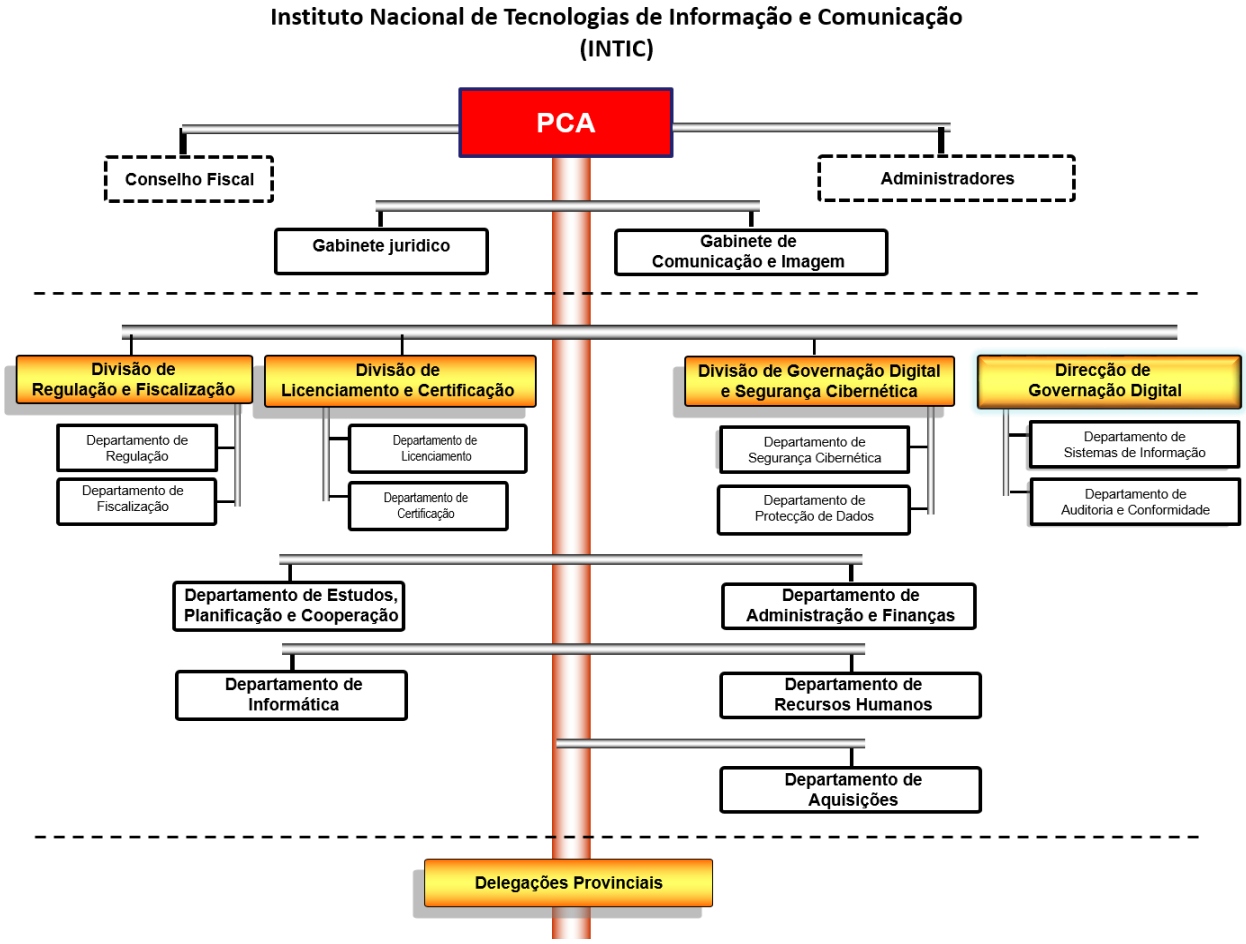

Figura 18: Estrutura orgânica do INTIC.
Fonte: https://www.intic.gov.mz/?page_id=568

3.1.3. Descrição da situação actual

Actualmente, o Instituto Nacional de Tecnologias de Informação e Comunicação tem na sua infra-estrutura de rede corporativa como provedor de serviços de internet (ISP) a GovNet que é a Rede Electrónica do Governo, tem como activos:

- Servidor de Ficheiros;
- Servidor Controlador de domínio;
- Servidor de Impressora;
- Telefones e câmaras IP;
- Switches e Roteadores;
- Computadores Laptops e Desktops, entre outros.

Ainda na infra-estrutura de rede corporativa do Instituto nacional de Tecnologias de Informação e Comunicação, em relação aos mecanismos de segurança temos: Uma máquina firewall e um IPS (Sistema de Prevenção de Intrusão).

3.1.4. Constrangimentos

Actualmente, podem ser listados os seguintes:

- Falta de um mecanismo capaz de realizar o inventário, detecção de alterações nos activos e que ainda descubra activos não autorizados na infra-estrutura de rede corporativa;
- Não é feita monitorização da disponibilidade dos activos na infra-estrutura de rede corporativa;
- Falta de um Sistema de Detecção de Intrusão (IDS), quer baseado em rede (NIDS) ou baseado em Host (HIDS) na infra-estrutura de rede corporativa;
- Não feita a gestão centralizada e automatizada de logs na infra-estrutura de rede corporativa;
- Capacidade de correlação de logs de segurança gerados pelos activos é praticamente inexistente para identificar ameaças em tempo útil;
- Inexistência de um mecanismo de capaz de realizar *scans* de vulnerabilidades aos activos da infra-estrutura de rede corporativa;

4. Capítulo IV – Proposta de Solução

4.1. Análise de soluções SIEMs

Para a realização da presente análise comparativa, foram consideradas as soluções Splunk, IBM QRadar e AlienVault OSSIM da AT&T Cybersecurity e de seguida foram definidos critérios (vide a tabela 1), que foram escolhidos de acordo com os seguintes aspectos em torno das plataformas SIEM:

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

No que diz respeito as principais funcionalidades e as características observar na implementação, para González-Granadillo *et. al* (2021), podem-se listar as seguintes: Regras de correlação, Fonte de dados, Processamento em tempo real, Visualização, Volume de dados, Análise de dados, Desempenho, Forensics, Complexidade, UEBA (User and Entity Behavior Analytics), Escalabilidade, Recursos de reação e relatório, Analise de risco, Armazenamento, Resiliência e Segurança.

Contudo, para o presente trabalho foram considerados relevantes para avaliação as seguintes: Regras de correlação, Processamento em tempo real, Volume de dados, Análise de dados, Forensics, Escalabilidade, Complexidade, Resiliência e Segurança.

Apresentados os aspectos que motivaram a escolha de cada um dos critérios, agora será feita a descrição de alguns deles segundo González-Granadillo *et. al* (2021):

- **Regras de correlação:**

Este recurso avalia o poder das regras de correlação para o sucesso da detecção de um evento por um SIEM. Enquanto a maioria dos SIEMs possui regras básicas de correlação, poucos deles têm recursos de pesquisa robustos e suportam linguagens de processamento de pesquisa para escrever pesquisas que podem ser utilizadas nos dados do SIEM.

- **Volume de dados:**

Este recurso avalia a possibilidade dos sistemas actuais suportarem grandes volumes de dados para operações de correlação, indexação e armazenamento. Analisar grandes volumes de dados provenientes de diferentes fontes é importante para obter mais *insights* dos eventos colectados e ter uma melhor monitorização.

- **Processamento em tempo real:**

Esse recurso considera a capacidade de um SIEM de lidar com dados em constante mudança. Ele avalia os controles em tempo real, monitorização e recursos de *pipeline* implantados pela ferramenta na prevenção ou reação à segurança cibernética, bem como os recursos de computação de desempenho que os SIEMs têm para eventos em tempo real.

- **Análise de dados:**

Versões mais recentes dos principais SIEMs suportam ampla integração com detectores de anomalias baseados em aplicativos e usuários. Essas capacidades incluem a análise do comportamento de funcionários, terceiros contratados e demais colaboradores da organização. Para isso, o SIEM deve contemplar a gestão de perfis de usuários/aplicativos e o uso de técnicas de aprendizado de máquina para detecção de mau comportamento.

- **Forensics:**

Além dos recursos de registro, alguns SIEMs oferecem recursos forenses de rede integrados que incluem capturas de pacotes de sessão completa de conexões de rede consideradas maliciosas com o objetivo de converter dados de pacotes em documentos, páginas da *Web*, VoIP e outros arquivos reconhecíveis.

- **Escalabilidade:**

Esse recurso considera a capacidade de uma implantação de SIEM crescer não apenas em termos de *hardware*, mas também em termos de número de eventos de segurança colectados na borda da infra-estrutura de SIEM.

- **Complexidade:**

SIEMs são conhecidos por serem difíceis de implantar e gerenciar. No entanto, é importante entender se o sistema analisado pode ser instalado para testes com baixa ou esforço moderado.

- **Segurança:**

Este recurso avalia a capacidade de implementar automação de segurança, bem como recursos de criptografia nativa presentes no SIEM durante a Monitorização, Detecção, Correlação, Análise e Apresentação dos resultados.

- **Resiliência:**

Resiliência ou tolerância a falhas é uma característica importante de qualquer sistema de monitorização crítico. É importante entender quais são os recursos de tolerância a falhas dos SIEMs existentes, por exemplo, se o mecanismo de correlação oferece suporte à tolerância a falhas; a forma como a recuperação de desastres e a replicação são suportadas no armazenamento de eventos; se os conectores suportarem alta recursos de disponibilidade.

- **Open-Source:**

Avalia a forma como o código fonte das soluções SIEM é disponibilizado, ou seja, se é *open-source* (código fonte aberto) ou não *open-source*, isto é, código fonte fechado.

- **Preço/Licença**

Esse recurso avalia o método de licenciamento associado à solução SIEM, ou seja, se a solução é Grátis ou Comercial.

Na tabela abaixo, os critérios são valorados como: Baixo (mal ou não implementado), Médio (parcialmente implementado) e Alto (totalmente implementado), a exceção do critério *open-source* que só assume valores binários (Sim ou Não) e Preço/Licença que assume os valores: Grátis ou Comercial.

Critérios	**Plataformas SIEM**		
	Splunk	**AlienVault OSSIM**	**IBM QRadar**
Regras de Correlação	Baixo	Alto	Médio
Processamento	Alto	Alto	Alto
Volume de dados	Alto	Médio	Médio
Análise de dados	Alto	Médio	Alto
Forensics	Médio	Alto	Alto
Escalabilidade	Alto	Baixo	Alto
Complexidade	Alto	Médio	Médio
Resiliência	Alto	Médio	Alto
Segurança	Médio	Médio	Alto
Open-Source	Não	Sim	Não
Preço/Licença	Comercial	Grátis	Comercial

Tabela 2: Análise comparativa de soluções SIEM.
Fonte: Adaptado de González-Granadillo et. al (2021).

As cores representam a avaliação em relação a valoração de cada critério de acordo com os objectivos que se pretendem alcançar, nomeadamente o vermelho para Mau, amarelo para Normal e verde para Bom.

	Mau	Normal	Bom
Splunk	4	2	5
AlienVault OSSIM	1	5	5
IBM QRadar	2	3	6

Tabela 3: Resumo da análise comparativa.
Fonte: Elaborada pelo autor.

Pela análise comparativa, chegou-se a conclusão de que a solução que melhor se adequa as condições e a realidade actual da Infra-estrutura de rede corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação é AlienVault OSSIM. Desta forma, o autor propõe a sua implementação.

Na tomada dessa decisão, três critérios tiveram maior impacto, respectivamente:

O primeiro deles é o Preço/Licença da solução AlienVault OSSIM que é grátis, assim, para sua implementação não haverá necessidade de nenhum capital financeiro por parte do Instituto Nacional de Tecnologias de Informação e Comunicação.

O segundo é o facto da solução AlienVault OSSIM ser open-source, ou seja, o código fonte é aberto. Isso permite que o Instituto Nacional de Tecnologias de Informação e Comunicação use-o para estudar, modificar de acordo com as suas pretensões, entre outras possibilidades, como distribuir de graça independentemente da finalidade.

O terceiro é o facto da complexidade da solução AlienVault OSSIM ser média, assim a sua implementação não demandaria uma quantidade de capital humano elevado de tal forma que o Instituto Nacional de Tecnologias de Informação e Comunicação não pudesse disponibilizar.

4.2. Descrição da solução proposta

4.2.1. Open-Source Security Information Management – OSSIM

Segundo Pinto (2019), o OSSIM é descrito pela própria AlienVault no seu site como um SIEM de código aberto rico em recursos completos com recolha, normalização e correlação de eventos (*logs*).

Em 2019, a AlienVault foi comprada pela empresa AT&T Cybersecurity, que segundo Vazão (2020), oferece vários serviços relacionados com a segurança, entre os quais dois SIEMs, um deles é *open-source*, o AlienVault OSSIM™, e o outro comercial, i.e., um produto pago, o Unified Security Management (USM) Anywhere™ que estende o OSSIM com melhorias em termos escalabilidade, resiliência, gestão eficaz de *logs*, administração consolidada e relatórios avançados.

De acordo com o *site*[5], o SIEM AlienVault OSSIM fornece uma plataforma unificada, projectada principalmente para ajudar organizações de médio porte a defender contra as ameaças avançadas. A plataforma AlienVault OSSIM oferece (5) cinco recursos de segurança essenciais em um único console, como ilustra a figura a seguir.

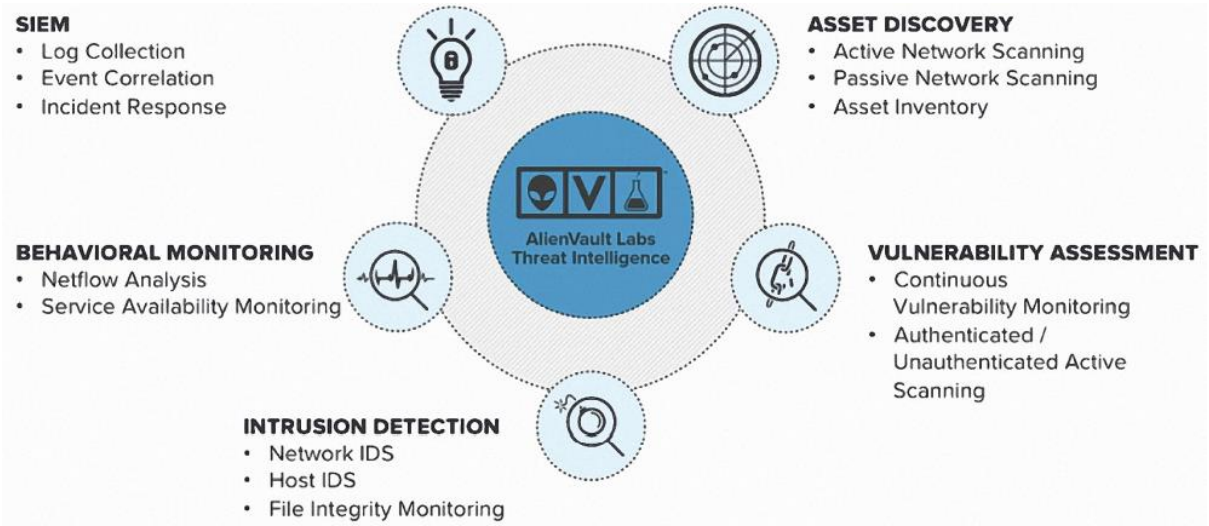

Figura 19: Principais funcionalidades do OSSIM/USM.
Fonte: AT&T Cybersecurity (2022) – USM Appliance™ User Guide

A seguir, far-se-á a descrição sucinta de cada umas das principais funcionalidades: Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioral Monitoring e SIEM de acordo com AT&T Cybersecurity (2022) – USM Appliance™ User Guide:

[5] *https://cybersecurity.att.com/products/ossim*

- **Asset Discovery**

O OSSIM descobre recursos no ambiente da organização, detecta alterações nos activos e descobre activos não autorizados na rede. A descoberta de activos utiliza ferramentas passivas, como a impressão digital do sistema operativo passivo e a descoberta de serviço passivo. A descoberta de activos também utiliza o *scanner* da rede, que pode ser programado/configurado para ser executado periodicamente ou executado manualmente.

- **Vulnerability Assessment**

Pode ser feita através de dois modos: não autenticados ou autenticados, identificando vulnerabilidades ou conformidade, comparando o software instalado nos activos com uma base de dados de vulnerabilidades conhecidas.

Com o *scanner* autenticado e o uso de uma conta de utilizador *admin*, o OSSIM pode verificar os activos com mais eficiência. As verificações de vulnerabilidades podem ser agendadas par ser realizadas periodicamente ou executadas manualmente.

- **Intrusion Detection**

Monitoriza o tráfego de rede em busca de actividades mal-intencionadas, monitoriza as mensagens de registo do sistema (*logs*) e as actividades do utilizador. A detecção de intrusão do OSSIM consiste em *Host* IDS e *Network* IDS.

