UNIVERSIDADE
EDUARDO
MONDLANE

*Faculdade de Engenharia*

*Departamento de Engenharia Electrotécnica*

*Curso de Engenharia Informática*

RELATÓRIO DE ESTÁGIO PROFISSIONAL

# Proposta de implementação de um SIEM para detecção de anomalias de segurança cibernética de uma rede corporativa. Caso de estudo: Grupo Meridian32

**Autor:**

Muianga, Frederico Sérgio

**Supervisores:**

Eng.º Délcio Chadreca (UEM)

Eng.º Víctor Guerra (ALTEL)

Maputo, Março de 2023

UNIVERSIDADE
EDUARDO
MONDLANE

*Faculdade de Engenharia*

*Departamento de Engenharia Electrotécnica*

*Curso de Engenharia Informática*

RELATÓRIO DE ESTÁGIO PROFISSIONAL

# Proposta de implementação de um SIEM para detecção de anomalias de segurança cibernética de uma rede corporativa. Caso de estudo: Grupo Meridian32

**Autor:**

Muianga, Frederico Sérgio

**Supervisores:**

Eng.º Délcio Chadreca (UEM)

Eng.º Víctor Guerra (ALTEL)

Maputo, Março de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

Curso de Engenharia Electrónica

# Proposta de implementação de um SIEM para detecção de anomalias de segurança cibernética de uma rede corporativa. Caso de estudo: Grupo Meridian32

FREDERICO SÉRGIO MUIANGA

Relatório a ser apresentado ao Departamento de Engenharia Electrotécnica, Faculdade de Engenharia da Universidade Eduardo Mondlane – UEM como requisito para a realização da disciplina Estágio Profissional. Supervisor: Eng.º Délcio Chadreca e a Directora do Curso: Eng.ª Ivone Cipriano

# UNIVERSIDADE EDUARDO MONDLANE

# FACULDADE DE ENGENHARIA

## Curso de Engenharia Electrónica

**TERMO DE ENTREGA DE RELATÓRIO DO ESTÁGIO PROFISSIONAL**

Declaro que o estudante Frederico Sérgio Muianga entregou no dia ____ / ____ / 2023 as ____ cópias do relatório do seu Estágio Profissional, com a referência: _____ intitulado: Proposta de implementação de um SIEM para detecção de anomalias de segurança cibernética de uma rede corporativa. Caso de estudo: Grupo Meridian32.

Maputo, _____ de Março de 2023

O (a) Chefe de Secretaria

_____

## Agradecimentos

Em primeiro lugar, quero agradecer a Deus pela vida que me concedeu e por me abençoar com essa oportunidade de me formar no curso de Engenharia Informática. Ele me capacitou para encarar e ultrapassar todos os desafios durante a formação académica.

Agradeço a minha avó por ter cuidado de mim e aos meus pais vivos (tia Inês Muianga e o tio Pedro Sitole) por investirem continuamente na minha educação e por cuidarem de mim.

O meu agradecimento vai especialmente para a minha companheira que me tem ajudado moralmente e me apoiado no meu trajecto profissional, muito obrigado.

Ao meu supervisor da Faculdade Engº. Délcio Chadreca vai o meu obrigado pela orientação e ajuda durante a elaboração do presente trabalho.

Agradeço ao meu supervisor da ALTEL Engº. Vítor Guerra pelo apoio e auxílio no enquadramento e execução das tarefas da organização e do trabalho.

O meu agradecimento vai para o Director-Geral da ALTEL Manuel Gaivão pelo voto de confiança e oportunidade que me concedeu de poder continuar o meu crescimento profissional da ALTEL.

## Resumo

Vivemos em um mundo digitalmente interconectado pelo grande motor de comunicação global que é a internet, esta interconexão trouxe à superfície problemas relativos à segurança cibernética, pois há mais espaço de acção para a execução de ataques cibernéticos. O uso de sistemas informáticos nos dias actuais pressupõem a necessidade de uso de mecanismos de segurança para o monitoramento de eventos, pois este monitoramento vem ajudar as organizações a ter uma visibilidade dos eventos de segurança e responder activa e proactivamente em cenário de um iminente ou eventual ataque cibernético. O presente trabalho foca-se no estudo e apresentação de uma proposta de solução para o monitoramento de eventos de segurança cibernética. Para a revisão de literatura de conceitos inerentes à segurança cibernética e soluções de Security Information and Event Management, o presente trabalho usou a metodologia de pesquisa qualitativa quanto a abordagem, que serviu a mesma para analisar a situação actual do ecossistema tecnológico da organização bem como a avaliação das soluções, com vista a permitir a identificação da solução que melhor se adequa ao caso de estudo. Foram endereçadas questões ao caso de estudo para melhor compreensão da situação actual. Arrola-se com este trabalho que a organização não possui mecanismos de monitoramento de eventos de segurança cibernética e o seu parque tecnológico é crítico para o monitoramento, porque as principais tarefas operacionais estão a ser executadas. Com a solução seleccionada e proposta, neste âmbito, a organização passa a ter um panorama de funcionamento da ferramenta e o grau de influência que a mesma possui graças a prova de conceito a ser implementada.



**Palavras-chave**: segurança cibernética, monitoramento de eventos de segurança, SIEM, infra-estrutura de TI.

## Abstract

We live in a world digitally interconnected by the great engine of global communication that is the Internet, this interconnection has brought to the surface problems related to cybersecurity, as there is more space for action to carry out cyberattacks. The use of computer systems nowadays presupposes the need to use security mechanisms for monitoring events, as this monitoring helps organizations to have a visibility of security events and to respond actively and proactively in the scenario of an imminent or eventual cyber attack. The present work focuses on the study and presentation of a proposed solution for monitoring cybersecurity events. For the literature review of concepts inherent to cybersecurity and Information Security and Event Management solutions, the present work used the qualitative research methodology regarding the approach, which served the same to analyze the current situation of the technological ecosystem of the organization as well as the evaluation of the solutions, with a view to allowing the identification of the solution that best suits the case study. Questions were addressed to the case study for a better understanding of the current situation. This work is related to the fact that the organization does not have mechanisms for monitoring cybersecurity events and its technological park is critical for monitoring, because the main operational tasks are being performed. With the solution selected and proposed, in this context, the organization now has an overview of how the tool works and the level of influence it has thanks to the proof of concept to be implemented.



**Key words**: cybersecurity, security event monitoring, SIEM, IT infrastructure.

# Índice

## Lista de símbolos

CTA – Cyber Threat Actor

DDoS – Distributed Denial-Of-Service

DLP – Data Loss Prevention

DoS – Denial-Of-Service

EDR – Endpoint Detection and Response

EPS – Events Per Second

ERP – Enterprise Resource Planning

FIM – File Integrity Monitoring

FSMO – Flexible Single Master Operation

GDPR – General Data Protection Regulation

GUI – Graphical User Interface

HIDS – Host-based Intrusion Detection Systems

IA – Artificial Intelligence

IoC – Indicator of Compromise

IoT – Internet of Things

IP – Internet Protocol

MitM – Man-In-The-Middle

NAC – Network Access Control

NAS – Network Attached Storage

NGFW – Next Generation Firewall

NIDS – Network-based Intrusion Detection Systems

NTA – Network Traffic Analysis

OTX – Open Threat Exchange

PoC – Prove of Concept

SGQ – Sistema de Gestão de Qualidade

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation and Response

SOC – Security Operation Center

SQL – Structured Query Language

STIX – Structured Threat Information eXpression

TAXII – Trusted Automated eXchange of Intelligence Information

TDIR – Threat Detection, Investigation, and Response

TI – Tecnologia de Informação

TIC – Tecnologia de Informação e Comunicação

TTP – Tactics, Techniques, and Procedures

UEBA – User and Entity Behavior Analytics

XDR – Extended Detection and Response

## Lista de figuras

## Lista de tabelas

# 1. CAPÍTULO I - INTRODUÇÃO

## 1.1. CONTEXTUALIZAÇÃO

Desde os primórdios que o ser humano se tem preocupado com a segurança da informação que transmite ou recebe, procurando de forma contínua garantir que a informação pertencente a si não seja alvo de qualquer individuo mal-intencionado e dotado de capacidades técnicas para a execução de algum ataque à infra-estrutura que armazena, processa e disponibiliza a informação.

Em um mundo moderno em que globalmente os dispositivos que compõem os sistemas informáticos encontram-se interligados, graças à internet, foram surgindo inúmeras ameaças, pois nesta grande rede de comunicação advém a facilidade de exploração de vulnerabilidades aliada a factores de interesse específico dos indivíduos mal-intencionados. Com este interesse, foram se desenvolvendo ferramentas e técnicas de ataque às infra-estruturas informáticas que põem em causa a segurança cibernética. As ameaças foram ganhando novos e sofisticados contornos no que toca às técnicas de penetrar à infra-estrutura de suas vítimas. Para responder à essa transformação das ameaças, os grandes fabricantes de soluções de segurança cibernética procuraram trazer soluções que pudessem fazer face a estas ameaças sofisticadas, através de colecta de dados dos diversos sistemas, monitoramento do comportamento dos sistemas, por meio de ferramentas especializadas neste tipo de actividades e resposta às tentativas de ataque, daí a necessidade das organizações olharem para esta problemática com mais seriedade para salvaguardar a sua informação.

O presente trabalho visa apresentar as actividades desencadeadas no processo de estágio profissional, assim como apresentação de uma proposta de implementação de uma ferramenta para detecção de anomalias de segurança cibernética em uma rede corporativa para incrementar a postura de segurança da organização em estudo. Como forma de o tornar claro, o mesmo está divido em 5 capítulos que são apresentados no subtítulo 1.2.

## 1.2. ESTRUTURA DO TRABALHO

O presente relatório está organizado da seguinte forma:

- **Capítulo 1 – Introdução**

  Neste capítulo, é dada uma abordagem introdutória sobre o trabalho, dando a conhecer o problema, a justificativa, a metodologia, os objectivos gerais e específicos do estágio.

- **Capítulo 2 – Revisão de literatura**

  Neste capítulo, é fornecida toda informação necessária para que seja possível compreender os conceitos inerentes ao monitoramento de eventos de segurança cibernética.

- **Capitulo 3 – Caso de estudo**

  Neste capítulo, é feita uma breve apresentação da instituição onde foi realizado o estágio, descrevendo as suas actividades, seus valores e sua organização. Serão igualmente apresentadas todas as actividades realizadas no período de estágio profissional, nomeadamente as actividades diárias na organização, assim como projectos envolvidos.

- **Capitulo 4 – Proposta de solução**

  Neste capítulo é apresenta a situação actual do caso de estudo no concernente à infra-estrutura de TI;

  Serão apresentadas possíveis soluções para o problema, os critérios a serem usados na escolha das possíveis soluções e a solução para o problema. Proposta para implementação de uma solução SIEM. Por fim, analise e apresentação dos resultados do trabalho.

- **Capitulo 5 – Conclusões e recomendações**

  Neste capítulo, são apresentadas as conclusões do projecto, o que foi possível de se obter como experiência ao longo do projecto e o que se pode fazer para melhorar o projecto.

## 1.3. PROBLEMA

O incremento de ataques cibernéticos tem obrigado as organizações a investir sistematicamente nos seus mecanismos de segurança cibernética, devido a sofisticação dos mesmos nos tempos actuais. Muitos destes ataques são bem-sucedidos, porque as organizações não possuem mecanismos para detecção e resposta ou estes sistemas não estão bem parametrizados e alinhados com as operações da organização para responder aos incidentes de segurança cibernética.

A ALTEL é uma empresa que faz parte do grupo Meridian32 das quais algumas organizações membro compartilham infra-estrutura informática que é gerida centralmente pela ALTEL. A importância de adoptar mecanismos de segurança cibernética ganha mais voz nestes cenários pois inúmeros utilizadores fazem uso desta infra-estrutura para execução de actividades operacionais sem contar com o facto de alguns sistemas do negócio da organização estarem hospedados nesta infra-estrutura.

Actualmente, toda a componente de segurança cibernética é gerida pelo departamento de IT da ALTEL e, pelo constatado existem mecanismos para protecção dos postos de trabalho, assim como para a rede corporativa a nível do perímetro. Porém, a organização não possui um sistema para monitoramento de eventos de segurança da rede, eventos estes que podem em algum momento dar visibilidade aos administradores da infra-estrutura informática sobre eventuais anomalias que podem indicar ou não alguma tentativa de ataque cibernético. Há tempos atrás, a organização sofreu um ataque cibernético, cujo impacto seria minimizado com a adopção de mecanismos de monitoramento de eventos de segurança da rede. Neste contexto, a presente pesquisa visa apresentar uma proposta de implementação de uma ferramenta SIEM para auxiliar no monitoramento de eventos de segurança cibernética.

Até que ponto uma ferramenta SIEM pode auxiliar no monitoramento de eventos de segurança cibernética na rede corporativa do grupo Meridian32?

## 1.4. JUSTIFICATIVA

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

Uma das principais motivações para o desenvolvimento deste trabalho é o facto deste tema ser de extrema importância para o desenvolvimento da minha carreira profissional na área de TI, outra motivação consiste na influência que este trabalho pode trazer à forma como as organizações dão valor à segurança da sua rede corporativa e, principalmente, como a postura de segurança deve ser encarrada nos dias actuais, pela forma como a globalização evoluiu as técnicas dos ciber-criminosos.

A implementação de ferramentas que auxiliam na segurança cibernética é um tema de vital importância, pois este virá despertar as organizações, no que diz respeito à forma como lidam com a segurança cibernética, na postura que se deve adoptar quando se estiver perante a tecnologia da informação, seja em um ambiente corporativo, assim como fora do ambiente corporativo. Este estudo trará ganhos significativos, na medida em que poderá influenciar em algumas situações na melhoria de práticas de segurança actualmente existentes.

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

## 1.5. OBJECTIVOS

### GERAL

- Propor a implementação de um Security Information and Event Management para a detecção de anomalias de segurança cibernética em uma rede corporativa;

### ESPECIFICOS

- Analisar a situação actual da infra-estrutura de TI no concernente ao monitoramento de eventos de segurança cibernética na rede do caso de estudo;
- Seleccionar a solução SIEM aplicável para o caso de estudo;
- Propor a ferramenta SIEM adequada para o caso de estudo;

## 1.6. METODOLOGIA

Com vista a alcançar os preceitos desta pesquisa e responder à questão de pesquisa, foi obedecida uma metodologia específica que abaixo é citada.

No concernente à abordagem a ser adoptada no presente trabalho, o autor fará o uso da abordagem qualitativa. Será abordagem qualitativa, visto que para se estudar um fenómeno em específico não se deve limitar nos conceitos abstractos apresentados por outros autores, mas sim aprofundar em conceitos de base que serão suficientes para perceber o fenómeno em estudo. Neste contexto serão analisados conceitos inerentes a segurança cibernética para melhor compreender o fenómeno de ataques cibernéticos, assim como a importância de monitorar a infra-estrutura de TI, em termos de eventos de segurança. Serão avaliadas as visões de diferentes autores na temática abrangente de segurança cibernética para posteriormente avaliar algumas visões orientadas especificamente ao SIEM. Será igualmente usada a abordagem qualitativa no processo de avaliação e selecção da solução SIEM aplicável para o caso de estudo.

No concernente aos objectivos, a pesquisa será considerada como exploratória, visto que o pesquisador fará uma exaustiva pesquisa com vista a se familiarizar com a temática de monitoramento de eventos de segurança cibernética para melhor compreender o impacto da ausência deste serviço em uma infra-estrutura de TI.

Quanto à participação do pesquisador, esta pode ser classificada como relação sujeito-objecto de pesquisa pois para este estudo o pesquisador apresentará um conjunto de questões que são endereçadas ao objecto de estudo e há uma interacção directa entre ambos para melhor percepção da situação actual do objecto de estudo. Para além da identificação da situação actual, o pesquisador apresentará algumas acções necessárias para resolução do problema identificado, desempenhando assim um papel activo, porquanto em algumas etapas da pesquisa será necessária a avaliação directa da população do estudo, neste caso a organização em estudo para avaliação da informação que pode ou não ser disponibilizada para esta pesquisa.

Para sintetização de toda a informação que constará na presente pesquisa, será usada uma técnica de colecta de dados que abaixo é apresentada.

Com vista a colectar informações relativas à postura da organização, no concernente ao monitoramento de eventos de segurança cibernética, serão endereçadas algumas perguntas ao caso de estudo em sessões de reuniões.

# 2. CAPÍTULO II – REVISÃO DA LITERATURA

Na presente secção, serão abordados conceitos primordiais para a compreensão da componente de segurança cibernética, sendo alguns deles: segurança cibernética, ameaças cibernéticas, actores de uma ameaça cibernética, ataques cibernéticos, principais tipos de ataques cibernéticos, factores que propiciam a exploração por parte de ciber-criminosos, mecanismos de segurança de informação, monitoramento de eventos de segurança e soluções SIEM.

## 2.1. Segurança cibernética

Vivemos em um mundo em constante transformação, no concernente às tecnologias adoptadas para melhorar a qualidade de vida do ser humano e as tecnologias de informação fazem parte deste grande ecossistema tecnológico. É difícil imaginar um mundo sem interconexão, entre os diversos sistemas. Nos primórdios, as tecnologias de informação funcionavam de forma isolada, porém actualmente é inimaginável ver estas tecnologias isoladas, pois estamos em um mundo globalizado. As ameaças à informação que flui nestes sistemas seguiu o mesmo curso evolutivo, ou seja, a cada progresso das tecnologias de informação, as ameaças também evoluíam. Em um mundo digitalmente interconectado surge a necessidade de garantir a segurança da informação que flui nestes sistemas, seja ela informação individual ou global, pois, a informação tornou-se um activo nuclear para a sobrevivência das organizações.

(Choudary, 2018) "*Segurança cibernética é o conjunto de tecnologias, processos e práticas projectados para proteger redes, computadores, programas e dados contra-ataques, danos ou acesso não autorizado"*.

Segundo (Bairu, 2020) segurança cibernética consiste na protecção de todo o parque de sistemas de informação contra ameaças ou vulnerabilidades dos mesmos.

A **segurança cibernética**, como os autores acima definem, consiste em aplicação de tecnologias e procedimentos para protecção dos activos de informação incluindo a principal informação contra vulnerabilidades e ameaças existentes. Percebe-se uma relação existente entre a segurança cibernética e a segurança da informação, sendo a segurança cibernética considerada um ramo da segurança de informação, focando na prevenção e protecção dos activos de informação em

uma infra-estrutura informática. Em algum momento, a segurança cibernética preconiza garantir que os pilares fundamentais da segurança da informação sejam satisfeitas aquando da manipulação da informação.

De acordo com (Oscarson, sem data) a segurança dos activos de informação geralmente é definida por três pilares fundamentais: confidencialidade, integridade e disponibilidade conforme ilustra **figura 1**, concordando (Vuorinen & Tetri, 2012) ao dizer que comumente abordagem da segurança da informação é assente no alcance da confidencialidade, integridade e disponibilidade de informações. Estes são os principais objectivos quando se trata de segurança da informação, devendo ser imprescindível ter em conta estes pontos quando estivermos a falar da segurança de informação.

- Confidencialidade: preconiza a prevenção de divulgação não autorizada ou uso de activos de informação;
- Integridade: preconiza a prevenção de alteração não autorizada de activos de informação por parte de terceiros;
- Disponibilidade: preconiza garantir o acesso autorizado de activos de informação no momento requisitado. Oscarson (Per, p.4)


*Figura 1 Pilares da segurança da informação, elaborado pelo Autor*

## 2.2. Ameaças cibernéticas

As ameaças cibernéticas são o grande problema para a segurança cibernética, pois estas é que vem explorar as vulnerabilidades dos sistemas que fazem uso do ciberespaço para penetrar e executar um ataque cibernético, com o intuído de roubar informação, ou mesmo causar danos em termos de disponibilidade dos serviços dos sistemas.

De acordo com (Da Silva et al., 2015), o ciberespaço é o meio de comunicação global entre vários sistemas informáticos.

É um conjunto de tecnologias que trouxeram um novo paradigma, no que tange às relações entre o ser humano e as tecnologias de informação, incluindo também a relação entre os seres humanos, este novo paradigma amplia os limites da criatividade humana, em termos de acesso às informações e comunicações.

O grande objectivo destas ameaças é de violar um ou mais pilares da segurança cibernética, nomeadamente a confidencialidade, integridade e disponibilidade de um activo de informação.

A ameaça cibernética tem como canal de actuação para execução de acções maliciosas o ciberespaço que é a infra-estrutura de TI que interconecta os diversos sistemas informáticos a nível global. Segundo (Oscarson, sem data), "*Activos podem ser pessoas, coisas criadas por pessoas ou partes da natureza. Na área de segurança da informação, os activos são frequentemente rotulados como activos de informação e englobam não apenas a informação em si, mas também os recursos que estão em uso para facilitar a gestão da informação"*.

Em suma, o activo de informação é todo elemento que compõe uma organização e que agrega valor à mesma.

## 2.3. Ataques cibernéticos

Com as bases apresentadas nos conceitos anteriores, temos segmentação para explorar a componente de ataques cibernéticos e alguns ataques comumente conhecidos. Os ataques cibernéticos são ataques direccionados a serviços providos por sistemas informáticos (websites, informações, entre outros serviços críticos providos por um computador ou conjunto de computadores). Estes ataques podem também ser direccionados a computadores individuais. O intuito de um ataque cibernético é comprometer a informação das suas vítimas.

Os ataques cibernéticos podem ser direccionados ou não direccionados. Nos ataques direccionados, o ciber-criminoso tem como objectivo uma vítima seja ela individual ou colectiva e direcciona o ataque conhecendo o seu alvo enquanto que nos ataques não direccionados o ciber-criminoso aproveita as vantagens que a internet dá, graças à interconexão para lançar ataques de forma deliberada sem ter um alvo específico.

Para (Biju et al., 2019), o processo de execução de ataques cibernéticos geralmente obedece quatro etapas que são: reconhecimento ou pesquisa, entrega, breach e infecção.

**Reconhecimento ou pesquisa:**

É a primeira etapa, pois é nela que o ciber-criminoso estuda a vítima para colecta de informações disponíveis que podem dar um mapa da vítima, no concernente à sua situação actual, em termos de uso de tecnologias de informação e dos dados e criticidade dos mesmos. É nesta fase que são identificadas as vulnerabilidades.

**Entrega:**

Nesta fase, o ciber-criminoso identifica a vulnerabilidade e o ponto de entrada para explorar a vulnerabilidade.

**Violação:**

Nesta fase, o ciber-criminoso já identificou a vulnerabilidade e explora a mesma para ganhar acesso não autorizado.

**Infecção:**

Nesta etapa, o ciber-criminoso executa o que pretende dentro do sistema da vítima pois o acesso ao sistema já está garantido.

Enquanto que (Bodeau et al., 2018) subdivide as etapas de um ataque cibernético em sete partes nomeadamente: reconhecer, armar, entregar, explorar, controlar, executar e manter. Fazendo um cruzamento destes distintos autores as fases apresentadas pelo segundo autor (Bodeau et al., 2018) focam-se em ameaças mais sofisticadas e avançadas, devido à fases de inteligência e permanência na infra-estrutura da vítima, enquanto que o primeiro autor apresenta fases que são comumente usadas pelos ataques cibernéticos mais conhecidos. Abaixo serão abordados estes tipos de ataques para melhor compreensão.

## 2.4. Principais tipos de ataques cibernéticos

Os ataques cibernéticos têm sido perpetrados por ciber-criminosos ao redor do mundo, vários são os relatos apresentados por entidades públicas e privadas. Vários foram os tipos de ataques usados para atingir determinados alvos no ano de 2022, factores como a adopção do teletrabalho e o conflito entre a Ucrânia e a Rússia serviram como catalisadores para a execução destes ataques. Como pode ser evidenciado pelo (O'CONNOR, 2022), a maioria dos ataques foram ransomwares, DDoS e roubo de dados através do phishing, engenharia social e outros métodos de roubo de credenciais.

Fazendo uma análise comparativa entre a realidade dos ataques no mundo e em Moçambique, percebe-se que Moçambique não está aquém de sofrer estes ataques, algumas organizações vem sofrendo ataques principalmente de phishing e ransomeware, porém, não são divulgadas informações em alguns casos porque as organizações pretendem salvaguardar a sua credibilidade no mercado. Para o melhor entendimento, alguns dos principais tipos de ataques cibernéticos serão apresentados abaixo:

**Denial-of-service (DoS) e distributed denial-of-service (DDoS)**

É um tipo de ataque em que o ciber-criminoso instala um malware em um computador na rede e sobrecarrega os recursos de outro computador que disponibiliza serviços, a ponto deste não conseguir responder à novas solicitações. Com esta circunstância o serviço provido pelo computador da vítima torna-se indisponível.

**Ataque de Password**

É um tipo de ataque em que a palavra-passe de um utilizador é obtida de forma ilegítima, seja por desencriptação, advinha, acesso não autorizado à bases de dados de credenciais, intercepção de textos planos, ataques de dicionários entre outras formas de acesso indevido.

**Ataque de SQL Injection**

É um tipo de ataque em que o ciber-criminoso insere código malicioso em um servidor, usando a linguagem SQL (Structured Query Language) para se ter acesso à informação protegida no servidor. O ciber-criminoso aproveita alguma vulnerabilidade de uma página web desprotegida que tenha ligação a um sistema de bases de dados em SQL.

**Phishing**

É um tipo de ataque em que são enviados múltiplos emails fraudulentos para utilizadores, fazendo parecer que o email é legitimo. O email enviado provém com uma formatação e conteúdo com intuito de enganar os utilizadores que recebem e indica algum link que os mesmos devam fazer clique. Ao fazer o clique no link malicioso são executados códigos que poderão dar acessos à máquina da vítima e permitir a execução da primeira fase de um ataque cibernético anteriormente apresentada que é reconhecimento, ou em um caso mais grave ter total controle da máquina vítima, podendo ter acesso à toda a informação da mesma.

**Man-in-the-middle (MitM)**

É um tipo de ataque em que o ciber-criminoso intercepta um meio de comunicação entre duas entidades, fazendo leitura da informação transitada de um ponto para o outro, podendo manipular em algum momento a informação interceptada. Para a execução deste tipo de ataque geralmente é explorada uma vulnerabilidade em uma rede que possibilita o ciber-criminoso se colocar entre dois pontos de comunicação.

**Malware**

É um tipo de ataque clássico em que softwares maliciosos são instalados na máquina da vítima sem a mesma saber. Geralmente estes tipos de códigos maliciosos são colocados em códigos aparentemente legítimos que a vítima pode executar em sua máquina e por trás executa o malware. Este tipo de ataque é comumente usado em softwares pirateados. Abaixo são listados alguns tipos de malware:

- **Vírus –** É um tipo de software malicioso que se anexa a um programa legítimo e o mesmo tem a capacidade de se replicar e modificar códigos maliciosos quando necessário.

- **Trojans –** É um tipo de programa malicioso com uma semelhança ao vírus pelo facto do mesmo se esconder em programas legítimos, a diferença é que não se replica e o principal objectivo é de criar backdoors para que um ciber-criminoso possa explorar.

- **Worms –** Este tipo de programa malicioso não ataca o computador que infecta, ele se instala em uma máquina através de anexos e propaga-se através do envio de email para os contactos da primeira máquina infectada. O principal objectivo deste tipo de programa malicioso é de sobrecarregar o servidor de email.

- **Spyware –** É um tipo de programa malicioso que o principal objectivo é colectar informação relativa à vítima e sistemas que a vítima usa,

enviando essa informação colectada para um computador remoto que é do ciber-criminoso.

- **Ransomware –** É um tipo de malware que encripta os dados da vítima, inibindo a mesma de aceder a informação. As vítimas deste tipo de malware são ameaçadas de publicação da sua informação ou perda da mesma, devendo a vítima efectuar um pagamento para recuperar a informação.

## 2.5. Factores que propiciam a exploração por parte de ciber-criminosos

Os ciber-criminosos perpetram os seus intentos maliciosos nas suas vítimas, graças a aplicação de conhecimentos na área de sistemas de informação e exploração de vulnerabilidades existentes nesses sistemas. De acordo com (Dand & Chudasama, 2021), vulnerabilidade é uma fraqueza existente em um sistema informático que pode ser usada para execução de acções maliciosas não autorizadas por parte de ciber-ciminosos, conceito que converge com (Yadav & Mallari, 2015) que apresenta como um bug relativo a um software que pode resultar em uma potencial ameaça ao sistema, esta ameaça advém do ciber-criminoso pois ele é o actor que explora estes bugs. Pela conceituação de vulnerabilidade dá para perceber que os ciber-criminosos são tendenciosos à exploração de fraquezas que os sistemas possuem para execução de acções maliciosas, há uma tendência destes actores de cibercrime estudarem mais sobre o funcionamento dos sistemas com vista a identificar potenciais pontos de entrada para a exploração, uma oportunidade de exploração de fraquezas pode ser considerada um vector de entrada para um ataque cibernético. Foram apresentados alguns tipos de ataques cibernéticos no subtítulo anterior para melhor a compreensão do fenómeno de exploração de vulnerabilidades. Não obstante, convém compreender melhor quais são os factores que permitem a exploração das vulnerabilidades por parte dos ciber-criminosos.

