UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Proposta de Implementação de um Security Operation Center para a Universidade Eduardo Mondlane. Estudo de Caso: Faculdade de Engenharia

Autor:

MUCAVELE, Cremildo Júnior

Supervisor

Engº Délcio Arnaldo Chadreca

Supervisor da Instituição

dr. Xavier Mahumane

Maputo, Dezembro de 2025.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Proposta de Implementação de um Security Operation Center para a Universidade Eduardo Mondlane. Estudo de Caso: Faculdade de Engenharia

Autor

MUCAVELE, Cremildo Júnior

Supervisor

_____

Engº Délcio Arnaldo Chadreca

Supervisor da Instituição

dr. Xavier Mahumane

Maputo, Dezembro de 2025.

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

TERMO DE ENTREGA DE RELATÓRIO DE ESTÁGIO PROFISSIONAL

Declaro que o estudante **Cremildo Mucavele Júnior** entregou no dia __/12/2025, às 02 cópias do seu relatório de Estágio Profissional com referência _____, intitulado: Proposta de Implementação de um Security Operation Center para a Universidade Eduardo Mondlane. Estudo de Caso: Faculdade de Engenharia

Maputo, aos __ de Dezembro de 2025.

A Chefe da Secretaria do DEEL

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

DECLARAÇÃO DE HONRA

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

Maputo, __ de Dezembro de 2025.

O Autor

_____

(Cremildo Mucavele Júnior)

Dedicatória

À minha Mãe, Marília Fernanda

Ao meu Pai, Cremildo Lourenço

Aos meus irmãos, Wendy e Ian

Aos meus avós, Maria Alice e Francisco Rel

Aos demais familiares e amigos.

Agradecimentos

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

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

Ao meu Pai, Cremildo Lourenço Mucavele, pelo seu apoio e os seus sábios conselhos que conduziram durante este longo percurso.

Agradeço aos meus irmãos, Wendy e Ian Mucavele pela paciência e por me manterem sempre motivado na luta para o alcance dos meus objectivos.

Ao Corpo Docente do Curso de Engenharia Informática, pelo conhecimento transmitido e pela dedicação à nossa formação. Agradeço especialmente ao Msc. Vali Issufo, dra. Bhavika Rugnath, Eng.ª Leila Omar, Eng.º Ruben Manhiça, Eng.ª Ivone Cipriano**,** Eng.º Felizardo Munguambe e, de forma muito especial, ao Eng.º Délcio Chadreca, pela orientação na escolha do tema, pela supervisão deste trabalho e pelos valiosos ensinamentos ao longo do processo.

A Faculdade de Engenharias, em especial ao Departamento de Tecnologias de Informação e Comunicação (DTIC), pelo acolhimento e excelente ambiente de trabalho no qual fui inserido, podendo desta forma, aprimorar os meus conhecimentos.

Agradeço aos meus primos Shenilla, Shaquille, Sheila, Stecha, Amorim, Cristovão, Mariana, e Abibo por sempre mostrarem-se disponíveis para me ajudar em tudo.

Por fim agradecer aos meus amigos Liasel Maria, Bruno Miguel e Marcio de Jesus.

Epígrafe

A diferença entre o impossível e o possível está na determinação de uma pessoa.”

Tommy Lasorda

Resumo

O presente trabalho propõe um projeto que abrange uma proposta de segurança de informação com o intuito de fortalecer os mecanismos de proteção, detecção e resposta a incidentes, assegurando maior resiliência à infraestrutura de tecnologia de informação da FEUEM.

Tal pesquisa foi desenvolvida com recurso a diferentes metodologias. Utilizou-se a metodologia descritiva, procurando analisar vulnerabilidades, lacunas e dificuldades enfrentadas, por meio da recolha de dados obtidos através de entrevistas e observação participante. Recorreu-se também à metodologia qualitativa, visando compreender os conceitos relacionados à segurança cibernética no contexto da realidade académica. A metodologia de estudo de caso foi aplicada por se tratar de uma investigação realizada num contexto real e específico, permitindo identificar particularidades do cenário estudado na Faculdade de Engenharia. Por fim, adotou-se a metodologia bibliográfica, considerando todos os materiais envolvidos na construção crítica com rigor científico, tais como livros e artigos, que sustentaram a interpretação do autor acerca do tema em análise.

Do estudo observou-se que a Faculdade de Engenharia apresenta fragilidades significativas na área de segurança de informação, sem monitoria de segurança, e resposta a incidentes, disto verificou-se que a implementação de uma plataforma SIEM/SOC é uma melhoria substancial robustez da segurança no local.

Palavras-chave: Faculdade de Engenharia, Segurança de Informação, Monitoria, plataforma SIEM/SOC, Infraestrutura

Abstract

This paper proposes a project encompassing an information security proposal aimed at strengthening the mechanisms for protection, detection, and incidence responce, ensuring greater resilience to the FEUEM information technology infrastructure.

This research was developed using different methodologies. A descriptive methodology was employed, seeking to analyze vulnerabilities, gaps, and difficulties faced, through the collection of data obtained via interviews and participant observation. A qualitative methodology was also used, aiming to understand the concepts related to cybersecurity in the context of academic reality. The case study methodology was applied because it is an investigation carried out in a real and specific context, allowing the identification of particularities of the scenario studied at the Faculdade de Engenharia. Finally, a bibliographic methodology was adopted, considering all the materials involved in the critical construction with scientific rigor, such as books and articles, that supported the author's interpretation of the topic under analysis.

The study revealed that Faculdade de Engenhariahas significant weaknesses in the area of information security, lacking security monitoring and incident response. It was found that implementing a SIEM/SOC platform would substantially improve the robustness of security on-site.

Keywords: Faculdade de Engenharia, Information Security, Monitoring, SIEM/SOC platform, Infrastracture

Índice

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e Acrónimos

CID	Confidencialidade, Integridade e Disponibilidade
FEUEM	Faculdade de Engenharias da Univesidade Eduardo Mondlane
IDS	Sistema de Detecção de Intrusão
IPS	Sistema de Prevenção de Intrusão
ISO	International Organization for Standardization
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond
OSSIM	Open-Source Security Information Management
PCN	Plano de Continuidade de Negocios
PIB	Produto Interno Bruto
SI	Sistemas de Informação
SIEM	Security Information and Event Management
SOC	Security Operation Center
SOAR	Security Orchestration, Automation, and Response
TI	Tecnologias de Informação
TICS	Tecnologias de Informação e Comunicação
XDR	Extended Detection and Response

Glossário

Activo:

Todo aquele recurso corporativo que possui valor para e na organização e que precisa ser protegido, tendo em conta que ele pode ser físico ou lógico e pode vir em forma de dados, equipamentos, pessoas, sistemas e infraestrutura de TI.

Ameaça:

Quaisquer categoria de eventos, acções, objectos, pessoas ou até situação com potencial para causar dano a um activo (ex.: vírus, hacker, erro humano, falha de energia). Acreditando que eles sempre estarão presentes nas organizações.

Ataque Cibernético:

Acção intencional realizada por um agente malicioso para comprometer sistemas, roubar dados, interromper serviços ou causar prejuízos.

Continuidade de negócios:

Planejamento e conjunto de estratégias para garantir que a organização continue operando mesmo após incidentes, falhas ou desastres.

Infraestrutura de rede:

Conjunto de equipamentos e tecnologias que permitem a comunicação e o funcionamento de uma rede de computadores (ex.: switches, routers, cabos, servidores).

Open-Source:

Software cujo código-fonte é disponibilizado ao público, permitindo uso, modificação e distribuição sem custo.

Log:

Registo automático das atividades que ocorrem em sistemas, aplicações e dispositivos, usado para auditoria, monitoramento e investigação

Governança:

Conjunto de políticas, processos e práticas que orientam a gestão de uma organização, garantindo controle, transparência e alinhamento com os objetivos estratégicos.

Endpoints:

Dispositivos físicos que se conectam a uma rede de computadores e trocam informações com ela. Ex: dispositivos móveis, computadores desktop, máquinas virtuais, dispositivos embarcados e servidores, além de dispositivos IoT como câmeras, geleiras, etc.

1. Capítulo I - Introdução

1.1. Contextualização

As soluções de segurança da informação assume um papel vital na sustentabilidade das organizações, sobretudo perante o crescimento exponencial de incidentes que comprometem a integridade, a confidencialidade e a disponibilidade dos dados. Ataques de várias naturezas têm-se tornado cada vez mais sofisticados, representando riscos significativos para infraestruturas tecnológicas de tal forma que essas comprometem directamente a continuidade de negócios, reforçando a necessidade de mecanismos de proteção e resposta como os *Security Operation Centers (SOC).*

O surgimento dos *Security Operations Centers (SOC)* está ligado à crescente necessidade de proteger activos digitais contra estas ameaças que se tornou crítica com a aceleração da tecnologia e a sofisticação dos ataques. Este que teve seu inicio da década de 80 onde constituía-se por um monitoramento manual, com analises simplistas de logs e actividades de rede, e soluções existentes na época erm baseadas em anti-virus e firewalls. Nos meados dos anos 2000 foi onde iniciou a maturidade dos SOC's como vemos hoje com a adopção de Sistemas de Gestão de Informação e Eventos de Segurança (SIEM), apos anos com a integração de EDR e *Threat Intelligence*, *SOAR*, etc.

1.2 Justificativa

A proposta de um *Security Operation Center* na Faculdade de Engenharia da Universidade Eduardo Mondlane se mostra necessária para fortalecer a segurança de informação na sua infraestrutura de rede, impactando positivamente a sua eficiência e segurança. Devido à ausência de mecanismos de monitoria contínua, a infraestrutura a nivel de segurança cibernetica apresenta abundantes riscos.

Esta proposta também mostra se particularmente crucial para uma instituição acadêmica como a Faculdade de Engenharias, por fortalecer a postura de segurança cibernética sendo fundamental para proteção dos ativos, resposta a incidentes, e garante a continuidade das operações. A proposta contribui também para o avanço do conhecimento académico ao demonstrar, por meio de um estudo de caso, como uma instituição de ensino pública pode estruturar e operacionalizar um *SOC* adaptado às suas condições e recursos.

Além disso, um *SOC* bem estruturado permite que a instituição deixe de atuar de forma reativa e passe a adotar uma abordagem proativa na gestão de ameaças, incluindo identificar anomalias em tempo real, prevenir ataques antes que se concretizem e criar uma base histórica de eventos capaz de orientar decisões estratégicas de segurança. Assumindo que os potenciais danos a instituição seriam graves no comprometimento dos dados em caso de um ataque e devido ao elevado volume de dados sensíveis, representa uma resposta essencial para mitigar os riscos.

1.3 Problematização

A crescente digitalização dos processos académicos, administrativos e científicos na Faculdade de Engenharia da Universidade Eduardo Mondlane tem aumentado significativamente o volume de dados sensíveis e críticos em circulação na sua infraestrutura tecnológica. Mostra-se evidente a necessidade da segurança de informação devido ao uso intensivo de plataformas de aprendizagem, laboratórios computacionais, sistemas de gestão académica, ferramentas de pesquisa e serviços online, muito além da FEUEM alberga serviços críticos, nomeadamente financeiros, de gestão, e académicos. Por essa razão, é imperativo que a se faça uma implementação procedimentos e mecanismos de monitoria da segurança de informação.

Diante deste cenário, surge a necessidade de avaliar se a proposta de um *SOC* poderia não apenas fortalecer a postura de segurança de informação da Faculdade de Engenharia, mas também agregar valor institucional ao melhorar a resiliência, a visibilidade sobre os eventos de segurança e a capacidade de resposta a incidentes.

1.4 Problema de Pesquisa

Uma pergunta de pesquisa deve expressar o problema de forma clara, objetiva e delimitada, orientando o percurso da investigação e definindo com precisão aquilo que se pretende responder ao final do estudo. (Gil, 2022) .

A presente pesquisa visa responder a seguinte pergunta de pesquisa:

Qual é o melhor modelo de *SOC* a propor, que oferecerá viabilidade, monitoria, segurança adequada, e tendo em conta os realidade da Faculdade de Engenharia da UEM"

1.5 Objectivos

Nesta secção, constituem-se como objectivos do relatório os seguintes:

1.5.1. Objectivo Geral

- Propor um Centro de Operação de Segurança para a Faculdade de Engenharias da UEM.

1.5.2. Objectivos Específicos

- Analisar as diferentes soluções SIEM/SOC, suas implementações, com base em metricas e criterios de escolha;
- Descrever as lacunas e riscos na infraestrutura de Faculdade de Engenharia de com auxílio de métodos de recolha de dados selecionados;
- Propor a solução que melhor se adeque as condições e a realidade da Faculdade de Engenharia.

1.6 Metodologia

1.6.1 Classificação da Metodologia

- **Quanto à natureza**

Gil define pesquisa aplicada como sendo um processo sistemático que tem como objectivo de gerar conhecimento para aplicação prática, utilizados para resolver problemas práticos e específicos. Busca-se obter respostas para problemas quotidianos, sendo que, está se sempre voltado a aplicação pratica de uma fundamentação teórica dados e informações necessárias, neste caso sobre segurança de informação. (Gil, 2022)

Levando-se em consideração a problematização e os objectivos que a presente pesquisa se propõe a alcançar, determina-se esta como uma pesquisa aplicada, por esta propor uma solução de um problema real, o Centro de Operação de Segurança a Faculdade de Engenharia.