- **Behavioral Monitoring**

A monitorização comportamental fornece uma visibilidade sobre padrões de tráfego e fluxos de rede (dados do NetFlow), que são usados para detectar anomalias que podem indicar violações da política de segurança.

Os dados usados para monitorização e análise comportamental são recolhidos de dispositivos de rede, fluxos baseados em *Port mirroring* (tráfego espelhado ou tráfego em modo promíscuo) e monitorização da disponibilidade de activos.

- **SIEM Event Correlation**

A inteligência de segurança do SIEM combina e correlaciona de *logs* colectados e outros dados para encontrar padrões anómalas ou mal-intencionados no tráfego da rede e no registo de actividades de computadores.

4.2.2. Arquitectura do OSSIM

Segundo Vazão (2020), os componentes da arquitetura da solução USM *Anywhere* são os seguintes: Web UI, USM *Server*, USM *Logger* e USM *Sensor*. A arquitetura da solução OSSIM é semelhante, mas não inclui o USM *Logger*, entretanto, para que se possa perceber melhor o seu funcionamento como um todo, serão explicados de seguida todos os componentes da figura abaixo.

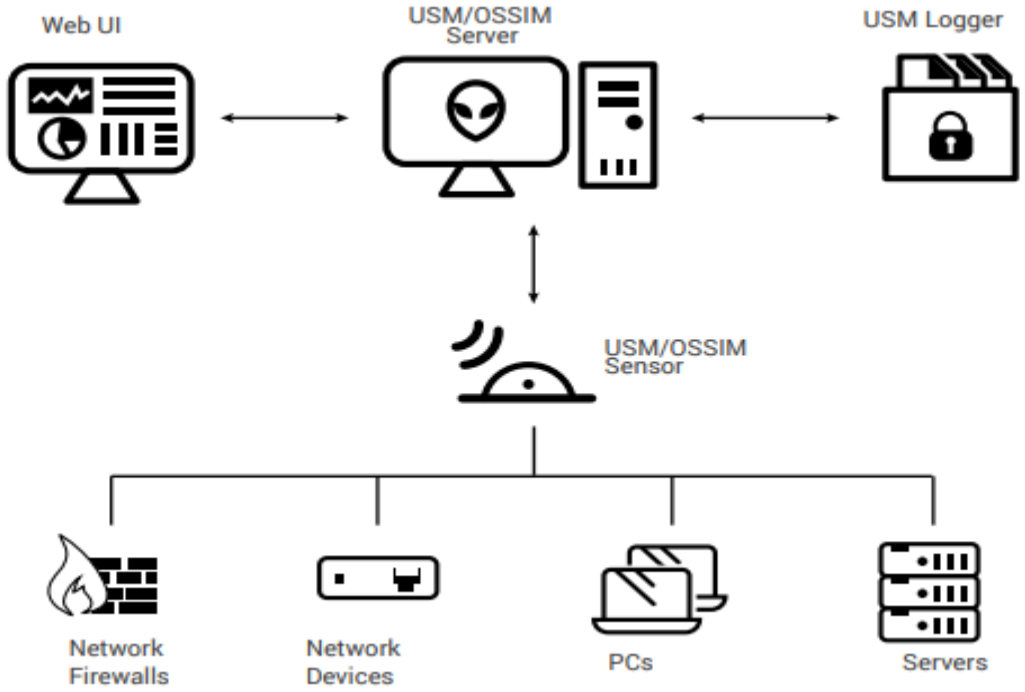

Figura 20: Arquitectura do OSSIM/USM.
Fonte: Adaptado de AT&T Cybersecurity (2022) – USM Appliance™ User Guide.

De acordo com AT&T Cybersecurity (2022) – USM Appliance™ User Guide:

- **OSSIM Sensor:** são instalados na infra-estrutura de rede corporativa que se pretende supervisionar e os dados recolhidos nos diferentes dispositivos são normalizados e enviados para o servidor para serem processados.
- **OSSIM Server & Web User Interface (UI):** agrega e correlaciona os logs recolhidos pelos OSSIM Sensors e inclui também a interface Web (Web UI), para que seja possível administrar a infraestrutura de rede, criar relatórios e gerir os eventos de segurança.
- **USM Logger:** O USM Appliance Logger só está disponível na versão USM e permite guardar os logs recolhidos pelos sensores, o mesmo acontecendo para a pesquisa forense e para a criação de relatórios de conformidade mais detalhados.

4.2.3. Activos, Risco e Ameaças no OSSIM

Segundo AT&T Cybersecurity (2022) – USM Appliance™ User Guide:

O princípio fundamental do OSSIM é que ele monitoriza os activos. Os activos são todos os dispositivos de uma organização que têm valor para a mesma, normalmente, são activos que podem ser monitorizados, recolher informações sobre *status*, integridade ou disponibilidade, configuração actividade e eventos. O valor prende-se com o custo do próprio dispositivo, o valor dos dados que ele armazena ou a informação que nele circula. A seguir indicam-se algumas características dos activos:

- Um activo é definido como através de endereço IP exclusivo;
- Os activos são organizados em redes com base no endereçamento IP;
- As redes são organizadas em locais ou regiões, com base da sua localização geográfica.

Quando a nossa organização é geograficamente dispersa, geralmente recorre-se a utilização de pelo menos um sensor para monitorizar cada local geograficamente independente. Cada sensor monitorizará o seu site e enviará informações para o OSSIM server sobre os activos que estão no mesmo local. *Plugins* são usados no Sensor OSSIM para extrair e normalizar dados de diferentes fontes de dados em eventos de formato padrão.

O OSSIM fornece uma ampla variedade de plugins que podem ser usados para recolher eventos para as fontes de dados mais comummente encontradas. Podemos ativar até 10 *plugins* por activo e até 100 plugins por Sensor

Na maioria das organizações, as prioridades das operações de segurança de rede são determinadas principalmente pelo risco, isto é, factores como o valor dos activos, o dano potencial que as ameaças específicas representam aos activos e as vulnerabilidades desses activos às ameaças e a probabilidade de que os ataques reais serão tratados.

No OSSIM os valores de risco são calculados para cada evento recebido do sensor OSSIM, bem como para eventos de segurança adicionais gerados como resultado de correlação ou correlação cruzada de vários eventos. O OSSIM gera um alarme para qualquer evento que tenha um valor de risco calculado maior ou igual a 1. A fórmula usada pelo OSSIM para calcular o risco de eventos individuais é a seguinte:

Risco = (Activo*Prioridade*Fiabilidade)/25, *o*nde:

- **Activo** – Ou valor do activo é um valor compreendido entre (0 e 5) que a organização atribui a cada activo.
- **Prioridade de evento** é uma classificação de prioridade compreendida entre (0 e 5) baseada no tipo de evento, como falha de autenticação, ataque na Web ou negação de serviço, que indica a urgência com a qual um evento deve ser investigado. A AlienVault fornece uma taxonomia de eventos para classificar vários eventos por categoria e subcategoria.
- **Fiabilidade** – do evento é uma classificação de fiabilidade compreendida entre (0 e 10) que especifica a probabilidade de um evento ser um ataque real ou um evento Falso Positivo.

Ameaças e vulnerabilidades são o que correlacionam a ocorrência de certos eventos com o risco e geram alarmes quando os valores de risco dos eventos excedem um valor limite específico (> ou = 1). Informações sobre ameaças específicas são obtidas de fontes como as relatadas pelo AlienVault Labs e pelo OTX.

Por exemplo, o OTX fornece indicadores de comprometimento (IoCs) e notificações de *hosts* maliciosos, que podem vincular activos por suas vulnerabilidades a ameaças específicas e notificação sobre eventos que envolvam hosts mal-intencionados conhecidos ou suspeitos.

O OSSIM também pode executar verificações que identificam as vulnerabilidades dos activos a ameaças específicas e identificadas, pois como descrito anteriormente, ele conta com um conjunto de ferramentas para executar este tipo de acções.

4.2.4. Características e Ferramentas do OSSIM

Segundo Pinto (2019), o OSSIM é um sistema centralizado de gestão de eventos e informações de segurança, com sistema operativo assente na distribuição GNU/Linux Debian, que o seu *download* pode ser feito gratuitamente e é composto por diversas ferramentas *open source* (código aberto) integradas, nomeadamente:

- **Nmap** – É uma ferramenta para descoberta de rede e auditoria de segurança. O nmap permite identificar quais os dispositivos que estão a ser executados nos seus sistemas, descobrindo os hosts disponíveis e que serviços correm, descobrindo portas abertas e detetando riscos de segurança.

- **P0f** – É uma ferramenta que utiliza uma matriz de sofisticados mecanismos de impressão digital de tráfego puramente passivo, com objectivo de identificar os intervenientes por traz de qualquer comunicação TCP/IP acidental.
- **ArpWatch** – Monitoriza a actividade numa rede, mantendo actualizada uma tabela com endereços Ethernet, i.e., endereços Media Access Control (MAC) e seus respectivos endereços IP. O Arpwatch é uma ferramenta importante na monitorização da rede contra ataques de Address Resolution Protocol (ARP), Arp Poisoning ou Arp Spoofing usados para realizar ataques mais sofisticados como (MITM) Man-in-the-Middle.
- **OpenVas** – É uma ferramenta de *scanner* de vulnerabilidades mais popular da actualidade. Segundo Miller *et al.* (2011) é uma versão GPL do Nessus, um popular software de código aberto ferramenta de varredura de vulnerabilidade. Esta ferramenta é usada para fornecer varreduras de vulnerabilidade de rede activos e adicionar essas informações valiosas ao banco de dados OSSIM.
- **Snort** – É um sistema de prevenção de intrusões de código aberto capaz de analisar o tráfego de rede em tempo real e o registo de pacotes (*logs*). Pode ser configurado para operar em três modos, nomeadamente: Sniffer (lê os pacotes da rede e exibe-os continuamente na consola); Packet Logger (regista os pacotes para o disco); NIDS (realiza detecção e análise no tráfego de rede).
- **Spade** – Esta ferramenta, é normalmente utilizada para obter conhecimentos sobre os ataques sem assinatura. A ferramenta detecta conexões anómalas analisando as portas utilizadas e o seu respectivo destino.
- **Tcptrack** – É um *sniffer* que mostra as informações sobre conexões TCP numa interface especifica para correlação de ataques. Fornece informações úteis para os administradores rastrearem cada conexão única aos seus servidores. O tcptrack também tem um recurso de filtragem, e utiliza o padrão de filtragem Packet Capture (PCAP) - idêntico ao usado no tcpdump.
- **Nagios** – É uma ferramenta poderosíssima de monitorização de sistemas, permitindo as organizações saber em tempo real sobre a disponibilidade de um certo recurso computacional, assim, possibilitando identificar e solucionar problemas nas infraestruturas de TI antes de estes afetarem os processos críticos do negócio.

- **Ntop** – É uma ferramenta para monitorizar e gerir sistemas de rede, além dos imensos recursos que providencia tem a capacidade de o demonstrar através de gráficos e informações detalhadas, permitindo uma melhor interação com o utilizador.
- **Osiris** – Host Integrity Monitoring System (HIMS) é utilizada para monitorizar equipamentos *Windows* e recolher em tempo real dados sobre alterações em arquivos utilizando *checksums*, alterações em portas, utilizadores e de *kernel*.
- **OSVDB** – Conforme Miller *et al.* (2011), o projeto Open Source Vulnerability Database mantém informações sobre vulnerabilidades e é incorporado ao OSSIM. É usado durante o processo de correlação de eventos e fornecido ao analista de segurança conforme necessário.
- **OCS-NG** – É um software que permite inventariar os activos de TI. Recolhe as informações sobre o *Hardware ou Software* de dispositivos, executando um cliente de OCS Inventory Agent. O OCS tem a capacidade de disponibilizar o inventário por *interface web*.
- **OSSEC** - É uma ferramenta de detecção de intrusão baseada em hosts que monitoriza *logs* de serviços e sistemas, faz verificação de integridade de arquivos, monitorização de políticas, detecção de *rootkits*, envia alertas em tempo real e resposta activa, i.e., permite a execução de uma acção baseada num evento.

  É uma ferramenta granular e personalizável podendo correr praticamente em todos os sistemas operativos.

4.3. Desenvolvimento da solução proposta

4.3.1. Descrição do cenário proposto para implementação da solução

Para testar a solução SIEM OSSIM da AT&T Cybersecurity e consequentemente motivar a direção do Instituto Nacional de Tecnologias de Informação e Comunicação a tomar uma possível decisão sobre a utilização da mesma é proposto o cenário da figura 17, que é relativamente similar ao da instituição, mas com a rede segmentada em sub-redes de acordo com a sua índole.

A montagem do cenário foi feita num ambiente virtualizado, com recurso a ferramenta de virtualização VMware *Workstation* 16 Pro serão criadas máquinas virtuais para cada uma das máquinas ilustradas no cenário para poder implementar a solução e realizar os testes.

Por não fazer parte do âmbito do presente trabalho, não serão abordados com detalhes os aspectos relacionados com a virtualização e/ou configuração dos serviços apresentados no cenário, com exceção do servidor SIEM OSSIM, entretanto serão ressaltados alguns aspectos com o objectivo de contextualizar os testes.

No cenário temos o mecanismo de segurança *Firewall* que é responsável por fazer a interligação das redes, roteamento de pacotes, delimitação do perímetro entre a rede interna e a rede externa e o controlo de tráfego.

– Na rede interna temos as seguintes sub-redes:

- **Subnet – Clients (192.168.1.0/24)**

É constituída por estações de trabalho, isto é, máquinas dos usuários que acedem aos serviços e recursos da infra-estrutura de rede corporativa, no cenário, colocou-se uma máquina (Usuário – 192.168.1.1) com o Sistema Operativo *Windows* 7.

- **Subnet – Servers (192.168.2.0/24)**

Nesta sub-rede, temos um servidor (*Win. Server* – 192.168.2.1) que é o Controlador de Domínio com as funcionalidades de *Active Directory Domain Services (*AD DS*), Dynamic Host Control Protocol* (DHCP) que foram instaladas e configuradas sobre o Sistema Operativo *Windows Server* 2012 x64.

- **Subnet – Security Management (192.168.3.0/24)**

Esta sub-rede é responsável pela gestão da segurança a nível de toda infra-estrutura de rede corporativa. Contém duas máquinas, nomeadamente…:

(*) Admin (192.168.3.2) que será usada para aceder à *interface web (*administrativa*)* da plataforma SIEM OSSIM.

(*) Na outra máquina teremos instalado e configurado o servidor SIEM OSSIM que possui uma porta espelhada, ou seja, Networking Monitoring que é uma interface da subnet Clients que irá actuar em modo promíscuo, desta forma, permitindo ao servidor receber todos os pacotes que passam pelos referidos *switches* e ainda monitorizar o tráfego de rede. Em relação ao segmento de rede DMZ e a subnet Servers as suas interfaces foram configuradas como Log Collection & Scanning (HIDS), permitindo assim ao Servidor colher os logs e realizar scan de vulnerabilidades aos hosts dessas subnets.

– Entre a rede interna e a rede externa temos o segmento rede:

- **DMZ (172.16.1.0/24)**

Nesta zona será disponibilizado um serviço *web* que se pretende assegurar acesso tanto para a rede exterior assim como para a rede interna, para tal, esse serviço foi configurado na máquina (172.16.1.1), e foi instalado propositadamente um serviço *web* que possui vulnerabilidades que serão exploradas pelo atacante para se poder analisar o processo de detecção de ataques cibernéticos no OSSIM.

– Finalmente, na rede externa (à *internet*-rede pública) temos:

- **Atacante (IP Público)**

O sistema operativo Kali Linux que é baseado na distribuição Debian e muito popular entre os profissionais e estudantes da área de segurança cibernética, este sistema possui um conjunto de ferramentas que permitem aos seus usuários realizar testes de intrusão. Desta forma, partindo da internet, o atacante com recurso à Kali Linux realizará testes de intrusão com objectivo de explorar algumas vulnerabilidades presentes no servidor *Web* e servidor *Windows Server* 12.