As vulnerabilidades que propiciam a exploração por parte de ciber-criminosos podem ser:

Desgaste com base na idade, que pode causar falhas e superaquecimento nos sistemas, estas duas vulnerabilidades podem ser exploradas por ciber-criminosos que pretendam causar indisponibilidade de serviços e informações como por exemplo através do ataque de DDoS.

Insuficiência de testes em implementações de soluções de TI, o facto de não se explorar ou testar novos sistemas de TI com vista a identificar variáveis que impactem na segurança e disponibilidade da informação provida por estes sistemas pode cegar os implementadores no concernente a pontos de vulnerabilidades existentes.

Desactualização dos sistemas, pode ocasionar pontos de entrada porque os ciber-criminosos possuem ferramentas de scan de sistemas conectados à internet que possuem vulnerabilidades, os fabricantes das soluções vulneráveis podem lançar actualizações para fechar as lacunas com vista a inibir que estas sejam exploradas para fins maliciosos. Se a organização não actualiza os sistemas dá espaço para exploração por parte dos ciber-criminosos.

Codificações inseguras, a aplicação de metodologias de codificação obsoletas e inseguras pode permitir que os ciber-criminosos possam ter acesso às informações sigilosas e até alterar o princípio de funcionamento de alguns sistemas apontando os mesmos para uma direcção maliciosa.

Falta de audit trial, permite que não exista visibilidade em termos de actividades nos sistemas informáticos, permitindo assim que os ciber-criminosos executem acções maliciosas sem ser detectada a actividade em específico, e até sem se saber a dimensão do ataque sofrido.

Pontos de comunicação desprotegidos e arquitecturas de rede inseguras, permite que sejam exploradas estas vulnerabilidades para penetração na rede da vítima de forma fácil sem passar por camadas de autenticação.

Processo de recrutamento inadequado, permite que ciber-criminosos possam explorar e penetrar em sistemas informáticos, pois em algumas situações podem ser recrutados funcionários com histórico que pode incrementar o risco dos sistemas informáticos através de culturas inseguras, histórico de associação com ciber-criminosos, etc.

Conscientização de segurança inadequada, possui uma relação com a vulnerabilidade acima. Pois o ponto de entrada de um ataque pode ser um colaborador da organização através da aplicação da engenharia social e tentativas de phishing.

Falta de auditorias periódicas aos sistemas de informação, pode ocasionar cegueira em termos das actividades dentro da infra-estrutura de TI, permitindo que os ciber-criminosos executem as suas acções de forma contínua e silenciosa em alguns casos.

## 2.6. Mecanismos de segurança de informação

Foi perceptível a importância de conhecer o ecossistema de segurança cibernética, desde os pilares da segurança da informação até às ameaças cibernéticas que põem em risco a informação e os seus sistemas. É sabido que os sistemas de informação ganharam seu espaço em termos de importância para a sobrevivência de organizações, principalmente nesta era em que o grande activo é a informação. Pela elevada importância, surgiu a necessidade de proteger estes sistemas devido às ameaças cibernéticas e aos ataques cibernéticos apresentados nos conceitos anteriores.

(Alshammari & Bach, 2013) afirmam que os sistemas de informação baseados em computador têm três componentes principais, a primeira componente são os computadores, a segunda componente é a rede e a terceira componente é humana.

Para (Alshammari & Bach, 2013) os mecanismos de segurança de informação são divididos em quatro partes, nomeadamente:

- Defesa técnica

  A defesa técnica abrange toda a técnica e tecnologias usadas para proteger computadores e redes. De entre estas técnicas e tecnologias são destacados: tecnologias de encriptação, firewalls, antivírus/anti-malware, sistemas de detecção e prevenção contra intrusões.

A **encriptação** permite uma troca de informação mais segura entre duas ou mais entidades, através de algoritmos que transformam os dados legíveis em dados codificados. Nesta comunicação, apenas os envolvidos podem visualizar e ler - esta técnica inibe acessos não autorizados a informações.

A **firewall** permite proteger sistemas de informação em uma rede. Sabendo que a infra-estrutura base de comunicação para o mundo globalizado é a internet, as organizações usam a mesma para troca de informações e os ciber-criminosos aproveitam essa conexão global para executar os seus ataques. A firewall permite filtrar as conexões de dentro da organização para fora e de fora para dentro, permitindo apenas as conexões que a política da organização autoriza. Este dispositivo funciona como um ponto de controlo de tráfego em que a conexão que estiver em conformidade passa e a que não estiver em conformidade é bloqueada.

O **antivírus/anti-malware** permite o monitoramento em tempo real dos sistemas operativos da organização para bloqueio de malwares que foram devidamente explanados na secção de tipos de ataques cibernéticos.

O **sistema de detecção e prevenção contra intrusões** é um sistema que dá visibilidade aos administradores de segurança de informação em tempo real sobre as tentativas de intrusão na rede da organização, através do monitoramento, análise de conexões e tentativas de exploração de vulnerabilidades por parte de ciber-criminosos. Para além da detecção, este sistema pode bloquear tentativas de intrusão.

- Defesa operacional

  A defesa operacional consiste na implementação de políticas de segurança de informação e na capacitação do pessoal técnico que

lida com os sistemas de informação da organização. O facto de implementar alguns mecanismos de defesa técnica não implica que a organização está totalmente segura pois existe um conjunto de elementos operacionais que parametrizam e fazem gestão destes mecanismos para responder às necessidades de segurança da informação da organização. Mecanismos de defesa técnica mal parametrizados e mal geridos podem abrir pontos de entrada de ataques.

- Defesa de gestão

  A defesa de gestão está mais focada em garantir a segurança de sistemas de informação, filtrando condignamente no processo de contratação de colaboradores através de implementação de padrões de contratação que garantem a segurança da informação ao contractar um novo colaborador para a organização. Esta fase é importante, pois ao contratar um colaborador sem conhecer o seu histórico e capacidades pode levar a organização a ter lacunas de segurança e permitir a instalação de backdoors que os ciber-criminosos usam para penetrar em uma infra-estrutura de uma vítima de ataque cibernético.

- Defesa física

  A defesa física preconiza a protecção dos activos de informação contra danos que podem resultar na perda de informação e perda de dinheiro, estes danos podem ser causados por negligência humana, desastres naturais ou mesmo acesso não autorizado aos activos de informação por parte de pessoas que pretendam sabotar a organização.

Para (Ribeiro et al., 2005), os mecanismos de segurança de informação são divididos em seis partes nomeadamente:

- Identificação de utilizadores

A identificação de utilizadores nesta abordagem consiste no cadastro dos utilizadores e autorização de acesso aos recursos apenas nos sistemas que deve ter acesso.

- Autorização e controle de acesso
  Este tipo de mecanismo foca-se em quais acções o utilizador tem permissão para executar no sistema devendo se autenticar e executar as acções que lhe foram concedidas as permissões.
- Protecção de dados armazenados
  Este foca-se na integridade dos dados protegendo-os contra malwares e tentativas de alterações indevidas.
- Protecção de dados em trânsito
  Estes mecanismos visam garantir a protecção dos dados em processo de comunicação contra intercepção, alteração indevida, bloqueios e exclusões.
- Auditoria de acesso às informações
  Estes mecanismos visam garantir registos de todas as actividades executadas pelos utilizadores dentro dos sistemas da organização, permitindo a visibilidade em termos de actividades caso seja necessário em processo de auditoria.
- Monitoração de potenciais intrusos
  Estes mecanismos vistam alertar aos administradores dos sistemas informáticos sobre potenciais ameaças existentes em sua infra-estrutura informática, estes mecanismos podem detectar e até mesmo bloquear ameaças à segurança da informação.

Fazendo-se uma análise comparativa das duas abordagens em termos de mecanismos de segurança de informação, percebe-se que os mecanismos apresentados por (Ribeiro et al., 2005) encaixam-se nos mecanismos de defesa táctica sustentados por (Alshammari & Bach, 2013), sendo esta abordagem mais abrangente no quesito de segurança de informação, porque temos partes que muitas organizações ignoram e que são de vital importância para a garantia de segurança da informação, nomeadamente a defesa operacional, defesa de gestão e defesa física os quais são importantes para a presente pesquisa.

## 2.7. Security Information and Event Management

Um SIEM é necessário para lidar com o incremento do nível de segurança cibernética, assim como a análise e gestão de forma centralizada da informação colectada.

Em um SIEM as informações cruciais no concernente a segurança cibernética advém de várias fontes, porém esta informação é centralizada em um único repositório para sua visualização e identificação de tendências que podem indicar tentativas de ataques cibernéticos.

Antes de avançar para detalhes mais profundos do SIEM, convém perceber o que seria um SIEM para (Fruhlinger, 2022). o termo "SIEM" foi realmente apresentado pelos analistas do Gartner em 2005, e eles continuam a avaliar os vários fornecedores usando sua metodologia do Quadrante Mágico.

Ainda de acordo com (Fruhlinger, 2022) o SIEM é a combinação de SIM e SEM sendo que SIM é uma ferramenta que providencia analise e relatórios de eventos de segurança que ocorreram no passado enquanto que o SEM é uma ferramenta que tem como intuito lidar com eventos de segurança em tempo real. Com esta abordagem de combinação de SIM e SEM, o SIEM pode ser visto como uma ferramenta que permite a colecta de informações relativas a eventos de segurança para permitir o processamento, a análise, e armazenamento de eventos de segurança para detecção de anomalias em uma rede corporativa, eventos estes que podem ser passados ou em tempo real para auxiliar os administradores de TI na identificação e resposta a anomalias no que tange a eventos de segurança cibernética.

O conceito do SIEM apresentado por (Fruhlinger, 2022) converge com o conceito apresentado por (Vielberth & Pernul, sem data) que conceitua o SIEM como o sistema que colecta dados relevantes de diversas fontes relevantes e realiza análises históricas sobre eventos de segurança. Além disso, ele suporta relatórios para fins de conformidade e investigação, analisando os dados históricos armazenados das mesmas fontes.

Pelos conceitos acima apresentados temos um panorama do que é realmente uma ferramenta SIEM. Como os autores definem, esta ferramenta tem o seu funcionamento inclinado na colecta de dados oriundos de fontes relevantes para

cada caso, dados estes que são normalizados para dar uma visibilidade mais inteligente sobre eventos de segurança em uma organização. Esta ferramenta permite ter visibilidade no concernente a eventos de segurança cibernética em uma organização, dotando os administradores de TI de uma ferramenta que auxilia na resposta a incidentes de segurança cibernética seja em termos históricos assim como em tempo real.

### 2.7.1. Anatomia de uma solução SIEM

O SIEM pode ser visto como uma máquina complexa, pois ele está subdividido em diversas partes. Para (Miller et al., 2011) SIEM simples pode ser dividido em seis peças ou processos nomeadamente

- **Origem**: pode ser considerado um dispositivo, uma aplicação ou outro tipo de origem em que serão colectados os logs para armazenar e processar no SIEM, temos como exemplo a firewall, roteadores, switches, servidores, etc.
- **Colecção de logs**: esta fase consiste basicamente na colecta de logs em que o dispositivo ou aplicação que gera o log pode enviar estes logs para o SIEM *"push"* ou o SIEM pode estabelecer uma sessão com o dispositivo ou aplicação para retirar directamente os logs *"pull"*.
- **Normalização de análise**: é o processo de transformação dos logs não formatados para um formato único e compreensível pelo SIEM, independentemente do tipo de dispositivo, do fabricante, etc.
- **Mecanismo de regras/Mecanismo de correlação:** o mecanismo de regras é processo que expande a normalização dos eventos para despoletar alertas no SIEM, baseados em condições dos logs e das regras estabelecidas no SIEM. Posteriormente, temos o mecanismo de correlação que é um subconjunto do mecanismo de regras e tem como função combinar vários eventos padrão de diferentes fontes em um único evento.

- **Armazenamento de log:** é o repositório de armazenamento de logs para fins de consulta de histórico, pode ser em uma base de dados, ficheiro de texto ou um ficheiro binário.
- **Monitoramento**: é a parte responsável pela interacção com os logs armazenados no SIEM, o intuito é trazer uma visibilidade útil dos logs armazenados no SIEM através de uma interface de utilizador.

Enquanto que (Vielberth, 2021) diz que um SIEM é composto por

- **Colecção**: nesta etapa ocorre a colecta de logs das diversas fontes através do envio da informação através da fonte de logs ou pelo carregamento dos logs através do SIEM.
- **Normalização**: consiste na uniformização dos dados colectados.
- **Enriquecimento**: é o processo de contextualização dos dados colectados para facilitação no processo de detecção de ataques cibernéticos.
- **Correlação e análise**: este é o processo em que o SIEM faz uma dedução do estado do ambiente corporativo em termos de segurança, esta dedução é feita com base nos eventos observados das diversas origens para ajudar na detecção de ataques.
- **Alerta e resposta**: é o processo que consiste na notificação de todos os intervenientes relevantes com vista a informar sobre possíveis detecções de incidentes de segurança cibernética.
- **Relatórios e troca de ameaças**: o SIEM nesta etapa deve permitir a visualização de relatórios de incidentes de segurança cibernética que podem ser usados para fins de conformidade ou mesmo por obrigações legais.

Pelas anatomias acima apresentadas, compreende-se que um SIEM deve, no mínimo, ter as componentes abaixo: origem, colecção de logs ou dados, normalização de análise, mecanismo de regras/Mecanismo de correlação, armazenamento de log, monitoramento, inclusive a possibilidade de exportação de relatórios de eventos segurança cibernética, a **figura 2** apresenta de forma sumária as componentes de um SIEM.

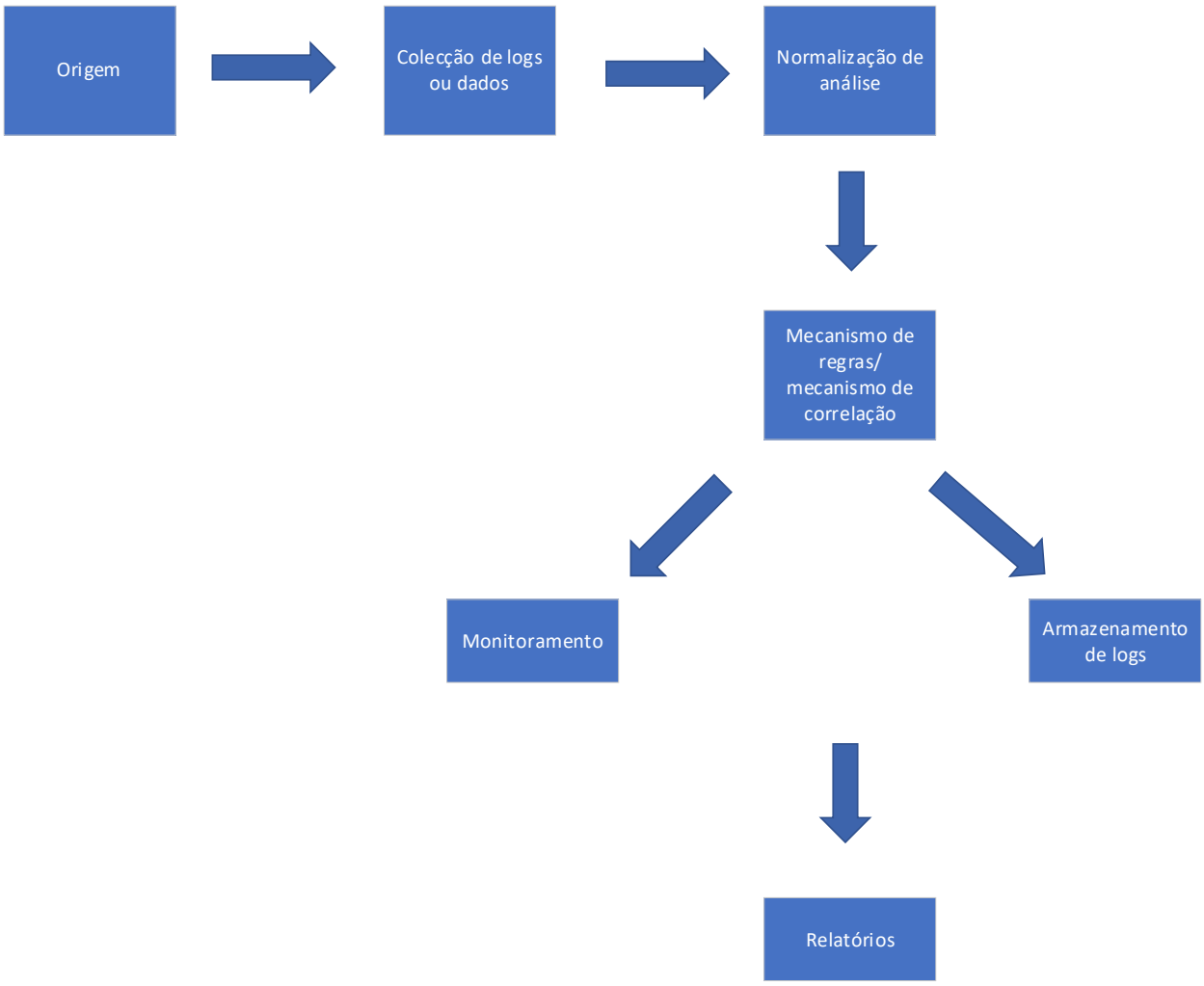



*Figura 2 Anatomia de um SIEM, elaborado pelo Autor*

### 2.7.2. Vantagens de uso de uma ferramenta SIEM

As soluções SIEM geralmente obedecem a combinação de algumas funcionalidades essenciais para a detecção de anomalias de segurança cibernética. Estas ferramentas unificam o monitoramento de ameaças e resposta às tentativas de ataques com a gestão de logs, esta informação advém de várias fontes em uma infra-estrutura de TI, o que poderá dar uma maior visibilidade às equipes que fazem gestão da segurança cibernética de uma organização. Antes de adoptar um sistema SIEM, convém perceber quais benefícios esta ferramenta poderá trazer para uma organização, e é neste contexto que abaixo são alistados alguns dos benefícios de adoptar uma ferramenta SIEM.

- **Agregação de dados**

  O SIEM agrega informações de eventos de segurança de toda infra-estrutura de TI, garantindo a colecta de forma centralizada. Por extensão, ele faz a procura e extrai informações de fontes anteriormente ocultas na rede, impedindo que hackers ocultem suas actividades maliciosas.

- **Normalização de dados**

  As soluções SIEM não apenas colectam dados elas normalizam também, ou seja, elas formatam os dados em qualquer formato desejável, permitindo a consistência na gestão de logs e uma fácil correlação. Beneficia tanto o processo de análise de ameaças SIEM, quanto à inteligência humana.

- **Conformidade**

  O SIEM pode permitir que uma organização garanta conformidade, pois estas soluções geralmente fornecem modelos de relatórios prontos para uso para a maioria dos requisitos de conformidade.

- **Detecção de ameaças e alerta de segurança**

  Um dos benefícios na adopção de uma solução SIEM em um contexto de segurança cibernética é a detecção de ameaças e os recursos de alerta de segurança.

- **Armazenamento de dados**

  As soluções SIEM, podem ajudar uma organização a armazenar os dados normalizados, organizá-los e pesquisar de forma fácil caso seja necessário.

### 2.7.3. Critérios de avaliação e selecção de ferramenta SIEM

Até esta etapa pode-se perceber em alto nível a importância da segurança cibernética para uma organização, seja ela colectiva ou individual. Tendo uma anatomia básica de alguns tipos básicos de ataques cibernéticos, mecanismos de segurança para responder a estes tipos de ataques básicos, foi crucial perceber condignamente como funciona um SIEM e o seu grau de importância para uma organização, visto que será apresentada posteriormente uma proposta de

implementação para o caso de estudo. Antes de avançar e propor uma ferramenta para um caso específico, é necessário observar os pontos a ter em consideração no processo de avaliação da melhor ferramenta para que a proposta responda às necessidades de cada caso. Neste subtítulo, serão apresentados alguns critérios a ter em consideração no processo de selecção de uma ferramenta SIEM.

Para (Mokalled et al., 2020), o processo de selecção de uma ferramenta SIEM deve obedecer a 5 critérios a ter em consideração, nomeadamente a plataforma, operações, integração, licenciamento e suporte:

- **Plataforma**

  Mandatório:

  - **Capacidade do sistema de gestão de logs**: a solução técnica deve abordar a colecta, normalização, indexação, compactação e arquivo, retenção (e todos os recursos usuais do Log Management Systems) de eventos e arquivos de log, juntamente com agregação, correlação, análise, relatórios e alertas.
  - **Tipo de plataforma SIEM**: o fornecedor deve apresentar detalhes sobre o tipo de plataforma SIEM disponível (por exemplo, dispositivos de hardware ou dispositivos virtuais ou apenas software).
  - **Suportando um conjunto estendido de fontes de log**: a plataforma deve ser capaz de analisar com suporte nativo as fontes de log mais difundidas, e uma lista dos obrigatórios deve ser apresentada pelo fornecedor.
  - **Customização de analisadores/conectores**: a plataforma deve ser capaz de suportar a criação de uma biblioteca de analisadores/conectores personalizados.
  - **Método para recuperar eventos/fluxos/logs**: o fornecedor deve especificar o método utilizado para recuperar eventos/fluxos/logs (por agente/suporte sem agente) e convém que o cliente esteja ciente sobre o método relevante que se encaixa no caso.
  - **Arquitectura hierárquica e modular/escalável**: a arquitectura deve ser escalável por meio de desbloqueio de licença ou adição de módulos, sem a necessidade de substituição e reconfiguração.

- **Gestão de fusos horários**: a arquitectura SIEM deve suportar muitos recursos diferentes de gestão de fuso horário, até mesmo fornecer fusos horários ao capturar arquivos de log que não têm nenhum.
- **Capacidade de computação da plataforma**: a cálculo para determinar o número apropriado de EPS (Eventos Por Segundo) sustentado e o valor de pico de EPS proposto devem ser declarados.
- **Capacidade de armazenamento da plataforma**: a plataforma deve ser capaz de armazenar os eventos/logs por um período de tempo acordado (por exemplo, em meses) para um acesso indexado rápido e um armazenamento a longo prazo.
- **Modelo de instalação**: o fornecedor deve especificar qual modelo de instalação está disponível (por exemplo, local, nuvem privada ou opção gerida).
- **Alta disponibilidade/opções de cache**: as opções de redundância/cache devem estar disponíveis para evitar perdas de transferência de eventos/arquivos de log no caso de instalação distribuída.
- **Disponibilidade de regras de correlação padrão e personalizáveis**: a plataforma deve incluir um conjunto de cenários de regras de correlação padrão e deve ser capaz de projectar outras regras de correlações.
- **Recursos de dashboards**: o dashboard deve ser capaz de priorizar rapidamente a resposta e a análise.
- **Relatórios customizáveis e de conformidade**: o fornecedor deve fornecer detalhes sobre a disponibilidade imediata de relatórios de conformidade e a geração de relatórios personalizáveis.
- **Capacidades de alerta**: capacidade de accionar alertas, por exemplo. enviar uma mensagem de notificação ou e-mail com vista a flexibilizar a resposta a incidentes.
- **Documentação técnica e ajuda online**: disponibilidade de documentação técnica, assim como ajuda offline e online.
- **Monitoramento**: a plataforma SIEM deve ser monitorada usando qualquer protocolo padrão para que possa ser adicionada na plataforma de monitoramento da empresa caso exista.

- **Software Seguro**: o fornecedor deve indicar o sistema operativo e a versão da plataforma SIEM, juntamente com as técnicas de “insurance by design” adoptadas.
- **Enriquecimento de contexto com base em logs colectados**: disponibilidade de regras de correlação para reunir e mesclar informações das diferentes fontes de log, para poder fornecer informações como Mac, IP, hostname, username, sempre que estiver disponível em algum lugar nos logs.
- **Suporte para colecta de logs em tempo real e diferidos**: o fornecedor deve fornecer detalhes sobre o suporte, normalização e indexação de logs recuperados em tempo real e de forma diferida (por exemplo, enviados por trabalhos em lote).

Bom para ter:

- **Capacidade multi-tenant (visualizações)**: o fornecedor deve fornecer detalhes sobre a capacidade da solução SIEM de exibir algumas visualizações com base no agrupamento de conectores (por exemplo, conectores associados a diferentes entidades geográficas ou com base em responsabilidades de gestão como sistemas, bases de dados, rede ou dispositivos de segurança).
- **Anonimização de logs, por exemplo para conformidade com GDPR**: deve fornecer detalhes sobre a anonimização de logs (por exemplo, pelo menos mascarando informações relacionadas à privacidade para alguns perfis de utilizadores).
- **Suporte a matriz de correlação MITRE ATT&CK**: Deve fornecer detalhes sobre o suporte da detecção de uso TTP da matriz MITRE ATT & CK.

- **Operações**

  Mandatório:

  - **Controle de acesso baseado em função**: a plataforma deve implementar um mecanismo de controle de acesso baseado em funções adequado à configuração de vários perfis de utilizadores com diferentes privilégios para implementar os princípios de responsabilidade e separação de funções.

- **Capacidade de Accounting**: a plataforma SIEM deve ter um recurso de log de auditoria para rastrear a actividade relevante do ponto de vista da segurança realizada pelos operadores.
- **Interface web para operação diária**: a interface da plataforma SIEM usada pelos utilizadores para análise diária deve ser baseada na web.

Bom para ter:

- **Fusos horários personalizáveis para a GUI**: uma interface deve permitir que o utilizador escolha em qual fuso horário todos os dados devem ser exibidos.

- **Integração**

  Mandatório:

  - **Integração do Active Directory para gestão administrativa**: o acesso à plataforma deve ser concedido apenas a utilizadores qualificados autenticados e autorizados através da base de dados do Active Directory da Empresa.

  Bom para ter:

  - **Integração com ferramentas de gestão de activos**: a capacidade de integrar a solução com ferramentas padrão de gestão de activos (por exemplo, base de dados de gestão de configuração).
  - **Gestão de casos e rastreamento de actividades de trouble-ticket**: a capacidade de gerir problemas de tratamento de incidentes e o suporte condicional de sistemas de registo de problemas de TI padrão (fluxos de trabalho, priorização, troca de e-mail KB).
  - **Modulo para ticketing**: o fornecedor deve fornecer detalhes em caso de disponibilidade de um sistema de registo de incidentes com o SIEM.
  - **Integração com ferramentas de gestão de vulnerabilidades**: um bom recurso é a capacidade de integração com ferramentas de gestão de vulnerabilidades.

- **Características avançadas**

  Bom para ter:

  - **Suporte a ferramentas de análise de Threat Intelligence**: a disponibilidade de ferramentas de análise de ameaças é uma vantagem se já estiver disponível pelo fornecedor e usando formatos padrão para troca, como: STIX, TAXII, IoC, outros formatos padrões.
  - **Suporte às actividades de análise forense**: É um valor adicional se as actividades de análise forense estiverem disponíveis (monitoramento de integridade de arquivos, pcaps, NetFlow, colecta de evidências).
  - **Suporte analítico**: É um valor adicional se houver suporte para detecção de anomalias, uso e perfil comportamental da entidade.
  - **Capacidades de resposta automática**: É um valor adicional se houver suporte para recursos de resposta automática (por exemplo, SOAR: resposta automática de orquestração de segurança).

- **Licenciamento e suporte**

  Mandatório:

  - **Tipo de licença preferencial**: o fornecedor deve especificar como a solução SIEM estaria disponível.
  - **Restrições de licenciamento**: o fornecedor deve indicar quaisquer limitações de licença, por exemplo, o que acontece no caso de exceder os limites mencionados na licença.
  - **Roadmap do projecto**: o fornecedor deve descrever as tarefas envolvidas no projecto de instalação e configuração da plataforma SIEM e os prazos correspondentes.
  - **Activação de licença atrasada**: a activação da licença deve iniciar somente após o término dos testes de aceitação em que todos os requisitos são atendidos.
  - **Suporte de assistência técnica e serviços profissionais**: o fornecedor deve incluir uma descrição do suporte técnico e serviços profissionais fornecidos/disponíveis.
  - **Treinamento**: Uma descrição do pacote de treinamento deve ser fornecida.