- **Quanto à abordagem**

As pesquisas qualitativas fornecem dados obtidos em condições naturalísticas, possibilitam a compreensão e interpretação aprofundada sob a perspectiva dos próprios participantes e produzem resultados que não poderiam ser alcançados mediante procedimentos quantitativos. (Gil, 2022)

Neste presente trabalho baseou-se na qualitativa por como explicado no conceito, busca compreender de forma detalhada e contextualizada, a realidade da infraestrutura de segurança da informação da instituição, assim analisando processos e desafios enfrentados no quesito de segurança da rede.

- **Quanto aos objectivos**

A pesquisa descritiva tem como objetivo descrever, com exatidão, os fatos e fenômenos de determinada realidade, analisando suas características, causas e relações sem manipulá-los. (Lakatos & Marconi, 2021)

O presente trabalho baseou-se na pesquisa descritiva porque tem como intuito analisar a situação da infraestrutura, e suas vulnerabilidades além de, caracterizar o elementos antes de se propor uma solução.

- **Quanto aos procedimentos**

De acordo com Lakatos e Marconi, a pesquisa bibliográfica caracteriza-se por recolher, analisar, interpretar e sistematizar informações já publicadas sobre determinado tema, permitindo ao pesquisador compreender o estado da arte, teorias existentes e diferentes abordagens sobre o assunto estudado. (Lakatos & Marconi, 2021)

O estudo de caso consiste em investigar de forma ampla, profunda e detalhada um fenômeno dentro de seu contexto real, permitindo compreender suas particularidades, causas, efeitos e relações, sem manipulação de variáveis. (Lakatos & Marconi, 2021)

A pesquisa tem caracter bibliográfico por fazer o uso de materiais como livros e artigos científicos para a interpretação do autor acerca do tema em causa. Tais materiais que são acessíveis ao público em geral de forma física ou via electrônica. Por fim, a pesquisa também é classificada como de estudo de caso, tendo em conta um envolvimento de

um estudo profundo e exaustivo de uma situação específica realizada dentro de um contexto real, que neste caso trata se da Faculdade de Engenharia.

- **Bases conceituais:**

Para se fazer a construção deste estudo foi feito a busca de bases conceituais, de tal forma que foram selecionados livros acadêmicos, artigos científicos relevantes e revisados por pares e normas técnicas relacionadas à Segurança da informação, Segurança Cibernetica, a dimensão do *Security Operation Center* e a utilização de SIEM.

De tal modo que os livros acadêmicos forneceram os conceitos fundamentais e definições teóricas sobre as áreas afins abordadas, enquanto os artigos científicos permitiram analisar pesquisas recentes consolidadas em diferentes ambientes, oferecendo subsídios para a comparação entre diferentes soluções de *SIEM/SOC*. Além disso, foram consultadas normas técnicas, que orientam as melhores práticas na gestão de segurança da informação e garantem conformidade com padrões internacionais, garantindo que a solução proposta esteja alinhada com requisitos de segurança, continuidade de negócios e governança de TI.

- **Cenario de pesquisa:**

A investigação foi realizada na FEUEM, responsável pela formação, pesquisa e extensão na área das engenharias, mas o autor concretamente esteve inserido no Departamento de Tecnologia de Informação e Comunicação (DTIC), responsável pela manutenção, gestão e suporte integral da área de Tecnologia da Informação. Tendo desemprenhado atividades nas subáreas de Servidores e *Data Centers*, Virtualização, Segurança da Informação, Suporte Técnico, Recuperação de dados e Continuidade de Negócio.

No cenário de pesquisa foram usados métodos de coleta de dados para auxiliar na busca de informações no ambiente de trabalho, permitindo obter uma compreensão mais precisa do funcionamento da infraestrutura e dos principais desafios enfrentados e eles foram os seguintes:

- Entrevistas: Sendo tais essenciais para obter informações detalhadas e aprofundadas;

- Observação participante: Com realizações que anotações ao interagir com sistemas e infraestrutura do local de estagio;
- Diário de Campo: Com base em situações observadas, o método ajudando a criação de observações objetivas de impressões subjetivas por parte do autor.

Para uma melhor definição dos participantes que compõem o estudo, foram estabelecidos critérios de amostragem que permitiram identificar adequadamente o público-alvo. A seleção dos participantes baseou-se em critérios de inclusão, definidos a partir das características necessárias para que os indivíduos fossem considerados aptos a integrar a pesquisa. Assim, foram incluídos Estudantes da Faculdade, Docentes e membros da área Administrativa, por apresentarem características metodológicas (os que com mais frequência acessam a rede) relevantes para o objetivo do estudo.

1.7 Motivação

A crescente informatização e melhoria da infraestrutura da Faculdade de Engenharia da Universidade Eduardo Mondlane (UEM) tem exposto sistemas acadêmicos, administrativos e científicos a riscos cibernéticos significativos. A Faculdade lida diariamente com dados sensíveis, sistemas interconectados, servidores e serviços digitais que requerem proteção constante. No entanto, a falta de uma estrutura para monitoramento e resposta a incidentes (de preferência a tempo real) pode deixar a instituição vulnerável a ataques, perdas de dados e interrupções nos serviços.

Iremos exemplificar a importancia com o estudo de caso: Violação de dados da Marriott *(Marriott Data Breach)* em 2018, uma das maiores redes de hotéis do mundo, expôs informações pessoais de centenas de milhões de clientes de vários países que fizeram reservas com a empresa.

A Marriott incorreu em quase US$ 30 milhões em despesas/custos totais de recuperação em decorrência da violação. Esse total inclui custos relacionados à investigação da causa da violação, à notificação dos clientes afetados, ao fornecimento a esses clientes de acesso por um ano a *software* de monitoramento de segurança, ao desenvolvimento de um call center internacional relacionado à violação e à implementação de medidas de segurança cibernética atualizadas para prevenir incidentes futuros.

E a empresa teve de parar de atender por uma semana isso adicionado aos custos incorridos do violação de dados, incrementando ainda mais os custos e quase colocou a empresa na falência.

Academicamente, o presente trabalho pretende produzir um conhecimento aplicado em cibersegurança em ambiente universitário propondo uma a aplicação de uma solução concreta sendo essa um Security Operation Center, que permitirá à faculdade adotar uma abordagem proactiva na gestão de segurança da informação, alinhando-se às boas práticas internacionais.

1.8 Estrutura do Trabalho

O presente Relatório encontra-se dividido em seis (6) capítulos, nomeadamente: Introdução, Revisão de Literatura, Caso de Estudo, Propsta de Solução, Discussão de Resultados, Conclusões e Recomendações, Referências Bibliográficas e por fim, Anexos e Apêndices.

- ✓ No capítulo 1 referente à Introdução, faz-se uma contextualização do tema, enuncia-se o problema que motivou a realização do trabalho, são identificadas e descritas as técnicas metodológicas usadas para atender aos objectivos traçados e apresenta-se a estrutura do trabalho.
- ✓ No capítulo 2 referente à Revisão de Literatura, são apresentados conceitos relacionados com o tema nomeadamente a segurança cibernética em infraestruturas, Incidentes de segurança, e por fim debruça-se em torno das plataformas SOC que serviram de referencial teórico para a realização da pesquisa.
- ✓ No capítulo 3 referente à Caso de Estudo, descreve-se o objeto de estudo, neste caso, a Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM), abordando sua infraestrutura atual, as funcionalidades existentes e as principais limitações identificadas;
- ✓ No capítulo 4 referente ao Proposta de Solução, neste faz-se uma análise de soluções com base em metricas, e escolhe se a melhor para resolver o referido problema.
- ✓ No capítulo 5 referente ao Discussão de Resultados, Apresenta-se a análise de literatura, no caso de estudo e na proposta de solução.
- ✓ No capítulo 6 referente à Conclusões e Recomendações, são apresentadas as conclusões resultantes da realização do trabalho e as recomendações ou planos para o futuro.
- ✓ Seguidamente as Referências Bibliográficas, são apresentadas as obras consultadas no âmbito da realização do trabalho.
- ✓ Seguidamente os Anexos, são apresentados os documentos complementares do trabalho.

2. Capítulo II – Revisão de Literatura

2.1 Segurança de Informação

De acordo com a norma ISO/IEC 27002 a Segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação;
Na sua nota 1 para a entrada continua dizendo: Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidas. (ISO/IEC, 2022)
Segundo (Stallings, 2023) a Segurança de Informação se apoia em 3 pilares, que são conceitos comumente chamados de tríade CID sendo estes:

- Confidencialidade: Preservar as restrições autorizadas ao acesso e à divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias. A perda de confidencialidade ocorre quando há divulgação não autorizada de informações.
- Integridade: Proteger contra a modificação ou destruição indevida de informações, incluindo garantir o não repúdio e a autenticidade das informações. A perda de integridade ocorre quando há modificação ou destruição não autorizada de informações.
- Disponibilidade: Garantir o acesso e o uso oportunos e confiáveis das informações. A perda de disponibilidade ocorre quando há interrupção do acesso ou do uso de informações ou de um sistema de informações.

É fundamental compreender que o principal objetivo da Segurança da Informação (*InfoSec*) consiste em proteger os sistemas de informação e todos os recursos a eles associados, considerados essenciais para o bom funcionamento das organizações.

Na sua escrita (Stallings, 2023) ainda aborda potenciais dificuldades ou cosntragimentos encontrados na Segurança de informação, com algumas razões tais como:

I. Ao desenvolver-se um mecanismo ou algoritmo de segurança específico, é sempre preciso considerar os potenciais ataques a esses recursos de segurança. Em muitos casos, ataques bem-sucedidos são projetados analisando o problema de uma maneira completamente diferente, explorando, portanto, uma vulnerabilidade inesperada no mecanismo.

II. Devido ao ponto acima citado, os procedimentos usados para fornecer determinados serviços são frequentemente contraintuitivos. Normalmente, um mecanismo de segurança é complexo e não é óbvio, a partir da descrição de um requisito específico, que medidas tão elaboradas sejam necessárias.

III. A segurança da informação e da rede é essencialmente uma batalha de inteligência entre um invasor que tenta encontrar brechas e o projetista ou administrador que tenta corrigi-las, sendo que a grande vantagem do invasor é que ele precisa encontrar apenas uma única vulnerabilidade, enquanto o projetista deve encontrar e eliminar todas as vulnerabilidades para alcançar a segurança perfeita.

2.2 Cibersegurança

Para (Stallings, 2023) Cibersegurança é a proteção da informação armazenada, transmitida e processada em um sistema interconectado de computadores, outros dispositivos digitais e dispositivos de rede e linhas de transmissão, incluindo a Internet. Agrupando politicas, mecanismos e práticas destinadas a proteger sistemas de informação, redes e dados contra ameaças e assegurando CID.

Cibersegurança é a prevenção de danos, proteção e restauração de computadores, sistemas de comunicação eletrônica, serviços de comunicação eletrônica, comunicação por fio e comunicação eletrônica, incluindo as informações neles contidas, para garantir sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio. (NIST, Estrutura de Gestão de Riscos para Sistemas de Informação e Organizações: Uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade, 2018)

No entendimento do autor cibersegurança envolve a protecção de informação em todo espaço cibernético, prevenção de ataques e uso de mecanismos adequados tais como, criptografia, os controles de acesso, autenticações, *firewalls*, protocolos seguros, gestão de risco, para a mitigação de riscos. A cibersegurança é fundamental para a protecção de organizações de todo porte garantindo que os seus ativos e dados permaneçam seguros, e para o trabalho em causa dada a natureza da instituição assegurando o CID para que os dados não sejam comprometidos.

2.3 Risco

Quando falamos de risco principalmente risco em relação a cibersegurança ou risco em temas como do presente trabalho da área de cibersegurança, é necessário usarmos como base definições como as do Organização Internacional para Padronização (ISO) ou Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) sendo que são fontes de normas reconhecidas internacionalmente para gestão de riscos e segurança.
A norma ISO 31000 define o risco como sendo, o Efeito da incerteza sobre os objetivos. Sendo que na sua nota 1 ele identifica que um efeito é um desvio do esperado, podendo ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.

De acordo com o *NIST* o risco é a medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento potencial, e normalmente é uma função de o impacto adverso, ou magnitude do dano, que surgiria se a circunstância ou evento ocorresse. (NIST, Estrutura de Gestão de Riscos para Sistemas de Informação e Organizações: Uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade, 2018)

Constatado pelo autor que enquanto o *NIST* foca-se na dimensão o magnitude do potencial dano, ao invés do *ISO* que foca-se no inesperado, independente de positivo ou não para caracterizar o risco.