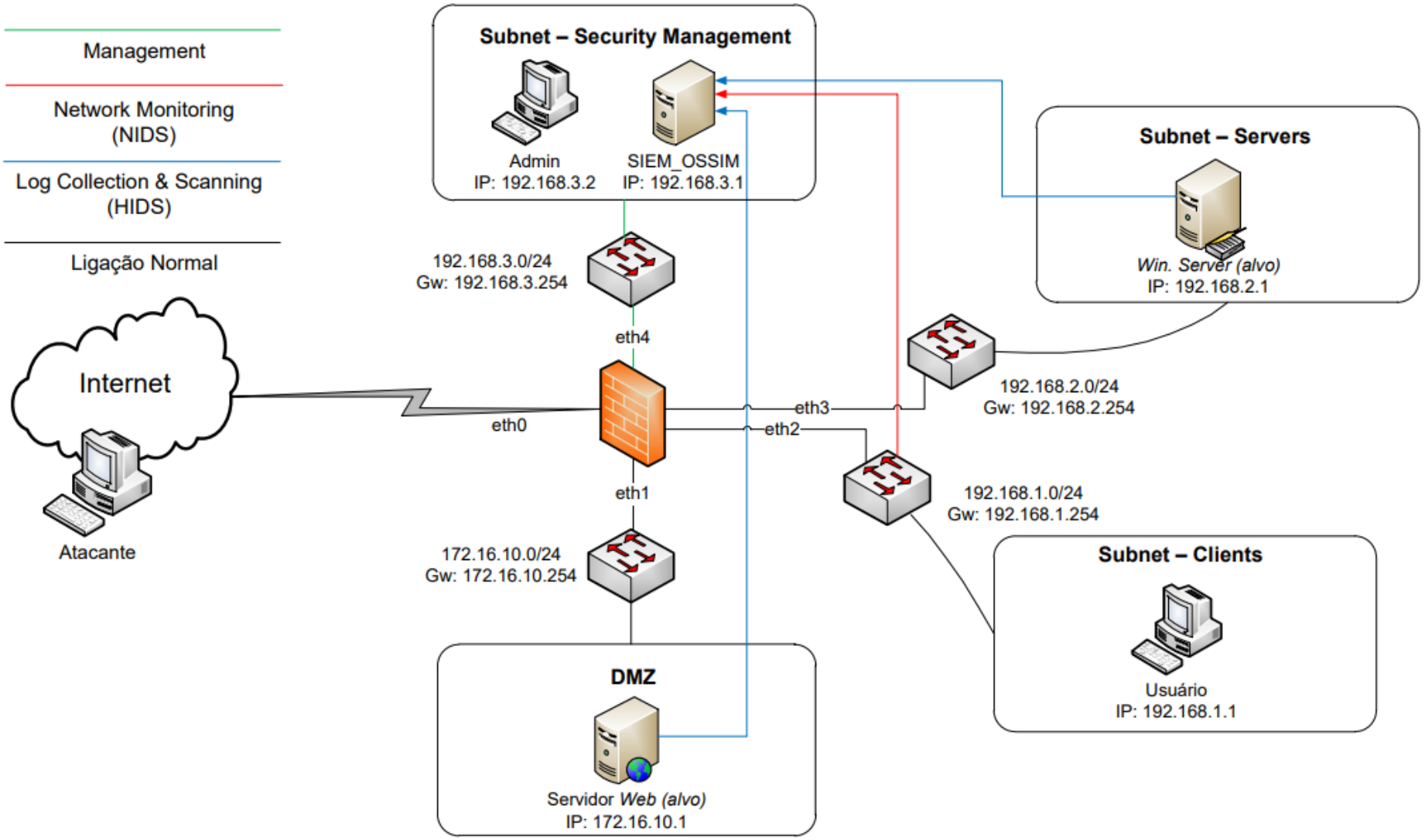

Figura 21: Cenário proposto para implementação da solução. Fonte: Elaborado pelo autor.

5. Capítulo V – Apresentação e Discussão de Resultados

5.1. Revisão da Literatura

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

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

A incidência de falsos positivos nos IPS mostrou-se altamente crítica e prejudicial à produtividade, visto que, tráfego legítimo é bloqueado devido a uma falsa suspeita de ataque cibernético, enquanto nos IDS, segundo Mamede (2006), fazem com que os administradores tenham de investigar cada um dos alertas de falsa intrusão, o que os pode levar a desligar o(s) alerta(s).

Em relação aos falsos negativos, tanto para um IDS ou IPS, representam um sério e grave problema de segurança, visto que nesse tipo incidência, tráfego ilegítimo chega até a infra-estrutura de rede corporativa.

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

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

Finalmente, debruçou-se em torno das plataformas SIEMs e com base no relatório da Gartner 2020, pudemos conhecer os principais vendors deste tipo de soluções.

6. Capítulo VI – Considerações Finais

6.1. Conclusões

Actualmente, as soluções SIEM emergem da necessidade adicionar mais um nível de segurança em infra-estruturas de redes corporativas de empresas ou instituições, em especial para aquelas que lidam diariamente com diversos dados sensíveis, por este e outros motivos as plataformas SIEMs devem ser vistas como uma obrigação.

O presente trabalho de pesquisa teve como objectivo geral propor a implementação de uma plataforma SIEM na Infra-estrutura de rede corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), assim, para se alcançar este objectivo geral foram definidos três objectivos específicos, apesar do último objectivo não ser relevante para o alcance do objectivo geral, pois o mesmo aborda questões de prova de conceito (testes).

- O primeiro, consistiu na análise da segurança cibernética na Infra-estrutura de rede corporativa do INTIC. Este foi um objectivo cumprido visto que foi possível descrever ao longo do trabalho sobre como é feita a segurança cibernética em infra-estruturas de redes corporativas no geral e com base nisso foi possível elaborar uma entrevista e um questionário para instituição o que nos permitiu saber o seu ponto de situação e os principais constrangimentos enfrentados;
- O segundo, que também foi cumprido, pois foi possível realizar uma análise comparativa entre soluções de plataformas SIEM. Onde para a escolha das soluções, fez-se um estudo em torno do relatório da Gartner 2020 a partir do qual selecionam-se três soluções SIEM, nomeadamente: Splunk, IBM QRadar e AlienVault OSSIM para uma análise comparativa, tendo a AlienVault OSSIM sido escolhida porque de entre três soluções era a que melhor se adequava as condições e realidade actual da instituição.
- Finalmente, o terceiro objectivo que consistia em implementar a solução SIEM escolhida numa infra-estrutura de rede corporativa virtualizada para efeito de testes. Que não foi possível cumprir pois questões tempo para a realização do trabalho e também a performance do computador utilizado não ajudou durante esse processo o que acabou demandando mais tempo para a sua realização.

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

Em relação a pergunta de pesquisa:

De que forma as empresas e instituições moçambicanas podem ter uma visão global sobre o que acontece em tempo real na sua infra-estrutura de rede corporativa de modo a detectar e/ou mitigar ataques cibernéticos cada vez mais sofisticados?

Terminado o trabalho, chegou-se a conclusão de que o uso de plataformas SIEMs pode ajudar as empresas e instituições moçambicanas a ter uma visão global sobre o que acontece em tempo real na sua infra-estrutura de rede corporativa de modo a detectar e/ou mitigar ataques cibernéticos cada vez mais sofisticados

6.2. Recomendações

Recomenda-se ao Instituto Nacional de Tecnologias de Informação e Comunicação que Implemente a solução proposta neste trabalho e que crie uma CSIRT Institucional (Equipe de Resposta a Incidentes Computacionais Institucional).

Em relação a futuros trabalhos de pesquisa, recomenda-se:

- Uso de SIEM para Business Intelligence;
- Gerador de eventos para testes de configurações de um SIEM;
- Analise de soluções de plataforma SIEM de alta disponibilidade;
- Implementação de uma plataforma SIEM em conformidade com a LGPD como por exemplo PCI DSS, HIPAA, ISO 27001 entre outras.

6.3. Constrangimentos

Durante a realização do presente trabalho de pesquisa encontram-se os seguintes:

- Dificuldades para conciliar o tempo para realização da pesquisa e prestação das actividades do estágio ao mesmo tempo;
- Falta de apoio no concerne a disponibilização de recursos computacionais para a realização de testes (prova de conceito) da solução proposta em ambiente virtualizado;
- O computador utilizado para realizar os testes não teve uma boa *performance*, tendo consequentemente impedido o autor de alcançar o terceiro objectivo;
- Entre outros.

Bibliografia

- **Referências Bibliográficas**

[1]. Barros, O. S. R., Gomes, U. de M., & Freitas, W. L. de. (2011). *Desafios Estratégicos para Segurança e Defesa Cibernética do Brasil*. 220.

[2]. Beúla, J. N. L. (2017). *Desenvolvimento de um sistema para o auxílio na denúncia, identificação e recuperação de viaturas roubadas*. Universidade Eduardo Mondlane.

[3]. Brownlee, N., & Guttman, E. (1998). *RFC 2350—Expectations for Computer Security Incident Response*. https://datatracker.ietf.org/doc/html/rfc2350#appendix-A

[4]. Claro, J. R. (2015). *Sistemas IDS E IPS - estudo e aplicação de ferramenta open source em ambiente linux*. 86.

[5]. Conceição, J. P. S. (2017). *Implementação de um sistema siem* [Monografia]. Universidade de Brasília.

[6]. Cruz, J. P. F. (2012). *Plataformas SIEM: Implementação, Configuração e Gestão* [Dissertação de Mestrado]. Universidade de Lisboa.

[7]. Dionísio, D. A. C. (2019). *Sistema Automático para Recolha de OSINT e Integração com Plataforma de Threat Intel* [Dissertação de Mestrado]. Universidade de Lisboa.

[8]. Filho, F. C. (2012). *ITIL v3 Fundamentos*. 176.

[9]. Filipe, J. G. C. (2020). *QRadar UBA: Deteção e Análise de Anomalias Comportamentais de Segurança em Utilizadores* [Dissertação de Mestrado]. Universidade de Lisboa.

[10]. Júnior, G. S., & Francisco, J. (sem data). *Storm IDS: um Sistema de Detecção de Intrusão Escalável e Distribuído*. 73.

[11]. Kumar, B. S. (2013). *Intrusion Detection System- Types and Prevention*. *4*, 6.

[12]. Lima, P. A. L. (sem data). *Segurança Cibernética: A necessidade de se estruturar, sistematizar e integrar a proteção cibernética das Infraestruturas Críticas Nacionais, Órgãos Estratégicos do Governo e Forças Armadas*. 24.

[13]. Mamede, H. S. (2006). *Tecnologias de Informação: Segurança Informática nas Organizações*. FCA.

[14]. Mendonça, N. M. L. (2015). *Gerador de eventos para testes de configurações de um SIEM* [Dissertação de Mestrado]. Universidade de Lisboa.

[15]. Michaque, E. A. (2017). *Proposta de um modelo de interoperabilidade entre os sistemas de informação usados na UEM*. Universidade Eduardo Mondlane.

[16]. Miller, D., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. (Eds.). (2011). *Security information and event management (SIEM) implementation*. McGraw-Hill.

[17]. Nascimento, F. P. do. (sem data). *Classificação da Pesquisa. Natureza, método ou abordagem metodológica, objetivos e procedimentos*.

[18]. República de Moçambique. (2021). *Política e Estratégia Nacional de Segurança Cibernética*.

[19]. Rodrigues, B. de S. G. (2015). *Open-source intelligence em sistemas SIEM* [Dissertação de Mestrado]. UNIVERSIDADE DE LISBOA.

[20]. Russell, P., de Menezes, A. F., & da Silva, G. M. (2002). *Firewall: Segurança de redes Linux*. 135.

[21]. Santos, R. S. dos. (2018). *Controlos de Cibersegurança em Ambientes MS Windows de Grandes Empresas: Integração Efetiva de Eventos Relevantes de Segurança no SIEM AlienVault* [Dissertação de Mestrado]. Universidade de Lisboa.

[22]. Scussiatto, L. (2017). *Avaliação de regras de firewall utilizando um motor de inferência* [Bacharelado]. Universidade de Caxias do Sul.

[23]. Tavares, L. A. D. N. (2015). *Análise de eventos de segurança: Baseado no OSSIM* [Dissertação de Mestrado]. Universidade do Minho.

[24]. Teixeira, C. F. A. (2021). *Segurança Cibernética em Redes Modernas: Como Proteger e Mitigar Ataques Cibernéticos*. Universidade Federal de Ouro Preto.

[25]. Vazão, A. P. H. (2020). *Implementação de sistema SIEM open-source em conformidade com o RGPD* [Dissertação de Mestrado]. Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

- **Outra bibliografia consultada**

[1]. *AT&T Cybersecurity (2022) – USM Appliance™ User Guide, disponível em: https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-user-guide.pdf (acedido no dia 15 Julho de Julho às 14:55).*

Anexos

Anexo 1: Especificações do Host e das Máquinas Virtuais

Sistema Operativo	Windows 10 Pro, 20H2
Arquitectura do Sistema	64 bits
Processador	Intel(R) Core(TM) i5 – 6200U @2.30GHz ~ 2.40GHz
RAM	16 GB
Hard Disk Drive (HDD)	500 GB + 2 TB

Tabela A1-1: Especificações do Host.

Sistema Operativo	Linux – Debian
Arquitectura do Sistema	64 bits (AlienVault_OSSIM_64bits.iso)
RAM	2 GB
Processadores	2 (2 Cores por processador)
Hard Disk Drive (HDD)	50 GB
Network Adapters	Subnet Security Management (192.168.3.0/24)
	Subnet Servers (192.168.2.0/24)
	Subnet Clients (192.168.1.0/24)
	DMZ (172.16.10.0/24)

Tabela A1-2: Especificações da máquina virtual SIEM_OSSIM.

Sistema Operativo	Windows 10
Arquitectura do Sistema	64 bits
RAM	2 GB
Processadores	1
Hard Disk Drive (HDD)	60 GB
Network Adapter	Subnet Security Management (192.168.3.0/24)

Tabela A1-3: Especificações da máquina virtual Admin.

Sistema Operativo	Windows 7
Arquitectura do Sistema	64 bits
RAM	1 GB
Processadores	1
Hard Disk Drive (HDD)	50 GB
Network Adapter	Subnet Clients (192.168.1.0/24)

Tabela A1-4: Especificações da máquina virtual usuário.

Sistema Operativo	Windows Server 2012 R12 Server GUI
Arquitectura do Sistema	64 bits
RAM	2 GB
Processadores	2 (2 Cores por processador)
Hard Disk Drive (HDD)	50 GB
Network Adapter	Subnet Servers (192.168.2.0/24)

Tabela A1-5: Especificações da máquina virtual Windows Server.

Sistema Operativo	Linux – Mint Cinnamon
Arquitectura do Sistema	64 bits
RAM	2 GB
Processadores	1
Hard Disk Drive (HDD)	50 GB
Network Adapter	DMZ (172.16.10.0/24)

Tabela A1-6: Especificações da máquina virtual Servidor Web.

Sistema Operativo	Linux – CentOs 7
Arquitectura do Sistema	64 bits
RAM	1 GB
Processadores	1
Hard Disk Drive (HDD)	35 GB
Network Adapters	Subnet Security Management (192.168.3.0/24)
	Subnet Servers (192.168.2.0/24)
	Subnet Clients (192.168.1.0/24)
	DMZ (172.16.10.0/24)

Tabela A1-7: Especificações da máquina virtual Firewall.

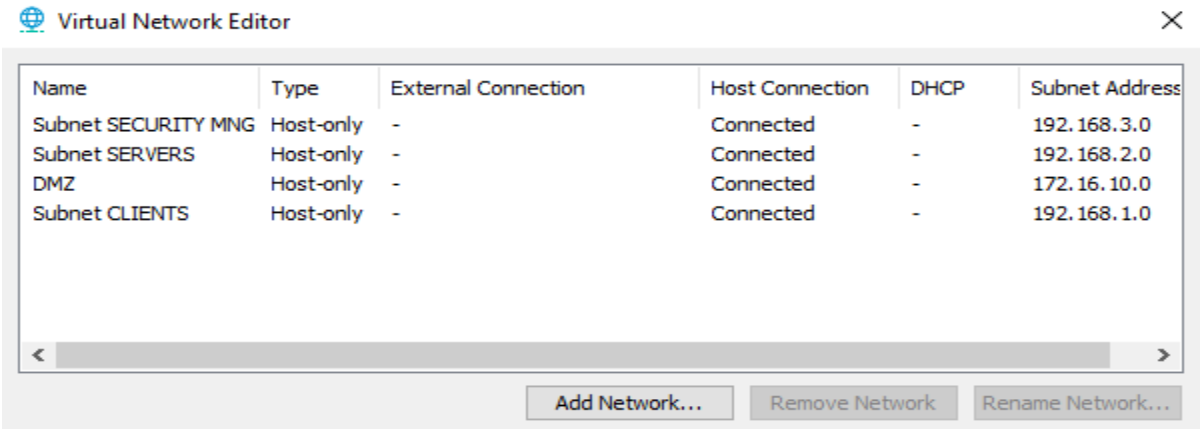

Figura A1-1: Network Adapters no VMware Workstation.

Anexo 2: AlienVault OSSIM – Instalação e Configuração

2.1. Instalação

AlienVault OSSIM é um produto em constante evolução. Por esse motivo, devemos sempre certificar de que estamos a usar a versão mais recente. A versão mais recente está sempre disponível em: https://cybersecurity.att.com/products/ossim/download Após realizar o download da versão mais recente do AlienVault OSSIM, configuramos na máquina virtual SIEM_OSSIM a imagem que foi baixada no CD-ROM e colocamos o sistema para inicializar.