Enquanto que os critérios apresentados por (Akbas, sem data) estão subdivididos em nove(9), nomeadamente:

- **Escalabilidade**: deve-se avaliar a capacidade que solução SIEM tem para permitir acomodar o incremento de necessidade em termos de crescimento da infra-estrutura actual e projectada sem criar entropia no funcionamento da solução.
- **Compatibilidade de logs**: deve-se avaliar a capacidade de compatibilidade com os formatos de diferentes logs.
- **Mecanismo de correlação**: deve-se avaliar se a solução tem a capacidade de pesquisar em vários dispositivos e logs para melhor criação de regras que dão melhor visibilidade e inteligência aos dados colectados.
- **Recursos forenses**: deve-se avaliar se solução oferece recursos de análise forense da origem do evento de segurança cibernética para se perceber melhor.
- **Dashboards**: deve-se avaliar se solução fornece a capacidade de criar facilmente dashboards e relatórios.
- **Inteligência de ameaças**: deve-se avaliar se solução tem a capacidade de integração com fontes de inteligência internas/externas.
- **Resposta a incidentes**: deve-se avaliar se solução permite resposta a incidentes decorrentes de actividades suspeitas na infra-estrutura informática.
- **Aprendizado de máquina**: deve-se avaliar se solução emprega a inteligência artificial, visto que esta capacidade pode permitir que uma organização responda de forma mais flexível a tentativas de ataques, sejam elas conhecidas, assim como desconhecidas. Uma boa solução SIEM para melhor resposta a incidentes de segurança cibernética deve adoptar algum mecanismo de inteligência artificial.
- **Performance**: Deve-se avaliar os requisitos mínimos, em termos de recursos computacionais para que a mesma tenha uma performance eficiente.

Pelos critérios apresentados acima, percebe-se o grau de minuciosidade que se deve ter em processo de adopção de uma ferramenta SIEM, devendo as soluções responder a algumas questões. A proposta de critérios apresentada pelo autor (Mokalled et al., 2020) é mais abrangente, pois cobre detalhes críticos por analisar

em uma solução SIEM, enquanto que a proposta de critérios apresentada por (Akbas, sem data) é mais superficial e limitada apenas na plataforma tecnológica.

### 2.7.4. Ferramentas SIEM

Na presente secção, serão apresentadas algumas soluções SIEM que serão avaliadas posteriormente para o caso de estudo. Como procedimento de selecção, serão usadas as recomendações e pesquisa feitas pelo Gartner de 2020 em termos de soluções SIEM, e posteriormente será usado como referência um relatório da soluction review vendor map.

**Gartner**

Segundo («Gartner», 2022) Gartner, Inc "*é uma empresa de pesquisa e consultoria tecnológica com sede em Stamford, Connecticut, que realiza pesquisas sobre tecnologia e compartilha essa pesquisa, tanto por meio de consultoria privada, quanto por programas executivos e conferências. Seus clientes incluem grandes corporações, agências governamentais, empresas de tecnologia e empresas de investimento.*

*Em 2018, a empresa informou que a sua base de clientes consistia em mais de 12.000 organizações em mais de 100 países. Em 2022, o Gartner tem mais de 15.000 funcionários localizados em mais de 100 escritórios em todo o mundo".*


*Figura 3 Quadrante mágico de gartner 2020*

***Fonte**: Gartner (2020)*

**Solution Review**

O Solutions Review é uma colecção de sites de notícias de tecnologia que agrega, selecciona e cria o melhor conteúdo nas principais categorias de tecnologia. A missão da Solutions Review é conectar compradores de tecnologia corporativa com os melhores vendedores de soluções.

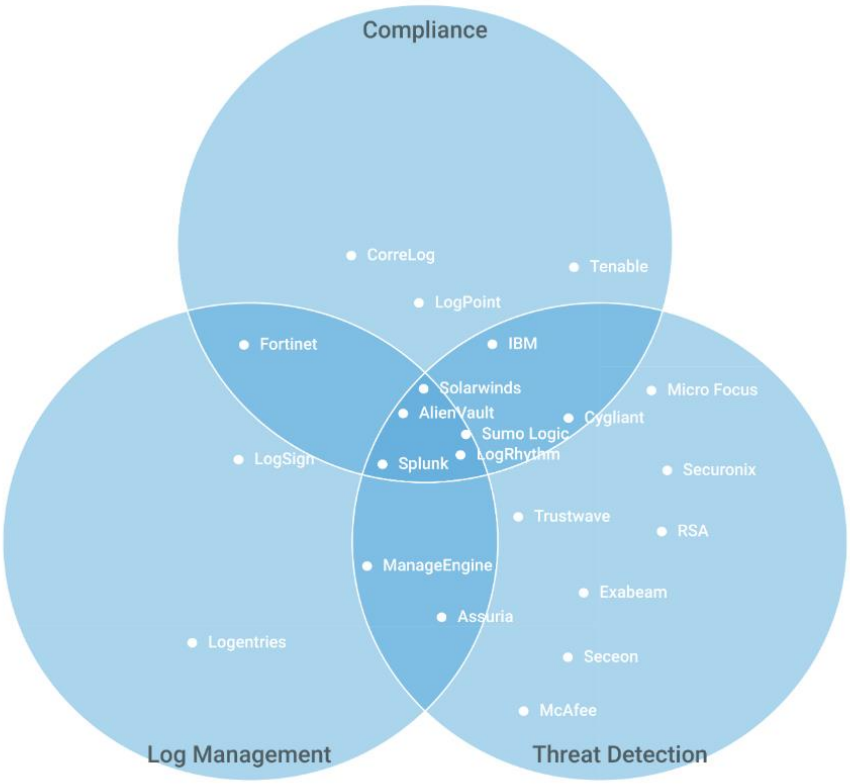



*Figura 4 Mapa de comparação dos fabricantes de soluções SIEM 2019*

***Fonte**: Solution Review 2019*

Pela avaliação do Gartner de 2020 conjugando com o mapa de comparação de soluções SIEM proporcionado pela Solution Review de 2019 no concernente a fornecedores de soluções SIEM, foram seleccionadas 4 soluções para a sua avaliação, nomeadamente:

- Splunk
- LogRythm
- AT&T/AlienVault
- Exabeam

#### 2.7.4.1. Splunk

De acordo com («Splunk», 2022) Splunk Inc. *"é uma empresa de software americana com sede em San Francisco, Califórnia, que produz software para pesquisa, monitoramento e análise de dados gerados por máquina por meio de uma interface estilo Web".* Fundada em 2003, a Splunk é uma empresa global — com mais de 7.500 funcionários, está presente em 21 regiões ao redor do mundo.

Splunk Enterprise Security (ES) é uma solução moderna da Splunk para gestão de eventos e informações de segurança (SIEM) fornece conhecimentos orientados por dados para visibilidade total da postura de segurança, para que uma organização possa proteger seus negócios e mitigar o risco em escala. Através da pesquisa e relatórios, análises avançadas, inteligência integrada e conteúdo de segurança pré-inserido, o Splunk ES acelera a detecção e investigação de ameaças, permitindo que a organização determine a abrangência de ameaças de alta prioridade ao seu ambiente para que possa agir rapidamente.

**Principais funcionalidades**

- Plataforma de dados aberta e extensível

  Faz a ingestão e monitora dezenas de terabytes de dados por dia de qualquer fonte para melhor visibilidade na infra-estrutura.
- Alerta baseado em risco

  Atribui riscos a utilizadores e sistemas, mapeia alertas para estruturas de segurança cibernética e acciona alertas quando o risco exceder os limites.
- Detecção avançada de ameaças

  Detecta ameaças avançadas com aprendizado de máquina e contém mais de 700 detecções prontas para uso em estruturas como MITRE ATT&CK, NIST, CIS 20 e Kill Chain.
- Inteligência de ameaças incorporada

  Prioriza alertas e acelera as investigações com inteligência de ameaças integrada ao Splunk Intelligence Management.
- Conteúdo de segurança de resposta rápida

  Obtém actualizações automáticas de conteúdo de segurança entregues directamente da equipe de pesquisa de ameaças do Splunk para ajudar a ficar actualizado em termos de ameaças novas e emergentes.
- Opções de implementação

  O Splunk Enterprise Security pode ser implementado de 3 formas dependendo da necessidade da organização, estas formas são: nuvem, local ou híbrido.

## Arquitectura do Splunk Enterprise Security (ES)

Segundo (*Components of a Splunk Enterprise deployment - Splunk Documentation*, sem data), a implementação mais simples é aquela que se obtém por padrão quando instala o Splunk Enterprise pela primeira vez em uma máquina, tendo uma instância autónoma que lida com indexação e pesquisa. Abaixo são listadas as componentes do Splunk ES e a **figura 5** apresenta em forma de diagrama as componentes do Splunk ES.

### Indexador

Os Indexadores do Splunk fornecem processamento e armazenamento de dados para dados locais e remotos e hospedam o armazenamento de dados Splunk primário.

### Cabeça de pesquisa

Uma cabeça de pesquisa é uma instância do Splunk Enterprise que distribui pesquisas para os indexadores. As cabeças de pesquisa podem ser dedicadas ou não, dependendo se também realizam indexação. As cabeças de pesquisas dedicadas não possuem índices próprios, além dos índices internos usuais. Em vez disso, eles consolidam e exibem resultados originados de pares de pesquisa remotos.

### Encaminhador

Os encaminhadores são instâncias do Splunk que encaminham dados para indexadores remotos para processamento e armazenamento de dados. Na maioria dos casos, eles próprios não indexam os dados.

### Servidor de implementação

Uma instância do Splunk Enterprise também pode servir como servidor de implementação. O servidor de implementação é uma ferramenta para distribuir configurações, aplicativos e actualizações de conteúdo para grupos de instâncias do Splunk Enterprise Secutiry. Pode ser usado para distribuir actualizações para a maioria dos tipos de componentes do Splunk: encaminhadores, indexadores e cabeças de pesquisas.

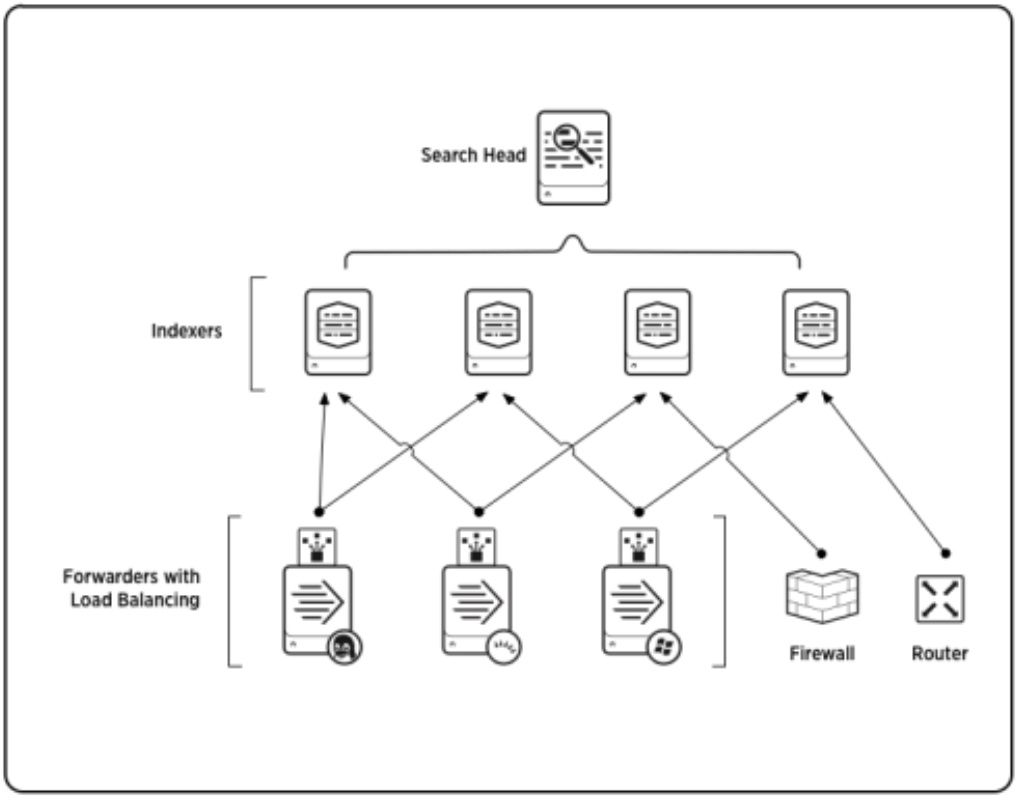



*Figura 5 Arquitectura do Splunk Enterprise Security*

***Fonte**: (*Components of a Splunk Enterprise deployment - Splunk Documentation, *sem data)*

**Recursos computacionais necessários para implementação do Splunk Enterprise Security (ES)**

| Função da máquina | Mínimo de CPU físico | Mínimo de CPU virtual | Mínimo de RAM |
|---|---|---|---|
| Search head | 16 Cores | 32 Cores | 32GB |
| Indexer | 16 Cores | 32 Cores | 32GB |

*Tabela 1 Requisitos de recursos computacionais para Splunk ES*

### 2.7.4.2. LogRythm

De acordo com («LogRhythm», 2022) LogRhythm, Inc. é uma empresa americana de inteligência de segurança especializada na gestão de informações e eventos de segurança (SIEM), gestão de logs, monitoramento e análise forense de redes e terminais e análise de segurança. A LogRhythm foi fundada em 2003 por Chris Petersen e Phillip Villella.

A plataforma LogRhythm SIEM é uma plataforma que fornece funcionalidades e análises de segurança. Com o LogRhythm SIEM uma organização possui módulos, painéis e regras incorporados que ajudam no monitoramento de ameaças, busca de ameaças, investigação de ameaças e resposta a incidentes de segurança cibernética.

**Principais funcionalidades**

- Suporte robusto para fontes de log e colecta de dados

  O LogRhythm SIEM oferece suporte pronto para uso para mais de 1.000 fontes de log, com a capacidade de ingerir fontes de log personalizadas, garantindo que todos os dados de log da rede possam ser colectados e analisados quanto a comportamentos de ameaças.
- Módulos de análise

  Os módulos de análise pré-construídos contêm modelos e alarmes que reconhecem padrões e características conhecidas de mau comportamento, seja de invasores mal-intencionados ou ameaças internas.
- Priorização de alarme

  A priorização de ameaças pontua e prioriza os alarmes com base no risco.
- Gestão de caso

  A gestão de casos melhora a conformidade com regulamentos ao centralizar a gestão colaborativa de incidentes e a colecta de evidências.
- Manuais pré-construídos

  A plataforma LogRhythm SIEM apresenta acções de automação de playbook pré-criados que fornecem contexto de ameaças críticas, agrupamento de casos e triagem rápida para que a organização esteja focada na resposta a incidentes.
- Conformidade simplificada

  Possui módulos de detecção de ameaças e conformidade pré-configurados na biblioteca abrangente da LogRhythm. Ao detectar automaticamente as violações à medida que elas ocorrem, as revisões manuais são removidas. O conteúdo de conformidade, incluindo regras, investigações e relatórios, são mapeados para os controles individuais de cada regulamentação.
- Opções de implementação

O LogRhythm pode ser implementado de duas (2) formas, dependendo da necessidade da organização. Estas formas são: na nuvem e local em um servidor ou uma máquina física.

### Arquitectura do LogRhythm SIEM

O LogRhythm SIEM é uma solução integrada que processa esses dados brutos de log para disponibilizar as informações em um contexto significativo e uniforme. Abaixo são listadas as componentes desta solução e a **figura 6** apresenta em forma de diagrama a interconexão destas componentes:

- O Gestor de plataforma e a sua base de dados associada contêm o registo dos eventos gerados pelo LogRhythm, incluindo os dados de configuração do LogRhythm.
- O Processador de dados encaminha os dados de log do Agente para o Indexador de Dados.
- O Indexador de dados é um servidor Windows ou Linux e deve ser protegido com controles de acesso rígidos colocados em dispositivos que podem se conectar ao repositório de log se implementado em uma DMZ ou em um ambiente não confiável.
- O Monitor do sistema colecta dados de log e os encaminha para um Processador de Dados.

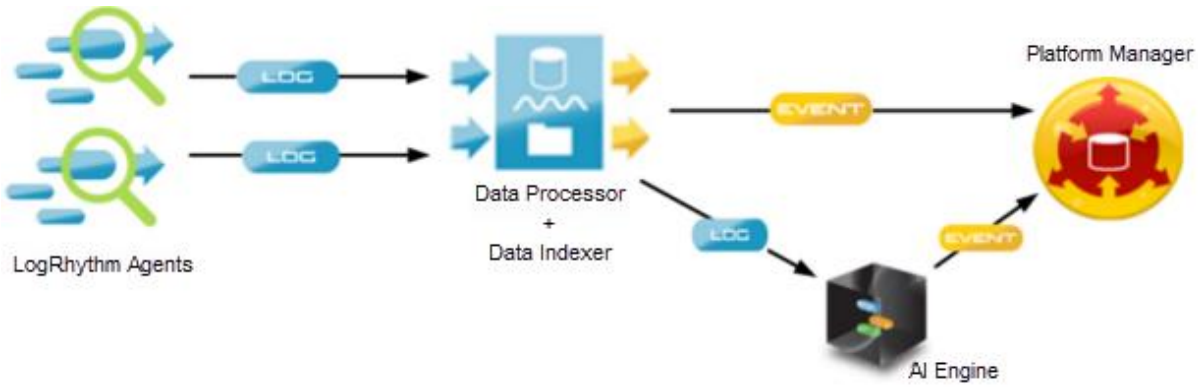



*Figura 6 Arquitectura do LogRythm SIEM*

***Fonte**: (*Review the Requirements for a New LogRhythm Deployment*, sem data)*

**Recursos computacionais necessários para implementação do LogRythm SIEM**

| Função da máquina | Mínimo de CPU físico | Mínimo de CPU virtual | Mínimo de RAM |
|---|---|---|---|
| Servidor | 16 Cores | 16 Cores | 32GB |

*Tabela 2 Requisitos de recursos computacionais para LogRythm SIEM*

#### 2.7.4.3. AT&T/AlienVault

De acordo com («AT&T Cybersecurity», 2022), AT&T Cybersecurity é uma organização desenvolvedora de serviços comerciais e de código aberto para gestão de ataques cibernéticos, anteriormente fundada como AlienVault, em 2007. Em 10 de julho de 2018, a AlienVault foi adquirida pela AT&T Communications, tornando-se uma subsidiária integral quando a aquisição foi concluída em 22 de agosto de 2018. Em fevereiro de 2019, a AlienVault foi renomeada para AT&T Cybersecurity.

A AT&T possuí uma solução que funciona como SIEM e a sua designação é USM Appliance, na versão comercial, e OSSIM na versão grátis e open-source. O USM é uma solução focada em mitigar riscos, identificar vulnerabilidades, detectar ameaças e priorizar a resposta às ameaças e vulnerabilidades de maior prioridade na infra-estrutura informática da organização.

**Principais funcionalidades**

- Descoberta de Activos

  Combina as principais tecnologias de descoberta e inventário para fornecer visibilidade dos dispositivos que estão na rede. O USM Appliance combina as principais tecnologias de descoberta e inventário para fornecer visibilidade dos dispositivos a monitorar.
- Avaliação de vulnerabilidade

  Identifica activos e dispositivos com software não corrigido, configurações inseguras e outras vulnerabilidades na rede de uma organização, abaixo são listadas algumas destas funcionalidades.

- Monitoramento Contínuo de Vulnerabilidades;
- Varredura activa autenticada/não autenticada;
- Verificação de remediação;

A verificação de vulnerabilidade interna integrada mantém a organização a par das vulnerabilidades em sua rede, para que possa priorizar a implementação e a correcção de patches.

- Detecção de intrusão

  Coordena a resposta a incidentes e a gestão de ameaças na rede de uma organização adoptando tecnologias de monitoramento de segurança integradas, inteligência de ameaças emergente do AT&T Alien Lab e fluxo de trabalho de circuito fechado contínuo para correcção rápida. Abaixo são listados alguns dos métodos usados para a detecção de intrusões.

  - IDS baseado em rede (NIDS)
  - IDS baseado em host (HIDS)
  - Monitoramento de integridade de arquivos (FIM)

O monitoramento de integridade de arquivos integrado em agentes baseados em host instalados em servidores alerta sobre modificações não autorizadas de arquivos de sistema, arquivos de configuração ou conteúdo.

O monitoramento do acesso à rede usando sistemas de detecção baseados em host e rede identifica quem tentou aceder aos sistemas, arquivos e conteúdo.

- Monitoramento Comportamental

  Identifica anomalias e outros padrões que sinalizam ameaças novas e desconhecidas na rede da organização, bem como comportamento suspeito e violações de políticas por utilizadores e dispositivos autorizados.

  - Análise NetFlow;
  - Monitoramento de Disponibilidade do Serviço;
  - Análise de protocolo de rede/captura de pacotes;

  O monitoramento comportamental integrado, colecta dados que ajudam a entender a actividade “normal” do sistema e da rede, o que simplifica a resposta a incidentes ao investigar um problema operacional suspeito ou um possível incidente de segurança. A captura completa de pacotes

permite a análise completa do protocolo do tráfego de rede, fornecendo uma reprodução abrangente do evento que ocorreu durante uma possível violação.

- Security Information and Event Management

  Identifica, contem e corrige ameaças na rede priorizando seu risco e resposta.

  - Gestão de registos;
  - Dados de ameaças OTX integrados;
  - Correlação de eventos SIEM;
  - Resposta a incidentes;

  A organização pode correlacionar automaticamente dados de log com inteligência de segurança accionável para identificar violações de política e receber procedimentos de resposta contextualmente relevantes e orientados por fluxo de trabalho.

  A organização também pode realizar análises forenses de eventos usando logs brutos assinados digitalmente. Os logs brutos também podem ser usados para atender aos requisitos de conformidade para preservação de evidências.

**Arquitectura do USM Appliance**

O USM Appliance combina várias tecnologias críticas de segurança em uma plataforma integrada. Esta appliance pode ser implantada como um único servidor ou distribuído em vários servidores (virtual ou hardware) para fornecer escalabilidade e disponibilidade adicionais, a **figura 7** ilustra do diagrama da arquitectura de uma solução USM.

As três componentes da arquitectura do USM Appliance que funcionam em conjunto para monitorar e fornecer segurança são:

- **Sensores da appliance USM**

  Distribuídos em toda a rede para colectar e normalizar informações de qualquer dispositivo na rede. Estes sensores podem processar logs e dados brutos de vários tipos de dispositivos, como firewalls, roteadores e servidores host.

- **USM appliance Server**

  Agrega e correlaciona informações que os sensores USM da appliance colectam. Fornece gestão, relatórios e administração de painel único por meio de uma interface de utilizador baseada na web.

- **USM appliance Logger**

  Arquiva com segurança dados brutos de log de eventos para pesquisas forenses e mandatos de conformidade.

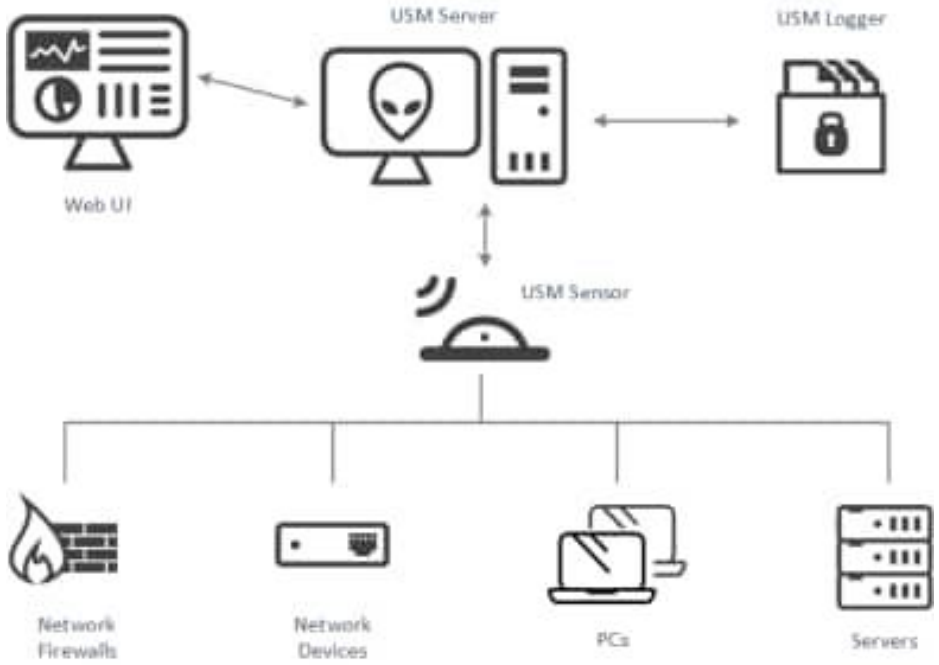



*Figura 7 Arquitectura do USM*

***Fonte**: (*About USM Appliance System Architecture and Components, *sem data)*

## Diferenças entre USM Appliance e OSSIM

| | Funcionalidades | OSSIM | USM |
|---|---|---|---|
| **Capacidades de segurança** | Descoberta e inventário de activos | Sim | Sim |
| | Avaliação de vulnerabilidades | Sim | Sim |
| | Detecão de intrusão | Sim | Sim |
| | Monitoramento comportamental | Sim | Sim |
| | Correlação de eventos SIEM | Sim | Sim |
| | Gestão de logs | Não | Sim |
| | Monitormento da nuvem AWS & AZURE | Não | Sim |
| | Monitormento de segurança de aplicativos na nuvem | Não | Sim |
| **Características adicionais** | Orquestração e automação de segurança | Não | Sim |
| | Integração com software de tickets (JIRA, SERVICENOW) | Não | Sim |
| | Suporte da comunidade via foruns do produto | Sim | Sim |
| | Alimentação pela OTX | Sim | Sim |
| | Inteligência contínua de ameaças | Não | Sim |
| | Suporte dedicado por telefone e email | Não | Sim |
| | Documentação de produto online e base de conhecimento | Não | Sim |
| | Painéis de análise rica e visualização de dados | Não | Sim |
| **Arquitectura de implementação** | | Apenas appliance virtual | Cloud, appliance fisica ou virtual |
| **Monitoramento de segurança** | | On-premises fisico e virtual | Ambientes na nuvem AWS e Azure<br>Aplicações Cloud<br>On-premises fisico e virtual |
| **Preços** | | Open-Source/Gratis | Pago dependendo do plano a assinar ou caracterisiticas da appliance |

*Figura 8 Diferenças entre AlienVault USM e OSSIM*

***Fonte**: Adaptado de (*Compare OSSIM to USM | AlienVault | AT&T Cybersecurity, *sem data)*

## Recursos computacionais necessários para implementação do USM Appliance

| | USM appliance ALL-IN-ONE | | | | |
|---|---|---|---|---|---|
| | Total cores | Memória RAM | Armazenamento | Interfaces de rede | Software de virtualização |
| Servidor | 8 | 16GB | 500GB/1TB | 6 x 1GbE | Vmware ESXI 4.0+ ou Hyper-V v3.0+ |
| Sensor remoto | 4 | 8 | 250GB ou 1TB | 2 x 1GbE | Vmware ESXI 4.0+ ou Hyper-V v3.0+ |

*Tabela 3 Requisitos de recursos computacionais para USM appliance all-in-one*

| | USM appliance Standard | | | | |
|---|---|---|---|---|---|
| | Total cores | Memória RAM | Armazenamento | Interfaces de rede | Software de virtualização |
| Servidor | 8 | 24GB | 600GB ou 1,2TB | 6 x 1GbE | Vmware ESXI 4.0+ ou Hyper-V v3.0+ |
| Logger | | | 900GB ou 1,8TB | 2 x 1GbE | |
| Sensor | | | 600GB ou 1,2TB | 6 x 1GbE | |

*Tabela 4 Requisitos de recursos computacionais para USM appliance padrão*

#### 2.7.4.4. Exabeam

De acordo com (Pizhin et al., 2021), a Exabeam é uma empresa que fornece uma plataforma de inteligência de segurança para as organizações. Foi fundada por Nir Polak, Domingo Mihovilovic e Sylvain Gil em 2013 e a mesma está sediada em San Mateo, Califórnia, Estados Unidos.

O principal produto da Exabeam é uma forma de plataforma Security Information and Event Management (SIEM) designada por **Exabeam Fusion**.

**Exabeam Fusion** é uma solução fornecida na nuvem que combina o SIEM com a detecção, investigação e resposta de ameaças (TDIR), detecção e resposta estendida (XDR).