2.3.1 Gestão de Risco

O programa e os processos de apoio visam gerir os riscos para as operações de organizações (incluindo missão, funções, imagem, reputação), ativos , indivíduos, outras organizações e a Nação, e incluem: estabelecer o contexto para atividades relacionadas a riscos; avaliar os riscos; responder aos riscos uma vez identificados; e monitorar os riscos ao longo do tempo. (NIST, Estrutura de Gestão de Riscos para Sistemas de Informação e Organizações: Uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade, 2018)

O ISO na sua norma 31000 define gestão de risco como sendo um conjunto de actividades coordenadas para dirigir e controlar uma organização em relação ao risco. (ISO, Gestão de riscos — Diretrizes, 2018)

Os objetivos da gestão de riscos podem ser derivados dos objetivos gerais da organização, e de suas atividades, tais sendo claramente definidos no início do processo de gestão de riscos em que devem também ser mensuráveis para que seja possível verificar seu alcance e para tal recomenda-se o uso de *KPIs* (indicadores-chave de desempenho.(ENISA, 2022)

Embora muitas atividades de gestão de riscos de cibersegurança se concentrem na prevenção de eventos negativos, elas também podem contribuir para o aproveitamento de oportunidades positivas. Ações para reduzir o risco de cibersegurança podem beneficiar uma organização de outras maneiras, como o aumento da receita (por exemplo, oferecendo inicialmente espaço excedente em suas instalações a um provedor de hospedagem comercial para hospedar seus próprios data centers e os de outras organizações, e posteriormente migrando um importante sistema do data center interno da organização para o provedor de hospedagem, a fim de reduzir os riscos de cibersegurança). (NIST, Cybersecurity Framework 2.0, 2024)

2.4 Plano de Continuidade de Negocio (PCN)

Plano de Continuidade de Negocio são informações documentadas que orientam uma organização a responder a uma interrupção e a retomar, recuperar e restaurar a entrega de produtos e serviços de acordo com seus objetivos de continuidade de negócios. (ISO, Segurança e resiliência — Sistemas de gestão de continuidade de negócios, 2019)

A continuidade operacional dos negócios, ou simplesmente continuidade de negócios, constitui um dos pilares fundamentais das organizações, pois envolve o planeamento e a implementação de estratégias para garantir a resiliência em situações adversas, como ataques, falhas tecnológicas ou crises organizacionais. Este conceito no âmbito institucional visa assegurar que as operações críticas sejam mantidas em funcionamento

ou, no pior dos cenários, que as atividades essenciais sejam restabelecidas de forma rápida e eficiente, minimizando assim os impactos negativos para a instituição.

Quando se fala de continuidade de negócios, (Munteanu, 2024) faz a análise de um ponto muito importante a ter em conta, sendo esse a resiliência digital que pode ser definido como a capacidade de uma organização garantir o preparo, responder e se recuperar de interrupções digitais, garantindo a continuidade das operações digitais, protegendo os ativos digitais e mantendo a integridade dos sistemas de informação e dos dados.

Ao ver do autor o plano de continuidade de negócios fornece uma estratégia para que exista resiliência nas organizações, garantindo a retomada dos serviços críticos após interrupções, o que é essencial não só para a maturidade das organizações mas também para a sua proteção contínua.

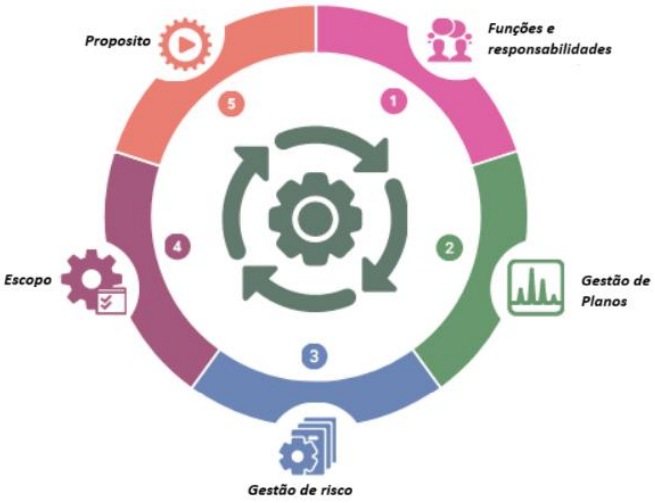

Figura 1: Diagrama de Plano de Continuidade de Negocios.

Fonte:Elaborada pelo autor

2.4.1 Tipos do Plano de Continuidade de Negocios

O PCN é aplicável a todas as áreas organizacionais, sendo este adaptado de acordo com as necessidades e particularidades de cada instituição. A sua implementação visa garantir que, em situações de interrupção ou falha operacional, as atividades essenciais possam ser restabelecidas de forma rápida e eficaz. Por exemplo, caso uma

empresa enfrente uma falha repentina no servidor imediatamente antes do lançamento de um produto estratégico, a existência de um modelo de continuidade de negócios permitirá que a equipa siga procedimentos previamente definidos para restaurar os sistemas críticos, comunicar-se com as partes interessadas e minimizar o tempo de inatividade, assegurando assim a continuidade dos processos e a mitigação dos impactos negativos sobre o negócio.

Os planos de continuidade devem abranger diferentes níveis de resposta, incluindo planos estratégicos, táticos e operacionais. (ISO, Segurança e resiliência — Sistemas de gestão de continuidade de negócios, 2019)

Podendo abranger diferentes abordagens, de acordo com a natureza e a complexidade das operações organizacionais, tendo os seguintes tipos:

I. Plano de Recuperação de Desastres (PRD);
II. Plano de Continuidade Operacional (PCO);
III. Plano de Gestão de Crises (PAC);
IV. Plano de Resposta a Incidentes (IRP);

Sendo sempre estes os citados como essenciais quando se aborda sobre continuidade de negócios.
Uma parte significativa do planeamento Continuidade Operacional e de Resposta a incidentes sob perspectiva de segurança é feita com propostas preventivas ou até de alguma forma preditivas que visam minimizar a probabilidade de um evento inesperado recair sobre nós.

2.5 Centro de Segurança de Informação (SOC)

Para que a segurança de uma empresa esteja em um nível satisfatório, existem modelos indicados para guiar a estruturação e a maturidade da segurança da informação, como definidos em livros e normas internacionais citadas pelo autor**,** que auxiliam na ideia de Segurança de Informação.

O *SOC* é composto por analistas, operadores e especialistas no assunto que monitoram endpoints de segurança, sensores, infraestrutura de TI, aplicativos e serviços. Eles

utilizam diversas tecnologias e processos, conforme as políticas organizacionais invocadas, para impedir o uso indevido da infraestrutura de TI e a violação de políticas, prevenindo e detectando ameaças e ataques cibernéticos, violações de segurança e abusos online, além de responder a incidentes cibernéticos. (Shahjee & Ware, 2022)

É a parte da organização que visa por proteger os ativos críticos da empresa, monitorando continuamente as ameaças emergentes, coletando eventos de segurança relevantes, analisando e priorizando esses eventos e respondendo a incidentes de segurança. Ela é uma uma combinação de pessoas, processos e tecnologia que protege os sistemas de informação de uma organização através de: projeto e configuração proativos, monitoramento contínuo do estado do sistema, detecção de ações não intencionais ou estados indesejáveis e minimização de danos causados por efeitos indesejados. (Rehman, 2021)

Ao ver do autor todas as referencias enfatizam a importância de pessoas, processos e tecnologias,também focando que um *SOC* é responsável pela deteção, monitoria, prevenção, investigação e resposta a incidentes de segurança**,** com uma atuação fortemente baseada na colaboração e coordenação entre as equipas**.**

Figura 2: Security Operstion Center.

Fonte:Elaborada pelo Autor

2.5.1 Funções do SOC

De acordo com (Baddi , Almaiah, Almomani, & Maleh, 2025), para fornecer conhecimentos sobre as funções necessárias no projeto do modelo operacional, descrevemos as funções principais mais comuns encontradas em *SOCs*. E é importante ressaltar que as funções podem ser adaptadas, tendo assim nomes diferentes e podem ser otimizadas para maior eficiência. A seguir, apresentamos as funções típicas de um SOC.

- Gestão de Vulnerabilidades;
- Detecção de Ameaças;
- Análise de Incidentes;
- Resposta a Incidentes;
- Prevenção de Incidentes;

Rehman além das principais funções lista algumas adicionais com menção à:

1. A análise os dados disponíveis e posterior criação/classificação de alertas com base no risco para a organização; e
2. Agregação de informações sobre agentes de ameaças, métodos de ataque e indicadores de comprometimento. (Rehman, 2021)

Na visão do autor as funções do *Security Operation Center (SOC)*, incluem a detecção proativa e rápida de ameaças, permitindo que a organização tenham uma ideia plena do que esperar de um *SOC* ao se propror a sua implementação. Dessa forma, garantindo que o *SOC* mantenha uma posição estratégica de prevenção e proteção, reduzindo riscos na organização, mas não só, também fortalecendo a resiliência frente a ataques e incidentes cibernéticos.

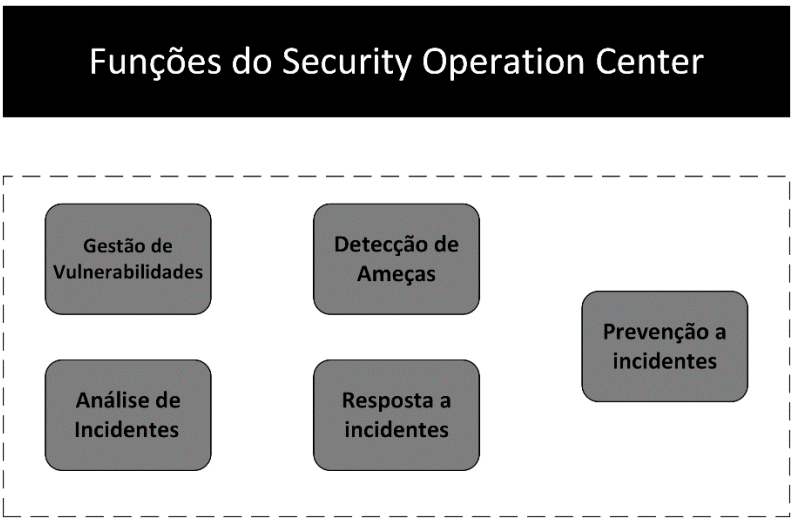

Figura 3: Funções do SOC.

Fonte: Adaptado de Baddi , Almaiah, Almomani, & Maleh (2025)

2.5.2 Tipos de SOC

Na avaliação do autor, a escolha do modelo de *Security Operation Center (SOC)* a ser implementado deve considerar cuidadosamente as necessidades específicas da organização, sua infraestrutura para não correr risco de escolher o tipo de *SOC* incorrecto para a organização, ou que não se alinhe com objetivos estratégicos relacionados à segurança da informação e cibernética que a mesma deseja atingir no momento. Deste modo, considera-se essencial examinar os vários tipos de *SOC* existentes.

2.5.2.1 SOC Interno

Segundo (Basta, Basta, Anwar, & Essar, 2025), o SOC interno é totalmente gerido pela própria organização, com equipamentos, pessoal e processos localizados fisicamente dentro da empresa. Este modelo permite maior controle sobre dados sensíveis, integração directa com os sistemas internos e personalização de processos de segurança conforme as necessidades da organização.

- **Localização**

  A implementação de um *SOC* interno requer a disponibilização de uma infraestrutura dedicada, incluindo uma sala fisicamente localizada nas instalações da organização, equipada com todos os hardwares, softwares e

ferramentas de monitorização necessários. Essa configuração demanda um planeamento prévio detalhado e pode acarretar implicações financeiras significativas, uma vez que envolve investimentos em equipamentos, manutenção e pessoal especializado, garantindo, contudo, maior controle e segurança sobre os dados e sistemas críticos da organização.

- **Custos e Recursos**

  A implementação e manutenção destes envolvem custos elevados, licenças de software e infraestrutura robusta. Esse modelo exige um orçamento significativo e a disponibilização de recursos que podem exceder a capacidade de muitas pequenas e médias organizações. Além disso, é necessário investir em pessoal qualificado, ferramentas adequadas, procedimentos estruturados e inteligência de ameaças, de modo a garantir a eficácia do *SOC* na detecção, monitoria e resposta a incidentes de segurança.

2.5.2.2 SOC Gerido

Um SOC gerido ou como denominado pelo autor (Rehman, 2021) um "*SOC* Terciarizado" é aquele que tem como seu principal objetivo aproveitar a experiência dos provedores de serviços, para beneficiar-se de seus processos já estabelecidos e obter acesso a informações contínuas sobre ameaças.

No entendimento do autor, é bastante comum e normal que pequenas e médias organizações não realizem investimentos completos em infraestruturas de grande porte, seja por não reconhecerem a criticidade das suas informações ou por não possuírem capacidade financeira e estrutural para implementar. Porém tal limitação pode comprometer a proteção dos activos informacionais e aumentar a vulnerabilidade da organização a incidentes de segurança e ciberataques, o que torna este tipo de SOC mesmo que problemático a longo prazo, uma solução para empresas que muito pouco investimento.