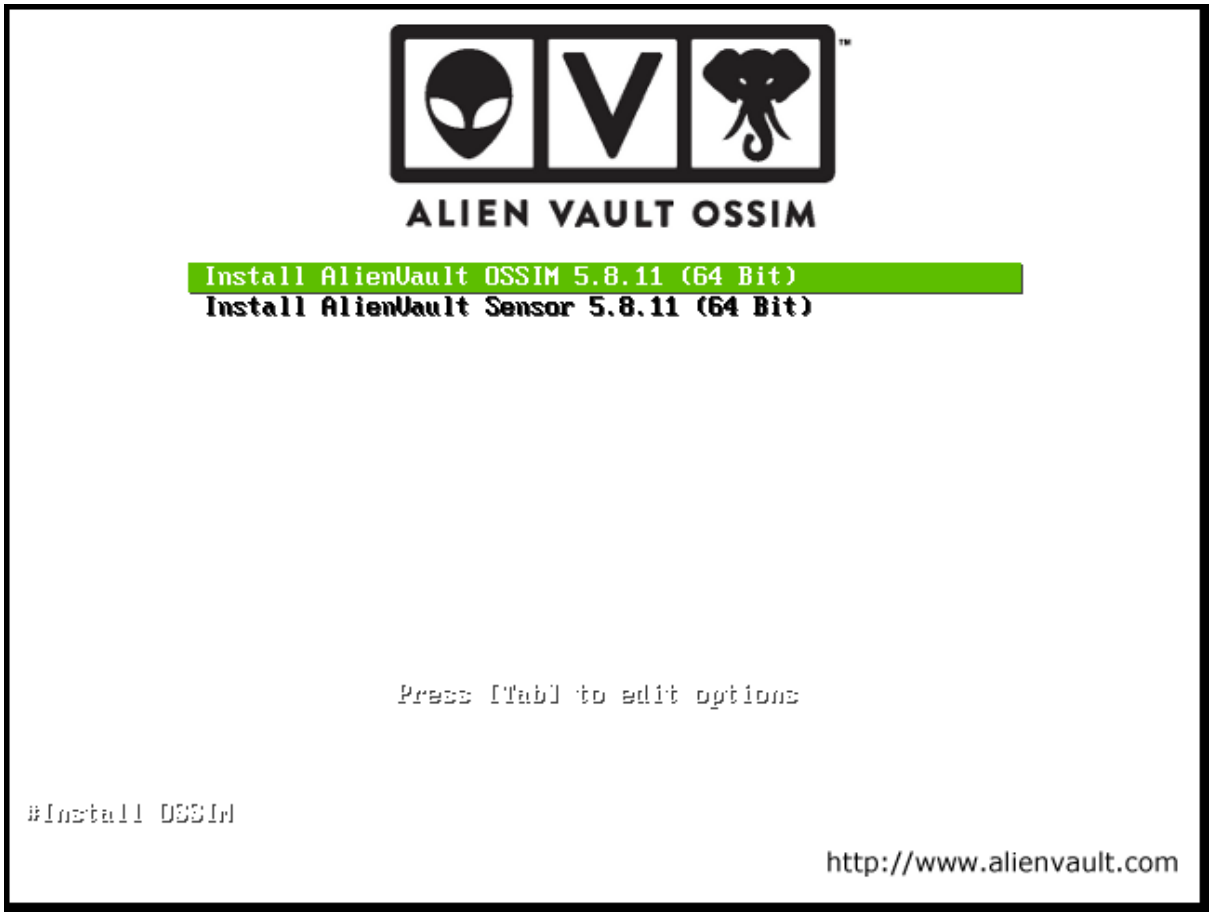

Figura A2-1: Componente a instalar.

Inicializado o sistema, realizaram-se algumas configurações básicas, como:

Componente a instalar (SO)	AlienVault OSSIM 5.18.11 (64 bits)
Language	English
Location (Country)	Mozambique
Base default locale	en_US.UTF-8
Keyboard layout	American English

Tabela A2-1: Configurações básicas na instalação.

2.1.1. Configuração de Rede

Neste ponto, configuramos o endereço IP na placa de rede de gestão que será usado na Web User Interface para aceder a interface administrativa do AlienVault OSSIM.

Figura A2-2: Configuração do IP do AlienVault OSSIM.

Depois de configurado o endereço IP do AlienVault OSSIM, foram realizadas ainda algumas configurações básicas de rede, como:

Network Mask	255.255.255.0
Gateway	192.168.3.254
DNS Server	172.16.10.1

Tabela A2-2: Configurações básicas de rede.

2.1.2. Configuração de usuário “root” e password

Nesta parte, o instalador nos permite configurar a conta “root”, que é uma conta super poderosa, isto é, dá acesso ao sistema administrativo do AlienVault OSSIM, de onde é possível realizar qualquer tipo de configuração a nível do sistema. Outras contas podem ser criadas após o processo de instalação.

É necessário definir uma password “root” conta administrativa do sistema pois um usuário mal-intencionado ou não qualificado com acesso root pode ter resultados desastrosos, então devemos tomar cuidado para escolher uma password de root que não seja de fácil acesso para adivinhar.

NB: A password Não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada ao administrador. Uma boa password terá uma mistura de letras, números e pontuação e deve ser alterada em intervalos de tempo regulares. O usuário root não deve ter uma password vazia. Se deixarmos o campo em branco, a conta root será desabilitada e a conta de usuário inicial do sistema terá o poder de se tornar root usando o comando “sudo”.

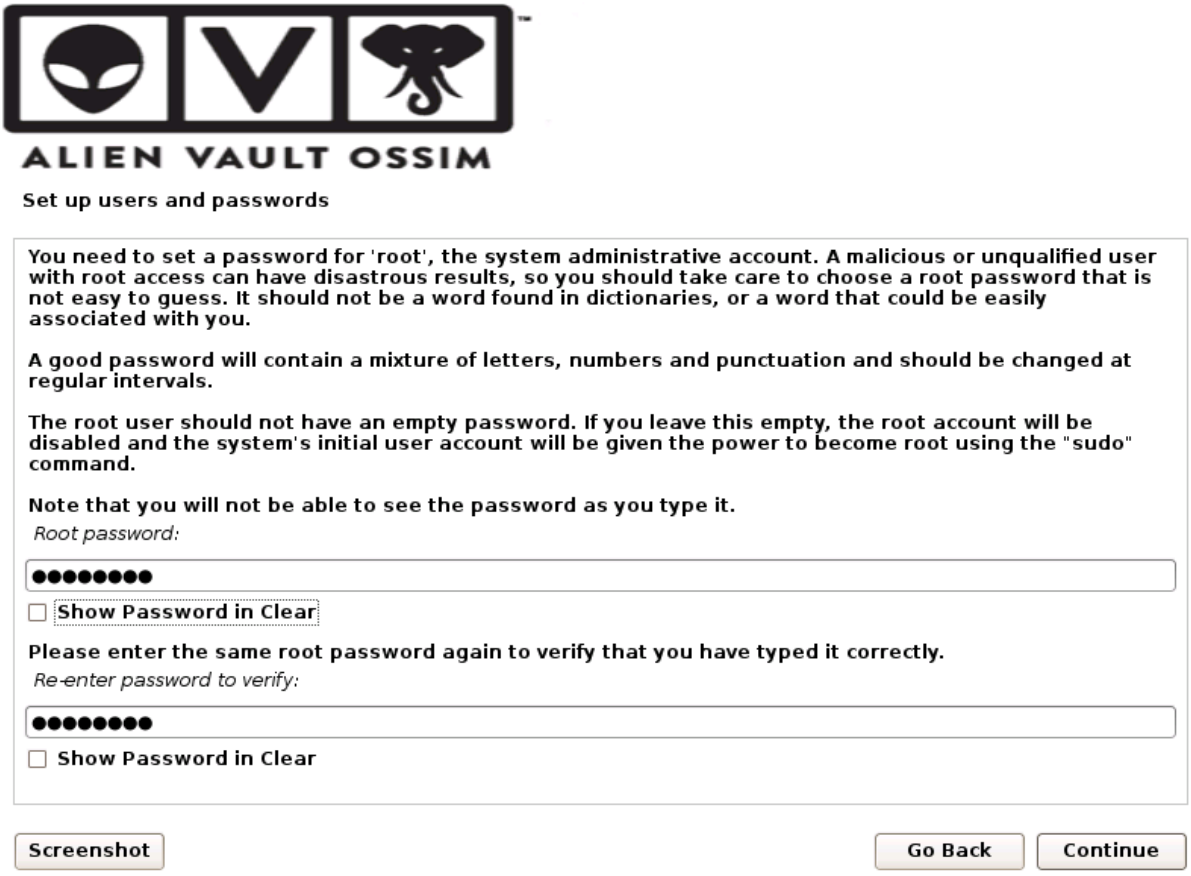

Figura A2-3: Definição da password da conta “root”.

2.1.3. Instalação do sistema base

Depois de definir a password para o utilizador root, a seguir é iniciado o processo de instalação do AlienVault OSSIM propriamente dito.

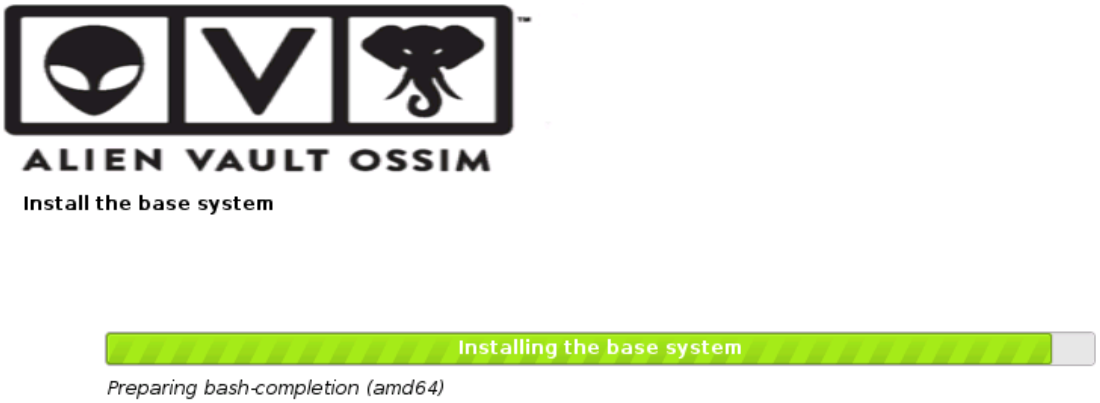

Figura A2-4: A instalar o sistema.

2.1.4. Finalizando a instalação

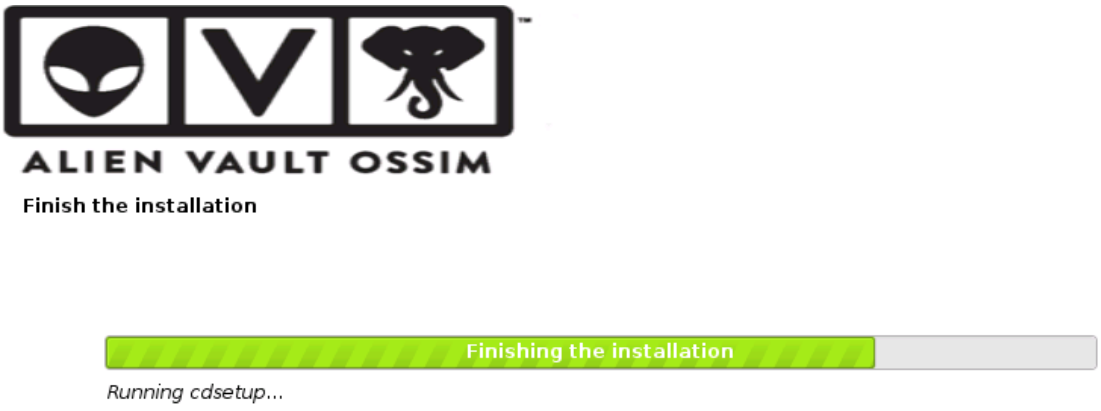

Figura A2-5: Parte final da instalação.

2.1.5. Acesso ao Sistema AlienVault OSSIM via terminal (CLI)

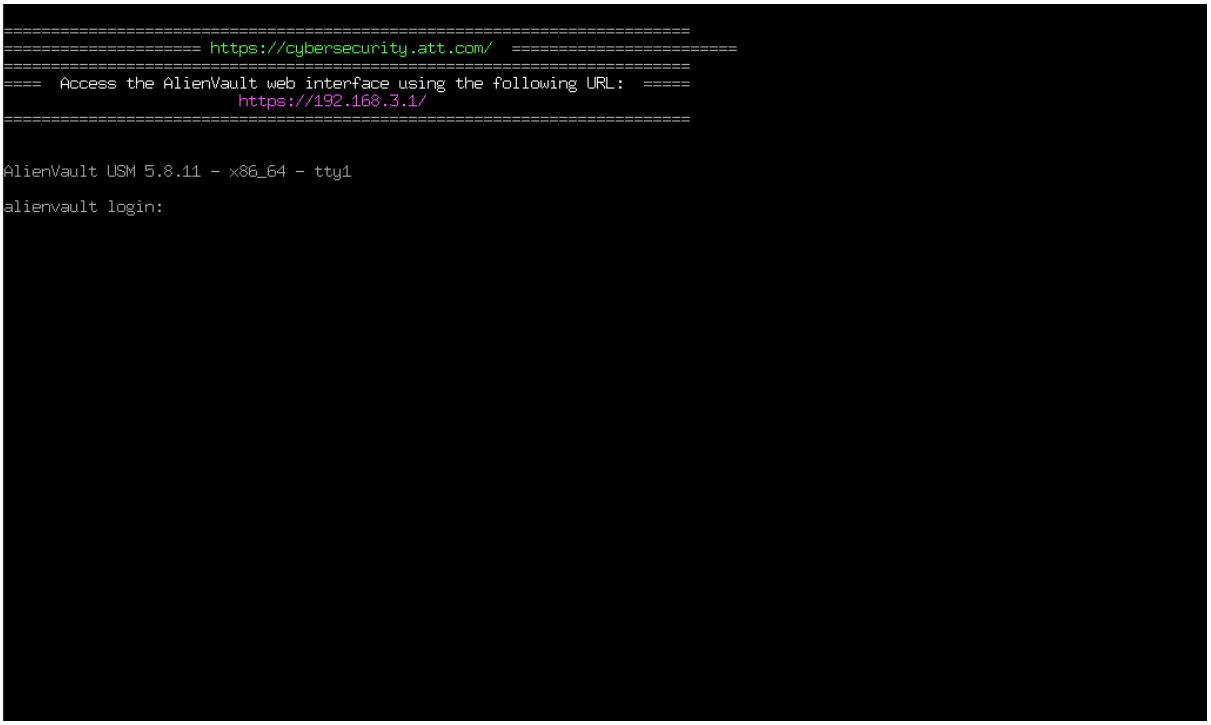

Figura A2-6: Acesso ao Sistema AlienVault OSSIM via terminal (CLI).

2.1.6. Acesso ao Sistema AlienVault OSSIM via Web User Interface (UI)

Para aceder a Web UI do Sistema AlienVault OSSIM colocamos e acedemos num navegador da máquina virtual Admin a seguinte URL: https//192.168.3.1/ e teremos o resultado abaixo.

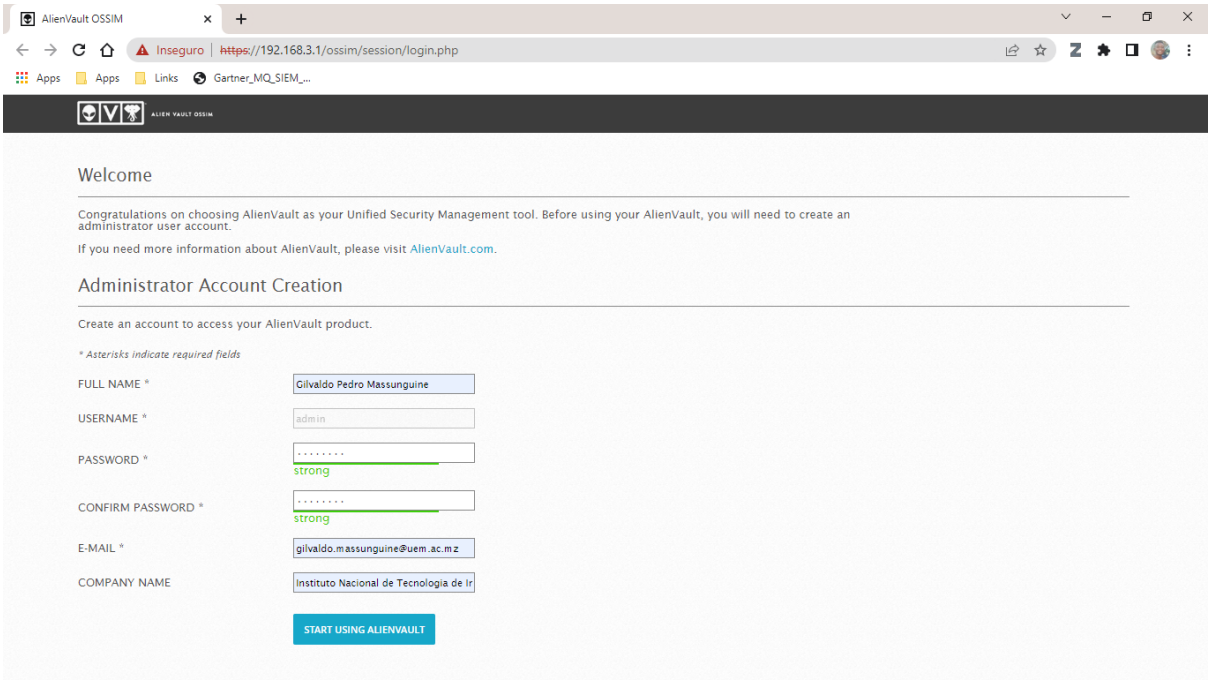

Figura A2-7: Criação de conta de administrador da Web UI.