Com análises comportamentais incorporadas ao Fusion SIEM, as organizações podem detectar ameaças perdidas por outras ferramentas. Fluxos de trabalho prescritivos e conteúdo pré-configurado permitem resultados bem-sucedidos e automação de respostas. O **Exabeam Fusion** também oferece armazenamento de log baseado em nuvem, pesquisa rápida e guiada e relatórios de conformidade abrangentes esperados de qualquer SIEM moderno.

**Principais funcionalidades**

- Armazenamento de dados centralizado e altamente escalável

  Permite uma boa visibilidade no parque tecnológico da organização, garantindo que, nenhum evento ou actividade esteja invisível.
- Relatórios de Auditoria e Conformidade

  Possui centenas de relatórios e painéis de conformidade predefinidos para uso, reduzindo a necessidade de o uso de métodos complexos de acesso a informações para auditores.

- Integração flexível

  Possui conectores pré-criados que integram totalmente mais de 500 ferramentas populares de segurança e TI para detecção, investigação e resposta a ameaças.
- Detecção baseada em comportamento

  Possui mecanismos para a análise de comportamento (UEBA) detectando ameaças avançadas como ataques baseados em credenciais, ameaças internas e ransomware que podem ser perdidas por outras ferramentas.
- Casos de uso prescritivos e centrados em ameaças

  Permite a criação de fluxos de trabalho prescritivos de ponta a ponta e conteúdo de segurança.
- Diagnóstico Automatizado de Incidentes

  Contém uma análise de comportamento com vista a avaliar a actividade anormal do utilizador para classificar automaticamente os incidentes por casos de uso centrados em ameaças.
- Investigação Automatizada

  Permite a demonstração das linhas de tempo inteligentes criadas automaticamente com vista a reunir evidências e as montam em linhas de tempo de incidentes coesas que aumentam a produtividade e garantem que nada passe despercebido.
- Resposta e Remediação

  Cria listas de verificação guiadas e acções de resposta automatizadas e manuais, reduzindo o tempo de resposta e permitindo fluxos de trabalho consistentes e repetíveis.

# 3. CAPÍTULO III – CASO DE ESTUDO

No presente capítulo, será apresentado o CASO DE ESTUDO para a melhor compreensão do tipo de organização em que se está a desencadear o trabalho. O estágio foi realizado na empresa ALTEL que é uma empresa membro do grupo Meridian32 que é o caso de estudo. A ALTEL é que administra todo o parque tecnológico do grupo Meridian32 que, por sua vez, é partilhado pelas diversas empresas do grupo no mesmo edifício. Será inicialmente apresentada a organização de estágio e, posteriormente, a organização que é o nosso caso de estudo.

## ALTEL

A empresa ALTEL, anteriormente designada ALCATEL Moçambique, fornecia equipamentos da Alcatel aqui em Moçambique.

A *ALTEL* foi fundada em 2003, a partir da alteração da denominação social da *Alcatel Moçambique*, numa fase de uma necessidade premente e de rápido crescimento dos meios de comunicação de voz e de dados em ambientes corporativos, tanto ao nível do sector público moçambicano, como das empresas privadas.

Em Junho de 2014, o Grupo Moçambicano *Meridian32* adquiriu 98% do capital social da *ALTEL*, imprimindo uma orientação muito focada na actualização tecnológica que o mercado das *TIC's* exigia, tornando possível uma maior abrangência de oferta de tecnologia, com o objectivo estratégico de colocar a empresa numa posição de destaque, ambicionando estabelecer-se como um dos *players* de referência e de liderança no sector dos integradores de *TIC's* em Moçambique e, num futuro breve, dos Países da SADC.

A *ALTEL* possui uma vasta experiência de mercado, orgulhando-se de contar com a confiança de mais de 800 clientes satisfeitos, provenientes de variados sectores de actividade, nomeadamente Administração Pública, Governo, Banca, Energia, Indústria, Saúde, Telecomunicações, entre outros.

A *ALTEL* é vista hoje como uma integradora de soluções e serviços de Tecnologias de Informação e Transmissão Rádio, acrescentando valor para os seus clientes no planeamento, implementação e assistência técnica das suas

infra-estruturas tecnológicas de informação e segurança electrónica, com distinção na qualidade do serviço prestado e pioneira no fornecimento de tecnologia de ponta, de acordo com as soluções mais recentes e disponíveis internacionalmente.

### 3.1. Serviços oferecidos pela ALTEL

Hoje em dia, com a evolução dos serviços *Cloud* e com o crescimento exponencial dos dados, as empresas enfrentam o desafio de terem de assegurar a continuidade da operação e a capacidade para processar a variação das exigências de tráfego que os utilizadores necessitam diária e simultaneamente, as infra-estruturas de TIC estão progressivamente mais complexas.

A oferta da *ALTEL* para soluções e serviços está centrada em seis principais linhas de negócio – Infra-estrutura de rede, Segurança lógica, Segurança electrónica (CCTV, Controlo de acessos), Comunicações unificadas, Computação para o utilizador final e Data *Centers*.

A *ALTEL*, enquanto integrador de soluções de comunicação, disponibiliza aos seus clientes um portfólio de serviços alargado, capaz de agregar valor às soluções de comunicação desenhadas em função d*e requisitos previamente identificados.*

A *ALTEL* providencia aos seus clientes serviços de integração de soluções e aplicações em diversas áreas e tecnologias, nomeadamente no que se refere a:

- Comunicações Unificadas – Soluções de comunicações unificadas, tais como "*IP Tel / VoiP*" "*unified messaging*", "*presence* & instant *messaging*", "*web*" e videoconferência/telepresença;
- *Data Centers* - Soluções Chave-na-mão de *Data Centers*;
- Infra-estrutura de Redes Seguras - Soluções de *networking* LAN/WAN/MAN seguras, nomeadamente ao nível de protecção de "*gateways*" e "*Networking*", conteúdos, Control de acessos e CCTV, entre outras.
- Radio Comunicações – Sistemas de Radiocomunicações HF, VHF e UHF..

### 3.2. Política de qualidade

Como forma de evidenciar o comprometimento da gestão de topo perante os seus colaboradores, clientes e outras partes interessadas, a *ALTEL* reconhece a importância da Qualidade na gestão das suas actividades e, desta forma, institui a presente Política no sentido de implementar e manter um Sistema de Gestão, em conformidade com os requisitos da norma IS*O 9001:2015*, com vista à melhoria contínua de todos os processos da empresa, satisfação dos Clientes e análise dos riscos inerentes. A Direcção Geral compromete-se desta forma a zelar pelo cumprimento escrupuloso da Política de Qualidade estabelecida e péla designação de um responsável (Gestor da Qualidade) que fará a sua actualização periódica, de acordo com as necessidades futuras da empresa. A presente Política encontra-se disponível a todos os Colaboradores e é divulgada pelos meios de comunicação interna da empresa para sua consciencialização, juntamente com a restante estrutura documental do sistema

### 3.3. Visão

Ser líder de referência no mercado nacional na área das TICs, pela qualidade e inovação dos serviços e soluções que proporciona aos seus clientes, contribuindo para o seu crescimento sustentável.

### 3.4. Missão

Proporcionar aos seus clientes soluções ambiciosas e compatíveis com os seus requisitos, sendo reconhecida como um parceiro de confiança, capaz de acompanhar e promover a evolução das suas necessidades.

### 3.5. Princípios

Garantir um ambiente para a operacionalização eficaz e eficiente dos processos que permita aos Colaboradores o desenvolvimento das suas competências, a sua criatividade e a sua motivação para benefício comum;

Cumprir os requisitos legislativos, normativos e regulamentares aplicáveis;

Aperfeiçoar e manter continuamente o SGQ, sensibilizando, formando e envolvendo todos os Colaboradores e todas as partes envolvidas que se considere relevante;

Analisar e melhorar constantemente a eficácia e a eficiência do SGQ, com vista à satisfação dos Clientes e outras partes interessadas;

### 3.6. Valores

- Liderança;
- Ética e profissionalismo;
- Trabalho em equipa;
- Competência;
- Comprometimento.

## GRUPO MERIDIAN 32

O grupo Meridian32 é uma holding de empresas de diversas áreas de actuação no mercado empresarial, actualmente encontra-se localizado na avenida Vladimir lenine, edifício TVSD.

Este grupo visa dar apoio com funções de back-office, assistindo um potencial investidor na entrada no mercado e potenciando o seu desempenho e resultados em forma de parceria. Teve início de actividade em 2000, o Grupo Meridian32 conta com mais de 100 colaboradores em áreas de especialidade bastante diferenciadas: centro de negócios, imobiliário, engenharia, arquitectura, ambiente, gestão social, sistemas de gestão, formação, contabilidade, fiscalidade, auditoria, cobranças, softwares de gestão, tecnologias de informação e telecomunicação, manutenção de edifícios.

Abaixo são desatacadas algumas das empresas do grupo:

- **REC (Real Estate Consulting)**, a única empresa moçambicana regulada pelo RICS (Royal Institution of Chartered Surveyors) e com técnicos membros do RICS (MRICS) residentes em território nacional. A REC é especializada em estudos de mercado, estudos de viabilidade e avaliações de todas as classes de activos (imobiliário, equipamentos, frotas, etc), avaliações de activos biológicos, desenvolvendo também projectos de engenharia, arquitectura e gestão de projecto em regime de colaboração com outras marcas associadas.

- **Zambujo & Associados**, é a empresa dedicada á inventariação de imobilizado, equipamentos, frotas e maquinaria, sua respectiva reconciliação com os registos contabilísticos, etiquetagem e valoração.
- **Predial** dedica-se à mediação imobiliária. Constituída por uma equipa dinâmica com conhecimento consolidado do mercado imobiliário, o nosso objectivo é apoiar os clientes no processo de aquisição, venda ou arrendamento de um imóvel. O nosso conhecimento permite-nos, não só oferecer as melhores soluções, mas também encontrar oportunidades para quem pretende investir no mercado imobiliário.
- **JA** desenvolve serviços de Gestão de instalações, venda, montagem e manutenção de geradores, ar condicionado e equipamentos diversos e a reabilitação e remodelação de espaços interiores e exteriores.
- **Fantoffice** é especialista na execução de soluções chave-na-mão para escritórios, comercializando ainda equipamento para hotéis, clínicas e espaços comerciais, com destaque para o mobiliário, sistemas de divisórias, estores e alcatifas.
- **Serenus**, é uma empresa a operar no sector da segurança privada, com 25 anos de experiência, especializada na protecção patrimonial, segurança personalizada, descaracterizada e guarda costas, inspecção, supervisão, segurança electrónica, monitorização e recepção de alarmes e reacção armada.
- No silo da Tecnologia, a **ALTEL** é a empresa tecnológica do grupo, especialista em Integração de Tecnologias de Informação, Segurança Electrónica e Radio Transmissão. Para a efectivação destes serviços, a ALTEL conta com uma rede alargada de parceiros tecnológicos de renome mundial, tais como a Cisco Systems, Alcatel Lucent, Huawei, Axis, Milestone, Genetec, Microsoft, VMWare, APC, Barret e Kenwood na área de rádio transmissão, entre outros.
- **Incentea** dedica-se à prestação de serviços profissionais nas áreas das Tecnologias de Informação e Comunicação, Inovação, Consultoria de Negócio, Engenharia de Produto.com soluções de ERP, sendo o maior representante dos produtos Primavera em Moçambique.

- **WidePartner** implementa Sistemas de Informação ERP nas mais diversas áreas de actividade como a Produção, Distribuição, Retalho e Serviços, entre outras, com recurso a produtos SAGE.
- **AccSys** oferece serviços de auditoria, contabilidade, fiscalidade, outsourcing, consultoria de gestão e implementação de sistemas de Gestão com a certificação ISO, apresentando-se no mercado como uma boutique provedora de soluções financeiras.
- **Amb&Veritas** é uma empresa com habilitações em consultoria ambiental (estudos de impacto e de viabilidade ambiental), aspectos sociais (reassentamento e negociação com populações), e formação apoiada na marca NOSA (marca líder nas áreas de Higiene e Segurança no Trabalho).

Grupo Meridian32 possui uma infra-estrutura informática partilhada entre as diversas empresas pertencentes ao grupo com excepção das empresas Serenus e JA que possui infra-estrutura autónoma e independente. Das 11 empresas acima apresentadas apenas 8 delas pertencem ao mesmo escritório de trabalho nomeadamente Accsys, ALTEL, Ambveritias, Fantoffice, Incentea, Predial, REC, Zambujo&Associados e fazem uso da mesma infra-estrutura informática administrada pela ALTEL.

### 3.7. Cenário actual

A administração de todo o parque tecnológico do grupo Meridian32 está sob a responsabilidade de uma das empresas do grupo focada nas TICs, neste caso a ALTEL. A **figura 9** ilustra o diagrama topológico da infra-estrutura de TI resumido.

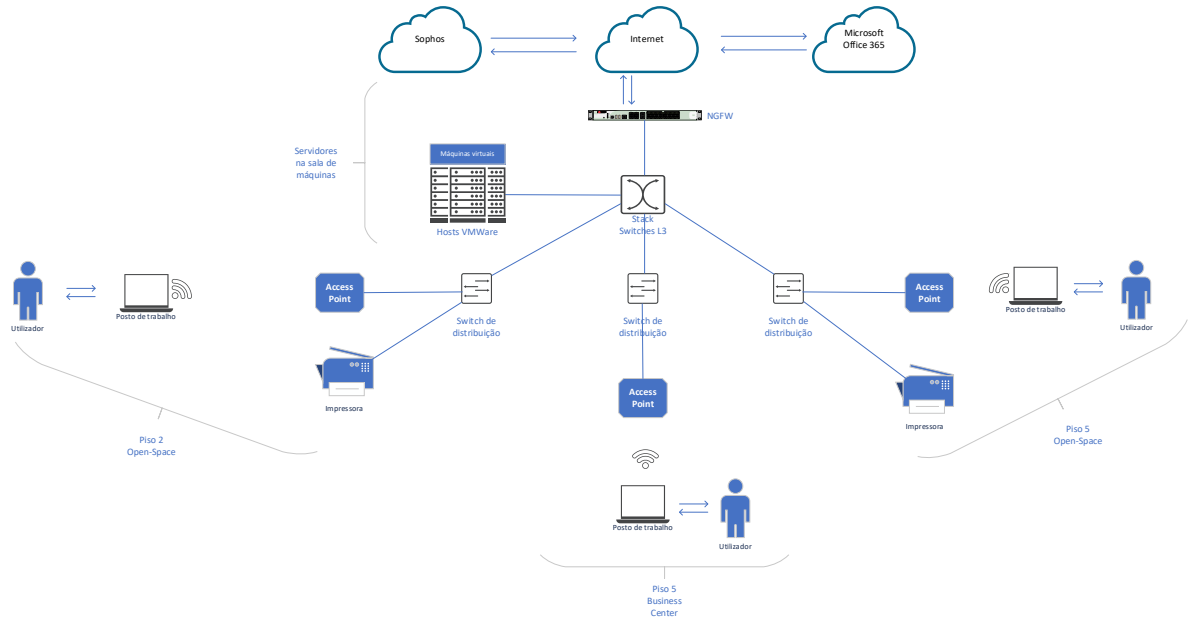



*Figura 9 Diagrama geral da infra-estrutura do grupo Meridian32, elaborado pelo Autor*

## 3.8. Parque tecnológico

A **tabela 5** apresenta o parque tecnológico da organização para melhor percepção da importância de salvaguardar toda a informação que nele trafega.

| Sala de servidores | | |
|---|---|---|
| **Tipo de equipamento** | **Quantidade** | **Serviço** |
| Servidor físico | 6 | VMWARE ESXI |
| Storage | 1 | Repositório de máquinas virtuais |
| NAS | 2 | Repositório de backup |
| NAS | 1 | File Server |
| Switch | 2 | Stack de switch de core |
| Switch | 3 | Switches de distribuição |
| Firewall | 1 | Next Generation Firewall (protecção em perímetro da rede LAN) |
| Servidores virtuais | 1 | Controlador de domínio |
| | 1 | Servidor Print Directory |
| | 1 | Servidor de Impressora |
| | 1 | Servidor de bases de dados |
| | 1 | Servidor ERP |

| | | |
|---|---|---|
| | 1 | Terminal de Serviços |
| | 1 | Servidor de controle de acessos |
| | 1 | Terminal de Serviços |
| | 1 | Servidor de backup |
| | 1 | Servidor de ServiceDesk |
| | 1 | Servidor de gestão documental |
| | 1 | Servidor de acesso remoto a cliente externo (OutSourcing) |
| | 1 | Servidor de testes |

*Tabela 5 Serviços da sala de servidores*

| Postos de trabalho | | |
|---|---|---|
| **Tipo** | **Sistema Operativo** | **Quantidade** |
| Laptop | Windows 10 Professional | 70 |
| Desktop | Windows 10 Professional | 3 |

*Tabela 6 Postos de trabalho*

| Serviços na Cloud | |
|---|---|
| **Tipo de serviço** | **Serviço** |
| Xtreme Detection and Response | Serviço para protecção dos endpoints |
| Office 365 | Aplicativos Office 365 Business Standard e serviço de email |

*Tabela 7 Serviços na Cloud*

- **Infra-estrutura informática**

  Actualmente esta empresa possui uma infra-estrutura mista, tendo alguns serviços críticos em execução na rede local e outros serviços na nuvem, nomeadamente o serviço de email e de protecção dos computadores e servidores.

  Os serviços críticos para o funcionamento da organização encontram-se na sala de servidores, que é uma sala especializada a alojar todos os serviços

críticos providos pelas TICs. Alguns dos serviços acima referenciados são o controlador de domínio, rede de voz, dados a cabo e Wi-Fi, servidor de ficheiros, ERP, Impressora.

- **Acesso às instalações**

  Para que se possa ter acesso ao escritório do grupo, existem mecanismos de segurança de acesso físico nos pontos de entradas aos principais compartimentos da organização, devendo a pessoa que necessita de acesso ter uma autorização que permite ser registada no sistema de controle de acessos de forma temporária, ou mesmo permanente para o caso de colaboradores. Pessoas não autorizadas não tem acesso físico às instalações. Além do sistema de controle de acessos, a organização possui o sistema de CCTV que permite monitorar em tempo real os movimentos nas instalações e fazer uma verificação de eventos passados em caso de necessidade.

- **Postos de trabalho**

  Os utilizadores do grupo Meridian32 que fazem uso e partilha da infra-estrutura informática e seus serviços no mesmo escritório, possuem computadores portáteis se conectando à rede de dados da organização. Os postos de trabalho possuem todas as ferramentas de produtividade necessárias para a execução dos seus trabalhos, incluindo o software de protecção do computador. Para aceder ao computador os mesmos são solicitados credenciais que são validadas no servidor de autenticação que é o controlador de domínio. O grupo permite que os seus colaboradores possam levar os seus computadores da organização para teletrabalho ou uso em suas residências, enquanto colaboradores de uma das empresas do grupo.

- **Postura de segurança actual**

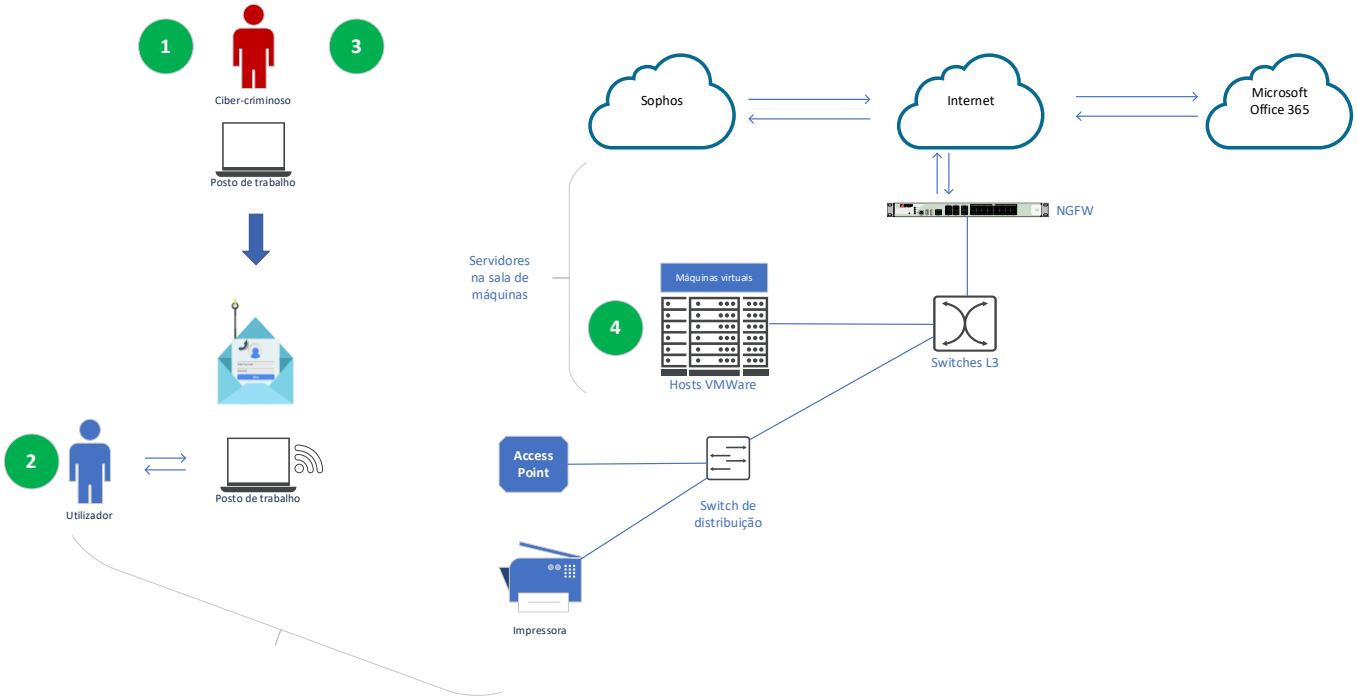
  O grupo Meridian32 possui uma infra-estrutura informática minimamente protegida, tendo uma *NGFW que é uma firewall com funcionalidades avançadas comparada com firewalls convencionais, tendo estas novas firewalls mecanismos de detecção de intrusão, um pouco mais de*

*inteligência envolvida nos mecanismos de análise de ameaças, possui também a detecção de malwares inspeccionando o tráfego para detecção de ameaças e posterior bloqueio em caso de necessidade*. Esta firewall do grupo Meridian32 protege a rede interna de ameaças externas. A organização possui um software de protecção instalado em cada posto de trabalho e servidores que é gerido através de um painel de administração localizado na nuvem do provedor da solução.

Os utilizadores necessitam de se autenticar no active directory que está na sala de servidores da organização para se ter acesso ao computador, aos serviços de internet, impressora, ERP, servidor de ficheiros. Fez-se uma combinação da NGFW com o software de protecção dos computadores para melhorar a segurança contra ameaças actualmente conhecidas.

A organização não possui planos de conscientização dos colaboradores sobre a temática de segurança cibernética com vista a aguçar a capacidade de resposta e detecção de tentativas de ataques cibernéticos.

Com a situação actual de segurança, a organização encontra-se minimamente protegida contra ameaças já conhecidas graças a firewall, software de protecção dos computadores, mecanismos de autenticação, porém mantém-se uma lacuna que é a exposição interna. Ou seja, pela forma como está a topologia da organização é fácil de um ciber-criminoso penetrar sem ser detectado na organização usando uma técnica como phishing, engenharia social, pois não existem ferramentas que detectam comportamentos anómalos na rede, podendo um ciber-criminoso se infiltrar com roubo de credenciais e fazer o uso das mesmas para explorar a infra-estrutura até conseguir roubar informações, conforme ilustra a simulação na **figura 10**.




**Legenda**:

Utilizador da organização

Ciber-criminoso

1 O ciber-criminoso envia um email de phishing à vítima

2 Acidentalmente a vítima cai no golpe sem perceber e suas credenciais ficam expostas para o ciber-criminoso, em simultâneo o ciber-criminoso consegue instalar uma backdoor no computador da vítima

3 Com acessos à máquina o ciber-criminoso começa a explorar e a estudar a infra-estrutura da vítima e colectando o máximo de informação possível

4 Informações sensíveis da organização ficam expostas e o ciber-criminoso continua as suas actividades sem ser detectado

*Figura 10 Cenário de um ataque, elaborado pelo Autor*

## 3.9. Descrição das actividades desenvolvidas

Nesta secção, serão apresentadas todas as actividades realizadas no período de estágio profissional, nomeadamente as actividades diárias na organização assim como projectos envolvidos.

Inicialmente, foi necessário compreender a fundo a estrutura da organização em termos de procedimentos operacionais diários, parque tecnológico e a sua operação para que as actividades pudessem correr da melhor forma. Foi elaborado um cronograma de actividades que ajudou na orientação das actividades, o mesmo pode ser encontrado no **Anexo 1.**

Durante o estágio profissional, o factor dedicação foi crucial para a realização de diversas actividades devido a sua complexidade. Foram realizadas diversas assistências em soluções de TI, no que diz respeito à instalação e configuração de infra-estrutura TI, nomeadamente switches de core e distribuição, firewall, servidores físicos, storages, NAS, sistema de virtualização e redes wifi.

### 3.9.1. Procedimentos operacionais de TI

O estágio profissional decorreu na ALTEL (Departamento de TI), tendo sido necessário perceber, antes, como é que a organização funciona, a nível operacional. Em destaque, teremos:

**Orientações básicas**

- Como aceder às instalações físicas da organização;
- As actividades diárias da organização;
- Como deverão ser usados os computadores dentro da organização;
- Quais as redes corporativas a que um utilizador seja ele normal ou administrador deverá fazer uso;

**Orientações a nível de administração de TI**

- Quais os serviços que organização faz uso a nível de TI;
- Procedimentos de como deverão ser feitas as assistências aos utilizadores locais, remotos, e a clientes externos;

- Composição da sala de servidores;
- Quais os activos e passivos;
- Procedimentos de administração do controlador de domínio;
- Procedimentos de administração dos switches, da firewall;
- Procedimentos de administração dos servidores, storage e NAS;
- Procedimentos de administração da solução de virtualização;

### 3.9.2. Actividades de administração das soluções de TI

**Migração do VMWARE da versão 5.5 para 6.7**

A infra-estrutura de servidores do grupo Meridian32, aquando do estágio profissional era assente na solução de virtualização VMWARE versão 5.5, que actualmente encontra-se obsoleta. Foi desenhada uma migração da versão 5.5 para a versão 6.7. Visto que o grupo dispunha de um repositório centralizado de máquinas virtuais que é um storage que disponibiliza datastores para os servidores armazenarem os ficheiros das máquinas virtuais, foi usada esta vantagem incluindo a disponibilidade de servidores extra para migrar a versão do VMWARE. Foi feita uma instalação do VMWARE 6.7 nos servidores físicos extras e, posteriormente, foram mapeados os datastores na nova versão e anunciadas as máquinas virtuais nos servidores extras.

O objectivo da migração para os servidores extras era de garantir que os anteriores com a versão 5.5 estivessem livres para posteriormente avançar com a instalação da nova versão do VMWARE. A migração foi um secesso.

**Migração dos sistemas operativos dos servidores virtuais**

O parque de servidores virtuais do grupo Meridian32 era assente no uso do sistema operativo Windows server standard 2012 R2, fez-se migração de todos os servidores virtuais na versão Windows server standard 2012 R2 para a versão Windows server standard 2022. A migração da maioria dos servidores foi uma instalação limpa do sistema operativo que prosseguiu com a instalação de raiz dos serviços. O servidor com particularidades a ter mais em atenção foi o domain controller, visto que vários serviços críticos estavam em execução no

mesmo, foi feita uma instalação do sistema operativo Windows server 2022 e o novo servidor juntou-se ao grupo do servidor com Windows server 2012 e foi feita a migração das roles FSMO.

### 3.9.3. Implementação de projectos

Durante o período de estágio profissional foi implementado um projecto de digitalização do arquivo histórico do MIREME, no qual as actividades desencadeadas consistiam no upgrade dos recursos computacionais dos servidores de gestão documental, na actualização do sistema de gestão documental do ministério para suporte a um módulo de arquivo histórico e instalação e configuração dos postos de trabalho e digitalizadores para o processo operacional no projecto.

# 4. CAPÍTULO IV – PROPOSTA DE SOLUÇÃO

Nesta secção, será apresentada a proposta de solução para o caso de estudo que é uma componente importantíssima para este trabalho, pois é com esta proposta que se poderá ter uma visão da solução a ser implementada e o valor que esta vem agregar no que tange à visibilidade de eventos de segurança cibernética para o caso de estudo. Foi apresentado no capítulo 3 a situação actual da organização em termos de uso de tecnologias de informação e comunicação e como a organização actualmente lida com eventos de segurança cibernética.