Um *SOC* Gerido é operado por um provedor externo especializado em segurança, que fornece monitorização contínua, análise de eventos e resposta a incidentes. (Stallings, 2023)

Deste modo é possível assegurar segurança e monitoria mesmo que no mesmo na ausência de uma infraestrutura completamente capaz de garantir a proteção **“**On Premise**”**

2.5.2.3 SOC Virtual ou Híbrido

Um *SOC* virtual como O *SOC* virtual combina recursos internos e externos, permitindo flexibilidade operacional. Parte da monitoria e análise é realizada internamente, enquanto serviços especializados são terceirizados, garantindo escalabilidade e acesso a tecnologias avançadas sem a necessidade de investimento integral em infraestrutura própria. (Muniz, McIntyre, & AlFardan)

Este modelo baseado em nuvem utiliza tecnologias e equipes de segurança remotas, em vez de uma infraestrutura física centralizada, para monitorar, detectar e responder a ameaças cibernéticas. Esse modelo oferece maior flexibilidade e custo-benefício, sendo adequado para organizações que necessitam de uma abordagem distribuída e escalável. A utilização da nuvem permite hospedar ferramentas e plataformas de segurança, como sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM), enquanto profissionais de segurança operam de locais geograficamente distribuídos, promovendo descentralização das operações, eficiência operacional e potencial economia de recursos.

2.5.2.4 SOC Free, Commercial, Open sorce

É importante mencionar 3 tipos de *SOC*, porém estes ligados a sua forma de aquisição e estes são o *SOC* Free, *SOC* Comercial e *SOC* Open Source.

O *SOC* Free caracteriza-se pela utilização de ferramentas gratuitas, geralmente disponibilizadas por comunidades de segurança ou fornecedores em versão limitada. Embora apresente restrições em funcionalidades avançadas, este modelo é uma alternativa viável para pequenas organizações ou instituições em fase inicial de implementação de segurança, permitindo-lhes adquirir experiência prática em monitorização e resposta a incidentes com baixo custo operacional. (Shahjee & Ware, 2022)

O SOC Comercial, por sua vez, é composto por soluções proprietárias e ferramentas licenciadas, fornecidas por grandes empresas de tecnologia e segurança. (Basta, Basta, Anwar, & Essar, 2025) Este modelo oferece maior nível de automação, suporte técnico

especializado e integração com outras plataformas corporativas, o que o torna mais adequado para organizações de médio e grande porte que exigem elevada confiabilidade e conformidade regulatória. Contudo, os custos de aquisição e manutenção podem ser significativamente elevados.

Já o *SOC* Open Source baseia-se em soluções de código aberto, desenvolvidas e mantidas por comunidades colaborativas. Esse modelo permite personalização, flexibilidade e transparência, além de reduzir custos de licenciamento. No entanto, requer equipes técnicas qualificadas para instalação, configuração e atualização contínua, além de maior esforço na integração das diferentes ferramentas que o compõem, como o Wazuh, TheHive, OSSIM e ELK Stack.. (Basta, Basta, Anwar, & Essar, 2025)

Abaixo podemos mostrar a tabela comparativa entre as soluções *SIEM/SOC* Open-Source disponíveis no mercado

Parametro	**Wazuh**	**OSSIM**	**SIEMonster**
Regras de Correlação	Bem implementado	Basica implementação	Basica implementação
Autenticação do usuário	Basica implementação	Basica implementação	Bem implementado
Tolerância a falhas	Bem implementado	Mal implementado	Mal implementado
Escalabilidade	Basica implementação	Não implementado	Não implementado
Visualização	Bem implementado	Bem implementado	Bem implementado
Suporte da Comunidade	Bom	Sem suporte (Descontinuiado)	Bom

Tabela 1: Comparações de SIEM/SOC Open-Source.

Fonte: Adaptado de Manzoor, Waleed, Jamali & Masood (2024)

2.5.3 Pilares do SOC

À medida que as ameaças no ciberespaço evoluem em sofisticação, tornando-se mais complexas e difíceis de detectar, os *SOCs* devem adaptar correspondentemente suas próprias capacidades e funções, refinando seus pilares estabelecidos.

Os pilares do *SOC* constituem um conjunto central de princípios orientadores que norteiam tanto o estabelecimento quanto o funcionamento de um *SOC*. Esses pilares fundamentais visam garantir que o *SOC* seja capaz de operar de forma eficiente, eficaz e de maneira a oferecer proteção robusta contra as ameaças cibernéticas contemporâneas. (Basta, Basta, Anwar, & Essar, 2025)

Os três (3) fundamentais pilares incluem:

Pessoas: analistas, engenheiros, gestores e peritos em resposta a incidentes;

Processos: políticas, procedimentos e fluxos de comunicação; e

Tecnologia: sistemas SIEM, IDS/IPS, firewalls, plataformas de automação e análise.

Os três pilares são fundamentais para assegurar a eficácia dos princípios e mecanismos de governança, melhor gestão de risco,e a priorização de detecção ameaças de acordo com as necessidades e objetivos do negócio.

2.5.4 Ciclo de Vida e Fases de implementação do SOC

Conforme Rehman e as diretrizes do NIST, o ciclo de um SOC abrangem 6 fases clássicas que ditam diretrizes de gerenciamento de incidentes, tais são:

- Planeamento: Aqui define-se a missão do *SOC*, o escopo, orçamento, aprovações executivas, objetivos de negócio, justificativas;
- Design: Nesta fase define-se a arquitetura do *SOC*, escolha de tecnologias, fontes de logs, estrutura da equipe, processos, governança, integração com TI e outras áreas;
- Implementação: Nesta fase ocorre a implantação efetiva das soluções na infraestrutura, tais como: *SIEM, IDS/IPS*, configuração de alertas, *Playbooks* de resposta, integração de logs, e por fim feitos os devidos testes;

- Operação: Operação diária, monitoramento 24/7, gestão de alertas, investigação, resposta a incidentes, gestão de vulnerabilidades, relatórios, manutenção da infraestrutura e processos;
- Melhorias: A última fase, em que ocorre o ajuste e se afina as detecções, automatizar tarefas repetitivas, ampliar cobertura, revisar processos, melhorar operações baseado nas lições aprendidas, incorporar novas ameaças, evoluir o SOC conforme a maturidade.

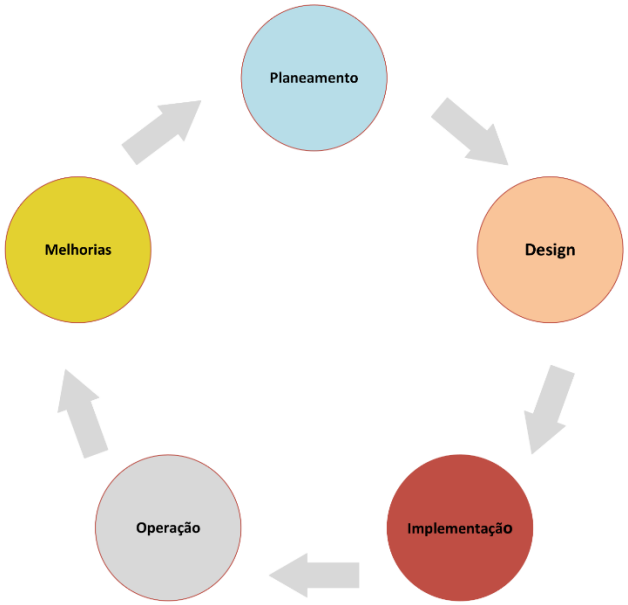

Figura 4: Ciclo de Vida do SOC.

Fonte: Adaptado de Rehman (2021)

Conceitualmente, deve-se sempre ter em mente as diferentes fases da iniciativa geral do SOC, tas fazes englobam as primeiras 4 (quatro) do ciclo de vida do SOC nomeadamente: Planeamento, *Design*, Implementação e Operação. Normalmente, as operações do *SOC* começam quando a construção é concluída e o *SOC* é entregue à equipe de operações em estado estável.

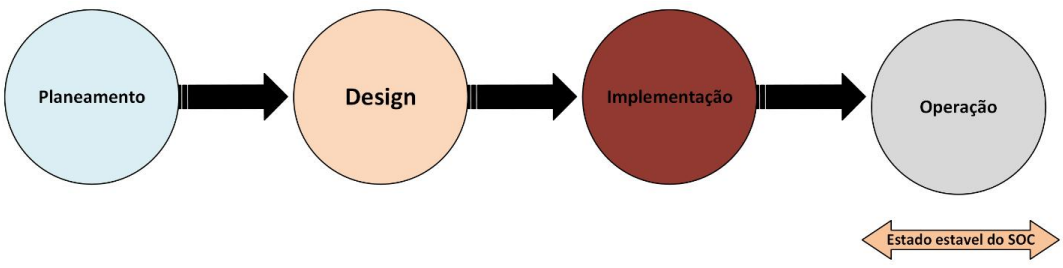

Figura 5: Fases de Implemetação de um SOC.

Fonte: Adaptado de Rehman (2021)

2.5.5 Arquitetura

A Arquitectura de um *SOC* é construído em torno de vários módulos principais distintos: geradores de eventos, coletores de eventos, banco de dados de mensagens, mecanismos de análise e software de gerenciamento de reações. O principal problema encontrado na construção de um *SOC* é a integração de todos esses módulos, geralmente construídos como partes autônomas, ao mesmo tempo em que garantem a disponibilidade, a integridade e a segurança dos dados e seus canais de transmissão. (Shahjee & Ware, 2022)

- Geradores de eventos: responsáveis pela criação e emissão de registros (logs) provenientes de diversos dispositivos e sistemas, como firewalls, servidores, roteadores e aplicações;
- Coletores de eventos: encarregados de agregar, normalizar e transmitir os eventos capturados pelos geradores para o sistema central do *SOC*;
- Banco de dados de mensagens: atua como o repositório central de armazenamento dos eventos coletados, garantindo a integridade, disponibilidade e rastreabilidade dos dados;
- Mecanismos de análise: constituem o núcleo inteligente do *SOC*, responsável por correlacionar eventos, identificar padrões suspeitos e gerar alertas de segurança;
- Software de gerenciamento de reações: é o módulo destinado à coordenação e execução das ações de resposta a incidentes, permitindo automatizar procedimentos operacionais (*playbooks*) e atribuir tarefas às equipas de segurança.

O autor mostra um modelo de arquitetura que vai de acordo com partes descritas anteriormente. No entanto, além dos aspectos puramente técnicos envolvidos em tal implementação, é necessário considerar a supervisão de uma infraestrutura de TI como um projeto operacional completo.

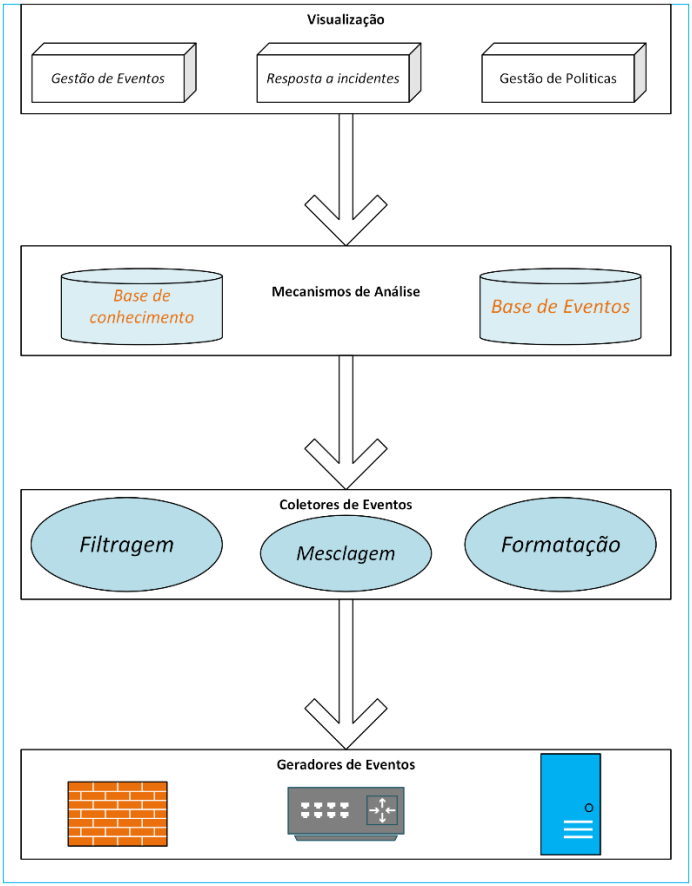

Figura 6: Arquitetura do SOC.

Fonte: Adaptado de Shahjee & Ware (2022)

2.5.6 Ferramentas

Proteger a informação vital e garantir que esta esteja sempre acessível devem fazer parte de um dos maiores desafios de qualquer organização. Um *SOC* é constituído pelas ferramentas de monitoria que o compõem. Usamos o termo ferramenta para nos referirmos ao conjunto de soluções tecnológicas integradas que podem ser implementadas em simultâneo, com o objetivo de fortalecer as camadas de segurança da organização. Tais ferramentas contribuem para uma monitoria contínua e eficaz dos sistemas, promovendo uma tomada de decisão mais informada e analítica no âmbito da gestão da segurança da informação. (Whitman & Mattord, 2021)

Tais ferramentas normalmente são:

2.5.6.1 SIEM (Security Information and Event Management)

O SIEM que significa “Gestão de Segurança da Informação e Eventos”, Ele é o sistema central de um *SOC* representa a combinação entre a gestão de informações de

segurança e a gestão de eventos de segurança, proporcionando uma visão unificada e abrangente dos potenciais riscos que podem afetar uma a organização. Facilitando a detecção de anomalias, o cumprimento de requisitos regulamentares e a resposta eficiente a incidentes.