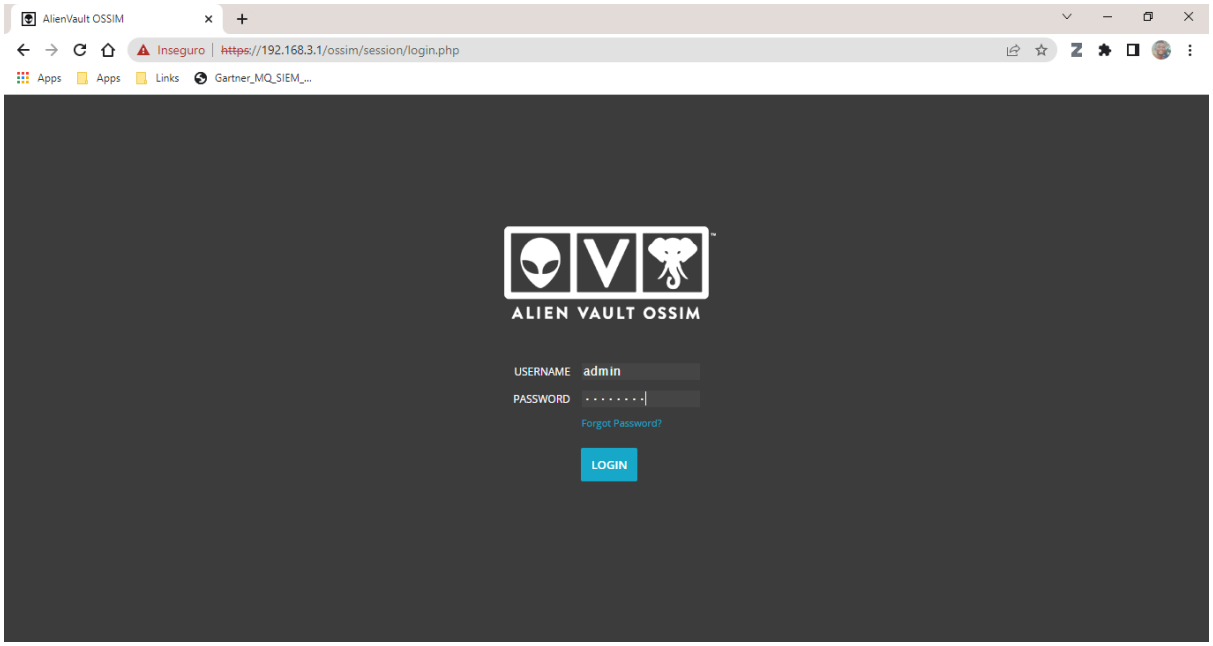

Figura A2-8: Login na Web UI.

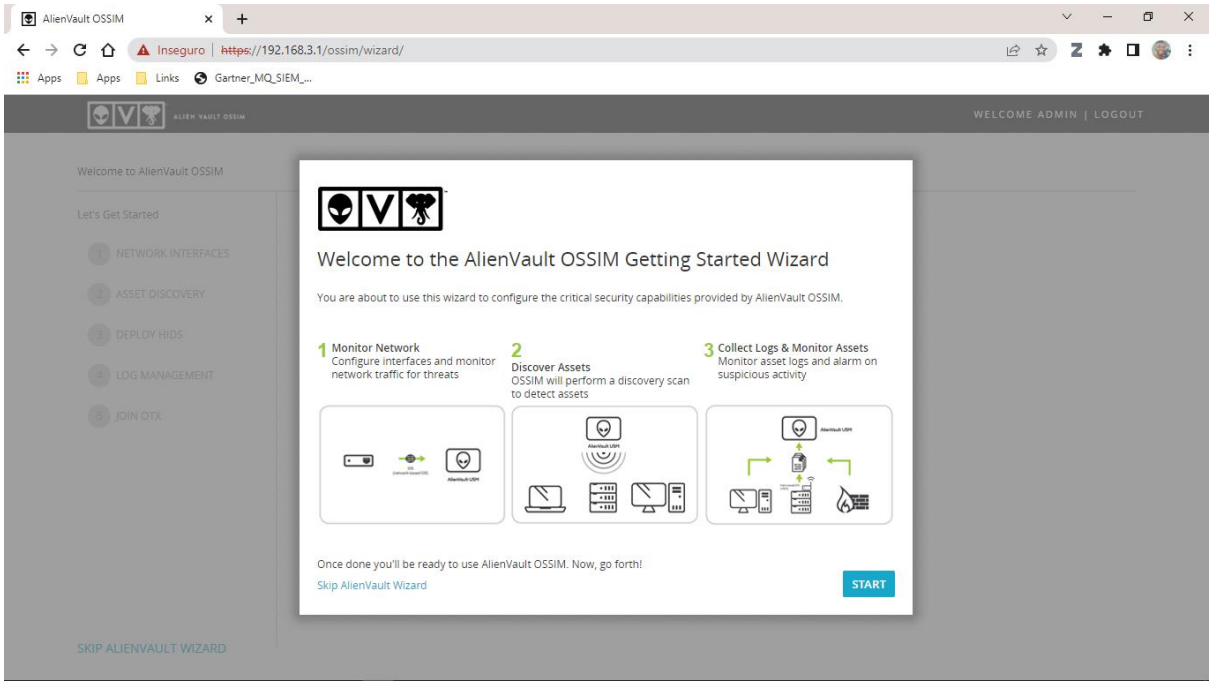

Figura A2-9: Welcome to the AlienVault OSSIM.

2.2. Configurações básicas

2.2.2. Tipos de Network Interface

As interfaces de rede do AlienVault OSSIM podem ser configuradas como:

- **Management:**

É configurada no AlienVault OSSIM via terminal (CLI) e permite aceder a Web User Interface (UI), essa interface não pode ser alterada na Web UI.

- **Network Monitoring**

Essa interface, escuta passivamente o tráfego de rede, e deverá ser configurada para funcionar em modo promíscuo, ou seja, requer um tap ou span de rede.

- **Log Collection & Scanning**

Colecta ou recebe logs de seus activos, executa uma varredura de activos ou implante de agente HIDS (Host-Based Intrusion Detection) e requer acesso roteável às suas redes.

- **Not in Use:**

É utilizada quando não se pretende usar uma determinada interface de rede.

2.2.3. Network Interface

- **Configuração da Interface Management**

Essa configuração é feita a nível do terminal (CLI) do AlienVault OSSIM.

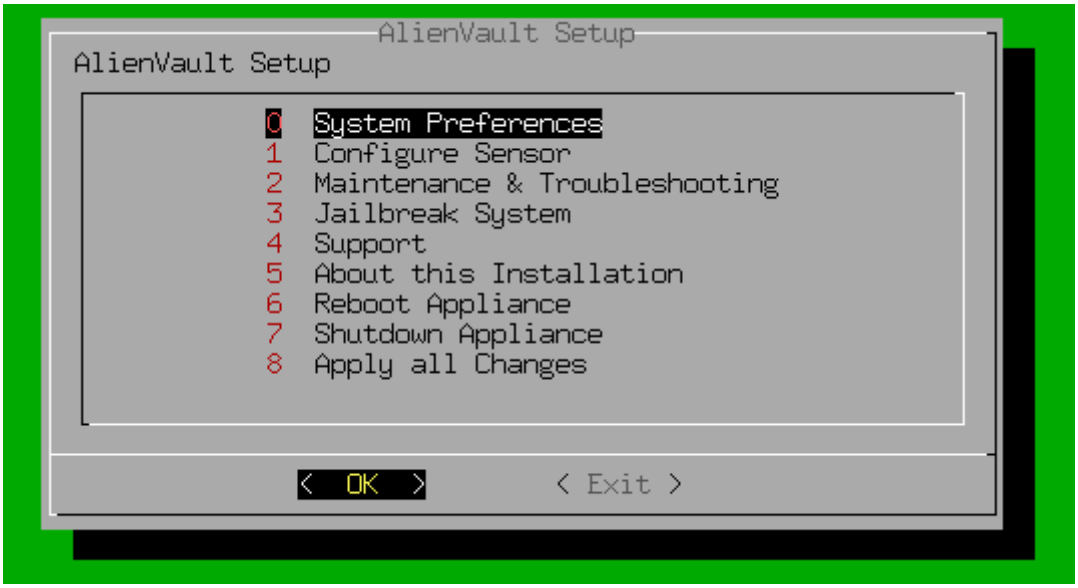

Figura A2-10: Preferências de Sistema.

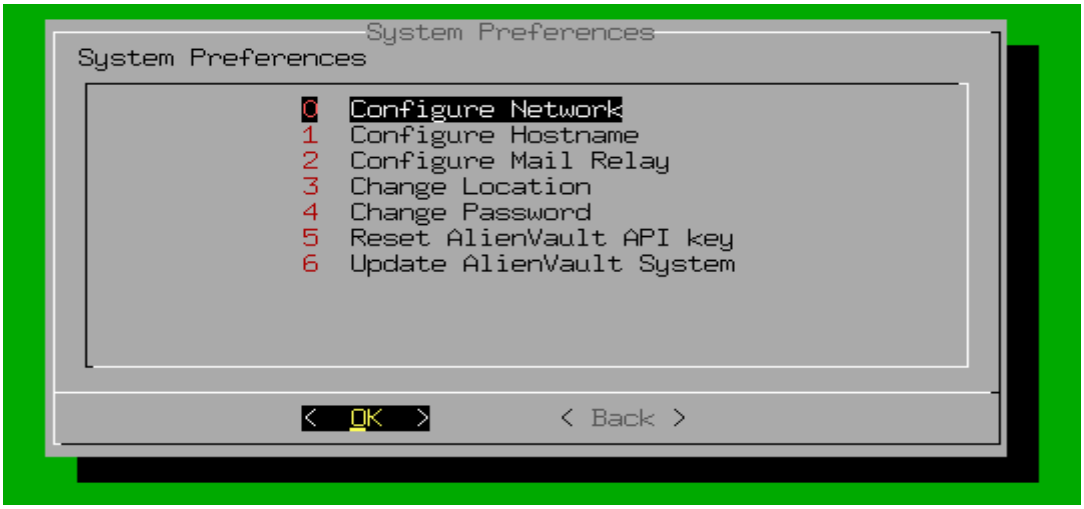

Figura A2-11: Configurar a rede.

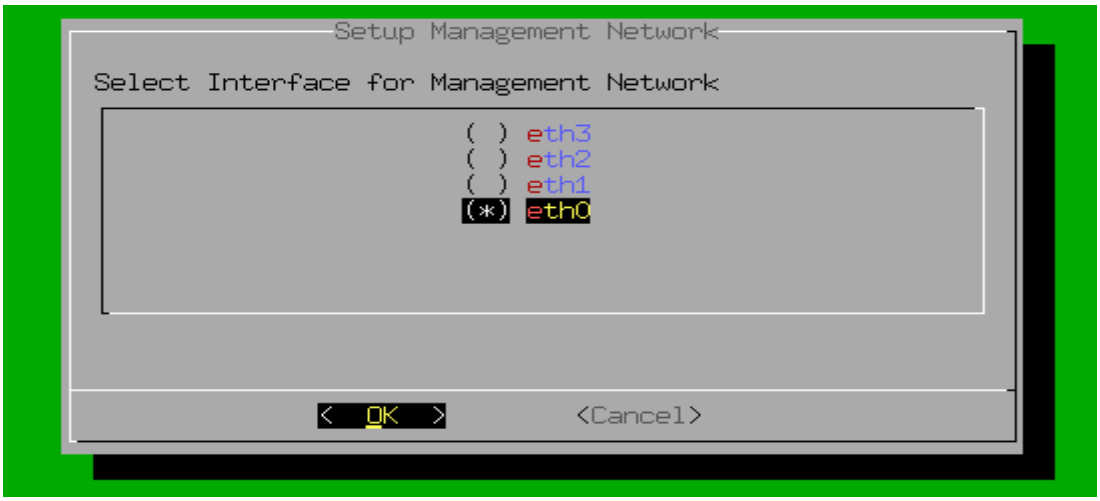

Figura A2-12: Selecionar a interface de gestão.

- **Configuração de Interface Network Monitoring**

Figura A2-13: Configurar o sensor.

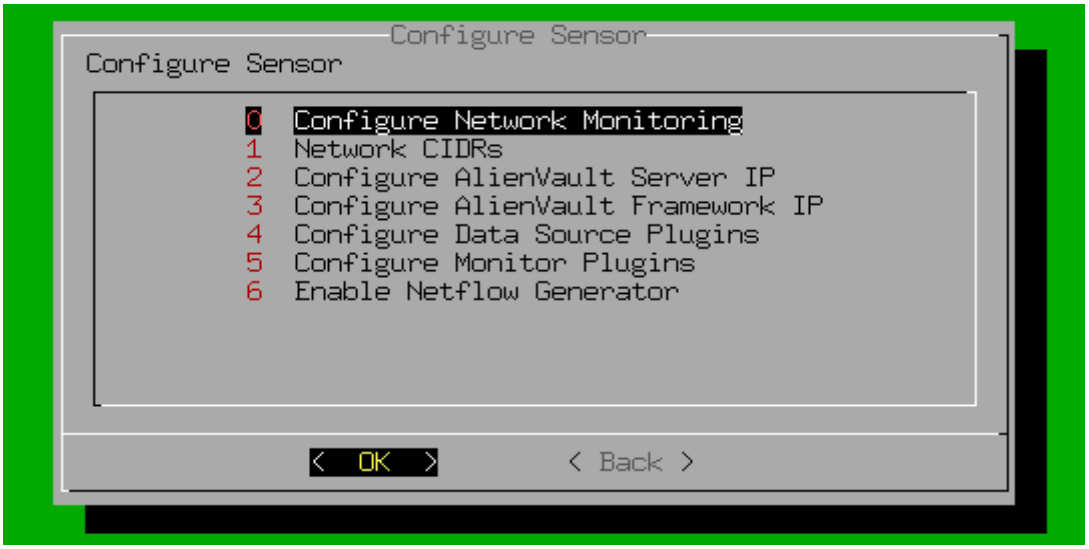

Figura A2-14: Configurar a Monitorização da rede.

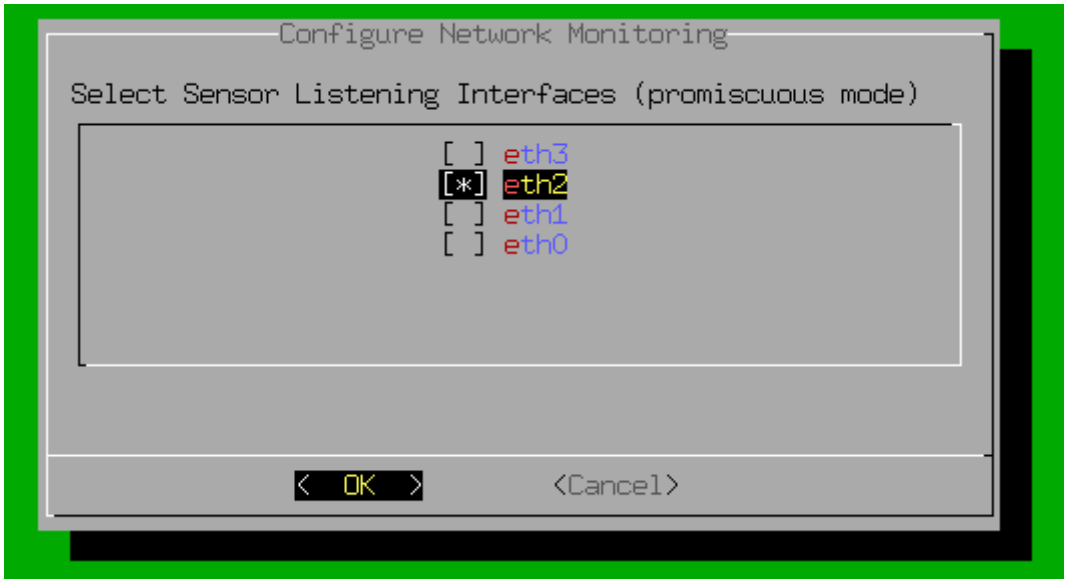

Figura A2-15: Selecionar as interfaces de monitorização.