## 4.1. Cenário pretendido com a proposta de um SIEM

Pelo cenário actual da organização, percebe-se a incapacidade no concernente à detecção de eventos de segurança na rede corporativa; assim sendo, na **figura 11** é demonstrada analiticamente a topologia e o cenário pretendido.

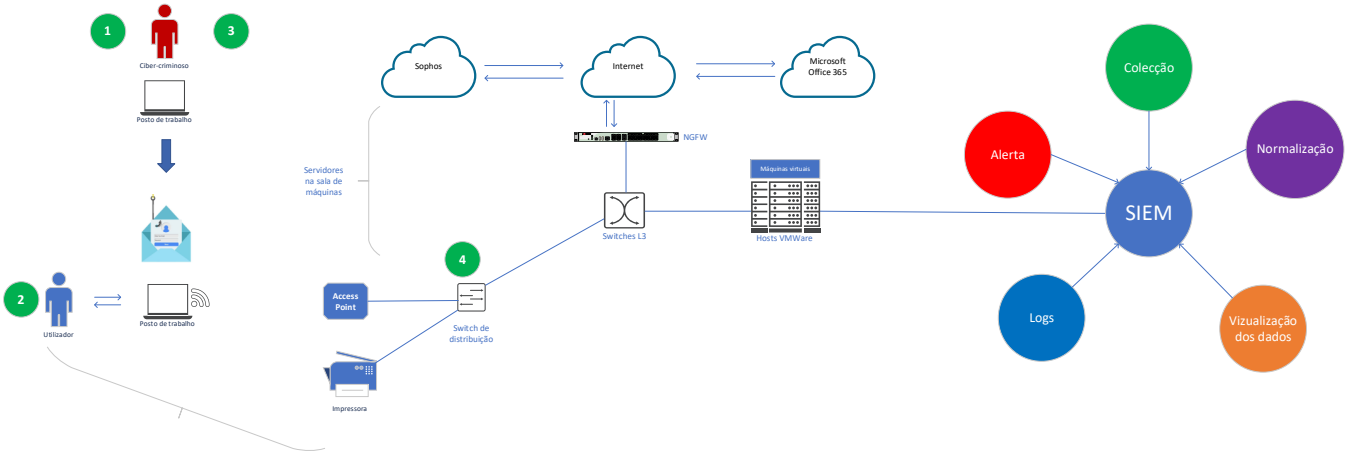



*Figura 11 Cenário com implementação de um SIEM, elaborado pelo Autor*

Com a implementação de um SIEM a organização passa a ter uma solução que monitora todos os eventos da rede corporativa dotando os administradores da infra-estrutura de TI de uma plataforma unificada para detecção de eventos ou incidentes de segurança cibernética. No cenário ilustrado pela figura 14 a organização passa a detectar comportamentos anómalos em termos de acesso aos recursos.

Se o ciber-criminoso por algum motivo consegue criar pontos de entrada na máquina de um utilizador ligado à infra-estrutura monitorada pelo SIEM, os administradores terão visibilidade das actividades e dependendo da forma como serão parametrizados

os alertas poderão receber notificações de actividades maliciosas, reduzindo assim a pontos cegos.

### 4.2. Selecção da melhor solução

Para se implementar alguma tecnologia em uma organização especifica precisa-se, de antemão, avaliar a pertinência da tecnologia e se é aplicável para a organização, sob pena da mesma não responder às necessidades e até criar entropia ao funcionamento da organização.

Para o caso de estudo foi seleccionada uma solução SIEM pelo facto de estes tipos de soluções permitirem recolha de informação proveniente de diversas fontes de dados em uma infra-estrutura de TI para e sintetizar estes dados para gerar alerta de eventos suspeitos que podem desencadear em um incidente de segurança cibernética, pois nos dias de hoje dados são gerados de múltiplas fontes. A fundamentação acima é defendida por (Maayan, 2019), olhando por outro lado a dimensão da infra-estrurura do caso de estudo percebe-se a necessidade de colectar dados, normaliza-los e alertar os administradores de TI em caso de detecção de uma anomalia de segurança cibernética, e uma solução SIEM é a ideal para este cenário.

É neste contexto que no presente trabalho foram estudados alguns critérios de selecção da melhor ferramenta SIEM para que a solução seleccionada seja a mais desejável possível para a organização em estudo. Dos vários critérios apresentados, os que melhor se adequam à presente pesquisa são os critérios apresentados por (Mokalled et al., 2020), salientar que os critérios apresentados na matriz que consta no **Anexo 3** são uma adaptação dos critérios apresentados pelo autor anteriormente citado.

Para cada uma das ferramentas SIEM será feita uma avaliação dos atributos com vista a preencher os critérios de avaliação, posteriormente será feita a selecção da melhor ferramenta com base nos valores atribuídos aos critérios. No **Anexo 3**, encontra-se a matriz de avaliação das ferramentas.

Alguns critérios apresentados na matriz acima possuem mais peso que outros para este caso em específico, nomeadamente possibilidade de implementação em alta disponibilidade, acesso da documentação online, opção grátis da solução.

Estes critérios tem elevado peso, porque o grupo Meridian32 possui uma equipe técnica e recursos computacionais para implementação de uma solução SIEM, a implementação desta ferramenta torna-se mais apetecível se em caso de aprovação para o avanço de implementação a equipe técnica local tenha acesso a documentação técnica da solução para melhor percepção do que será implementado em sua infra-estrutura e como implementar. A questão da alta disponibilidade joga um papel importante pelo facto de garantir que a infra-estrutura esteja a ser monitorada, em caso de falha de um dos servidores ou componentes da solução SIEM.

Outro aspecto preponderante na escolha da solução reside na possibilidade de exploração e/ou uso grátis da solução para melhor perceber se a mesma poderá responder às expectativas ao se decidir usá-la. Não se pode forçar uma organização a fazer um investimento financeiro de uma solução que posteriormente pode não responder às suas expectativas. Os restantes critérios são de elevada importância porque cobrem aquilo que é a essência de um SIEM pelo que se pode evidenciar na matriz uma boa parte das soluções responde a esses critérios.

É com base na matriz de avaliação das ferramentas SIEM que a solução seleccionada para esta pesquisa é a solução da **AlienVault**; neste caso, será o **OSSIM** que é a versão grátis da solução **USM**.

### 4.3. Proposta

Toda a componente de infra-estrutura crítica da organização já foi identificada, conforme se pode encontrar na secção 3 ponto 3.8, com esta informação é fácil de apresentar um conjunto de recomendações, em termos de parametrização da solução para que a mesma dê a visibilidade pretendida através da alimentação pelos logs para enriquecimento de dados para posterior tomada de decisão. No **Anexo 4**, encontra-se a informação mais detalhada da infra-estrurura em que o SIEM será implementado.

O objectivo desta proposta é dotar o grupo Meridian32 de uma solução SIEM por forma a recolher os logs dos servidores, equipamentos de segurança, de rede, actividades nas aplicações principais, visibilidade das vulnerabilidades e actividade dos utilizadores, por forma a classificar os mesmos para auxiliar a equipe que administra a infra-estrutura de TI.

É recomendável que o OSSIM seja instalado no ambiente de virtualização VMWare ESXi com vista a colectar a informação oriunda de diversas fontes, deverão ser alocados recursos computacionais para instalação da appliance virtual.

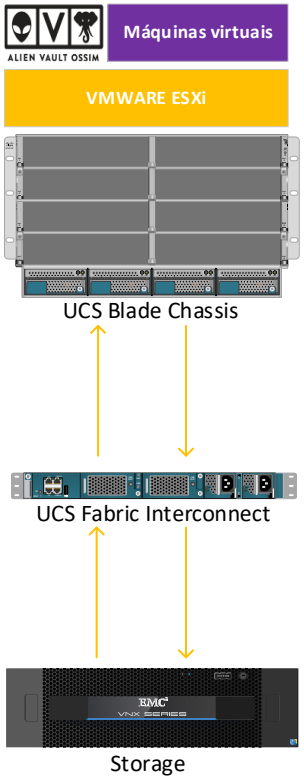



*Figura 12 Servidor proposto para instalação do OSSIM, elaborado pelo Autor*

Para melhor guiar a organização no processo de instalação e implementação da solução selecionada, são apresentadas as etapas no manual de configuração que se encontra no **Anexo 5**.

## 4.4. Análise dos resultados

O presente trabalho centrou-se em um estudo para a apresentação da proposta de implementação de ferramenta SIEM para detecção de anomalias de segurança cibernética. Visto que este estudo se desencadeou aquando do estágio profissional este factor propiciou a fácil colecta de informação da situação actual do caso de estudo e análise da melhor ferramenta que se adequa à realidade da organização. Posteriormente será necessário apresentar um passo a passo e recomendações no processo de implementação da ferramenta seleccionada para a organização.

Para que se pudessem alcançar os objectivos de estudo, fez-se uma revisão de literatura em que foram explorados conceitos inerentes ao problema em estudo apresentado na parte introdutória da pesquisa.

Foi possível no capítulo 2, com a revisão de literatura, perceber conceitos inerentes à segurança cibernética, assim como perceber o grau de pertinência do estudo. Com estes conceitos, foi fácil compreender o fenómeno de segurança cibernética e o grau de importância que esta tem para a sobrevivência de inúmeras organizações em uma era globalizada em que a informação se tornou um dos activos mais importantes. Com os conceitos explorados, adquiriu-se um panorama conceptual da importância de implementar mecanismos de segurança cibernética nos dias de hoje e principalmente o porquê que as organizações devem monitorar os eventos de segurança da sua infra-estrutura de TI. Visto que a presente pesquisa centra-se na proposta de uma ferramenta de monitoramento de eventos de segurança foram apresentados os conceitos relativos a esta ferramenta para melhor compreensão da mesma em termos de funcionamento. Foram igualmente apresentados alguns critérios defendidos por alguns autores em termos de selecção da melhor ferramenta SIEM critérios estes que seriam posteriormente usados como base para avaliação da melhor ferramenta SIEM para o caso de estudo. No processo de selecção das ferramentas por avaliar, foram usadas avaliações previamente feitas por entidades credíveis da área.

No capítulo 3 é apresentado o caso de estudo para melhor compreensão da sua dimensão e criticidade, em termos de uso das tecnologias de informação para o andamento das suas operações diárias. Fazendo um cruzamento da informação

teórica e o grau de necessidade de monitoramento da infra-estrutura por parte da organização em estudo, percebeu-se o porquê com grande urgência a organização necessita monitorar a sua infra-estrutura.

Visto que este trabalho foi desenvolvido aquando do estágio profissional, e ainda no mesmo âmbito foram apresentadas as actividades desenvolvidas na área de TI, como parte da agenda de estágio para melhor familiarização com a realidade da organização em termos de procedimentos e operações.

A proposta da solução é apresentada no presente capítulo, esta deriva de todas as actividades desenvolvidas nos restantes capítulos anteriores. Inicialmente, foi necessário agendar uma pequena reunião com os responsáveis da ALTEL e do grupo Meridian32 para apresentação da actividade de avaliação do cenário actual da organização, em termos de monitoramento de anomalias de segurança cibernética para avançar com processo de colecta de informação. O processo de colecta de informação consistiu em pequenos briefings com os ITs locais e consulta de documentos existentes em termos da topologia da organização nas TIs. Com esta informação colectada foi possível fazer uma avaliação da necessidade de forma mais profunda e apresentar a solução proposta para o caso de estudo. Para que a organização possa aproveitar este estudo em caso de necessidade de implementação da ferramenta SIEM, é apresentado ainda no presente capítulo referenciando o **anexo 5** o passo a passo de implementação que poderá servir com guião para os ITs.

Para demonstrar o grau de visibilidade e impacto que esta ferramenta pode trazer para uma organização, foi feita uma instalação protótipo (PoC) que monitorará apenas algumas máquinas pré-seleccionadas para esta avaliação. Este protótipo foi instalado em um servidor virtual com recursos suficientes para o efeito.

Os resultados desta implementação PoC são apresentados abaixo em cada um dos pontos crítico seguidos pelas evidências em print screen.

## Dashboard

Com informação colectada das fontes de dados seleccionadas no PoC conseguiu-se rechear a dashboard com informação crítica que poderá auxiliar o caso de estudo na tomada de decisão em termos de anomalias de segurança cibernética, a **figura 13** demonstra o exemplo da dashboard resultante do PoC.


*Figura 13 Dashboard resultante do PoC*

## Análise de alarmes

É possível fazer uma avaliação e análise dos alarmes despoletados pelo OSSIM como indicação de alguma tentativa de intrusão. Com dados normalizados fica mais fácil de analisar cada evento que possa ter algum impacto negativo no funcionamento da infra-estrutura de TI da organização.

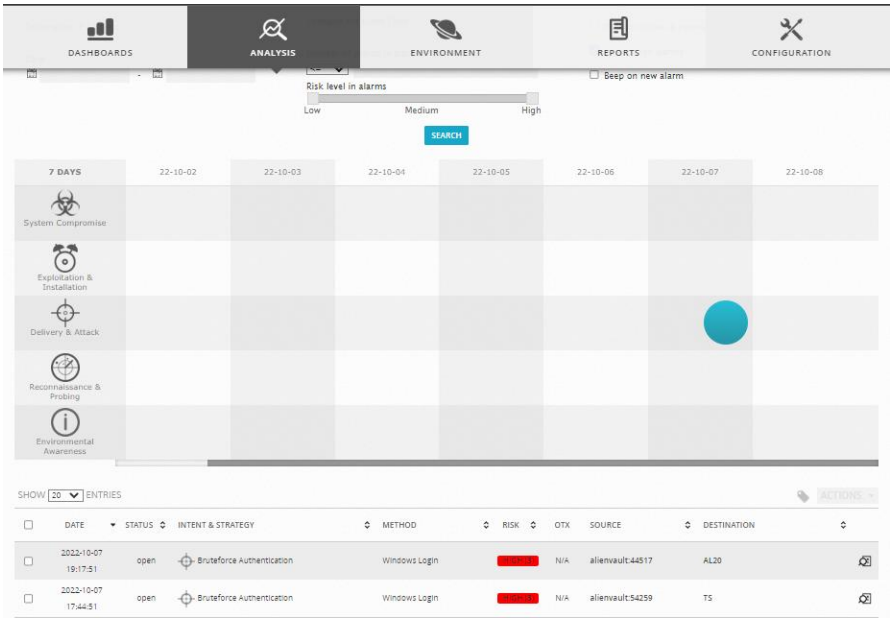



*Figura 14 Análise de alarme resultante do PoC*

## Análise de SIEM

Para além dos alarmes pode-se fazer uma análise de eventos que tenham ocorrido ou que estejam a ocorrer graças ao monitoramento real-time que o OSSIM permite. As análises SIEM do OSSIM permitem triangular os eventos e organizar os mesmos para a facilidade de análise, a organização poderá analisar de forma mais amigável e centralizada os eventos de segurança cibernética.

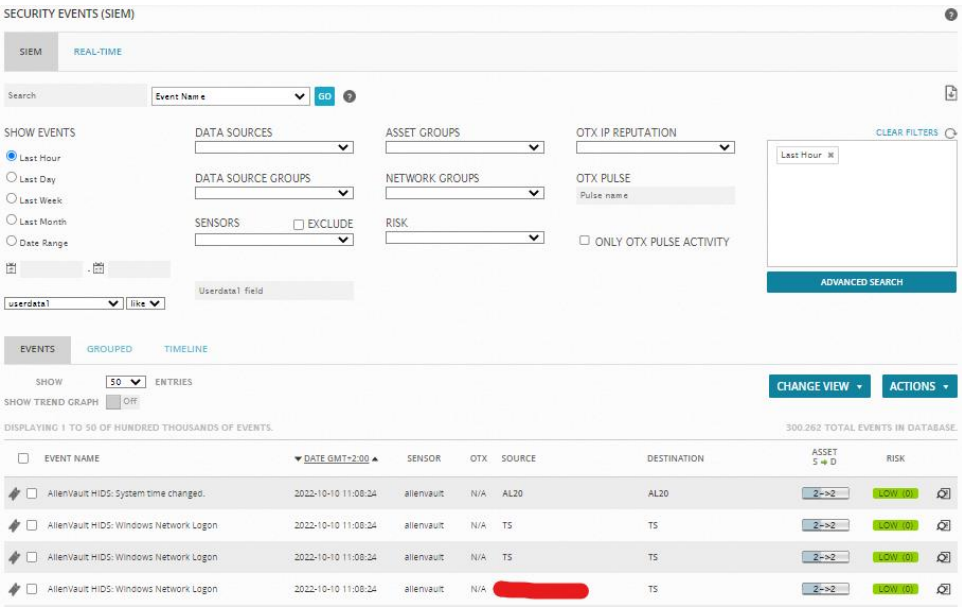



*Figura 15 Análise SIEM resultante do PoC*

### Análise e gestão de tickets

Com esta ferramenta será possível cria automaticamente tickets relativos aos eventos de segurança cibernética assim como fazer a gestão dos mesmos, esta funcionalidade é crucial aquando da gestão de eventos de segurança porque auxiliará os administradores de TI para ter visibilidade dos problemas que estão ou não resolvidos.

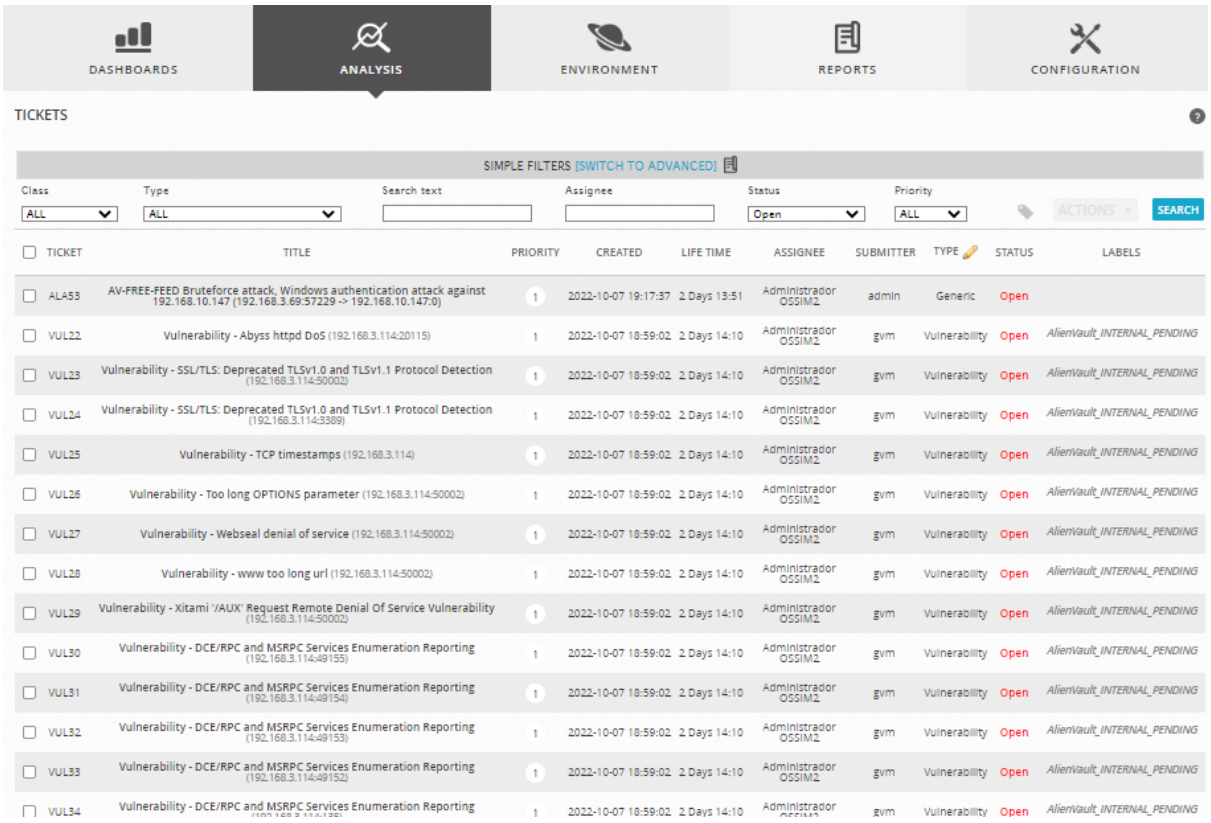



*Figura 16 Gestão de tickets no PoC*

## Gestão dos activos

Com as parametrizações e facilidades que o OSSIM traz no processo de monitoramento dos activos a organização passa a ter uma ferramenta que auxiliará na catalogação e gestão dos activos monitorados em termos de eventos de segurança cibernética, conforme se pode evidenciar na imagem abaixo.

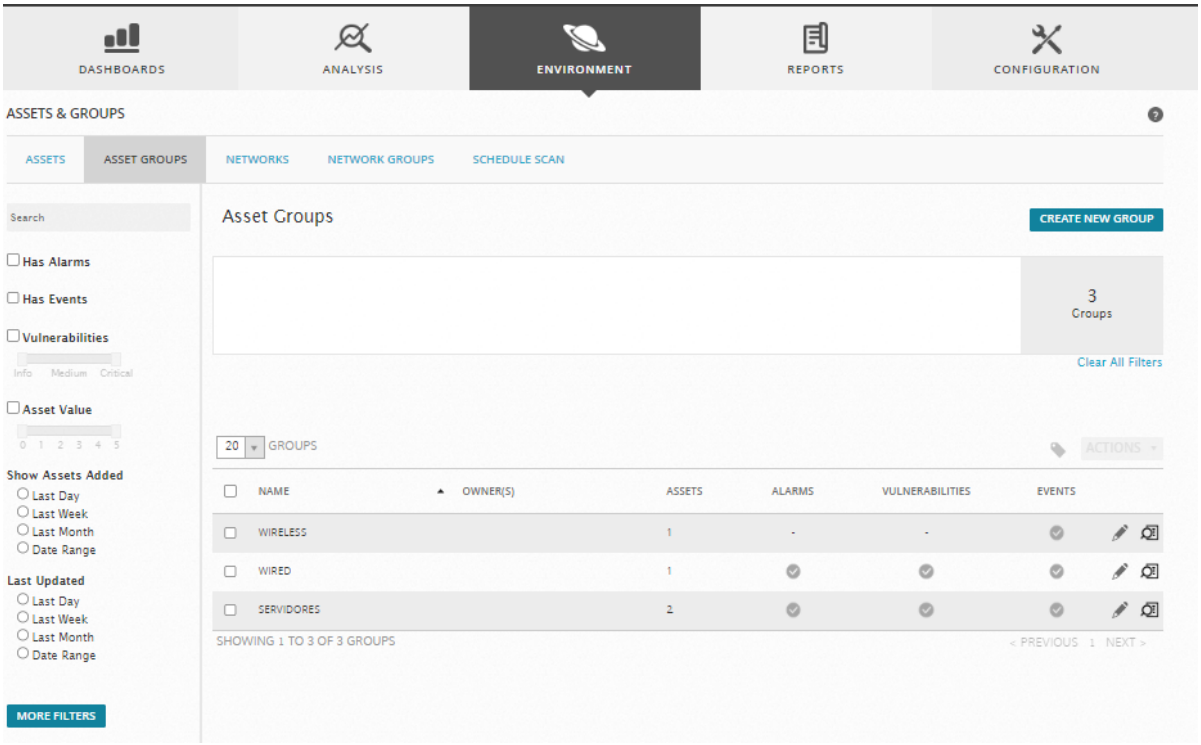



*Figura 17 Gestão de activos resultante do PoC*

## Gestão de vulnerabilidades

Como pode evidenciar a imagem abaixo o OSSIM passará a fazer uma avaliação em termos de vulnerabilidades dos activos em monitoramento, este processo de avaliação das vulnerabilidades permitirá ter visibilidades das brechas que possam existir nos activos monitorados. Esta informação é crucial porque dará uma direcção aos administradores de TI em termos de quais activos e vulnerabilidades ter em atenção.

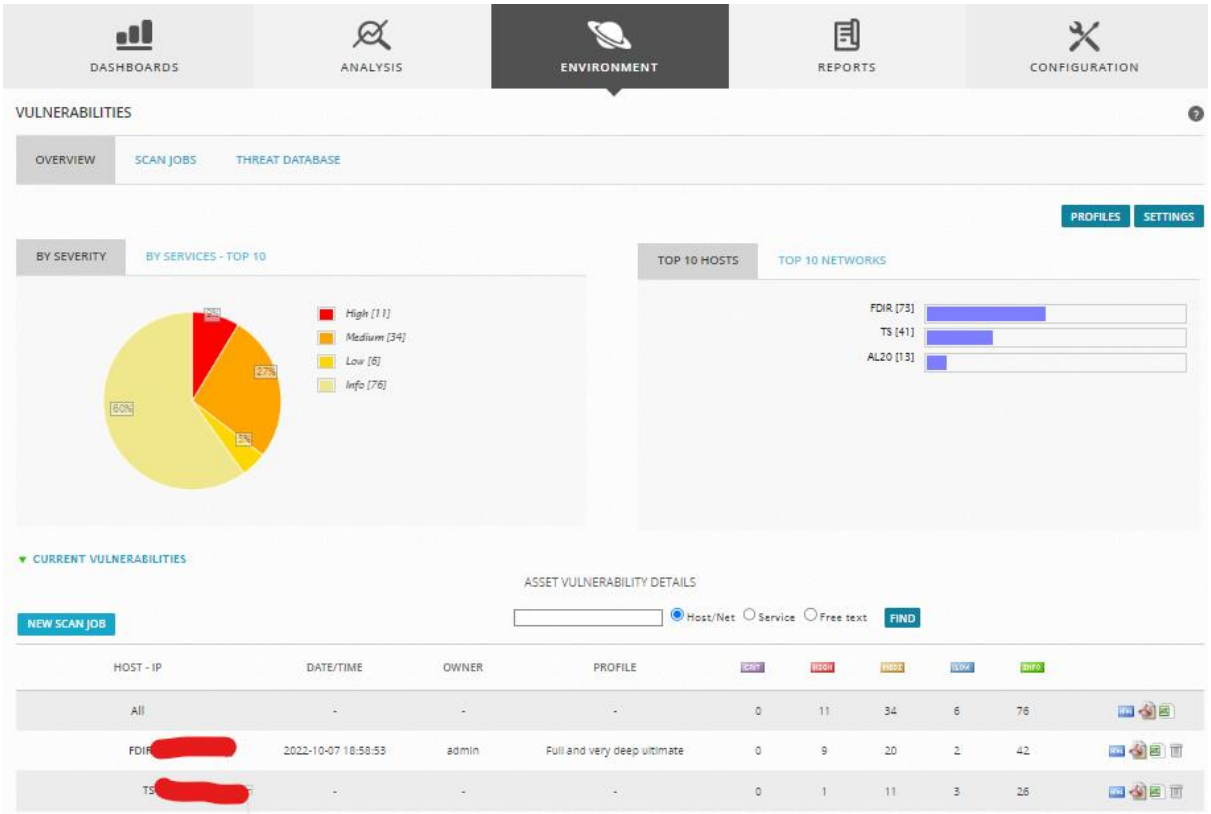



*Figura 18 Gestão de vulnerabilidades resultante do PoC*

## Monitoramento de serviços

Para além de monitoramento dos eventos de segurança cibernética o OSSIM pode monitorar os activos da organização, dependendo dos serviços que requerem atenção. No PoC feito foram seleccionados apenas alguns activos a monitorar e o serviço de monitoramento é a disponibilidade conforme se pode evidencia na imagem abaixo.