Estas soluções realizam a gestão centralizada de logs, geração automática de alertas, monitorização em tempo real e correlação de eventos, permitindo identificar comportamentos suspeitos e padrões de ataque. Além disso, possibilitam o rastreio e o registro detalhado de dados de segurança para fins de conformidade e auditoria, integrando ainda recursos de análise de comportamento de utilizadores e entidades (*UEBA*), que aprimoram a capacidade de deteção proativa de ameaças internas e externas.

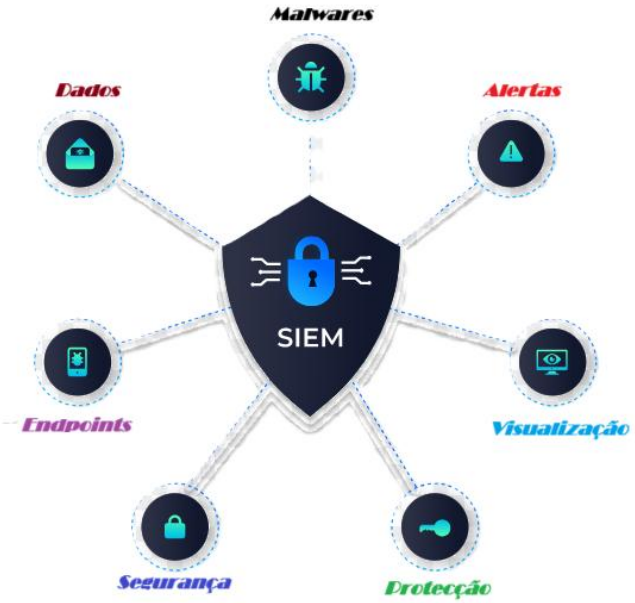

Figura 7:Security Information Event Managment.

Fonte: Elaborado pelo autor

As soluções de *SIEM* são o núcleo de um *SOC*, desempenham um papel crucial nos *SOCs* modernos sendo responsáveis por coletar, correlacionar e analisar eventos de segurança provenientes de diversas fontes, como *firewalls*, *antivírus*, IDS/IPS e sistemas operacionais para fortalecer a segurança. (Basta, Basta, Anwar, & Essar, 2025)

O surgimento do conceito *SIEM* surge a partir de dois que a bastante eram abordados:

- **Plataforma SEM - Security Event Management:**

As plataformas SIM centralizam e analisam registros de segurança, permitindo compreender tendências, uma análise histórica de logs, gerar relatórios e apoiar auditorias de conformidade. (Manzoor, Waleed, Jamali, & Masood, 2024)

- **Plataforma SIM – Security Information Management:**

O SEM fornece visibilidade em tempo real dos eventos de segurança concentra-se no monitoramento em tempo real de eventos de segurança, realizando correlação, alerta e resposta imediata a incidentes. (Manzoor, Waleed, Jamali, & Masood, 2024)

Existem varias variações na estrutura de uma plataforma *SIEM*, com componentes específicos adicionais, contudo um *SIEM* na sua forma mais simples pode ser dividido em cinco (5) partes como pode ser visto na figura abaixo.

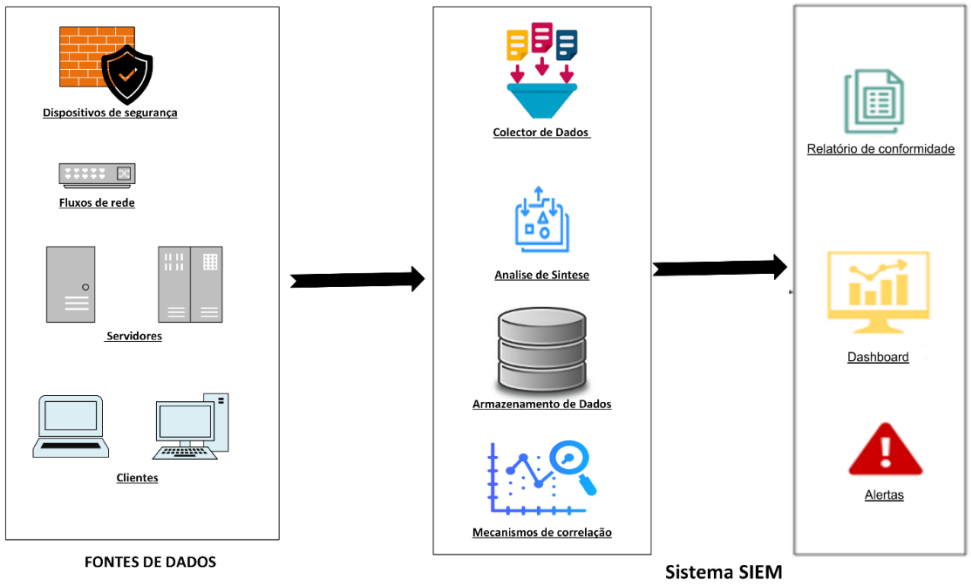

Figura 8: Arquitetura SIEM.

Fonte: Adaptado de Manzoor, Waleed, Jamali & Masood (2024)

E estas são: *Data sources, Data collection and normalization, Data storage, Correlation engine, e Dashboard, reporting and alerting.*

- Soluções de plataformas SIEM

A plataforma Gartner é pioneira na área de análises, actuando ou seja fazendo um *review* de diversas soluções de TI disponíveis no mercado, tudo isso disponível na sua

plataforma. Os seus Quadrantes Magicos como são chamados, são considerados umas das principais fontes de informação para as organizações.

Figura 9: Quadrante Magico de Gartner.

Fonte: Gartner (2024)

Existe a classificação do quadrante Magico feito pela plataforma Gartner que pode se dispor da seguinte forma:

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

Tabela 2: Interpretação do quadrante Mágico da Gartner.

Fonte: Elaborado pelo autor

2.5.6.2 IDS/IPS (Intrusion Detection and Prevention Systems)

Os *IDS/IPS* são projetados para detetar e prevenir atividades suspeitas na rede. O IDS atua de forma passiva, identificando e reportando anomalias, enquanto o IPS atua de forma proativa, bloqueando o tráfego malicioso em tempo real.

A detecção de intrusão é o processo de monitorar o tráfego de sua rede e analisá-lo à busca de sinais de possíveis intrusões, como tentativas de exploração e incidentes que possam ser ameaças iminentes à sua rede. (Stallings, 2023) Temos de olhar para as suas incidências de alertas sabendo que existem quatro (4) tipos de alertas IDS/IPS a ter em conta:

Resultado do Teste	Se evento A ocorrer	Se evento A não ocorrer
Teste indica “A”	Verdadeiro Positivo	Falso Positivo
Teste indica “Não A”	Falso Negativo	Verdadeiro Negativo

Tabela 3: Tipologias de Alerta IDS/IPS.

Fonte: Adaptado de Stallings (2023)

– Verdadeiro Positivo:

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

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

– Falso Positivo:

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

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

E alguns exemplos de sistemas de deteção e prevenção de intrusões incluem soluções como: Snort, Suricata, Spunk, e Zeek.

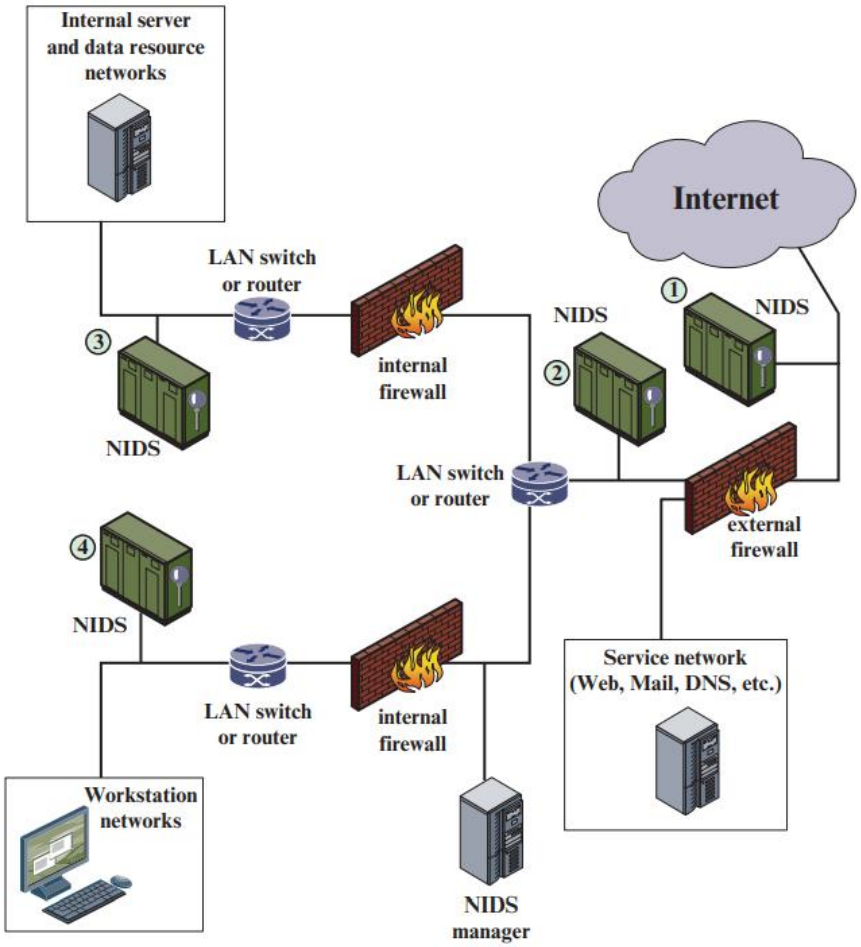

Figura 10: Network-Based Intrusion Detection Systems.

Fonte: Stallings (2023)

2.5.6.3 SOAR (Security Orchestration, Automation and Response)

Security Orchestration, Automation, and Response (SOAR) é um termo comum que se refere a tecnologias que permitem às operações de segurança coletar e analisar informações usando recursos humanos e de máquinas, além de automatizar fluxos de trabalho digitais para responder a incidentes de forma mais eficiente e eficaz. As ferramentas visam automatizar tarefas repetitivas e orquestrar respostas a incidentes, e elas integram diversas tecnologias de segurança, reduzindo o tempo de reação e aumentando a eficiência das equipes do SOC. (Mughal, 2023)

Entre os principais SOAR utilizados atualmente destacam-se:

- TheHive;
- Cortex XSOAR;
- Splunk Phantom.

2.5.6.4 Ferramentas de gestão de vulnerabilidades

Estas são essenciais para identificar, priorizar e corrigir falhas de segurança em sistemas e aplicações, escaneando automaticamente activos digitais para identificar vulnerabilidades de segurança e, em seguida, fornecer informações para priorizar e abordar esses riscos. Tem como principais funções: a identificação de vulnerabilidades, avaliação e priorização de riscos e orientação para remediação, garantindo que as organizações possam proteger proactivamente redes, aplicativos e bancos de dados contra ameaças cibernéticas.

Alguns exemplos incluem:

- OpenVAS;
- Nessus;
- Qualys.

2.5.6.5 Detecção e Resposta de Endpoint

De acordo com Stallings, as soluções *EDR* monitoram continuamente os dispositivos terminais (endpoints) em busca de comportamentos suspeitos, fornecendo visibilidade detalhada e resposta automatizada a incidentes em estações de trabalho e servidores. Funciona com recurso a análise de dados para a detecção de comportamentos suspeitos, bloqueando atividades maliciosas e auxiliando na investigação e correção de ataques. O *EDR* oferece uma protecção mais avançada que o antivírus comum, combinando monitoramento contínuo com acções de respostas automatizadas. (Stallings, 2023)

2.5.7 Papéis desempenhados no SOC

Rehman e Baddi são unânimes em definir os papéis desemprenhados no Centro de Operações de Segurança sendo composto por uma estrutura organizacional multidisciplinar, na qual diferentes funções e responsabilidades são atribuídas para assegurar uma monitorização contínua, detecção, resposta e mitigação de incidentes de segurança.

Sendo estes papéis os seguintes:

- Analista de SOC Nível 1 (Monitoria e Triagem)

  Responsável pela monitoria em tempo real dos alertas e eventos de segurança. Actua na identificação inicial de incidentes, triagem de falsos positivos e classificação da gravidade das ocorrências.
- Analista de SOC Nível 2 (Investigação e Resposta a Incidentes)

  Responsável pela análise aprofundada dos incidentes, investigando a origem, extensão e impacto das ameaças. Este profissional utiliza ferramentas como *SIEM, IDS/IPS e EDR* para correlacionar eventos, validar ataques e coordenar respostas técnicas; (Rehman, 2021)
- Analista de SOC Nível 3 (Inteligência e Engenharia de Segurança)

  É composto por profissionais especializados em análise de ameaças avançadas e engenharia de segurança. Eles desenvolvem regras de correlação, scripts de automação, e realizam avaliações proativas de vulnerabilidades;
- Gestor do SOC

  Responsável por coordenar as actividades da equipa, definir políticas operacionais, gerir recursos humanos e tecnológicos, assegurar a conformidade com normas e seus regulamentos, no geral tratando da estratégia e processos do *SOC*;
- Engenheiro de Segurança

  Responsável pela implementação e manutenção da infraestrutura tecnológica do SOC, além do *design* e ánalise de ameaças. (Baddi , Almaiah, Almomani, & Maleh, 2025)

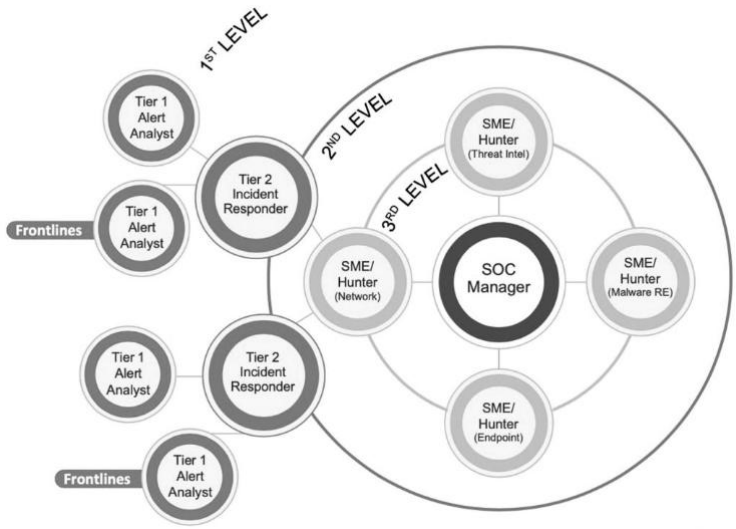

Figura 11: Niveis de Papeis desempenhados no SOC.