- **Interfaces de Rede no OSSIM**

NIC	VMware Network	Propósito	Status
eth0	Subnet Security Mng	Management	–
eth1	Subnet Clients	Log Collection & Scanning	–
eth2	DMZ	Network Monitoring	–
eth3	Subnet Servers	Log Collection & Scanning	–

Tabela A2-3: Network Interfaces.

- **Configure Networks Interfaces – Web UI**

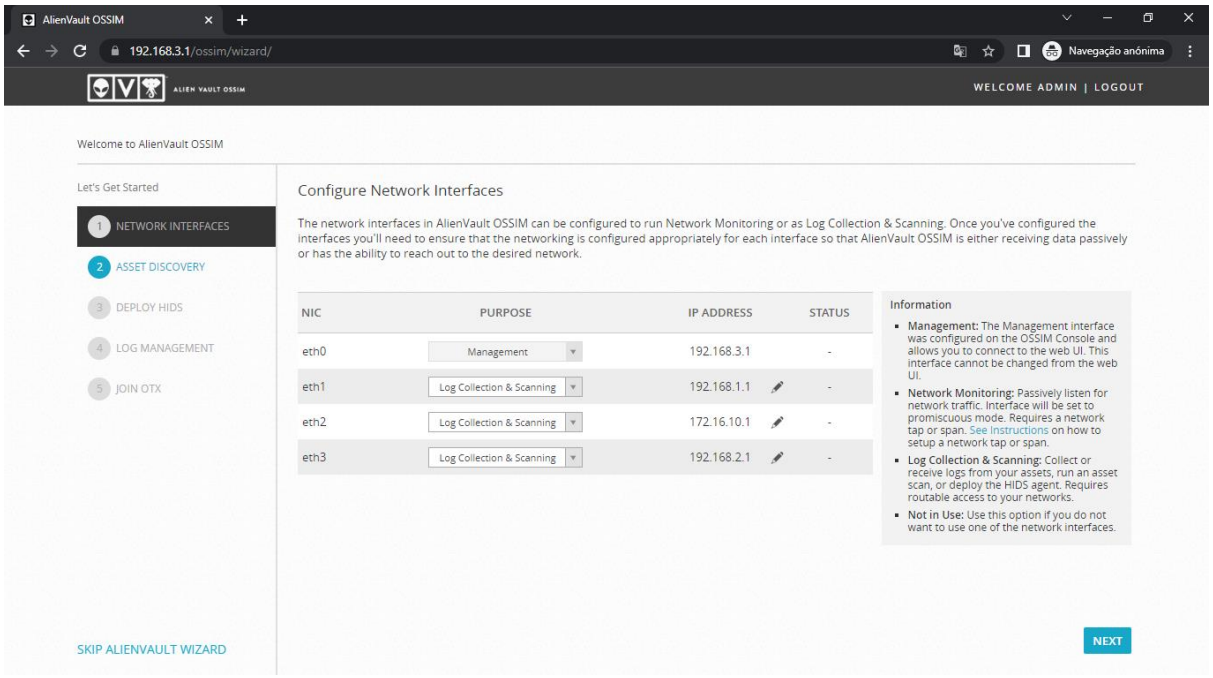

Figura A2- 16: Configuração de Network Interfaces na Web UI.

2.2.4. Asset Discovery

- **Scan & Add Assets**

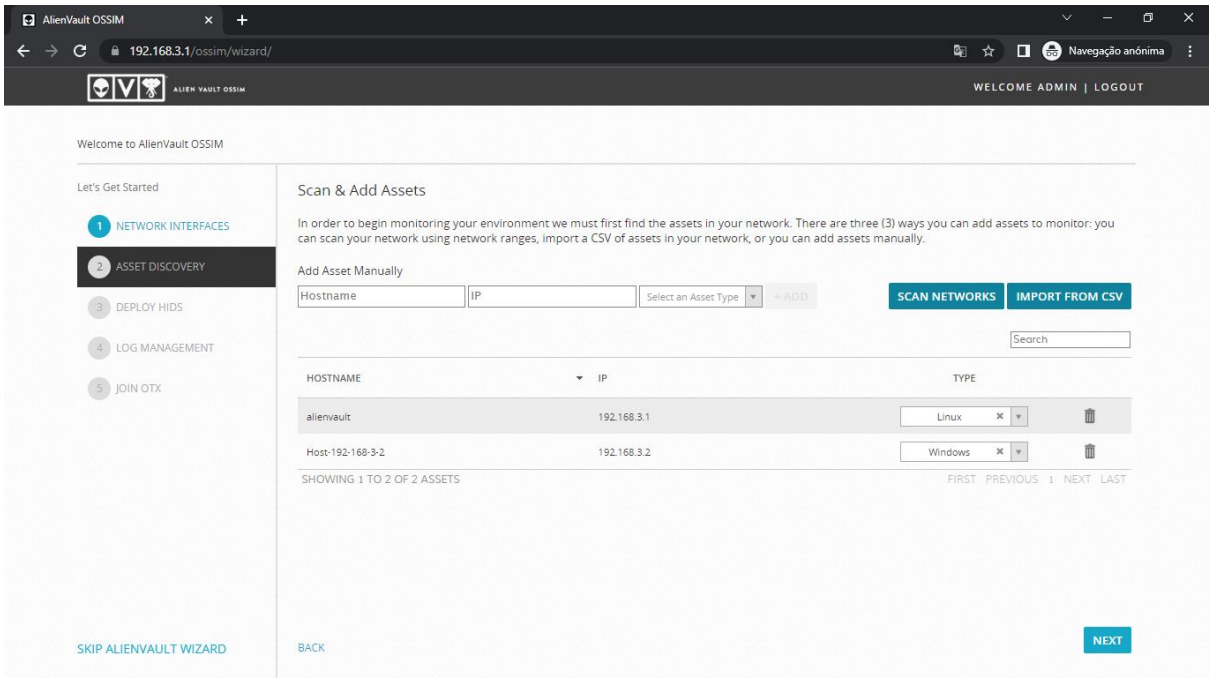

Figura A2-17: Descoberta de activos.

.

- **Scan Networks**

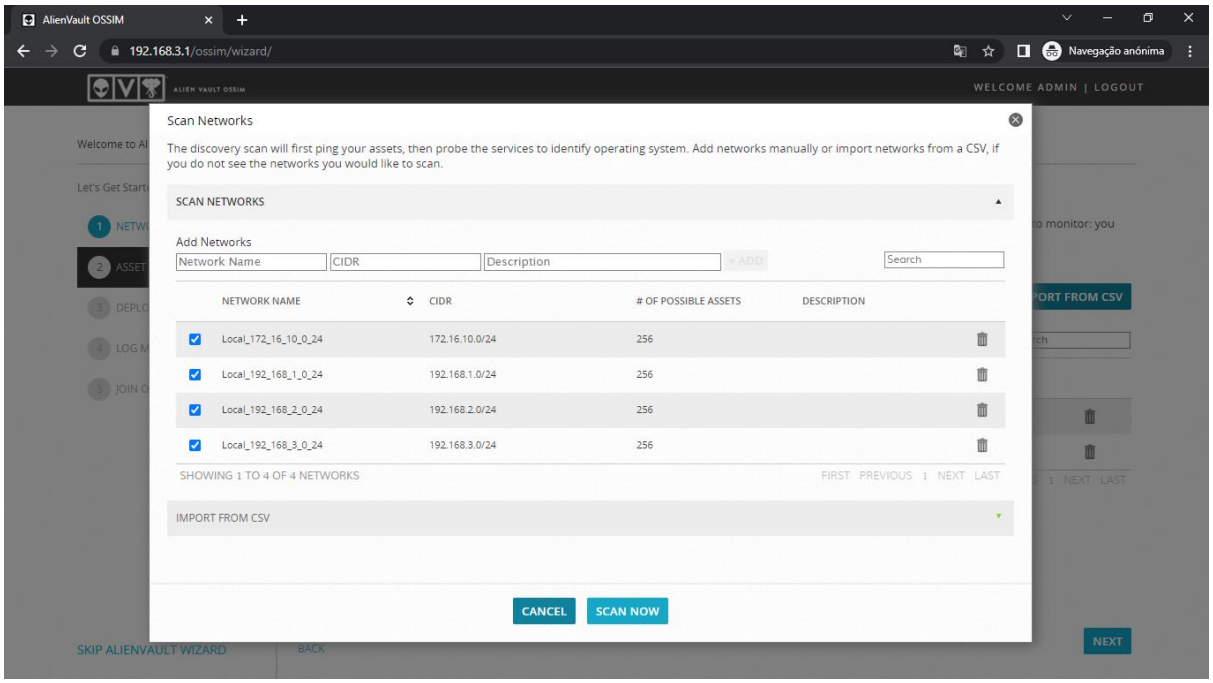

Figura A2-18: Escolha das redes a efectuar o scan de activos.

- **Procurando activos nas rede selecionadas**

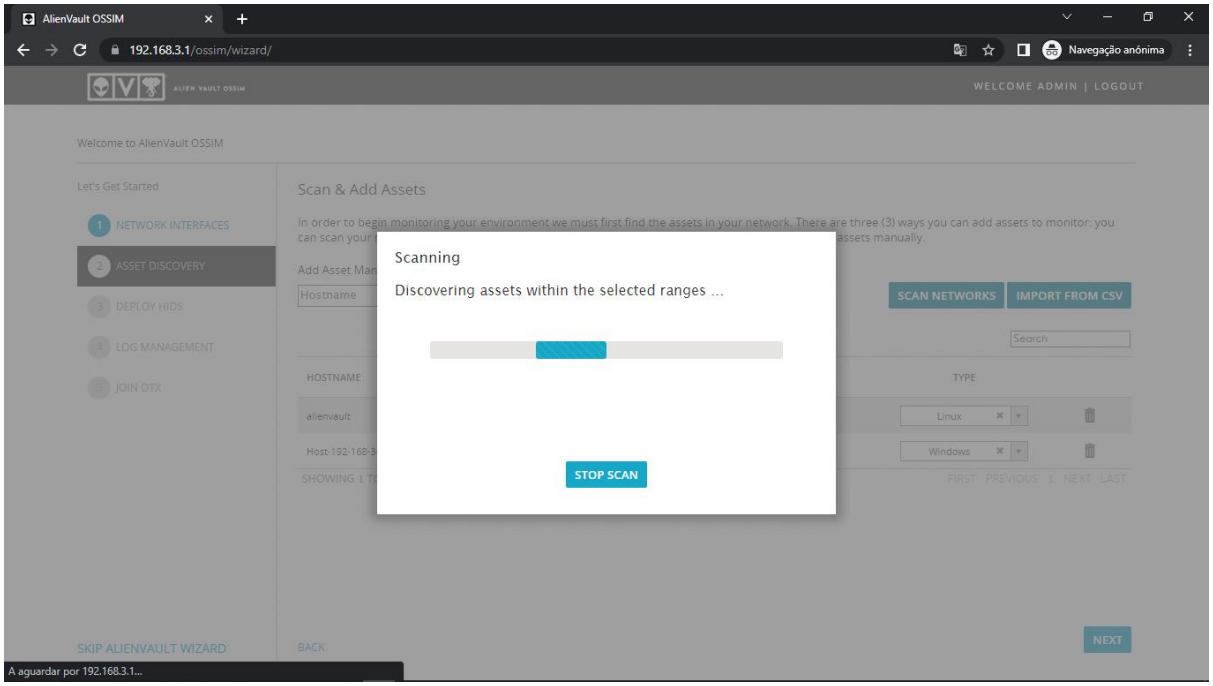

Figura A2-19: Procurando assets nas redes selecionadas.

- **Activos encontrados**

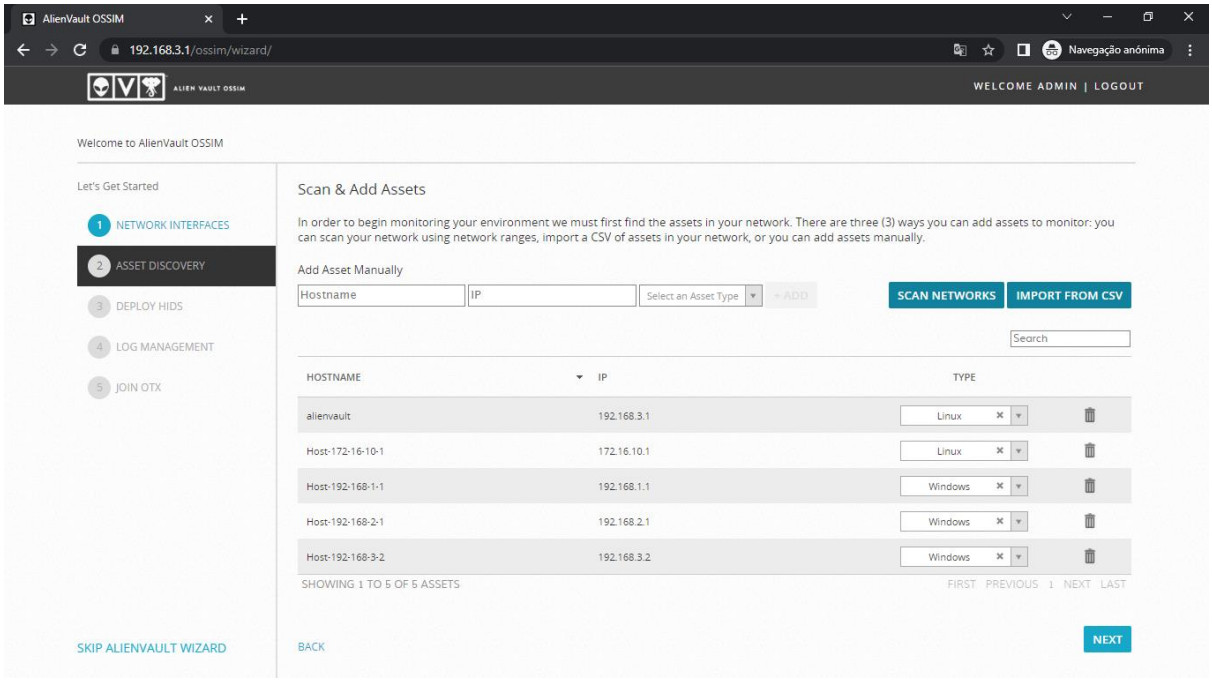

Figura A2-20: Activos encontrados.

- **Configurações de rede nas VMs**

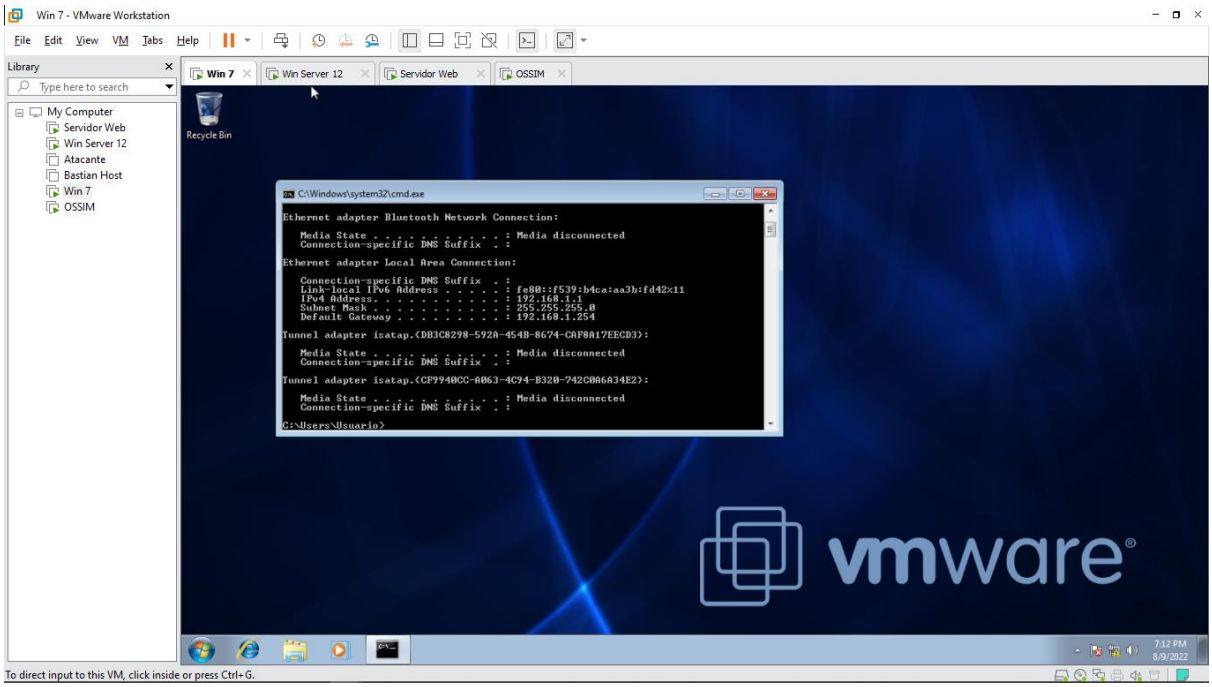

Figura A2-21: VM Windows 7.