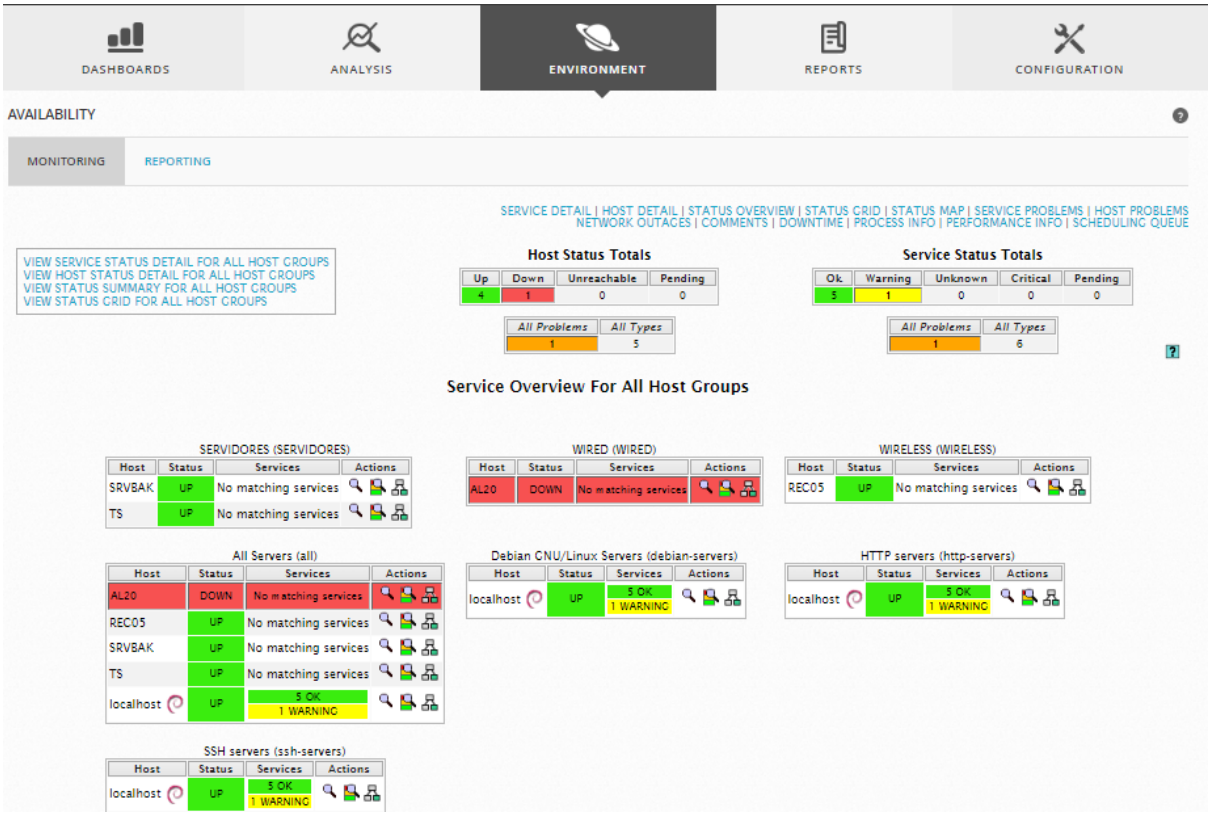



*Figura 19 Monitoramento de serviços resultante do PoC*

## Eventos de detecção

Para além da alarmística provida pelo OSSIM, esta permite o monitoramento e análise das detecções em termos de agentes instalados nos activos no processo de monitoramento.

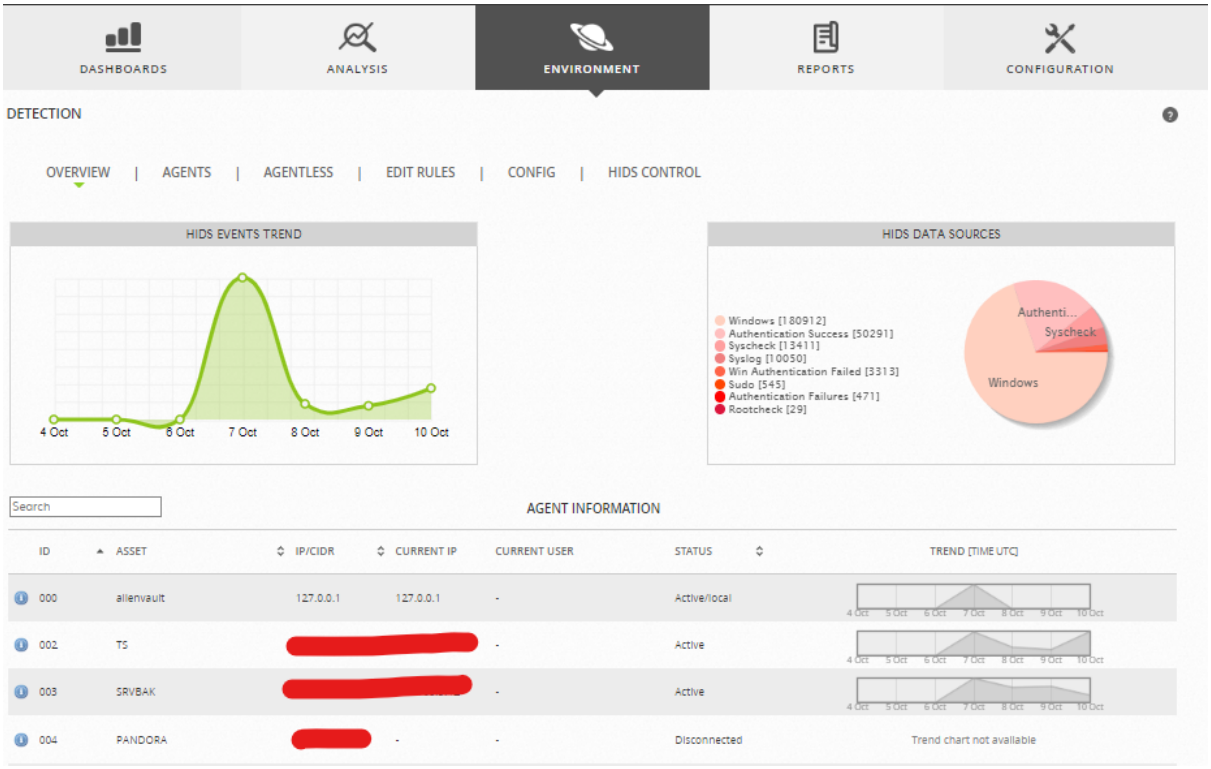



*Figura 20 Eventos de detecção dos activos monitorados resultante do PoC*

## Relatórios

Uma das vantagens do uso do OSSIM é a possibilidade de gerar relatórios que podem servir para análise dependendo do objectivo, evidência em caso de necessidade de conformidade com algum padrão internacional de segurança da informação.

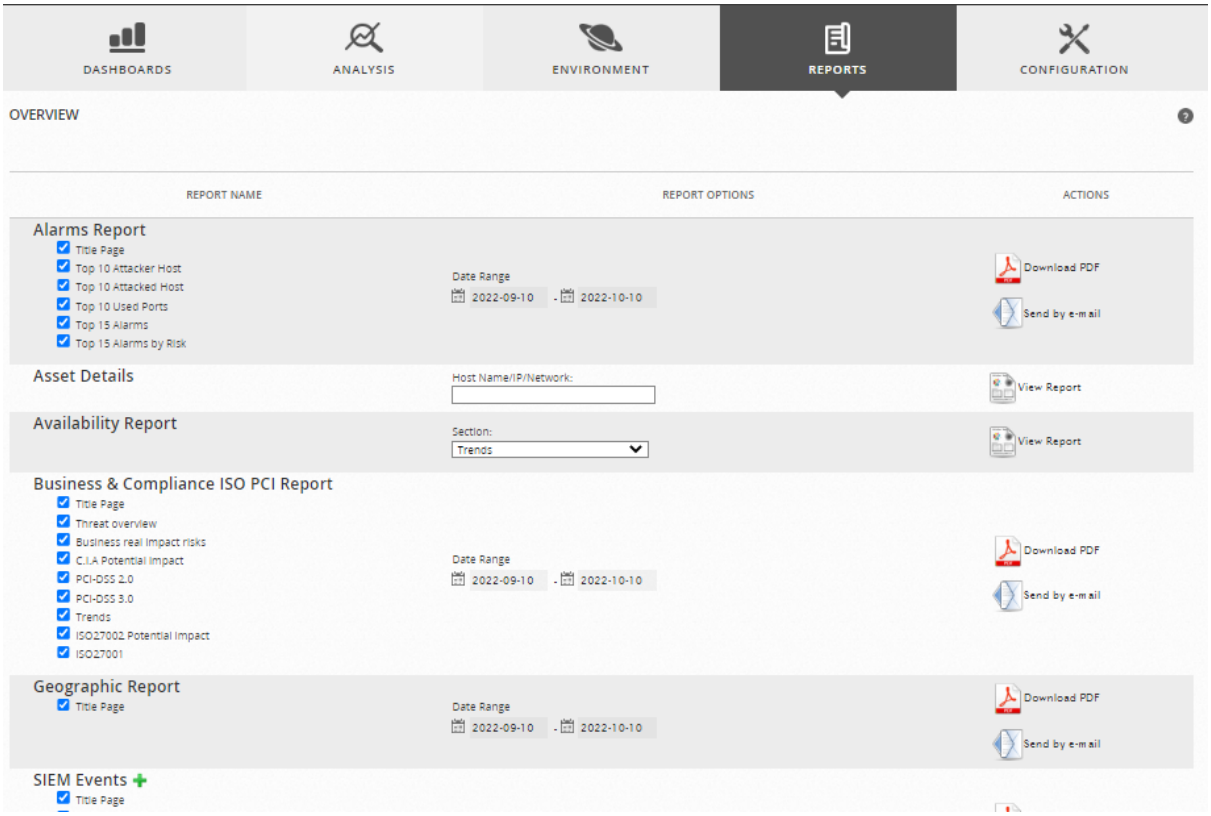



*Figura 21 Relatórios do OSSIM resultante do PoC*

# 5. CAPÍTULO V – CONCLUSÕES E RECOMENDAÇÕES

## 5.1. CONCLUSÃO

De acordo com os objectivos específicos citados no capítulo 1, conclui-se com o presente trabalho que o primeiro objectivo específico foi alcançado, conforme se evidencia no capítulo 3 onde é apresentado o caso de estudo, dando a conhecer a sua dimensão e área de actuação no mercado. Para que se pudesse ter toda a informação relativa à organização, foi feito um estágio profissional na mesma, com vista a adquirir experiência da área de TI e identificação de pontos de melhoria para a organização, no quesito de monitoramento de eventos de segurança cibernética, aplicando conhecimentos de engenharia informática adquiridos aquando da realização do curso de engenharia informática. Com esta abertura para realização do estágio profissional, foi mais fácil identificar a situação actual em termos de uso das TI e, de antemão, compreendeu-se que a organização não possui um mecanismo de monitoramento de eventos de segurança cibernética. Com o parque tecnológico da organização percebeu-se a criticidade do mesmo e a necessidade de monitoramento dos eventos de segurança.

A solução identificada para resolver o problema identificado é o SIEM, conforme encontra-se patente na revisão de literatura. O SIEM é uma solução que dá visibilidade aos administradores de TI, em termos dos eventos de segurança cibernética em uma infra-estrutura de TI especifica, foi compreendido ainda no capítulo 2 o princípio de funcionamento do SIEM e alguns critérios de avaliação de uma solução SIEM. Analisando a visão de alguns autores foi criada uma tabela de avaliação de algumas soluções para selecção da melhor para o caso de estudo, com estas constatações o segundo objectivo específico fica satisfeito.

Com a avaliação das ferramentas seleccionadas, foi proposta uma solução que fosse de acordo com as necessidades e requisitos da organização. A proposta apresentada no capítulo 4 poderá auxiliar a organização no processo de implementação da mesma. Caso necessitem instalar em sua infra-estrutura, é apresentado o passo a passo de como implementar a solução seleccionada. Como forma de demonstrar a solução SIEM em funcionamento, foi implementado um PoC para melhor ilustração em pleno funcionamento da solução. Com estas constatações o terceiro objectivo específico fica satisfeito.

## 5.2. RECOMENDAÇÕES

O presente trabalho teve como principal foco a proposta de implementação de uma solução SIEM para o monitoramento de eventos de segurança cibernética. Aproveitando PoC implementado, a organização usada como caso de estudo pode ter conhecimento do tipo de informação que este SIEM poderá trazer em usa infra-estrutura visto que foram seleccionadas algumas máquinas de teste para o monitoramento, posto isto. Recomenda-se que a organização faça a implementação desta solução seleccionada para expandir a abrangência da visibilidade em termos de eventos de segurança cibernética.

# 6. CAPÍTULO VI – REFERÊNCIAS BIBLIOGRÁFICAS


1. *About USM Appliance System Architecture and Components*. (sem data). Obtido 20 de setembro de 2022, de https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm
2. Akbas, E. (sem data). *How to Select the Right SIEM Solution?* Obtido 3 de setembro de 2022, de https://www.peerspot.com/articles/how-to-select-the-right-siem-solution
3. Alshammari, M., & Bach, C. (2013). Defense Mechanisms for Computer-Based Information Systems. *International Journal of Network Security & Its Applications*, *5*(5), 107–114. https://doi.org/10.5121/ijnsa.2013.5509
4. AT&T Cybersecurity. (2022). Em *Wikipedia*. https://en.wikipedia.org/w/index.php?title=AT%26T_Cybersecurity&oldid=1109511390
5. Bairu, G. (2020). *Forum Guide to Cybersecurity: Safeguarding Your Data*. 75.
6. Biju, J. M., Gopal, N., & Prakash, A. J. (2019). *CYBER ATTACKS AND ITS DIFFERENT TYPES*. *06*(03), 4.
7. Bodeau, D., Fox, D. B., & McCollum, C. D. (2018). *Cyber Threat Modeling: Survey, Assessment, and Representative Framework*. 119.
8. Choudary, A. (2018, dezembro 17). An Introduction to Basic Fundamentals of Cyber Security. *Edureka*. https://www.edureka.co/blog/cybersecurity-fundamentals-introduction-to-cybersecurity/

9. *Compare OSSIM to USM | AlienVault | AT&T Cybersecurity*. (sem data). Obtido 20 de setembro de 2022, de https://cybersecurity.att.com/products/ossim/compare
10. *Components of a Splunk Enterprise deployment—Splunk Documentation*. (sem data). Obtido 19 de setembro de 2022, de https://docs.splunk.com/Documentation/Splunk/9.0.1/Capacity/ComponentsofaSplunkEnterprisedeployment
11. Da Silva, T. M., Teixeira, T. D. O., & De Freitas, S. M. P. (2015). Ciberespaço: Uma nova configuração do ser no mundo. *Psicologia em Revista*, *21*(1), 176. https://doi.org/10.5752/P.1678-9523.2015V21N1P176
12. Dand, P., & Chudasama, D. (2021). *Vulnerability*. *7*, 2021. https://doi.org/10.37591/JWNS
13. Fruhlinger, J. (2022, março 16). *What is SIEM? Security information and event management explained*. CSO Online. https://www.csoonline.com/article/2124604/what-is-siem-security-information-and-event-management-explained.html
14. Gartner. (2022). Em *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Gartner&oldid=1095694877
15. LogRhythm. (2022). Em *Wikipedia*. https://en.wikipedia.org/w/index.php?title=LogRhythm&oldid=1100372876
16. Maayan, G. D. (2019, outubro 1). What is SIEM and Why is it So Important? *DATAVERSITY*. https://www.dataversity.net/what-is-siem-and-why-is-it-so-important/
17. Miller, D., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2011). *Security Information and Event Management (SIEM) Implementation*. 35.

18. Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2020). The Guidelines to Adopt an Applicable SIEM Solution. *Journal of Information Security*, *11*(01), 46–70. https://doi.org/10.4236/jis.2020.111003
19. O'CONNOR, P. (2022, setembro 26). *The biggest cyber attacks of 2022 | BCS*. https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/
20. Oscarson, P. (sem data). INFORMATION SECURITY FUNDAMENTALS. *InFormation Security Fundamentals*, 13.
21. Pizhin, U., Kusumov, Z., Amirou, K., Gustafson, M., Faraguna, C., Gon, M., Holm, A., Shah, U., Jhaveri, N., & Suter, W. (2021, fevereiro 6). *Exabeam—Wiki*. Golden. https://golden.com/wiki/Exabeam-YX9W9M3
22. *Review the Requirements for a New LogRhythm Deployment*. (sem data). Obtido 19 de setembro de 2022, de https://docs.logrhythm.com/docs/deploy/standard-installations-and-upgrades/install-a-new-logrhythm-deployment/review-the-requirements-for-a-new-logrhythm-deployment
23. Ribeiro, B. de P., Segre, L. M., & Quintao, P. L. (2005). *Segurança da informação: Definições, mecanismos, mercado e estratégias de negocio*. 8.
24. Splunk. (2022). Em *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Splunk&oldid=1110916834
25. Vielberth, M. (2021). Security Information and Event Management (SIEM). Em S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of Cryptography, Security and Privacy* (pp. 1–3). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1681-1

26. Vielberth, M., & Pernul, G. (sem data). *A Security Information and Event Management Pattern*. 12.
27. Vuorinen, J., & Tetri, P. (2012). *The Order Machine – The Ontology of Information Security*. 20.
28. Yadav, T., & Mallari, R. A. (2015). Technical Aspects of Cyber Kill Chain. *arXiv:1606.03184 [cs]*, *536*, 438–452. https://doi.org/10.1007/978-3-319-22915-7_40

# ANEXOS

## Anexo 1 - Cronograma de actividades do estágio

| Nome da Tarefa |
| --- |
| **Plano de Estágio profissional** |
| Entrega do cronograma de actividades à faculdade |
| **Fases das actividades no estágio** |
| **Fase 1 - Conhecendo a organização** |
| Apresentação da organização |
| Apresentação dos colaboradores |
| Actividades no departamento de TI |
| Apresentação do parque tecnológico do grupo Meridian32 |
| **Fase 2 - Conhecendo procedimentos no uso das TICs** |
| **Orientações procedimentais no uso dos serviços de TI na óptica do utilizador** |
| Acesso físico às instalações |
| Uso dos computadores |
| Conexão à rede provisória |
| Conexão à rede corporativa |
| **Orientações procedimentais na administração dos serviços de TI** |
| Apresentação da sala de servidores |
| Bastidor de activo e passivos |
| Servidores físicos |
| NAS |
| Storage |
| Switches |
| Firewall |
| **Procedimentos de administração** |
| Software de virtualização (VMWARE ESXI) |
| Administração dos equipamentos de rede (Switches de core e de acesso) |
| Administração da firewall |
| Administração dos equipamentos de armazenamento (Storage e NAS) |
| **Fase 3 - Identificação de problema** |

| |
|---|
| Colecta de informação |
| Reunião com o supervisor na organização |
| Registo de necessidades |
| Avaliação das necessidades identificadas |
| Selecção do problema identificado para resolução |
| Pesquisa das soluções |
| Apresentação da solução ao supervisor da organização |
| **Fase 4 - Desenvolvimento do relatório de estágio** |
| Elaboração do problema |
| Justificativa |
| Apresentação dos objectivos |
| Desenvolvimento do relatório |
| **Fase 5 - Entrega do relatório à faculdade** |

**Anexo 2 - Questões endereçadas aos responsáveis de TI**

1. Possuem mecanismos de segurança cibernética implementados? Se sim, quais?

2. Se possuem soluções de segurança cibernética, fazem monitoramento contínuo dos eventos gerados por essas soluções?

3. É feita a revisão periódica das configurações dos mecanismos de segurança cibernética?

4. Possuem procedimentos já implementados para resposta a incidente de segurança cibernética?

5. As soluções de segurança cibernética emitem alertas aos administradores de TI? Se sim, quais são os meios de notificação?

6. Já sofreram algum ataque cibernético? Se sim, qual foi o ataque?

7. Qual foi o vector de entrada?

8. Como é que responderam ao ataque?

9. O ataque cibernético foi detectado pelos mecanismos de segurança cibernética instalados?

10. Possuem solução para backup automatizado da informação? Os backups estão encriptados?

11. O posto de trabalho dos utilizadores tem EDRs, as políticas e os eventos de segurança são revistos?

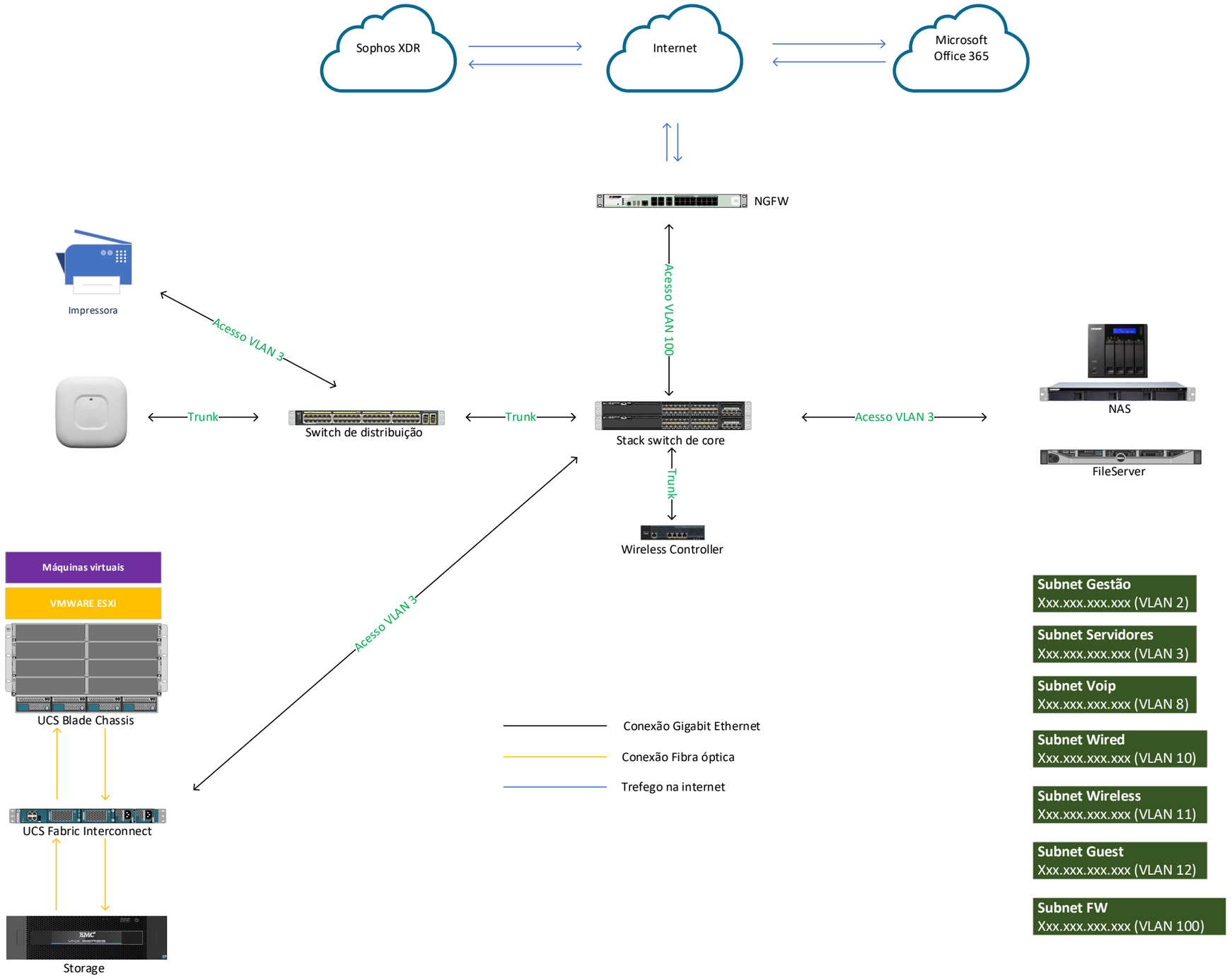
12. Os utilizadores estão conscientes da criticidade da temática de segurança cibernética?

13. Está implementado um programa de conscientização dos utilizadores para a temática de segurança cibernética?

## Anexo 3 - Matriz de avaliação de ferramentas SIEM

| | | Solução SIEM | | | |
|---|---|---|---|---|---|
| **Critério** | **Requisito** | **Splunk ES** | **LogRythm** | **AlienVault USM** | **Exabeam** |
| Plataforma | Capacidade do Sistema de Gestão de Logs | Sim | Sim | Sim | Sim |
| | Tipo de plataforma SIEM | Virtual appliance/cloud | Software para Windows Server | Virtual appliance/cloud | Software na cloud |
| | Suportando um conjunto estendido de fontes de log | Sim | Sim | Sim | Sim |
| | Método para recuperar eventos/fluxos/logs | Sim | Sim | Sim | Sim |
| | Gestão de fusos horários | Sim | Sim | Sim | Sim |
| | Capacidade de computação da plataforma | Sim | Sim | Sim | Sim |
| | Capacidade de armazenamento da plataforma | Sim | Sim | Sim | Sim |
| | Modelo de instalação | Cloud, on-premises e hibrido | Cloud, On-premises, SaaS | Cloud, on-premises | Cloud |
| | Alta disponibilidade/opções de cache | Não especificado | Sim | Sim | Não especificado |
| | Disponibilidade de regras de correlação padrão e personalizáveis | Sim | Sim | Sim | Sim |
| | Recursos de dashboards | Sim | Sim | Sim | Sim |
| | Relatórios customizáveis e de conformidade | Sim | Sim | Sim | Sim |
| | Capacidades de alerta | Sim | Sim | Sim | Sim |
| | Documentação técnica e ajuda online | Pouca | Boa | Sim | Pouca |
| | Monitoramento | Sim | Sim | Sim | Sim |
| | Enriquecimento de contexto com base em logs coletados | Sim | Sim | Sim | Sim |
| | Suporte para colecta de logs em tempo real e diferidos | Sim | Sim | Sim | Não especificado |
| | Suporte a matriz de correlação MITRE ATT&CK | Sim | Sim | Sim | Sim |
| Operações | Controle de acesso baseado em função | Sim | Sim | Sim | Sim |
| | Capacidade de Accounting | Sim | Sim | Sim | Sim |
| | Interface web para operação diária | Sim | Sim | Sim | Sim |
| | Fusos horários personalizáveis para a GUI | Sim | Sim | Sim | Sim |
| Integração | Integração do Active Directory para gestão administrativa | Sim | Sim | Sim | Não especificado |
| | Gestão de casos e rastreamento de actividades de trouble-ticket | Sim | Sim | Sim | Sim |
| | Modulo para ticketing | Sim | Sim | Sim | Sim |
| | Integração com ferramentas de gestão de vulnerabilidades | Não especificado | Não especificado | Não especificado | Sim |
| Características avançadas | Suporte a ferramentas de análise de Threat Intelligence | Sim | Sim | Sim | Sim |
| | Suporte às actividades de análise forense | Sim | Sim | Sim com integração AlienApp for AT&T Cybersecurity Forensics and Response | Sim |
| | Suporte analítico | Sim | Sim | Sim | Sim |
| | Capacidades de resposta automática | Sim com integração ao SOAR | Sim com integração SOAR | Sim | Sim |
| Licenciamento e suporte | Tipo de licença preferencial | Workload e Injest | Subscrição e licença perpétua | Subscrição e licença perpétua | Subscrição |
| | Restrições de licenciamento | Não especificado | Não especificado | Não especificado | Não especificado |
| | Activação de licença atrasada | Não especificado | Não especificado | Não especificado | Não especificado |
| | Suporte de assistência técnica e serviços profissionais | Sim | Sim | Sim | Sim |
| | Documentação guia | Sim e gratis | Sim e gratis | Sim e gratis | Não especificado |
| | Open-Source | Não | Não | Sim | Não |
| | Opção Gratis | Não | Não | Sim | Não |
| | Facil instalação | Não | Sim | Sim | Não |

## Anexo 4 - Topologia da infra-estrutura de TI



## Anexo 5 – Manual de configuração OSSIM

### Instalação do OSSIM

A AlienVault especifica requisitos computacionais para instalação do OSSIM os mesmos são básicos como se podem evidenciar abaixo:

- 2 CPU cores
- 4-8 GB RAM
- 50 GB HDD
- E1000 placas de rede compatíveis

Dependendo da necessidade de expansão da abrangência no monitoramento, estes requisitos serão ajustados, nesta fase deverão ser alocados os recursos abaixo no VMWare ESXi:

- 3 vCPU cores
- 8 GB RAM
- 80 GB HDD
- E1000 placa de rede

A organização encontra-se a usar o VMWare ESXi 6.7.

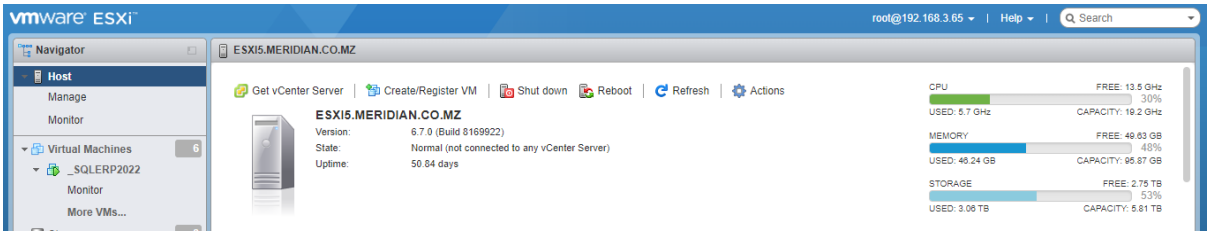



*Figura 1 VMWare ESXi 6.7*

A appliance deverá ser instalada no servidor recomendado anteriormente que será um dos servidores do chassis blade.