Fonte: Baddi, Almaiah, Almomani & Maleh (2025)

2.5.8 Metricas do SOC

Métricas eficazes são usadas para medir o progresso. No caso do *SOC*, as métricas demonstram o valor dos investimentos em *SOC*.Com base em autores contemporanios relevantes como Basta, Rehman e Mughal A categoria de métricas escolhida é a de desempenho, pois medir o desempenho do *SOC* é fundamental para compreender a eficácia das operações do *SOC* e identificar áreas de melhoria. A seguir, estão as principais métricas que podem ser usadas para medir o desempenho do *SOC*:

- *Mean Time to Detect (MTTD):* o tempo médio entre a invasão inicial de um atacante e o tempo que a equipe do *SOC* leva para detectar um incidente de segurança. Um *MTTD* menor indica que a equipe do *SOC* é mais eficiente na detecção e resposta a incidentes.
- *Mean Time to Respond (MTTR):* O *MTTR* mede o tempo que a equipe do *SOC* leva para responder e resolver um incidente de segurança. Um *MTTR* menor indica que a equipe do SOC é mais eficiente na resolução de incidentes e na redução do impacto de violações de segurança.
- *False Positive Rate*: O false positive rate ede o número de alertas gerados pela equipe do *SOC* que não correspondem a incidentes de segurança reais. Uma taxa de falsos positivos mais alta pode indicar que a equipe do *SOC* está desperdiçando recursos com alarmes falsos e não se concentrando em ameaças reais.
- *Alert Volume*: O volume de dados de eventos agregados de dispositivos de rede, endpoints, plataformas em nuvem e aplicativos de negócios permite avaliar as lacunas de cobertura onde o registro adicional de logs deve ser ativado.

2.6 Playbooks

Para que uma organização opere com um alto nível de segurança e integridade, é essencial que todos os sectores e equipas cooperem de maneira coordenada, assegurando que todas as etapas de segurança sejam seguidas de forma rigorosa e eficiente. Nesse contexto, faz-se uso de *playbooks*, que funcionam como guias documentados e continuamente actualizados, descrevendo procedimentos e fornecendo instruções detalhadas e passo a passo. Esses instrumentos permitem que as equipes de

segurança detectem, respondam e se recuperem de incidentes de forma estruturada e eficaz, fortalecendo a postura de segurança da organização e garantindo a continuidade das operações.

Esses guias (*Playbooks*) operacionais permitem automatizar tarefas repetitivas, reduzir o tempo médio de resposta e promover a transferência de conhecimento entre analistas. Além disso, os *playbooks* contribuem para a maturidade operacional do *SOC*, ao viabilizar a melhoria contínua e a adaptação constante às novas ameaças cibernéticas. (Whitman & Mattord, 2021)

3. Capítulo III – Caso de Estudo

3.1 Faculdade De Engenharia Da Universidade Eduardo Mondlane (FEUEM)

A Faculdade de Engenharia é uma unidade orgânica da Universidade Eduardo Mondlane, com autonomia pedagógica e científica no âmbito dos cursos que leciona, bem como de autonomia administrativa, patrimonial e financeira relativamente aos seus próprios recursos, dentro dos limites legais estabelecidos. A Faculdade de Engenharia usufrui ainda de autonomia regulamentar e disciplinar, igualmente enquadrada nos parâmetros legais vigentes.

A Faculdade de Engenharia foi fundada em 1962 com uma estrutura de chefia centralizada, onde cada curso estava associado a um Departamento específico, oferecendo inicialmente quatro cursos: Engenharia Civil, Engenharia Electrotécnica, Engenharia Mecânica e Engenharia Química, com duração de seis anos (três anos dedicados a matérias gerais-básicas e três anos a disciplinas específicas de engenharia, incluindo gestão). Após a Independência, os departamentos assumiram o estatuto de Faculdade, adoptando uma gestão não centralizada mas com coordenação inter-faculdades, estrutura que se manteve até 1980, quando se regressou ao modelo inicial de 1962. Em 1970, a duração dos cursos foi reduzida para cinco anos (com dois anos de formação geral-básica), as disciplinas passaram a ser semestrais (em vez de anuais) e as horas de ensino foram aumentadas, tendo sido introduzidos nesse mesmo ano os cursos de Engenharia de Minas e Engenharia Metalúrgica, os quais, no entanto, não se mantiveram devido à sua longa duração (cinco e oito anos, respectivamente).

Actualmente, a Faculdade de Engenharia é composta por cinco departamentos académicos, nomeadamente Departamento de:

- Engenharia Civil (DECI);
- Engenharia Electrotécnica (DEEL);
- Engenharia Mecânica (DEMA);
- Engenharia Química (DEQUI);
- Cadeiras Gerais (DCG);

Cinco Departamentos não Académicos:

- Departamento de Património e Manutenção (DPM);
- Departamento do Registo Académico (DRA);
- Departamento de Tecnologias de Informação e Comunicação (DTIC);
- Departamento de Administração e Finanças (DAF);
- Departamento de Informação e Biblioteca (DIB);

3.1.1 Visão, Missão, Valores

3.1.1.1 Visão

A Faculdade de Engenharia tem como Visão:

- Sermos uma referência nacional, regional e internacional na formação, treinamento e investigação em engenharia.

A Faculdade de Engenharia orienta a sua actividade para os seguintes objectivos gerais:

- Providenciar uma educação padrão à sociedade e conhecimento científico internacional;
- Providenciar compreensão da importância da tecnologia em áreas como economia, ecologia e sociedade no geral.

3.1.1.2 Missão

A Faculdade de Engenharia tem como Missão:

- Desenvolver competências e conhecimentos científicos na área de engenharia e contribuir na formação do homem.

3.1.1.3 Valores

A Faculdade de Engenharia tem como pilares da sua atuação os seguintes valores:

- Liberdade Académica;
- Ética e Imparcialidade;
- Responsabilidade;
- Confiança;
- Proatividade;
- Colegialidade;
- Engajamento Social e Comunitário;
- Autonomia Institucional.

3.1.2 Estrutura orgânica

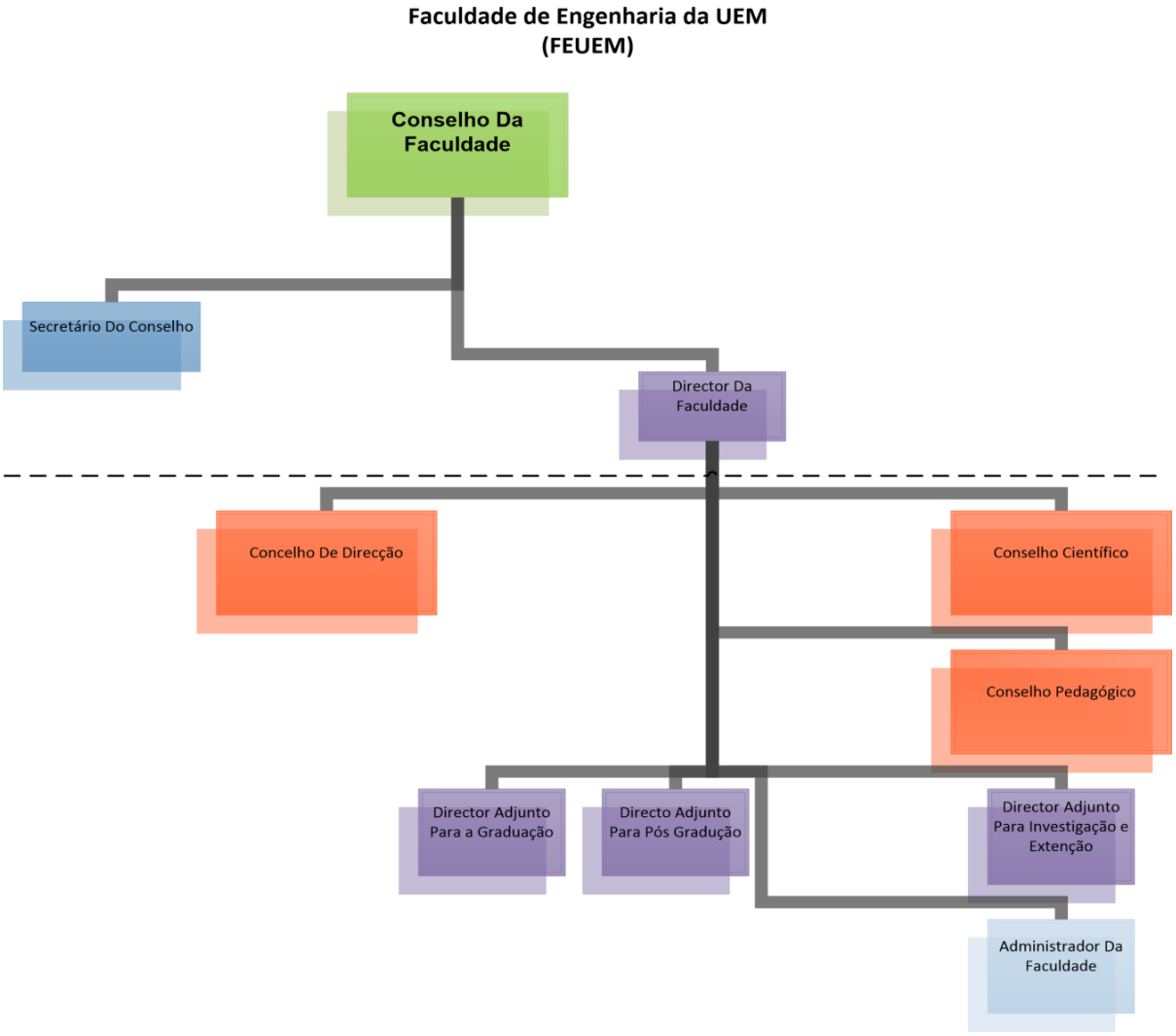

Figura 12: Organograma da Faculdade de Engenharia.

Fonte: DTIC

3.2 Actividades realizadas pelo autor durante o estágio

Durante o período do estágio, o autor na instituição foi colocado no sector de TICs, concretamente na área de Infraestrutura de TI, tendo trabalhado com um equipe relativamente pequena porém dinâmica, colaborativa e disciplinar dada a natureza compacta do sector de momento. O autor tendo adquirido conhecimentos através da troca de conhecimentos e experiências em áreas técnica e interpessoal. Foram realizadas actividades tais como apresentadas na tabela abaixo:

Actividades realizadas	Seu Impacto	Competências adquiridas
1. Realizar verificação completa de antivírus nos computadores da instituição; 2. Bloquear ou desativar contas de utilizadores inativos ou não autorizados	Reduzir riscos de infecções, e melhorar a protecção contra malwares. Aumentar a conformidade com políticas de segurança, e diminuição das *Shadow accounts*	Utilização de ferramentas antivirus, boas práticas de higiene digital, e Manutenção preventiva de TI
Realizar suporte técnico ao sector de estágio e a Administração	Garantir o funcionamento dos sistemas e softwares de forma ininterrupta, para reduzir o tempo de indisponibilidade dos serviços e melhorar a produtividade	Diagnóstico e resolução de problemas de suporte técnico, desenvolvimento de comunicação profissional e interpessoal, e prática de Conhecimento sobre Hardware e Software
Executar cópias de segurança e procedimentos de recuperação de dados	Assegurar a Continuidade de Negócios, garantindo a integridade e disponibilidade dos dados no caso de falhas e ataques.	Prática na gestão de cópias de segurança e recuperação de na dados, suas boas práticas, e ferramentas.
Administrar servidores e sistemas operativos de servidores	Testar seu desemprenho, verificar sua configuração e dos seus serviços.	Configuração de Serviços de Rede com foco no Windows Server (ex: DNS, DHCP, Active Directory, WSUS)
Replicação da infraestrutura em ambientes virtuais para análise de segurança	Identificar fragilidades na segurança, e estudar soluções para as mesmas.	Aplicação dos conceitos de Virtualização, e Análise de vulnerabilidades

Tabela 4: Mapa de atividades realizadas pelo autor.