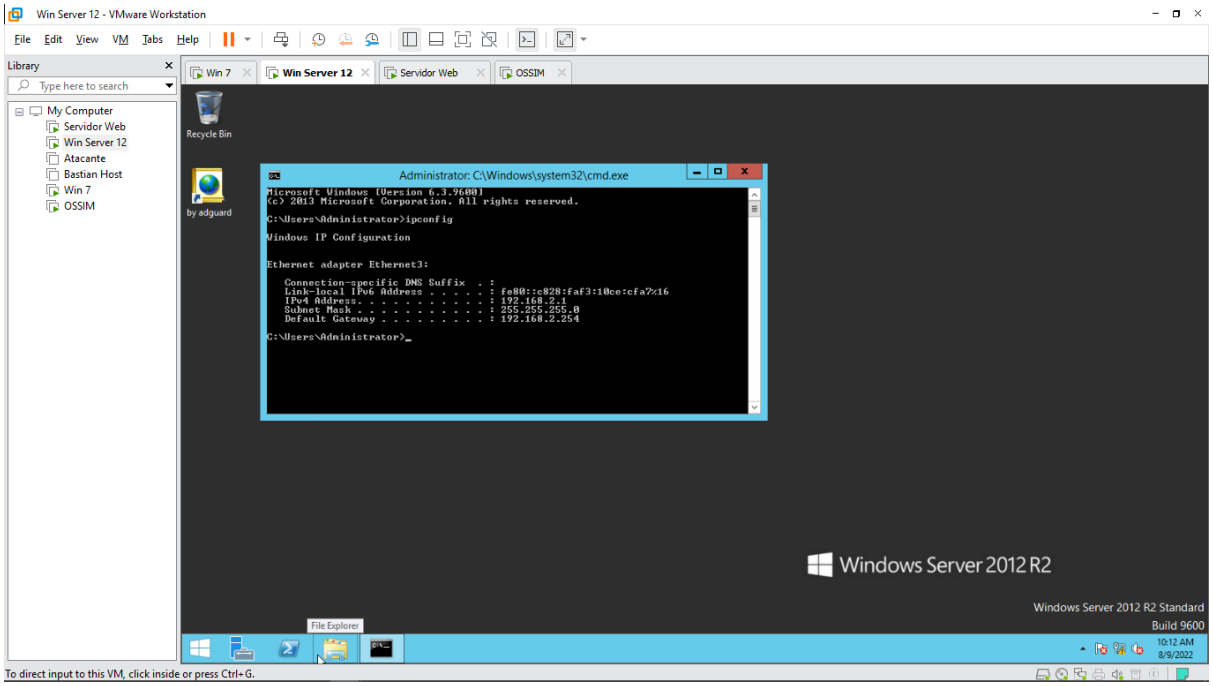

Figura A2-22: VM Windows Server 2012 R12.

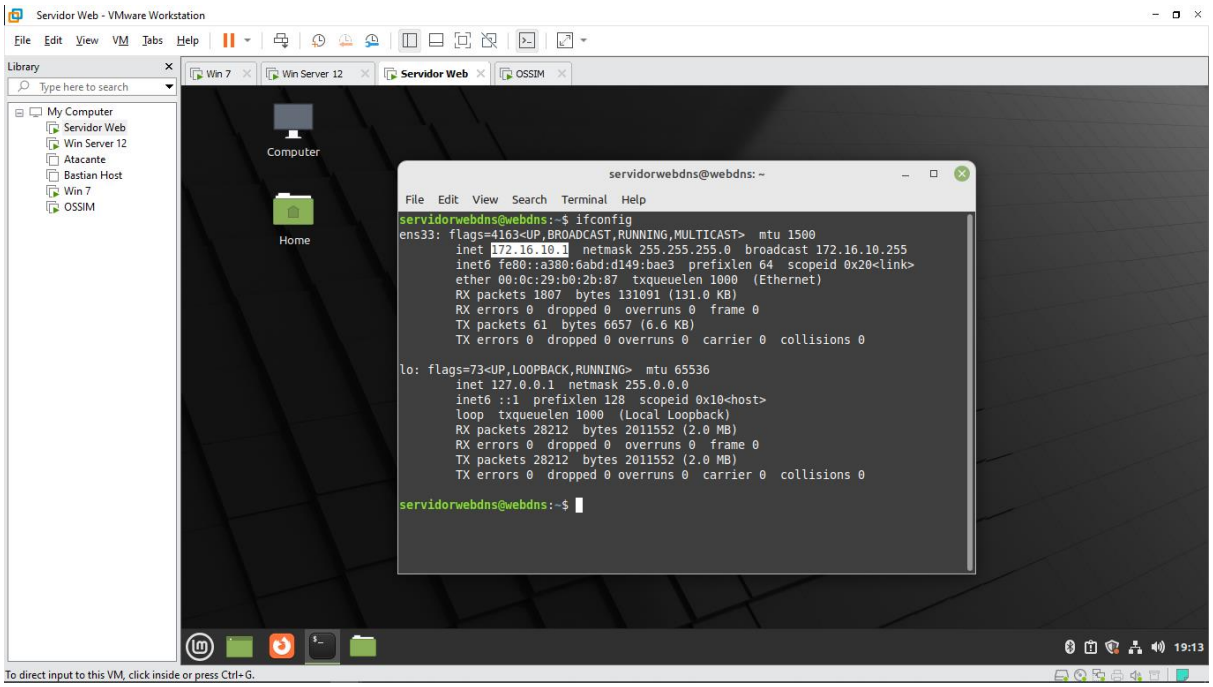

Figura A2-23: VM Servidor Web.

2.2.5. Deploy HIDS

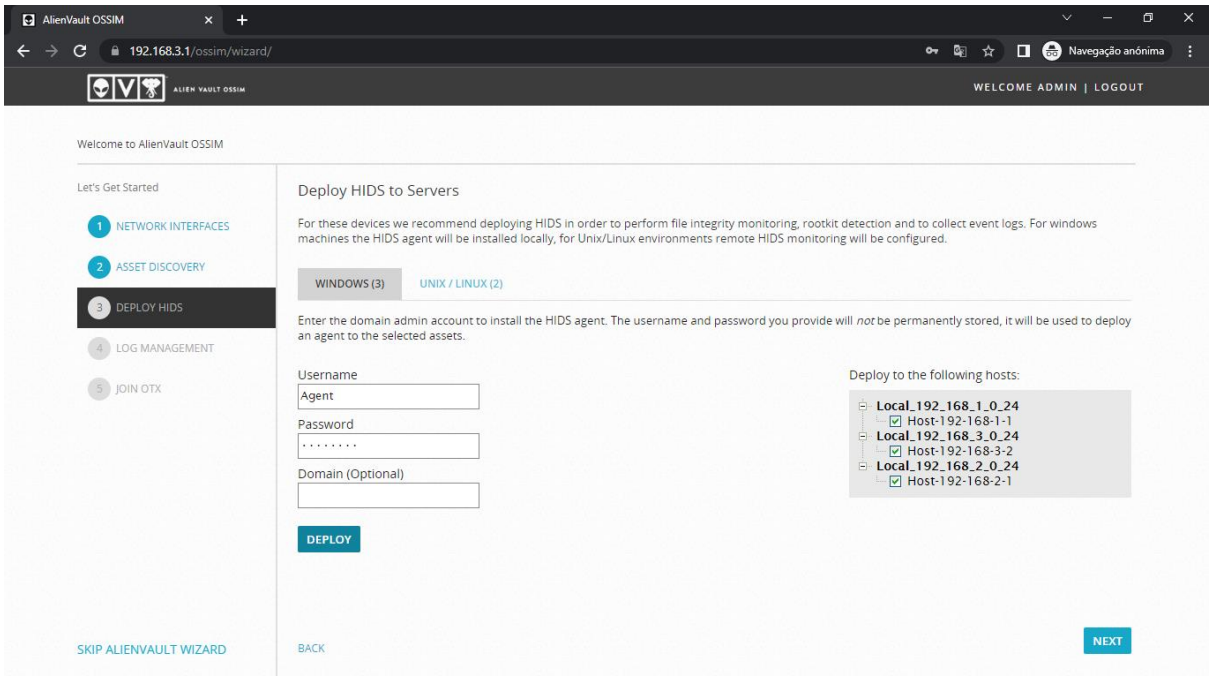

Figura A2-24: Configuração de usuário para fazer Deploy HIDS para Windows.

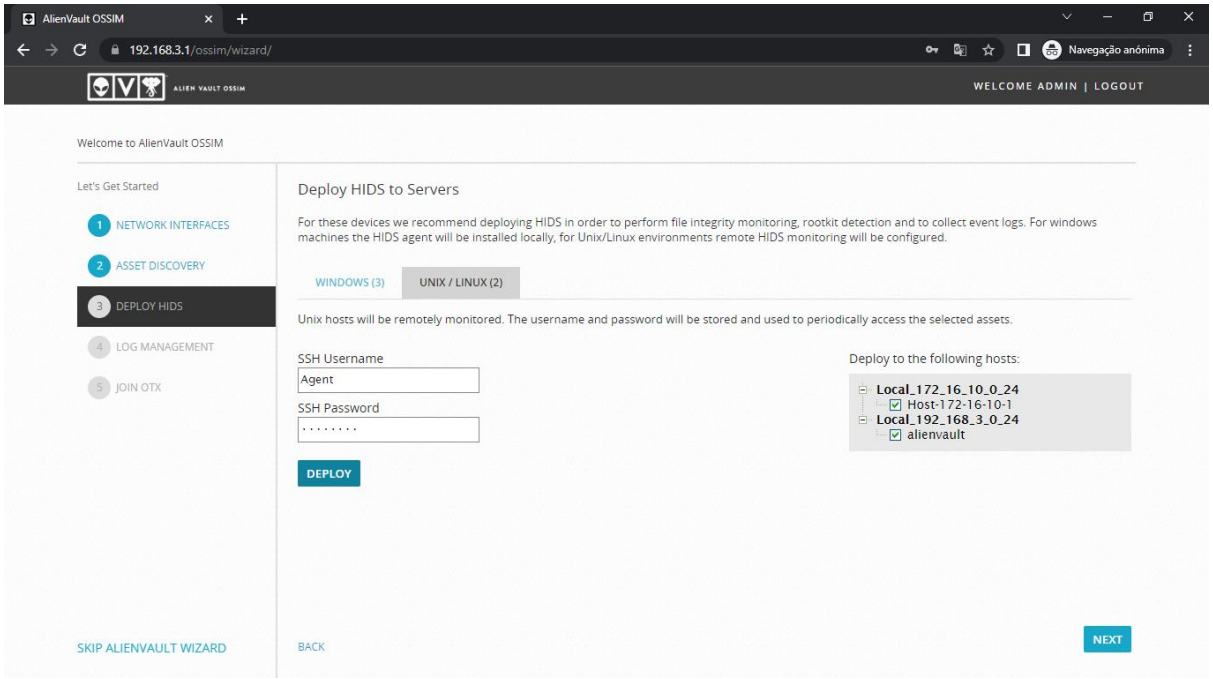

Figura A2-25: Configuração de usuário para fazer Deploy HIDS para Linux.

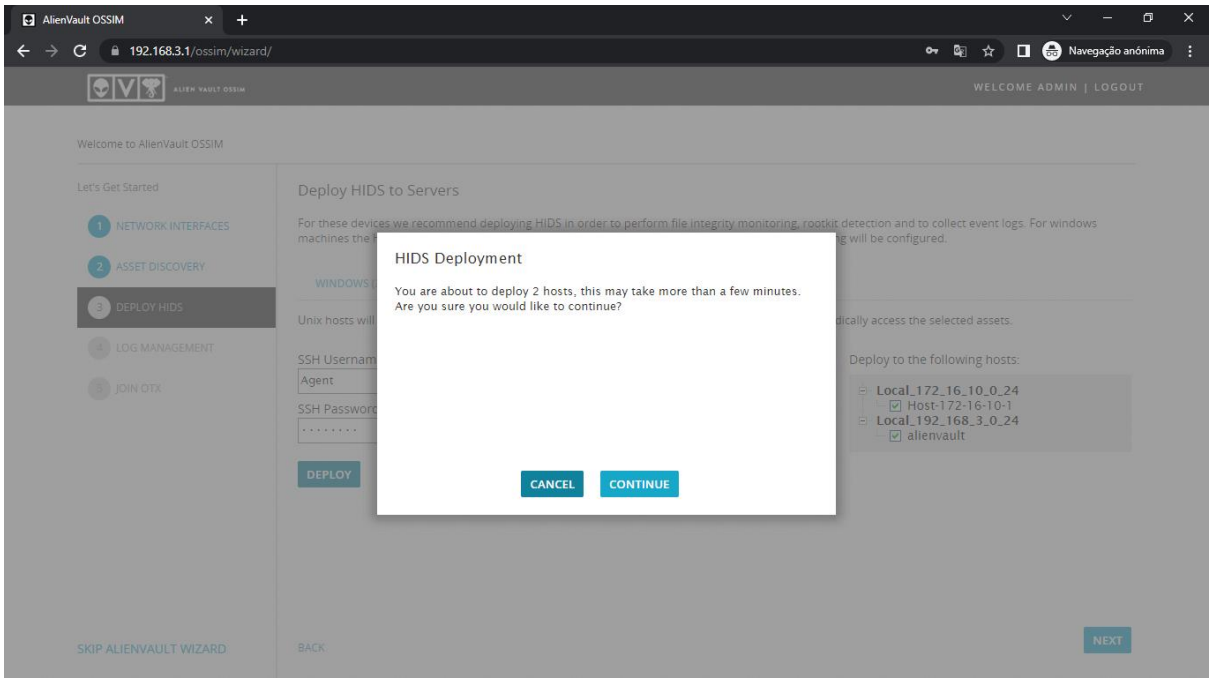

Figura A2-26: Confirmação do HIDS Deployment.

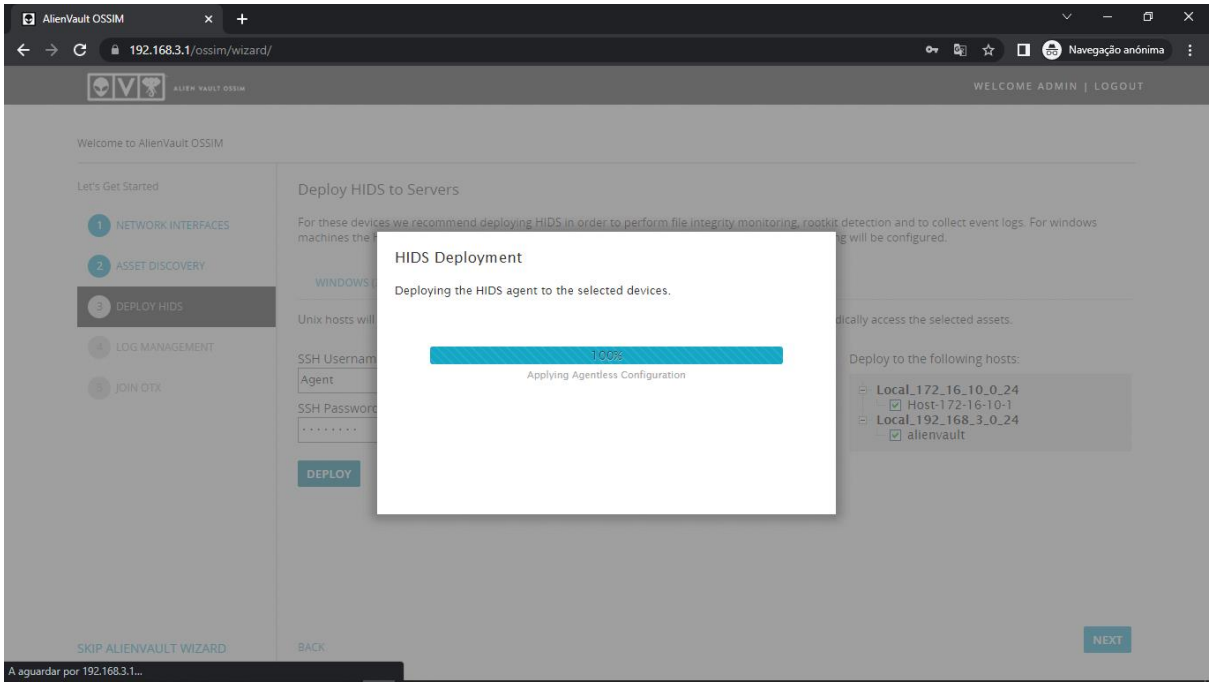

Figura A2-27: Fim do Deployment.