Visto que a infra-estrutura de servidores está toda ela a funcionar na VLAN dos servidores não há necessidade de criar múltiplas interfaces virtuais na máquina OSSIM.

## Criação da appliance virtual

- Seguindo as recomendações acima, a organização deverá garantir aquando da criação da appliance virtual do OSSIM que a mesma tenha as propriedades apresentadas na imagem abaixo.

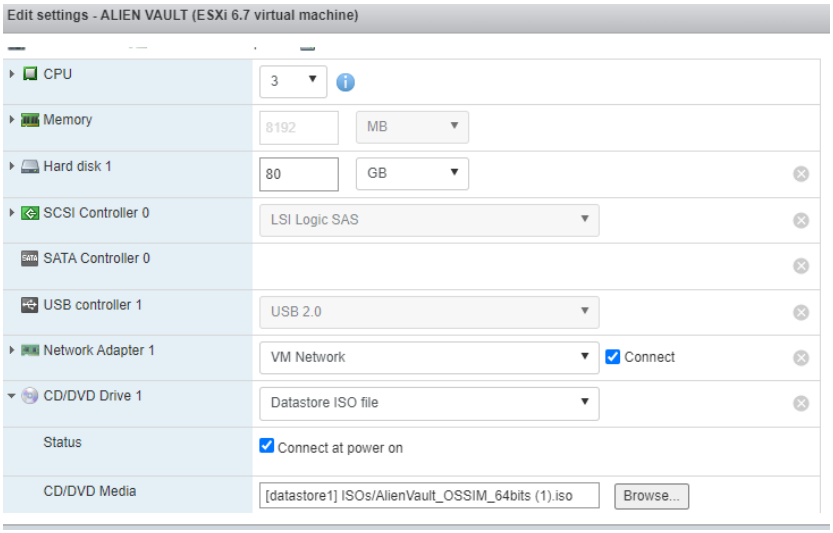



*Figura 2 Especificações da appliance virtual OSSIM*

- Deverá montar a imagem ISO do sistema AlienVault OSSIM para que se possa prosseguir com a instalação.
- Deverá ligar a máquina virtual e abrir a consola para a instalação, conforme ilustra a imagem abaixo, posteriormente deverá seleccionar a primeira opção **Install AlienVault OSSIM 5.8.11 (64 Bit)**.

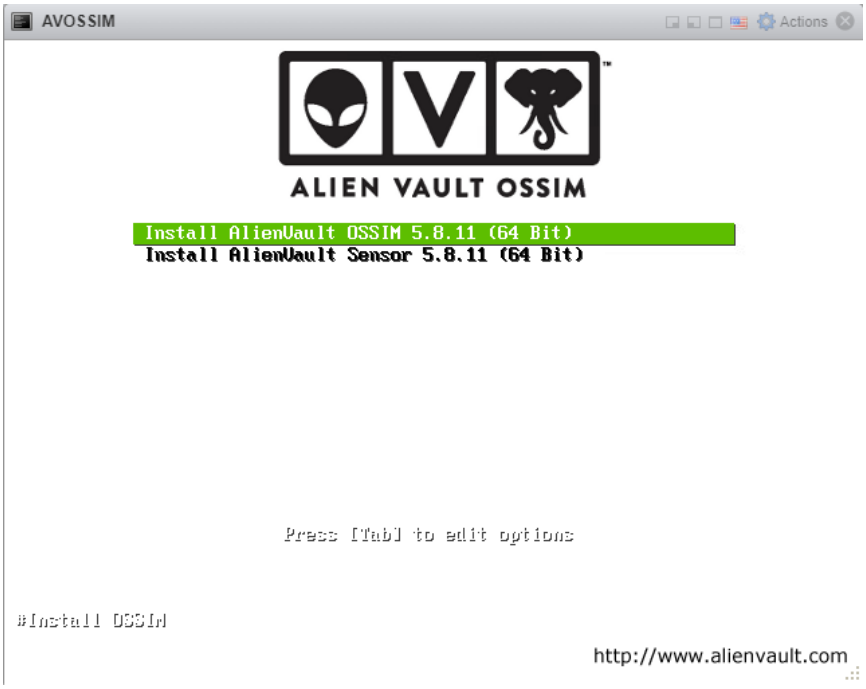



*Figura 3 Instalação OSSIM passo 1*

- Deverá seleccionar o idioma, a região e o layout do teclado de introdução do texto no OSSIM para prosseguir.

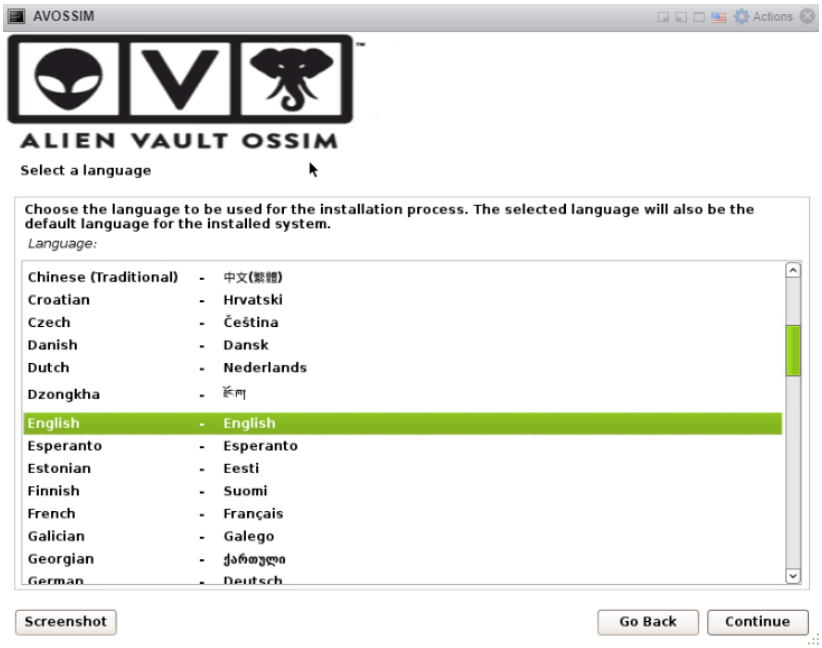



*Figura 4 Instalação OSSIM passo 2*

- Findas as configurações acima na instalação deverá configurar mais alguns parâmetros conforme ilustram as imagens abaixo.

- **Rede**

Endereço IP, máscara, gateway e DNS (Deverá usar o endereço IP disponível na VLAN 3 dependendo da regra de distribuição da organização)


*Figura 5 OSSIM – Configuração IP – passo 1*


*Figura 6 OSSIM – Configuração IP – passo 2*


*Figura 7 Configuração IP – passo 3*

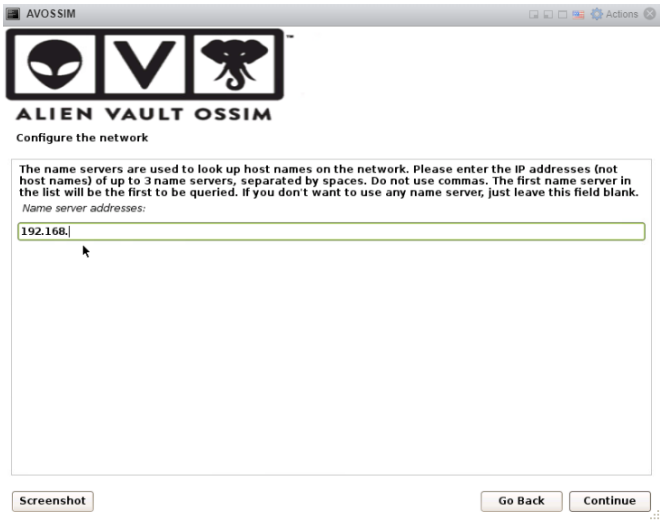



*Figura 8 Configuração IP – passo 4*

- **Credenciais do utilizador root**

Deverá criar credencias fortes e seguras para o utilizador root visto que é a conta de administração global e caso algum utilizador mal-intencionado tenha acesso a estas credenciais pode aproveitar para criar danos à infra-estrutura de TI da organização.

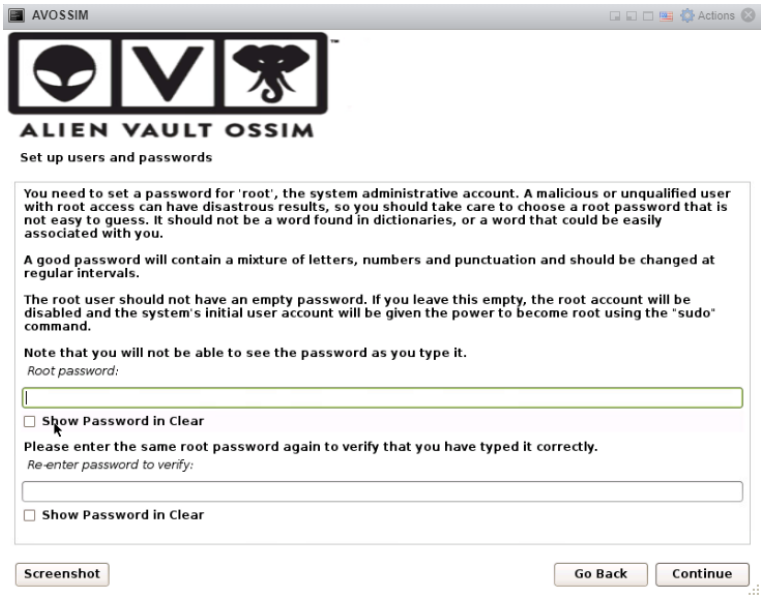



*Figura 9 Configuração credenciais*

**Nota**: Após o término da instalação, deverá permitir na regra da firewall que o endereço IP do OSSIM tenha acesso à internet para integração com o OTX da AlienVault para actualização das ameaças cibernéticas existentes.

## Configuração recomendável do OSSIM

Finda a instalação, dever-se-á prosseguir com as configurações do OSSIM. É crucial ressaltar que esta ferramenta pode ser acedida via navegador web através do endereço IP configurado no processo da instalação.

Assim sendo, dever-se-á digitar o endereço IP em um navegador para iniciar com as configurações.

Ao aceder através do navegador pela primeira vez, deverá definir as credenciais do administrador do portal para administração e configuração do OSSIM conforme ilustra a imagem abaixo.

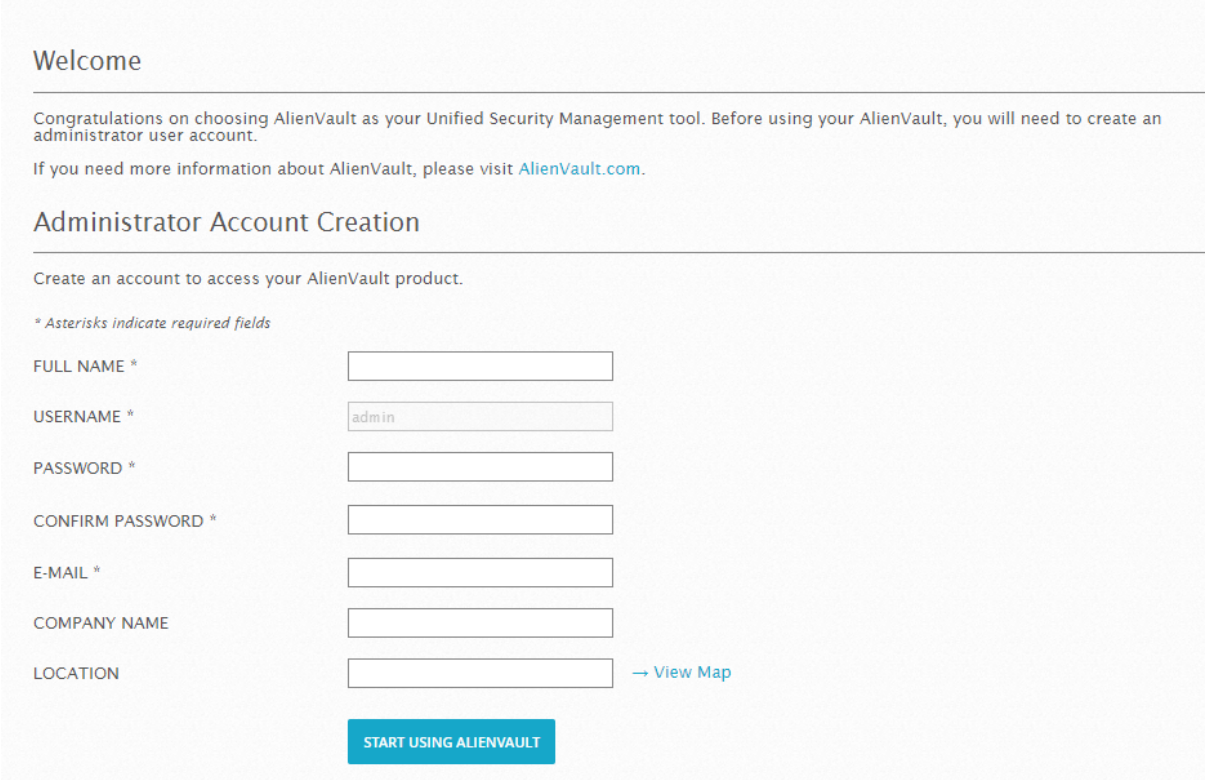



*Figura 10 Configuração conta de acesso GUI*

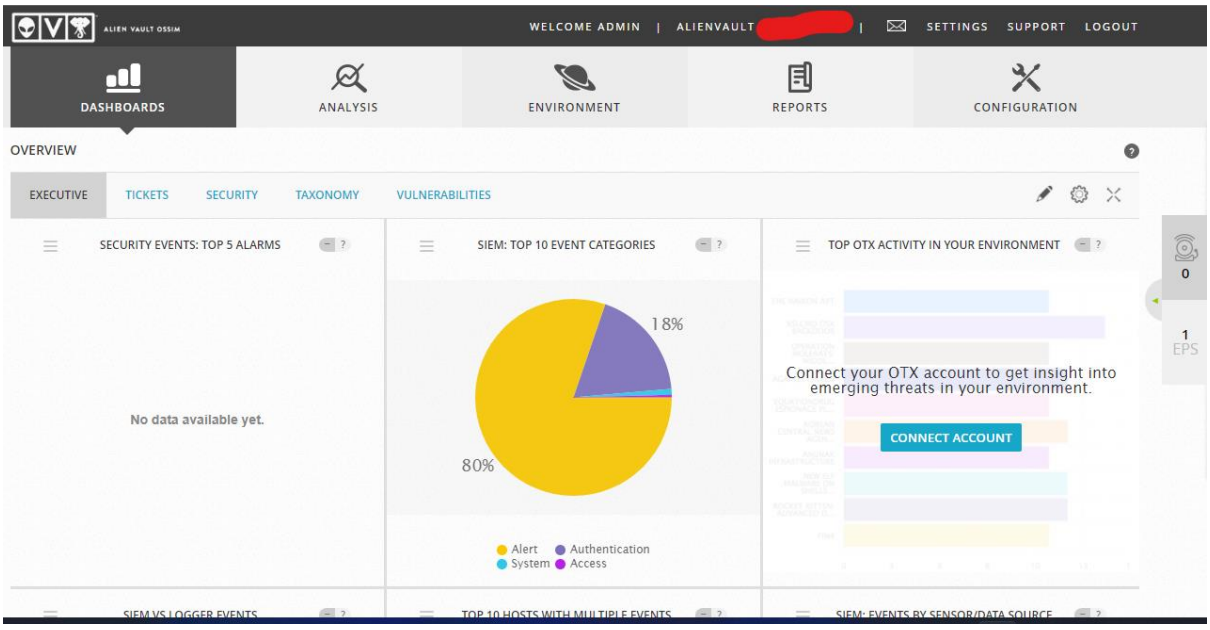



*Figura 11 OSSIM página inicial*

- **Backup**

  Deve-se criar uma política de backup da base de dados do OSSIM que deverá ser executado as 2h de madrugada. A organização

poderá definir o período de retenção dos eventos para melhor gestão de armazenamento e pesquisa de informações críticas relativas a eventos de segurança que tenham acontecido no passado. Para efectuar a configuração dos backups a organização deverá ir a opção **CONFIGURATION→MAIN→BACKUP**.

- **Parametrizações base**

  A organização deverá definir as configurações base para o funcionamento do OSSIM, nomeadamente o período para o timeout do login dos utilizadores operadores, o sistema de ticket, envio de notificação por SMTP visto que a mesma possui o serviço de email, pode-se configurar a notificação para que os administradores possam receber alertas vindos do OSSIM.

- **Activos e Grupos**

  A organização deverá criar grupos de activos para melhor controle e monitoramento dos mesmos, esta opção pode ser encontrada no menu **ENVIROMENT → Assets&Groups**.

  Os activos deverão estar separados nos seguintes grupos de acordo com a realidade do grupo Meridian32:

  GRUPO 1 – Agrupamento dos servidores críticos da organização.

  GRUPO 2 – Agrupamento dos servidores não críticos.

  GRUPO 3 – Agrupamento dos activos que usam rede a cabo.

  GRUPO 4 – Agrupamento dos activos que usam rede a wireless.

  GRUPO 5 – Agrupamento dos activos da rede.

- **HIDS**

  O grupo Meridian32 possui a sua infra-estrutura informática maioritariamente a funcionar com o sistema operativo Windows, sendo Windows 10 para os computadores dos colaboradores e Windows Server 2022 para os servidores. Nesse contexto, deverão ser instalados os agentes OSSEC para a recolha de logs e verificação de eventos no registry e integridade de ficheiros em todos os servidores Windows. A instalação pode ser encontrada no menu **ENVIROMENT → DETECTION → AGENTS**. O OSSIM permite a

instalação do agente através do download de um ficheiro.exe pré-configurado ou através da instalação remota.

- **Scan de vulnerabilidades**

  Com a configuração dos grupos de activos a serem monitorados é recomendado que a organização configure o scan de vulnerabilidades dos mesmos de forma periódica. Estes scans são cruciais visto que a organização não possui um mecanismo para gestão de vulnerabilidades o OSSIM permitirá que a organização faça uma gestão de vulnerabilidades assim como abertura de tickets e co-relacionamento dos dados para identificação de falhas nos sistemas que possam ocasionar vulnerabilidades e despoletar alertas críticos de segurança.

- **NIDS**

  Não será necessário que a organização instale algo adicional para o monitoramento baseado em snort com vista à detecção de ameaças na rede pois o sistema já está pré-configurado, devendo garantir apenas que a interface usada para monitorar os activos de rede esteja no modo promíscuo, o que foi feito na instalação do OSSIM.

- **Políticas**

  A organização deverá criar algumas políticas que irão orientar o OSSIM, em termos do comportamento que deverá adoptar na forma de processamento de eventos, ou seja, estas políticas irão definir algumas condições de acções no SIEM com base em determinadas entradas, estas políticas poderão auxiliar a organização na resposta a incidentes de segurança de informação. No seu funcionamento, as políticas permitirão enviar emails para os administradores de TI em caso de accionamento de uma delas.

  A organização poderá criar políticas para:

  - Resposta a comprometimentos das contas dos utilizadores;
  - Equipamentos offline;
  - Falhas em equipamentos críticos na infra-estrutura;
  - Tentativas de ataques;

Para criar uma política a organização deverá:

- O activo a ser abrangido na política deve estar a ser monitorizado;
- Deve-se indicar o que monitorar no activo;
- Deve-se criar um grupo de fonte de dados para se aplicar a política;
- Criar a política;
- Ordenar condignamente as políticas tendo em conta que o OSSIM interpreta de forma hierárquica;

- **Integração com OTX**

  A organização deverá criar uma conta no portal https://otx.alienvault.com/ para posteriormente integrar a conta com a instalação do OSSIM. O OTX fornece acesso aberto a uma comunidade global de pesquisadores de ameaças e profissionais de segurança, fornece dados de ameaças gerados pela comunidade, permite pesquisa colaborativa e automatiza o processo de actualização da infra-estrutura de segurança com dados de ameaças de qualquer fonte. Para integrar o OSSIM com o OTX, após a garantia de criação da conta OTX com sucesso, a organização deverá na navegação do OSSIM ir a opção **CONFIGURATION→OPEN THREAT EXCHANGE**.

**Ambiente de simulação do OSSIM**

Para ilustração do funcionamento da ferramenta foi preparado um ambiente em VMWARE que será implementada a solução SIEM com vista a fazer colecta mínima de informação de alguns activos para ilustração das suas potencialidades.

A applicance do OSSIM foi instalada na solução de virtualização VMWARE ESXI 6.7, fazendo uso dos seguintes recursos:

- 4 CPU cores
- 16 GB RAM
- 200 GB HDD
- E1000 placas de rede compatíveis

c

*Figura 12 Servidor para instalação do OSSIM PoC, elaborado pelo Autor*

O servidor físico usado é um HP ProLiant ML350e Gen8 que hospeda o VMWARE ESXI 6.7, este servidor possui duas interfaces físicas gigabit Ethernet agrupadas como única interface e conectadas no modo acesso à VLAN 3 de servidores directamente no switch de core. Infelizmente a organização não colocou as interfaces dos servidores do VMWARE em modo trunk para permitir melhor segregação das redes e interfaces virtuais. O OSSIM instalado irá se comunicar com toda a infra-estrutura graças à capacidade de roteamento inter-vlan que está implementada na rede e a procura será feita da rede VLAN 3 para as restantes redes alvo.

Para efeitos de testes serão monitorados três (3) servidores (VLAN 3), 1 laptop na rede wifi (VLAN 11) e outro laptop na rede a cabo (VLAN 10). Seguindo as recomendações apresentadas na secção 3 serão organizados os activos em grupos. Abaixo encontra-se o diagrama da solução de simulação para uma ilustração em termos topológicos.

Nesta fase de testes, não será instalado o NIDS para monitoramento dos equipamentos de rede, porque temos apenas uma interface virtual do OSSIM e o NIDS necessita de uma interface no modo promiscuo para envio de pacotes de monitoramento dos equipamentos de rede como por exemplo switches.

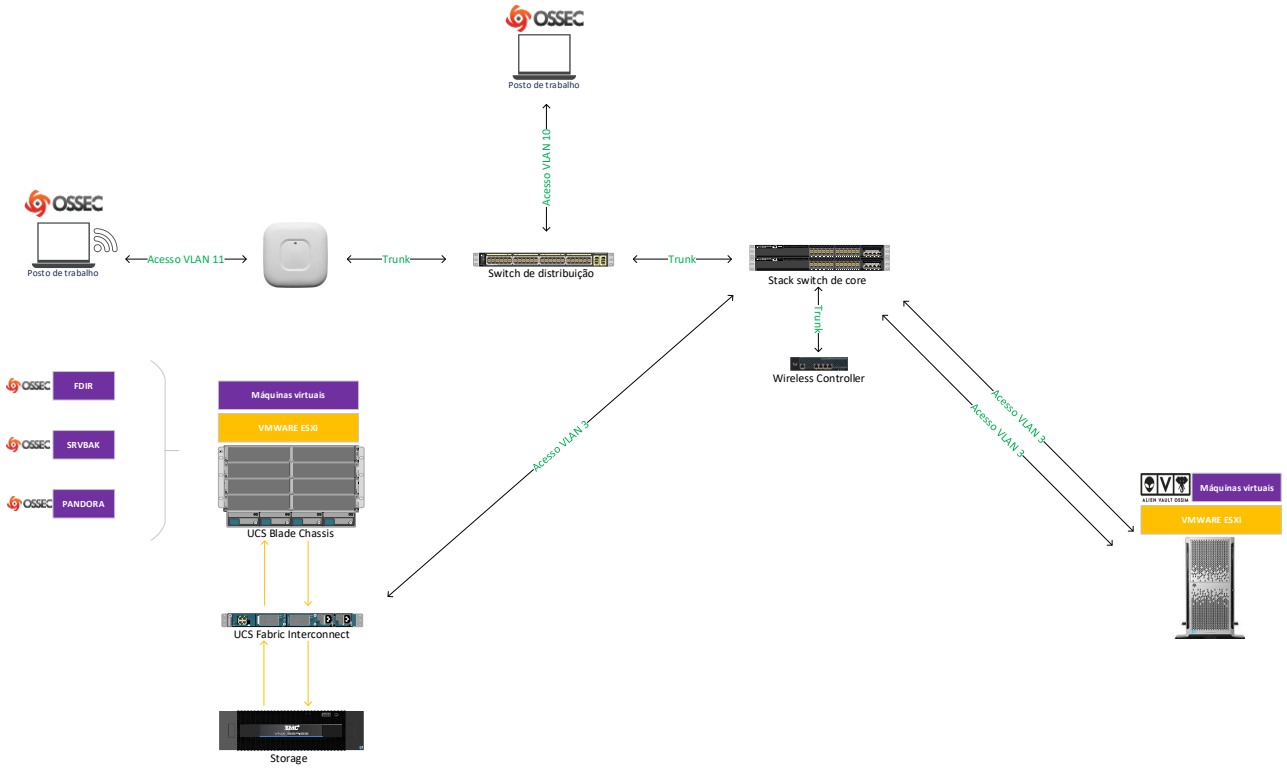



*Figura 13 Diagrama do PoC, elaborado pelo Autor*

Actividades desencadeadas:

1. Instalação do OSSIM no VMWARE ESXI 6.7

   Seguindo todos os passos e recomendações de instalação, foi feito o deployment do OSSIM com as características anteriormente destacadas.

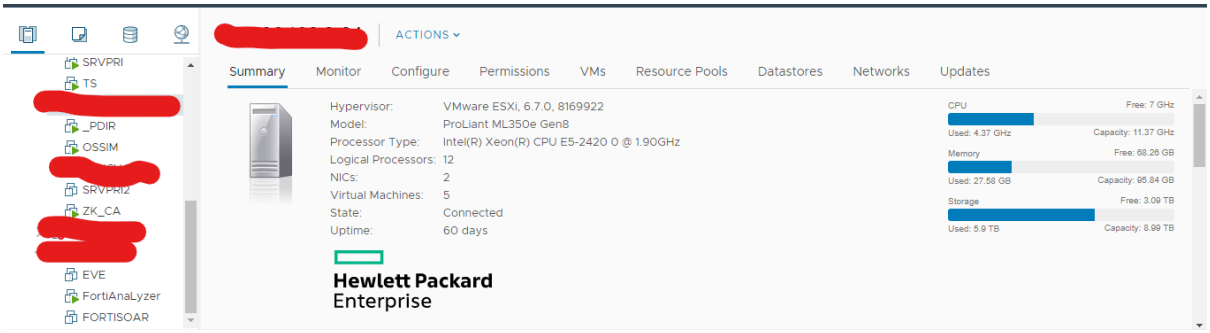



*Figura 14 Recursos do servidor usado no PoC*

2. Backup

   Foi feita a configuração dos backups conforme ilustra a imagem abaixo, respeitando algumas das recomendações feitas na secção anterior.

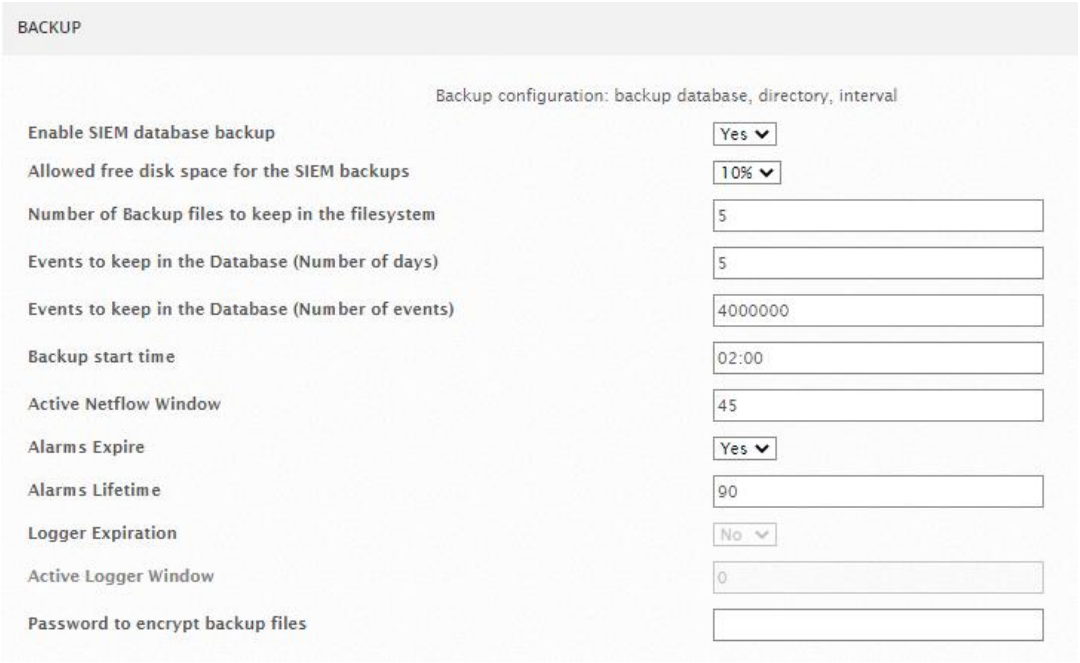



*Figura 15 Configuração de backups no OSSIM*

3. Parametrizações base
    - Nas parametrizações base foi configurado o comportamento base para os tickets habilitando esta funcionalidade e permitindo a notificação por email.