Fonte: Elaborada pelo autor

No decorrer das atividades, o autor constactou as seguintes dificuldades e lacunas, sendo eles os seguintes:

1. A verificação de fragilidades em relação aos servidores, verificando a sua não adequada configuração, essas assim criando, falhas, perdas de conexão e mais importante, vulnerabilidades de segurança;
2. A falta de uso eficiente e devida integração de *firewalls* a rede da FEUEM, gerando dessa forma, um elevado nível de exposição de segurança da rede e seus usuários;
3. Com base nos dados coletados através das entrevistas, o autor constatou, em contacto com a equipa da DTIC, que a falta de controles adequados sobre usuários e dispositivos na rede representa um risco significativo, comprometendo de forma acentuada a segurança das informações críticas da instituição.

O estágio foi fundamental na sua prática, não só para a aplicação teórica do conhecimento, mas para a identificação de lacunas presentes no local de estagio, concretamente a Faculdade de Engenharias, principalmente em questão a segurança cibernética devido a problemas acima citados como o exemplo da ausência do uso eficaz de *firewalls*, controle de acesso e em geral falta de mecanismos de segurança de informação, que fazem parte de elementos dos *SOC*.

Ausência tal que cria além de uma dificuldade de identificações de ataques a tempo útil, também de uma interrupção dos serviços comprometendo a sua qualidade. Dado a alta complexidade dos ataques cibernéticos de varias naturezas, a Faculdade de Engenharia torna-se uma instituição com bastantes riscos e mais vulnerável tais ataques e devido à dimensão e relevância da Faculdade, existe uma necessidade imediata de alinhamento às normas internacionais de segurança da informação, com premasia a ISO e NIST

3.3 Descrição da Situação Actual

Atualmente, a Faculdade de Engenharia da UEM (FEUEM) possui na sua infraestrutura de rede uma sala de servidores onde se encontra um router (*backbone*) que recebe o sinal proveniente do Centro de Informática da UEM (CIUEM) através da fibra ótica. Esse sinal é distribuído por todos os departamentos da faculdade a partir de um switch gerível (Switch L3) da CISCO, como ilustra a figura abaixo:

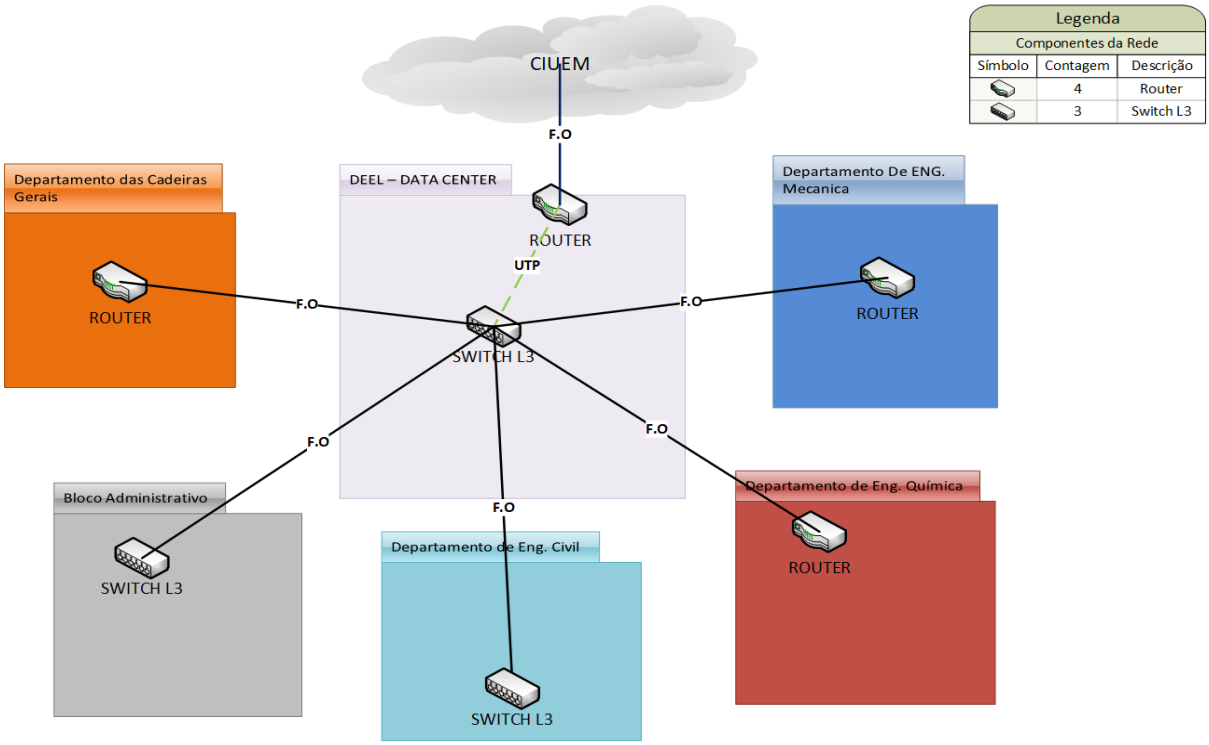

Figura 13: Topologia do DataCenter da DEEL.

Fonte: Elaborado pelo autor

4. Capitulo IV - Proposta de Solução

4.1 Análise Soluções e Escolha da Solução

Para a realização da presente análise comparativa, foram consideradas as soluções Splunk, Microsoft Sentinel e Wazuh e de seguida foram usados critérios e métricas (vistos na tabela 5), que foram escolhidos de acordo com os seguintes aspectos em torno das plataformas SIEM/SOC:

- Metricas de desempenho operacional;
- Criterios de funcionalidade.
- Custo: Grátis ou Comercial; e
- Open-source: Código Fonte aberto ou Fechado;

Ao fazer se a analise baseada nos autores Basta & Basta, e também em normas internacionais que medem a eficacia real das soluções com base nas métricas de desempenho operacional internacionalmente utilizadas, os autores priorizam as seguintes métricas fundamentais para a eficácia de um *SIEM/SOC* como: *Mean Time to Detect, Mean Time to Respond, Alert Volume e False Posetive Rate*.

Deste modo foram definidos pesos para as métricas ajudando a uma tomada valida de decisão.

Para auxiliar na análise focou-se em autores como González-Granadillo et. al (2021) e Manzoor et al. (2024) que fazem a comparação dos *SIEM/SOC* no ambito de criterios tais como: Análise de dados, Regras de correlação, Escalabilidade, Complexidade, Tolerância a falhas e Segurança. Porque mesmo sendo critérios principais nem todos tem a mesma importância, por isso foram definidos pesos tal como nas métricas, sendo que cada peso define a influência relativa de cada criterio no resultado final.

Explicar-se-há abaixo sobre os criterios abordados na análise.

- Regras de correlação:

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

- Análise de dados:

Versões modernas de *SIEM*s suportam ampla integração com detectores de anomalias baseados em aplicativos e usuários. Com a aplicação de detecção comportamentos anômalos tanto de funcionários, terceiros contratados e demais colaboradores da organização. Contemplanto gestão de perfis de usuários/aplicativos, para uma melhor analise descritiva, diagnotica, preditiva e prescritiva.

- Escalabilidade:

Este recurso refere-se a capacidade de um sistema *SIEM* implantado de não apenas crescer em termos de *hardware* e de número de eventos de segurança colectados, mas também de adaptar-se ao crescimento da infra-estrutura.

- Complexidade:

SIEMs podem ser no geral difíceis de implantar e gerenciar. No entanto, é importante compreender se o sistema em questão pode ser instalado para testes e experimentação com baixo ou limitado à moderado esforço.

- Segurança:

Neste têm-se análise da capacidade de implementar automação de segurança, bem como recursos de criptografia nativa presentes no *SIEM* durante a Monitoria, Detecção, Correlação, Análise e Apresentação dos resultados.

- Tolerância a falhas:

Tolerância a falhas é uma característica importante de qualquer sistema de monitorização crítico, mesmo por ser a capacidade so seu funcionamento mesmo na eventualidade de ocorrerem falhas. Este garantindo que o sistema mantenha sempre mantenha a coleta e análise de eventos ativa.

- Open-Source:

Normalmente avaliam a forma como o código fonte das soluções *SIEM* torna-se disponivel, ou seja, se é do tipo open-source (código fonte aberto) “permitindo ser modificado e adequedo” ou não open-source, isto é, código fonte fechado.

- Custo

Esse recurso avalia forma que licença está associada à solução *SIEM*, ou seja, se a solução é Grátis ou Comercial (paga).

Abaixo temos a nossa matriz comparativa disposta com os 12 parâmetros escolhidos para a devida análise, tendo os seus pesos e eles sendo eles caracterizáveis em: Baixo (mal ou não implementado), Moderado (parcialmente implementado) e Alto (devidamente implementado), com exceção do parâmetro *Open-source* que possui a dualidade de posições (Sim ou Não) e Custo que somente toma as posições de: Grátis ou Comercial

Metricas & Criterios	**Pesos**	**Plataformas SIEM/SOC**		
		Microsoft Sentinel	**Wazuh**	**Splunk ES**
Mean Time to Detect	10%	Moderado	Moderado	Baixo

Mean Time do Recover	10%	Baixo	Moderado	Moderado
False Positive Rate	10%	Moderado	Moderado	Baixo
Alert Volume	10%	Baixo	Baixo	Baixo
Regras de Correlação	5%	Alto	Alto	Alto
Escalabilidade	5%	Alto	Baixo	Alto
Complexidade	2.5%	Alto	Moderada	Alto
Tolerancia a falhas	7.5%	Alto	Moderada	Alto
Segurança	10%	Alto	Alto	Alto
Analise de Dados	7.5%	Moderado	Moderado	Alto
Open-Source	7.5%	Não	Sim	Não
Custo	15%	Comercial	Gratis	Comercial

Tabela 5: Tabela comparativa de soluções SIEM/SOC.

Fonte: Elaborado pelo autor

As cores representam a avaliação em relação a valoração de cada metrica e critério de acordo com os objectivos que se pretendem alcançar, nomeadamente o Vermelho para Mau (não aceitável), Laranja para Moderado (aceitável) e Verde para Bom (pretendido). Para a busca de uma matriz de decisão valida a esta pesquisa, foi destacado como opção a seguinte abordagem de pontuação de cada uma com base em valores numéricos, ou seja, quantificados: Bom = 1; Moderado = 0.5; Mau= 0.25.

Para se concluir a analise da matriz foi se feito cálculo do desempenho de métricas e critérios com base na seguinte formula: %Metrica/Criterio = Peso (%) x Valor numerico.

	Sentinel	**Wazuh**	**Slunk**
Veredito	**67.5%**	**72.375%**	**76.25%**

Tabela 6:Conclusão da análise comparativa.

Fonte: Elaborada pelo autor

Para decisão, define-se que a percentagem obtida pela solucão na matriz de decisão é muito importante para tomar a decisão de qual proposta será adequada a realidade da Faculdade de Engenharias. Porém pela natureza de criterios ainda mais impactantes para o estudo em causa tais como Custo e *Open-Source* que fará com que a Faculdade de Engenharias para sua implementação não necessite de desponibilizar nenhum capital financeiro para aquisição da solução, também que use o modelo da solução para futuros estudos, modifique o de acordo com as suas pretensões, entre outras possibilidades, além do facto do Wazuh poder ser implementado em organizações com infraestruturas de pequeno e médio porte, como no caso da Faculdade de Engenharia sem a necessidade investimento para melhoria de imediato da sua infraestrutura, por tudo isso foi escolhida a solução Wazuh em deternimento da solução Slunk apesar desta apresenta um melhor porcentual na matriz comparativa.

4.2 Descrição da Solução Proposta

4.2.1 Wazuh

O Wazuh é descrito como um sistema de gerenciamento de informações e eventos de segurança (*SIEM*) de código aberto que desempenha um papel central em proporcionar visibilidade de segurança por meio da coleta e correlação de logs, alertas de intrusão e anomalias do sistema em infraestrutura distribuída. (Islam, 2024)

O Wazuh iniciou seu desenvolvimento por volta de 2004, sendo primordialmente uma integração para um Sistema de Detecção de Intrusão de Código Aberto Baseado em Host, ou como escrito nas literaturas inglesas OSSEC o feito por Daniel Cid, sendo baseado pelo mesmo.
Em 2015, junto com Santiago Bassett e sua equipe criou-se o Wazuh baseado no OSSEC, com a visão de modernizar e ampliar suas funcionalidades. O Wazuh introduziu uma arquitetura mais escalável, conjuntos de regras aprimorados e RESTful APIs.