2.2.6. Log Management

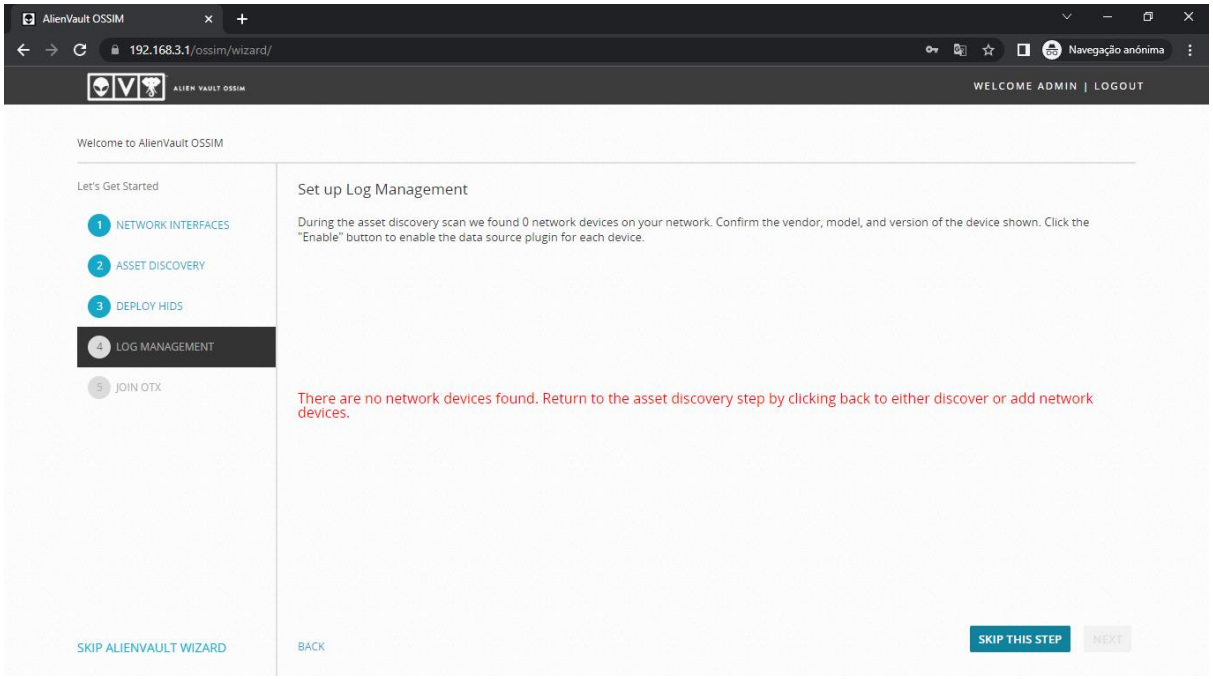

Figura A2-28: Configuração de Log Management.

2.2.7. Join OTX

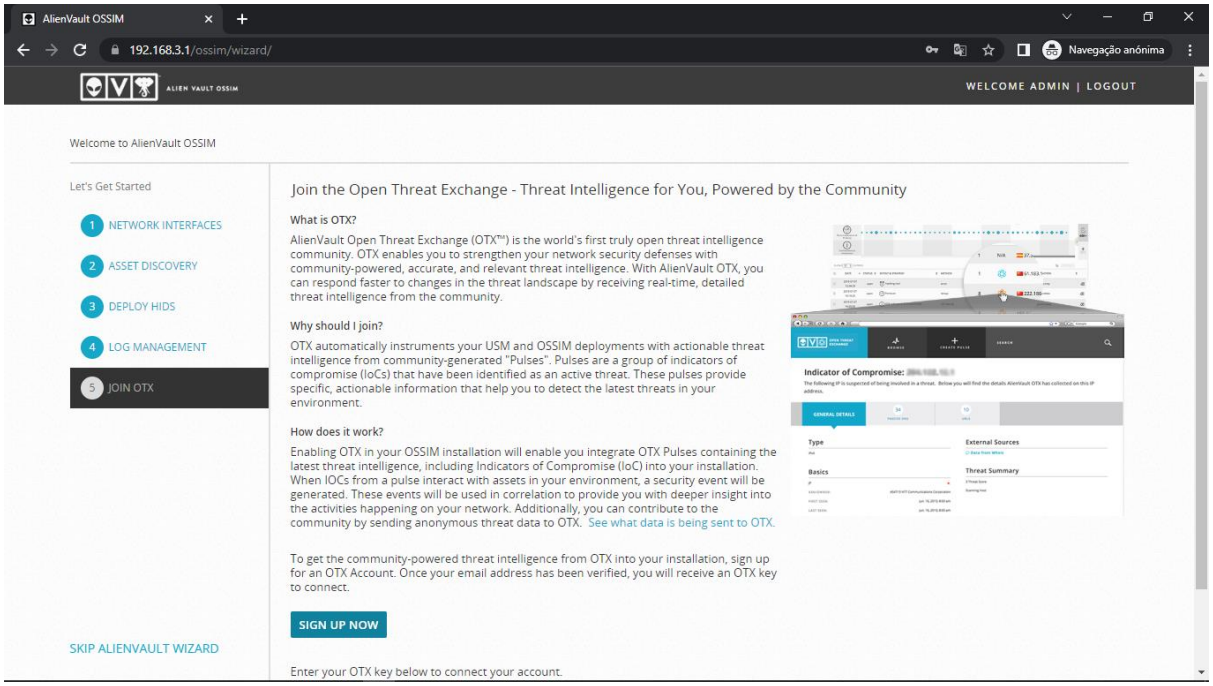

Figura A2-29: OTX.

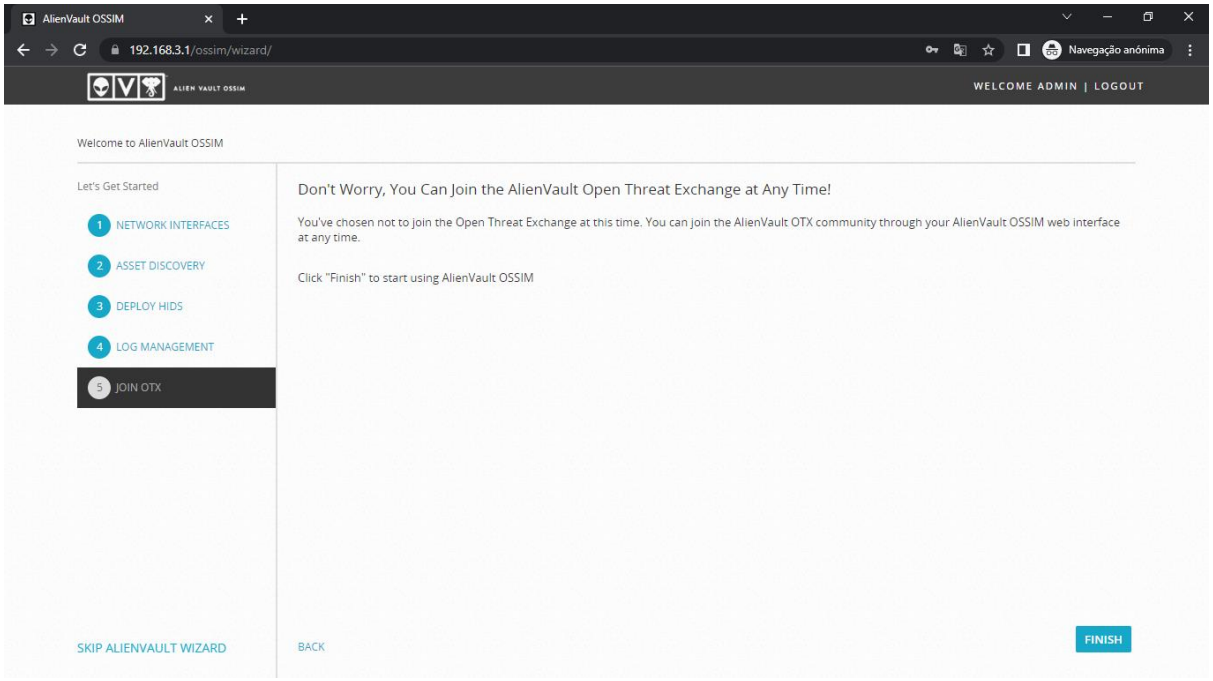

Figura A2-30: Configuração do OTX.

2.2.8. Dashboard

Exibe todos os gráficos, tabelas e gráficos de segurança da rede, assim como status de implantação, rede e dispositivos do OSSIM Appliance, visualizações de ameaças e pulsos OTX.

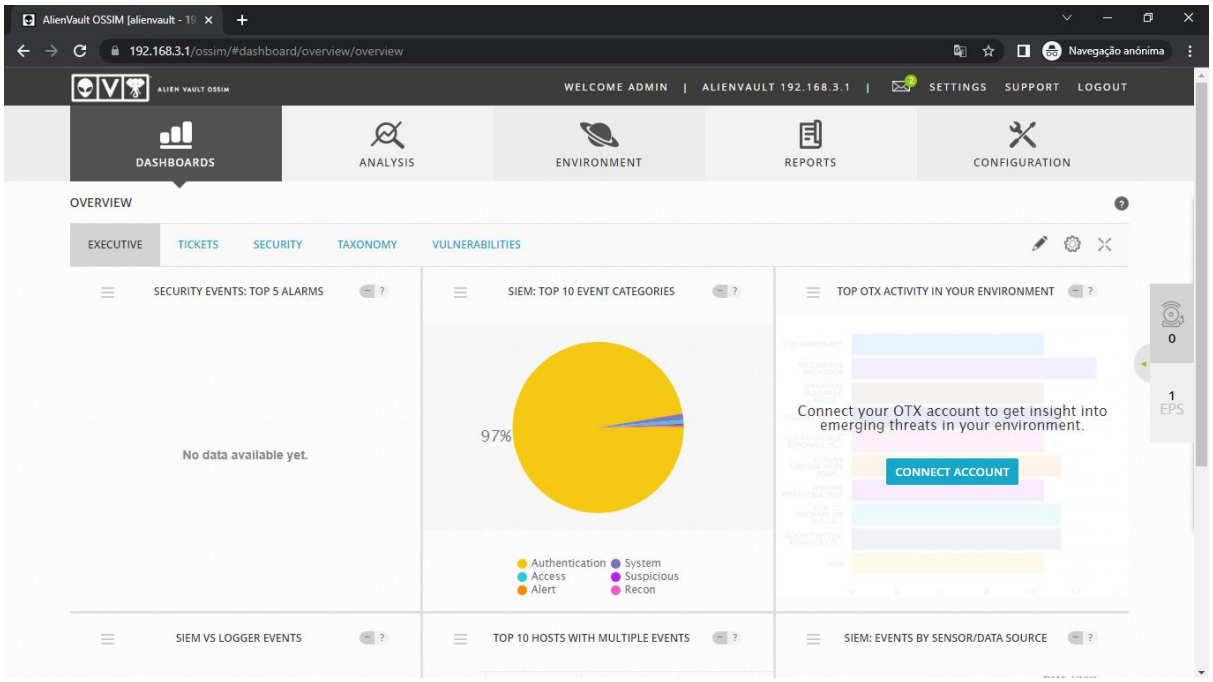

Figura A2- 31: Dashboard.

Anexo 3: Guião de Entrevista

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Entrevista

1. Quais activos existem na infra-estrutura de rede corporativa?
2. Quais são activos críticos da infra-estrutura de rede corporativa?
3. É feita a monitorização dos activos na infra-estrutura de rede corporativa? Se a resposta foi SIM, que software ou plataforma é usado?
4. Com que frequência é feita a análise de vulnerabilidades e a atualização dos softwares (sistemas operativos) dos activos na infra-estrutura de rede corporativa?
5. Caso um activo do tipo estacão de trabalho de um usuário seja comprometido por um ataque cibernético, no âmbito da resposta a incidentes que procedimentos devem ser tomados?
6. A instituição possui “quadros” qualificados/preparados para gerir uma plataforma SIEM?

Anexo 4: Guião de Questionário

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Questionário

NB: As questões a seguir são de resposta única [Sim ou Não], na grelha de respostas marque com X na opção correspondente.

1. O Instituto Nacional de Tecnologias de Informação e Comunicação possui uma Política de Segurança da Informação?
   1.1. A Política de Segurança da Informação foi devidamente difundida e publicada para todos os funcionários?
   1.2. Os funcionários estão devidamente instruídos sobre as suas responsabilidades e papéis pela Segurança da Informação?
2. Existe um inventário dos activos importantes da Infra-estrutura de Rede Corporativa do Instituto Nacional de Tecnologias de Informação e Comunicação?
3. Em relação aos computadores dos usuários, o Sistema Operativo (S.O) destes é actualizado periodicamente?
4. Actualmente, quais dos seguintes Mecanismos de Segurança são usados:
   4.1. Firewall?
   4.2. Sistema de Detecção de Intrusão (IDS)?
   4.3. Sistema de Prevenção de Intrusão (IPS)?
   4.4. Endpoint: Antivírus?
   4.5. Network Access Control (NAC)?
   4.6. Virtual Private Network (VPN)?
   4.7. Plataforma SIEM?
5. O Instituto Nacional de Tecnologias de Informação e Comunicação possui um plano claro e preciso de Resposta a Incidentes de Segurança?

Grelha de Respostas:

P	1	1.1	1.2	2	3	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5
Sim	X	X	X		X	X		X					X
Não				X			X		X	X	X	X	

Anexo 5: Exemplo de Correlação de Eventos

Timestamp	Nr. Evento	Fonte	Destino	Evento
10:10:01 CST	1035	192.168.1.200	10.10.10.25	Login no servidor falhou
10:10:02 CST	1036	192.168.1.90	10.10.10.21	Login no servidor efectuado
10:10:03 CST	1037	192.168.1.200	10.10.10.25	Login no servidor falhou
10:10:04 CST	1038	192.168.1.91	10.10.10.35	Login no servidor falhou
10:10:05 CST	1039	192.168.1.10	10.10.10.2	Login no servidor efectuado
10:10:06 CST	1040	192.168.1.10	10.10.10.3	Login no servidor efectuado
10:10:07 CST	1041	192.168.1.200	10.10.10.25	Login no servidor falhou
10:10:08 CST	1042	192.168.1.201	10.10.10.54	Login no servidor falhou
10:10:09 CST	1043	192.168.1.10	10.10.10.34	Login no servidor falhou
10:10:10 CST	1044	192.168.1.200	10.10.10.25	Login no servidor efectuado

Tabela A5-1: Exemplo de tentativas de autenticação registados num SIEM.

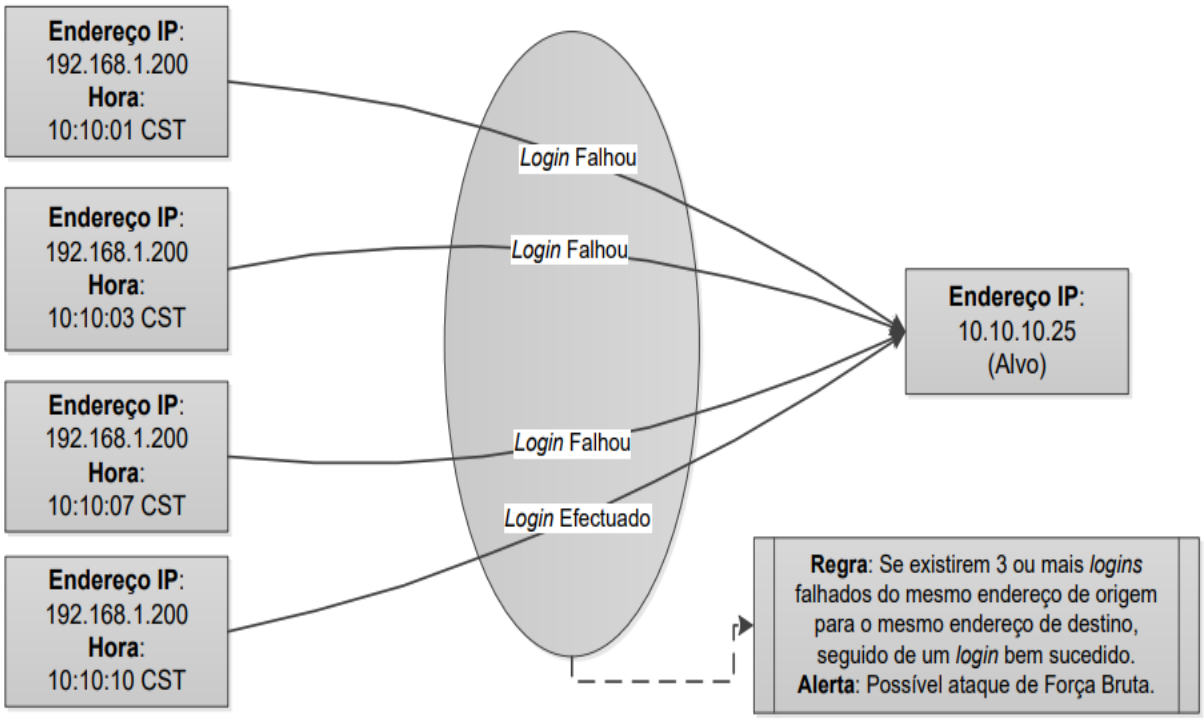

Figura A5-1: Exemplo de regra de correlação - Ataques de Força Bruta.