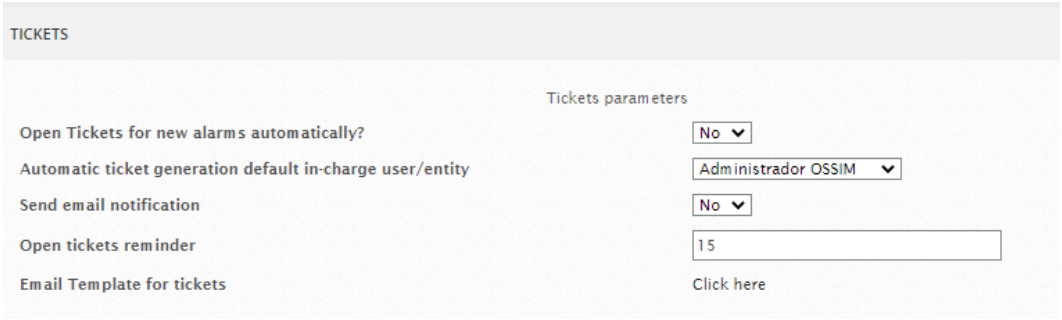



*Figura 16 Configuração de tickets*

- O método de login na plataforma será via contas locais.
- A política de password respeita os parâmetros abaixo.

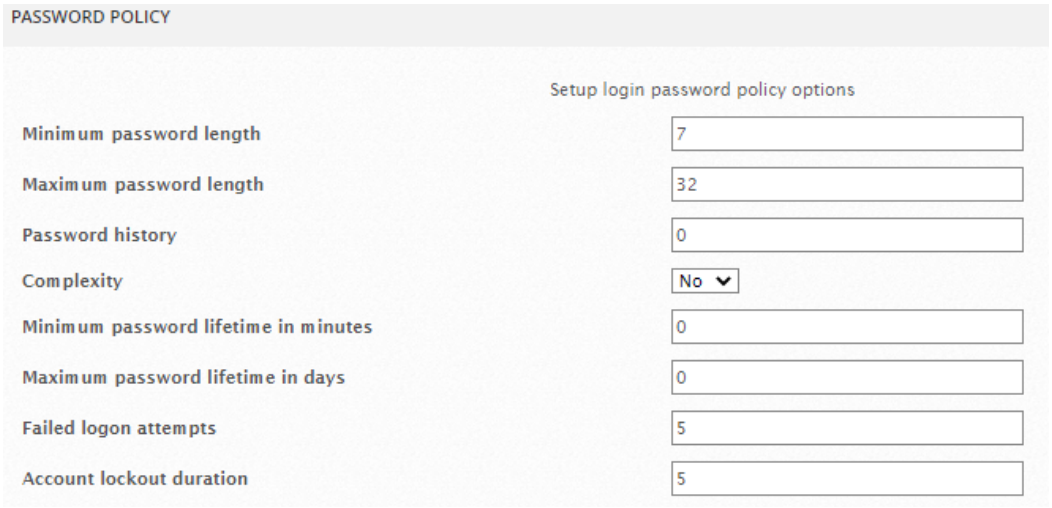



*Figura 17 Configuração da política de passwords*

- As configurações de actividades dos utilizadores, scâner de vulnerabilidades scanner, detecção e netflow serão o padrão.
- Foi configurado o servidor SMTP para envio de notificações em caso de alertas. Para tal, foi necessário recorrer a opção **CONFIGURATION→DEPLOYMENT→click no ícone →General Configuration**

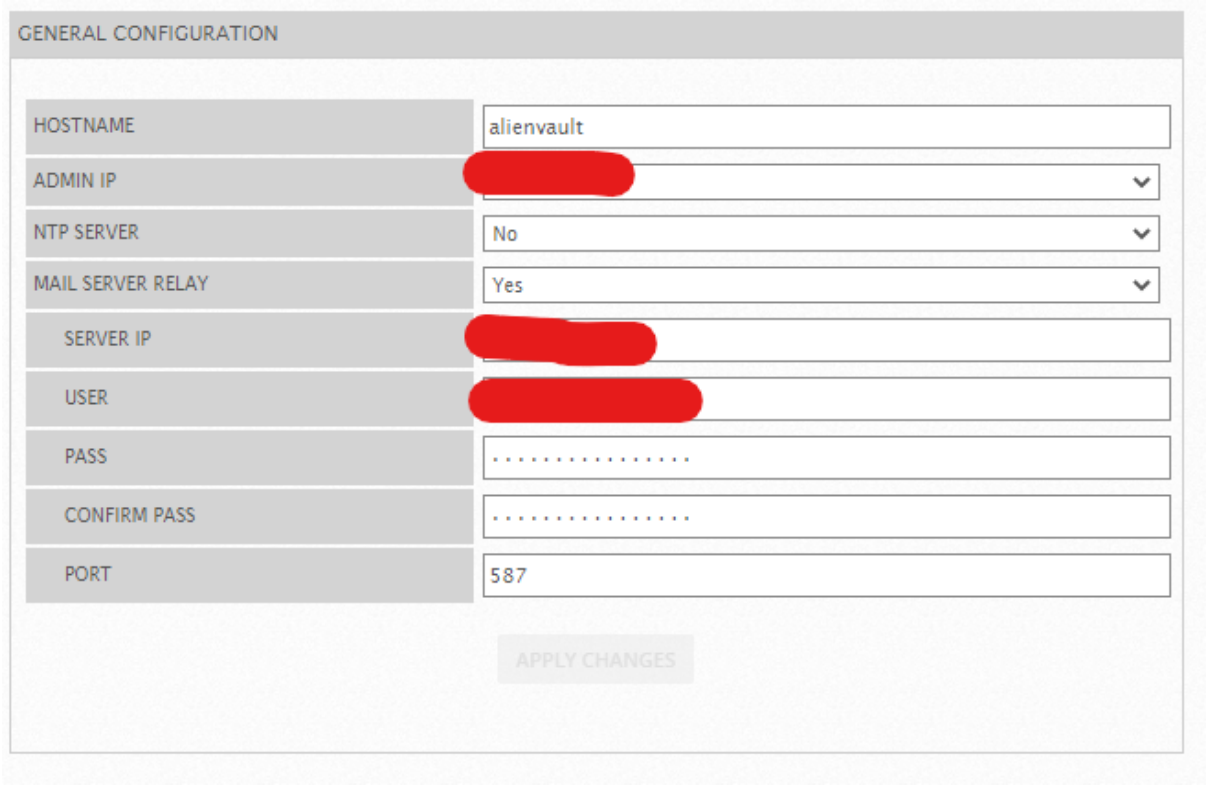



*Figura 18 Configuração de SMTP*

4. Activos e Grupos

Foram criados 3 grupos de activos, respeitando as recomendações apresentadas na secção anterior. Visto que esta implementação é de teste, apenas serão criados os grupos **servidores**, **wired** e **wireless**.

Para a criação dos grupos é necessário, em primeiro lugar, fazer a pesquisa dos activos através da opção **ENVIRONMENT→ASSETS&GROUPS**.

Neste contexto, foram seleccionados três (3) servidores, nomeadamente servidor de backup, servidor de print directory e servidor de servicedesk.

Para os postos de trabalho foram seleccionados dois (2) computadores um (1) para a rede a cabo e outro para a rede wifi.

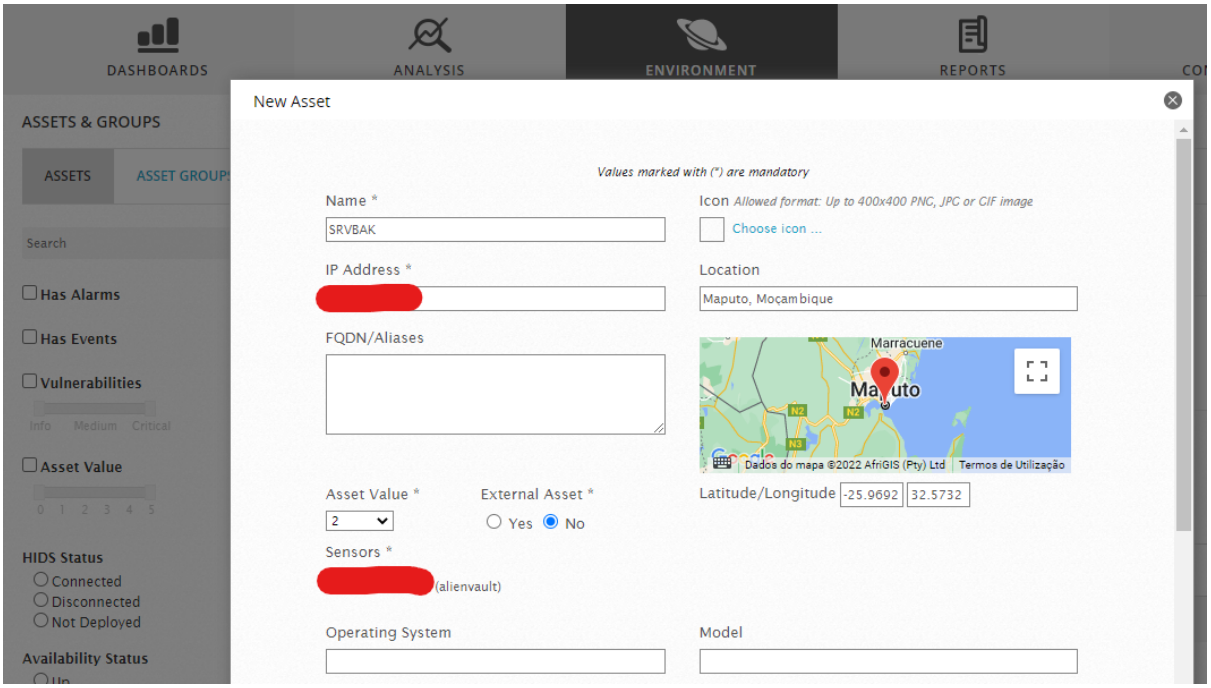



*Figura 19 Configuração dos activos*

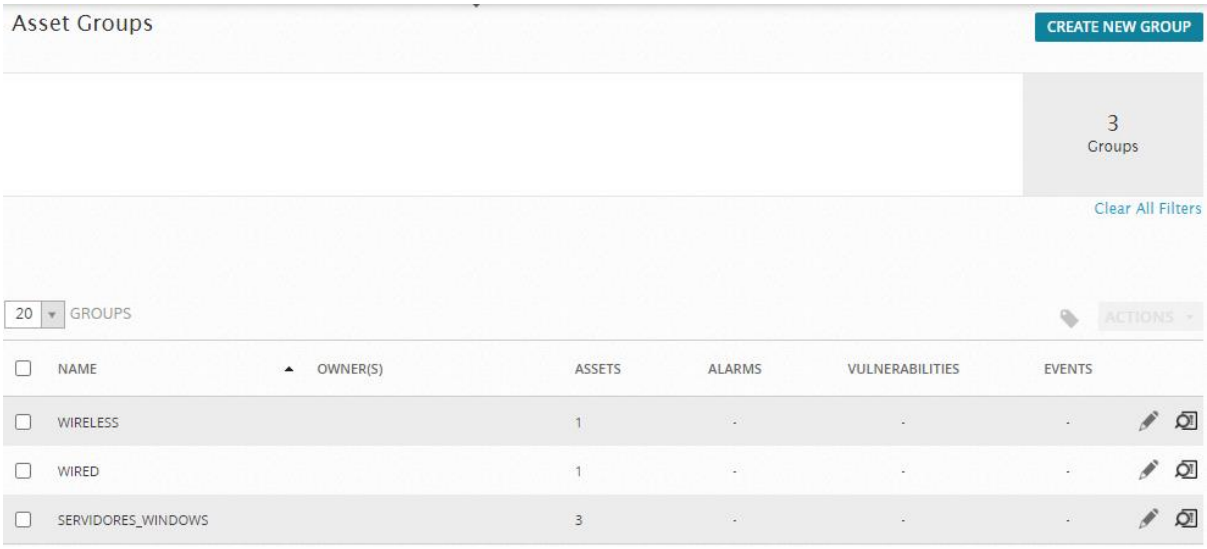



*Figura 20 configuração dos grupos de activos*

5. HIDS

Foram instalados agentes para recolha de informação nas máquinas destacadas.

Para a instalação dos agentes, foi feita recorrendo à opção **ENVIROMENT→ASSETS&GROUPS→ASSET GROUPS→Selecção do grupo de activos para instalar o agente→Selecção do activo a instalar o agente→ACTIONS→Deploy HIDS Agent**.

Posteriormente, deverão ser digitadas as credenciais de um administrador e seguidamente a instalação. Salientar que estes agentes podem ser instalados remotamente e localmente, baixando o ficheiro de instalação no portal do OSSIM.


*Figura 21 Lista de activos com HIDs*

6. Scan de vulnerabilidades

   O scan de vulnerabilidades vem activada por padrão, não há necessidade de modificar as configurações na secção **CONFIGURATION→ADMINISTRATION→MAIN→VULNERABILITY SCANNER**

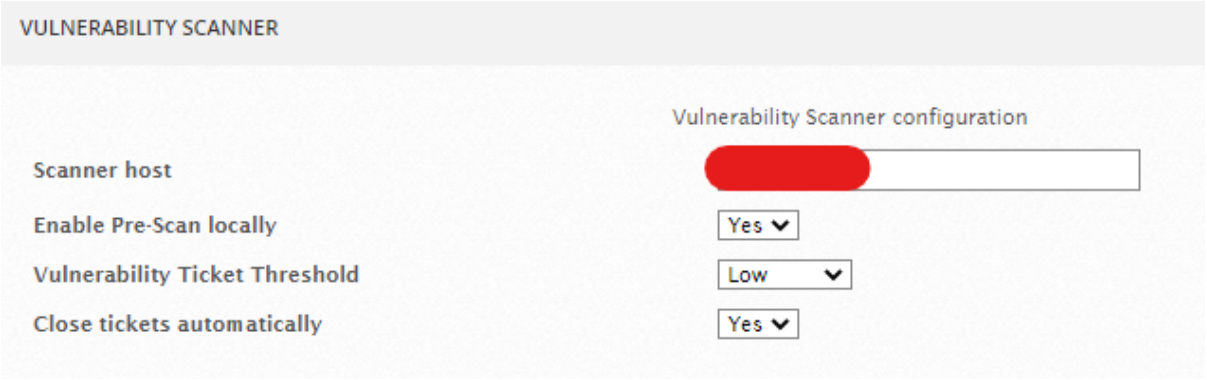



*Figura 22 Configuração do scanner de vulnerabilidades*

Para efectuar um scan de vulnerabilidades é crucial criar um **JOB** de scan, para tal foi criado um **JOB** com o nome **M32VSCAN** para iniciar o scan de vulnerabilidades dos activos seleccionados, assim sendo, recorreu-se à opção **ENVIROMENT→VULNERABILITIES→SCAN JOBS** o profile seleccionado foi **Full and very deep ultimate**

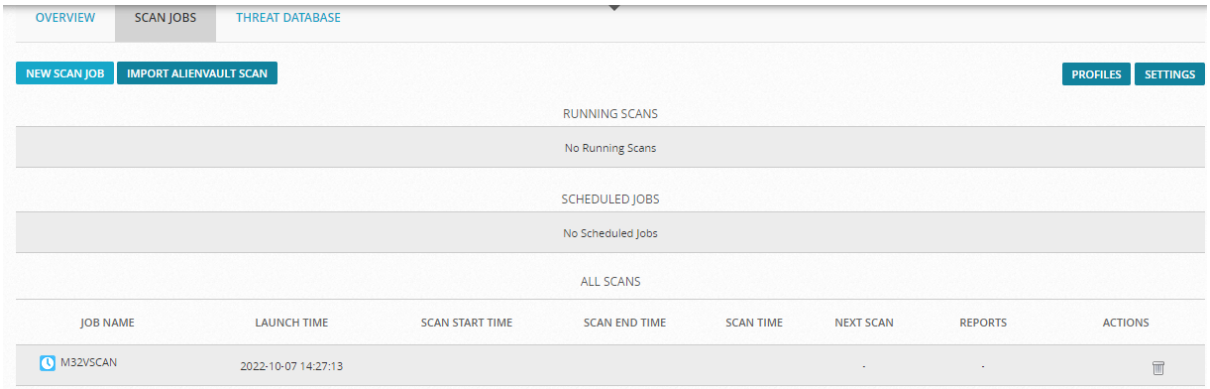
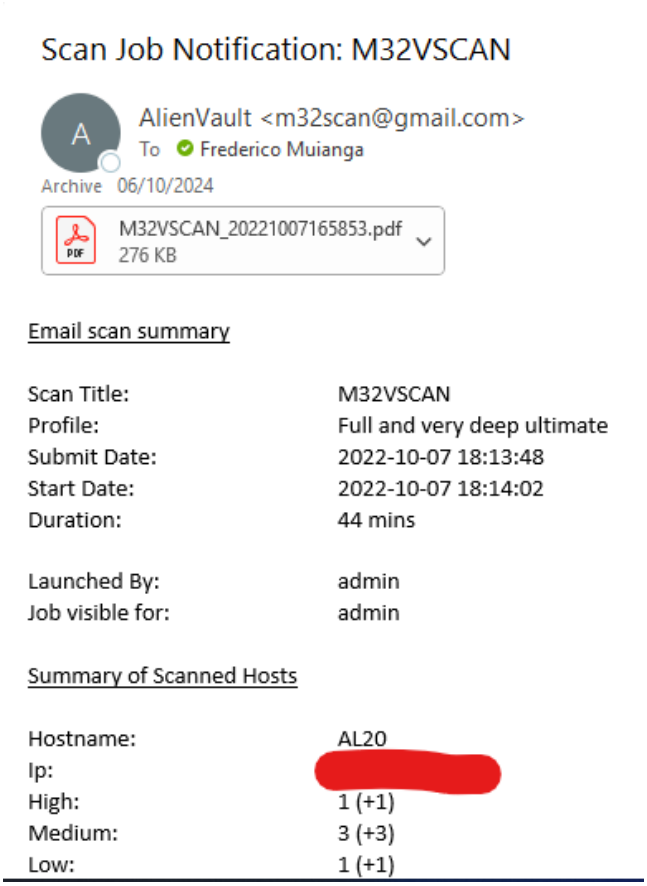



*Figura 23 Exemplo de scan de vulnerabilidades*

Após o scan o OSSIM envia um email para os destinatários seleccionados no processo de criação do JOB de Scan para ilustração do relatório de scan de vulnerabilidades.



Scan Job Notification: M32VSCAN

AlienVault <m32scan@gmail.com>
To Frederico Muianga
Archive 06/10/2024

M32VSCAN_20221007165853.pdf
276 KB

Email scan summary

| | |
|---|---|
| Scan Title: | M32VSCAN |
| Profile: | Full and very deep ultimate |
| Submit Date: | 2022-10-07 18:13:48 |
| Start Date: | 2022-10-07 18:14:02 |
| Duration: | 44 mins |
| Launched By: | admin |
| Job visible for: | admin |

Summary of Scanned Hosts

| | |
|---|---|
| Hostname: | AL20 |
| Ip: | [redacted] |
| High: | 1 (+1) |
| Medium: | 3 (+3) |
| Low: | 1 (+1) |

*Figura 24 Exemplo de notificação do resultado do scan de vulnerabbilidades*

Foi gerada uma dashboard para verificação do resumo dos resultados do scan na plataforma do OSSIM.

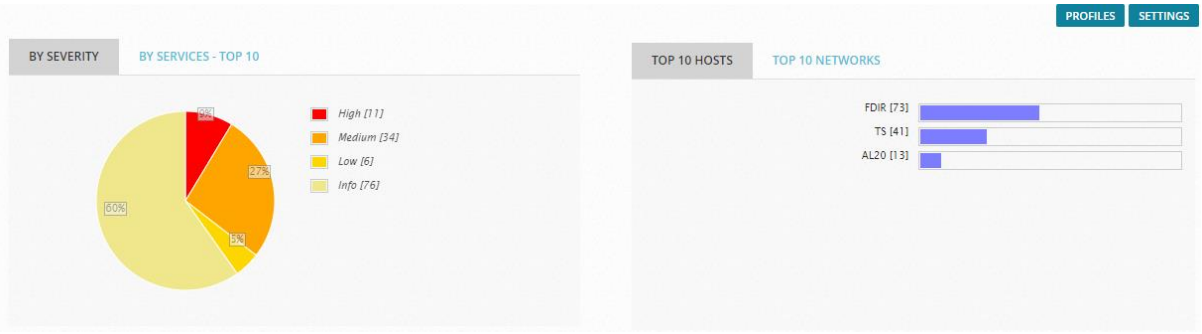



*Figura 25 Dashboard do scan de vulnerabilidades*

Foram gerados relatórios individuais dos activos em que foi feita a avaliação de vulnerabilidades para posterior análise e remediação.

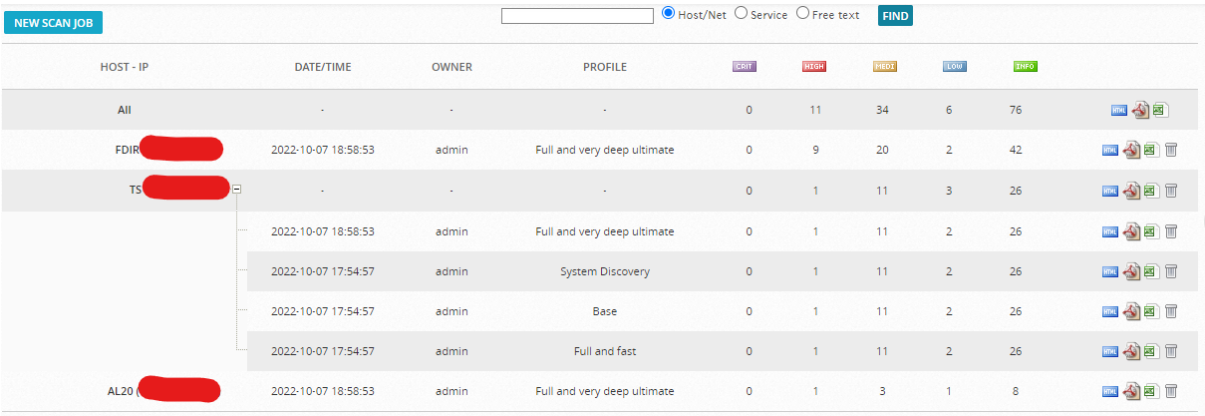



*Figura 26 Relatórios de scan de vulnerabilidades*

7. Integração com OTX

   Foi criada uma conta no OTX da AlienVault para integração com o OSSIM, para integração com o OTX foi necessário recorrer à opção **CONFIGURATION→OPEN THREAT EXCHANGE**

   Após a criação da conta no OTX é gerada uma chave única que será colocada no OSSIM, a chave pode ser encontrada no portal https://otx.alienvault.com/ seguindo o caminho **SETTINGS→OTX Key**

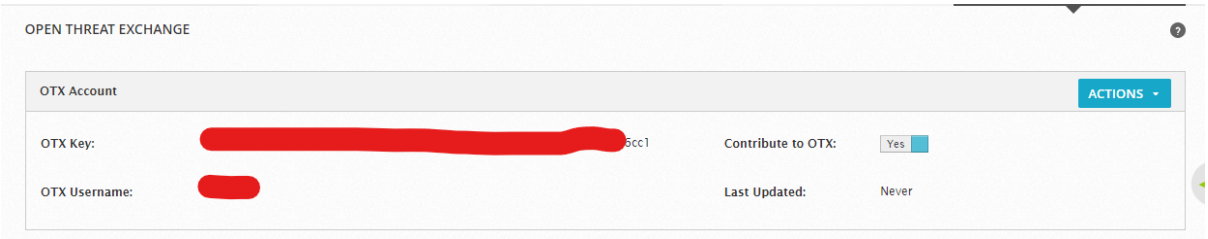



*Figura 27 Integração com OTX*

Após a integração com o OTX, o OSSIM recebe actualizações constantes, em termos de ameaças cibernéticas existentes. Esta informação poderá ser útil para os administradores de sistemas para fortificação dos seus mecanismos de segurança.


*Figura 28 Eventos recebidos do OTX*

8. Políticas

Para efeitos de testes foram criadas duas políticas, nomeadamente uma para alerta em caso de actividades suspeitas nas contas dos utilizadores e outra em termos de disponibilidade de algum servidor crítico.

O objectivo destas políticas é de demonstrar o poder que o OSSIM tem para alertar em caso de eventos que podem ser um IoC (Indicador de Comprometimento) de um activo na rede da organização. O OSSIM interpreta as regras no formato decrescente e convém que estas políticas sejam o mais específico possível para melhor se triangular o evento e prosseguir com a investigação ou tomada de medidas antes de comprometer a infra-estrutura da organização.

- Alerta de actividades nas contas dos utilizadores;

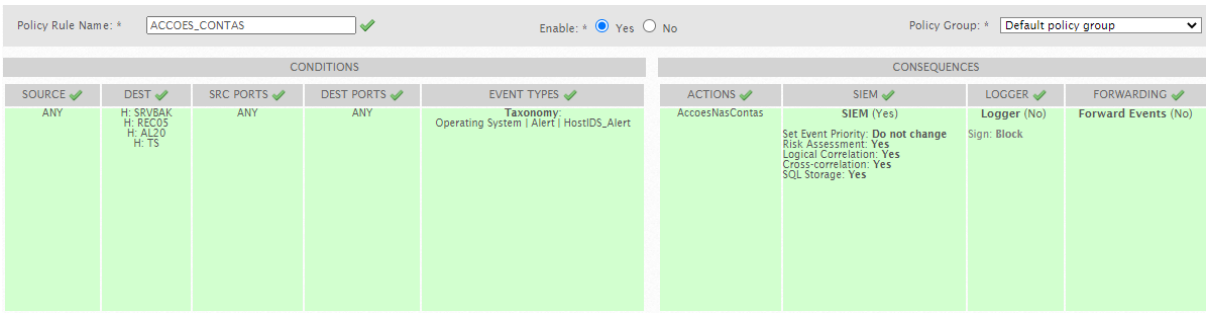



*Figura 29 Exemplo de uma política de alerta*

- Equipamentos offline;

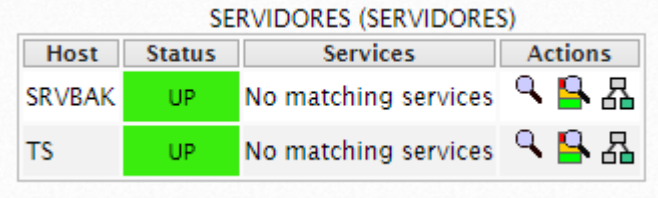



*Figura 30 Monitoramento de disponibilidade de activos críticos*

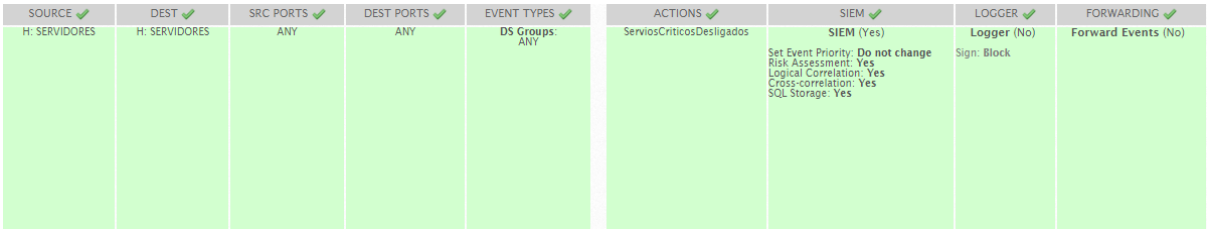



*Figura 31 Exemplo de política de monitoramento de disponibilidade de activos críticos*

## Políticas de teste


*Figura 32 Resumo de políticas criadas no PoC*