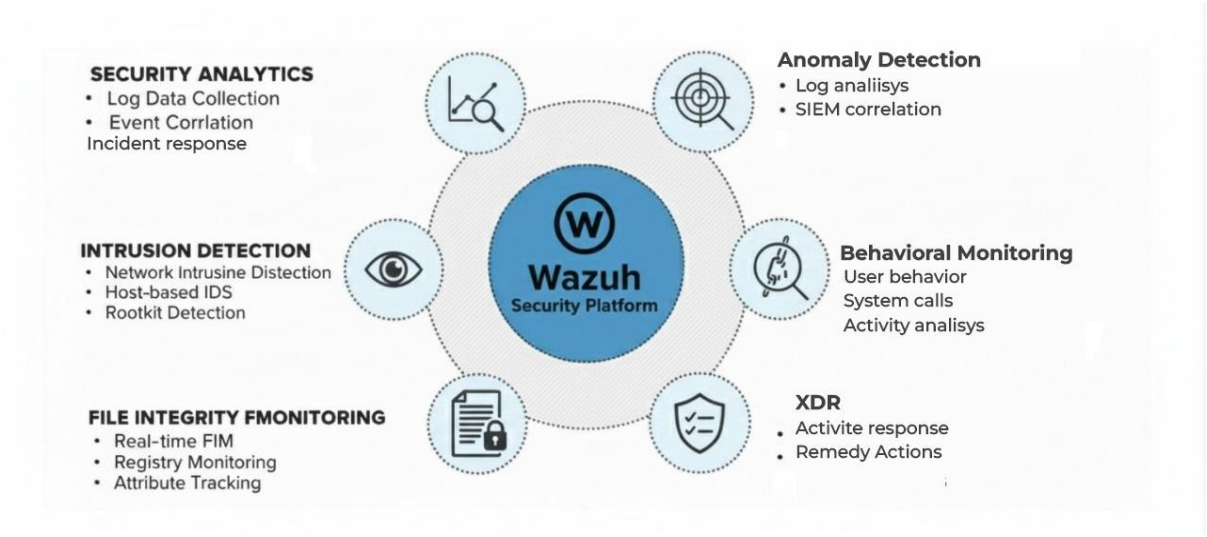

Figura 14: Principais funcionalidades do Wazuh.

Fonte: Elaborado pelo autor

A seguir, será feita uma explanação concisa sobre cada uma das principais funcionalidades: *Intrusion Detection, SIEM, File Integrity Monitoring, Detecção de Malware e Anomalias, Behavioral Monitoring, e XDR* de acordo com Wazuh™ (2025) User Manual:

- **Intrusion Detection**

  Realiza a detecção de intrusões com a análise de logs, tráfego de rede e atividades do sistema em busca de comportamentos suspeitos. Identificando tentativas de ataque, acessos não autorizados e violações de segurança usando um conjunto ou motor regras predefinidas e e indicadores de comprometimento (IOCs).

- **Behavioral Monitoring**

  É feito observância do comportamento dos usuários, processos e sistemas ao longo do tempo. Com base nos agentes que monitoram continuamente o comportamento desses sistemas, como chamadas de sistema, processos em execução e atividade de rede, assim permitindo detectar desvios em relação a um comportamento normal (anomalias), ataques internos e atividades suspeitas que possam indicar *rootkits* ou uso indevido

- **File Integrity Monitoring**

  Monitora-se em tempo real alterações em arquivos, diretórios e chaves de registro críticas do sistema (conteúdos, permissões, proprietário), onde é sempre essencial

para detectar se um atacante tentou modificar arquivos críticos ou mesmo importantes, tais como os de configuração do sistema ou de aplicações web.

- **Detecção de Malware e Anomalias**

  Agentes verificam atividades nos endpoints em busca de atividades e processos suspeitos, utilizando um método baseado em anomalias para identificar processos ocultos, arquivos camuflados e inconsistências no sistema. Também se integra a serviços como VirusTotal para enriquecer a análise de arquivos suspeitos, ajudando a prevenir infecções e ataques avançados.

- **SIEM Event Correlation**

  A inteligência e segurança do *SIEM* combina e correlaciona logs, estes colectados de múltiplos dispositivos (servidores, redes, nuvem). Com o uso de descodificadores e regras complexas para analisar a sequência e o contexto dos eventos, transformando eventos isolados em alertas de segurança acionáveis, e permitindo a criação de alertas em tempo real e de relatórios de segurança consolidados.

- **Extended Detection and Response (XDR)**

  É oferecida a visibilidade e detecção em *Endpoints* (EDR), comumente na nuvem, permitindo a Resposta Ativa (*Active Response*), automatizando ações de remediação, como o bloqueio de um endereço IP malicioso ou encerrar um processo no endpoint assim que uma ameaça é detectada. Sendo assim uma capacidade unificada da plataforma Wazuh de oferecer uma visão unificada de ameaças.

4.2.2 Arquitetura do Wazuh

Segundo (Islam, 2024) a arquitetura do sistema do Wazuh possui uma modularidade, tanto que, o sistema está dividido em componentes que têm responsabilidades bem definidas tais como a coleta, análise, armazenamento, visualização. Sendo também esta arquitetura composta por camadas, desde processamento á visualização.

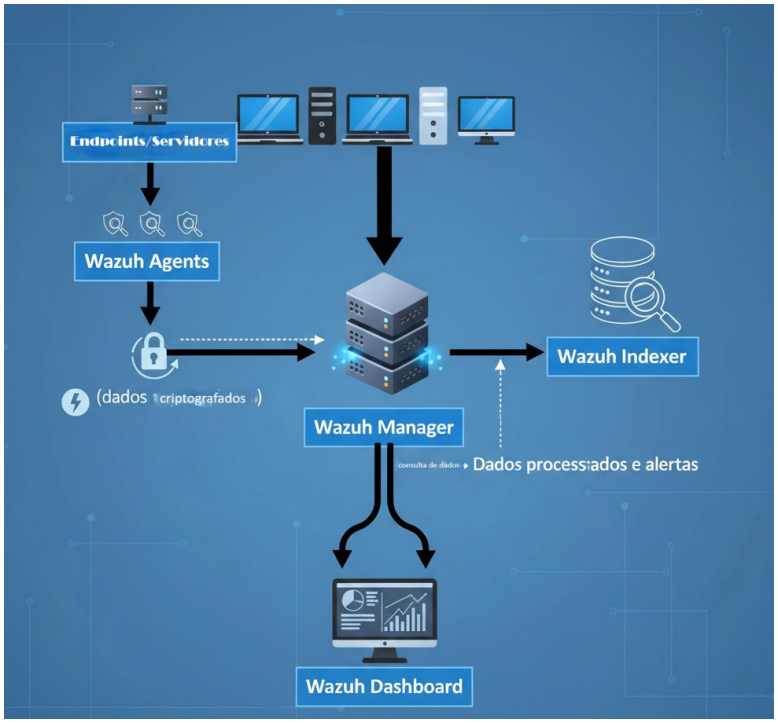

Figura 15: Arquitetura do Wazuh.

Fonte: Adaptado do Wazuh™ (2025) User Manual

O Wazuh™ (2025) User Manual explica a sua arquitetura de "deployment" como tudo-num ("all-in-one") entretanto que se possa perceber melhor o seu funcionamento como um todo, serão explicados de seguida todos os componentes da figura abaixo segundo a documentação do Wazuh:

- **Agent (Agente)**

  São intalados com o propósito de coleta dados de segurança dos dispositivos monitorados (endpoints, servidores, estações de trabalho.Sendo um software leve e multi-plataforma que tem a responsabilidade de executar ações como de: Monitorar integridade de arquivos, Detectar intrusões locais, Observar comportamento do sistema, Enviar esses dados criptografados de forma segura.

- **Manager**

  Sendo o núcleo do sistema, é responsável por analisar e correlacionar os dados recebidos dos agentes, i.e, eventos, detectando anomalias e comportamentos suspeitos, gerando alertas e relatórios de segurança. Ele também é integrável a outras soluções tais como ELK Stack, Splunk, AlienVault.

- **Indexer**

  É o motor de busca que armazena e indexa grandes volumes de dados de segurança enviados pelo Manager, permitindo buscas e análises em tempo quase real. Com a responsabilidade de manter logs, alertas e eventos de segurança de forma estruturada, garantir consultas rápidas e análises detalhadas, e servir de base para visualizações no dashboard.

- **Dashboard**

  Fornece uma interface visual para administração, monitoramento e análise
  É a interface do Sistema onde é feita a administração, o monitoramento e gerenciamento dos dados, permitindo que o usuário explore os alertas indexados, monitore o status da infraestrutura e gerencie a configuração do Wazuh

4.2.3 Ameaças, Activos & Risco

O Wazuh tem como um princípio fundamental a monitoria dos activos em uma infraestrutura. Para ele activos são todos os dispositivos de uma organização que possuam valor desde servidores, estações de trabalho, dispositivos de rede, aplicações, base de dados, entre outros. Estes activos são monitorados, recolhendo suas informações sobre status, integridade ou disponibilidade, configuração actividade e eventos.

O Inventário de Ativos (*Asset Inventory*) identifica e classifica os componentes de hardware e software, permitindo:

- Descobrir novos ativos na rede;
- Detectar alterações em sistemas monitorados;
- Acompanhar versões de software, vulnerabilidades e conformidade.

Para o Wazuh quaisquer acções que podem explorar vulnerabilidades, causar potencial dano e comprometer a segurança dos ativos são consideradas ameaças.

A ideia de identificação e analise de ameaças pode ser vista através de:

- Detecção de intrusões (IDS/IPS);
- Regras de correlação de eventos SIEM;

- Integração com feeds de Threat Intelligence: onde o Wazuh pode ser integrado com o VirusTotal, OTX (AlienVault Threat Exchange) ou MISP, para comparar indicadores de comprometimento;
- Monitoramento de comportamento;

A probabilidade de uma dada ameaça explorar qualquer que seja a vulnerabilidade em um ativo, causando nele algum impacto negativo vai constituir Risco.

O Wazuh faz sempre a avaliação do nível de risco operacional e técnico através de factores como a Gestão de Vulnerabilidades com a sua identificação de falhas de segurança conhecidas em sistemas e *softwares*, o Monitoramento de Conformidade verificando se os sistemas seguem políticas e normas, Relatórios e Dashboards permitindo uma visão de risco contínua.

Embora o Wazuh não atribuía um valor a um ativo como soluções como o Microsoft Sentinel por exemplo, ele resolve este problema de uma forma diferente configurando grupos de agentes como por exemplo “servidores críticos” serem tratados como ativos mais sensíveis e de maior risco. Com isso é possível refletir sua criticidade através da configuração das políticas, regras e grupos de agentes.

Para o Wazuh a Prioridade de evento é uma classificação de prioridade compreendida entre (0 e 15) baseada no tipo de evento, como falha de autenticação, ataque na Web ou negação de serviço, que indica a urgência com a qual um evento deve ser investigado. Ele faz a prioridade de forma nativa fornecendo uma variedade de regras (no arquivo *ruleset*) e no contexto dos eventos para classificar vários eventos por categoria e subcategoria.

O Wazuh também classifica a fiabilidade possuindo um campo chamado *rule.reliability* (herdado do OSSEC) e também usa mecanismos de correlação no módulo de SIEM para medir a credibilidade do evento. Isto onde cada regra no Wazuh possui atributos como: nível de severidade, grau de confiança no alerta (0–10), Frequência (quantas vezes precisa ocorrer para ser considerado válido).

4.2.4 Características e Ferramentas do Wazuh

De acordo o artigo “*Overview of Wazuh and Experiment Setup*” do ano de 2023 publicado no *Advanced International Journal of Multidisciplinary Research*:

O Wazuh é uma solução de segurança de código aberto que oferece detecção de ameaças, visibilidade e gerenciamento de conformidade. Ele foi projetado para ajudar organizações de todos os portes a detectar, responder e se recuperar de incidentes de segurança. O Wazuh coleta e analisa dados relacionados à segurança de múltiplas fontes, como logs, arquivos de configuração, chaves de registro e eventos do sistema em tempo real. Ele correlaciona os eventos para identificar potenciais ameaças à segurança e gera alertas.

Diferente de soluções como o *Open-Source Security Information Management* da AT&T *Cybersecurity*, que foi descontinuada em 2024, que é baseada em OSSEC e Snort e assente em GNU/Linux Debian, e integra muitas ferramentas tais como map, P0f, ArpWatch, OpenVas, Snort, spade, Tcptrack, Nagios, entre outros.

O Wazuh é uma plataforma baseada e evoluída a partir do Open Source Security (OSSEC), estendendo e modernizando as funcionalidades centrais do OSSEC.

O OSSEC é uma ferramenta *Open source* de segurança e monitoramento de sistemas. Sendo ele um *Host-based Intrusion Detection System*, ou seja, um sistema de detecção de intrusões baseado em hosts, fazendo a verificação de integridade de arquivos, monitorização de políticas, detecção de rootkits, envia alertas em tempo real e resposta activa, i.e., permite a execução de uma acção baseada num evento.

O Wazuh possui recursos nativos ou métodos de integração, assim focando se em uma arquitetura unificada com o seu próprio conjunto de componentes centrais, utilizando a modularidade e capacidade de processamento de dados para integrar as informações de segurança, substituindo a necessidade de agrupar muitas ferramentas separadas no seu core.

Importa realçar que as ferramentas ou seja seus módulos internos de acordo com o in LabFIB de Barcelona:

- **Intrusion Detection (IDS) -** Detecta actividades suspeitas e padrões de ataque com base em logs e regras pré-definidas.
- **File Integrity Monitoring (FIM) -** Monitora alterações em arquivos críticos do sistema;

- **Rootkit/Malware Detection -** Identifica e alerta sobre possíveis rootkits ou modificações maliciosas no sistema;
- **Vulnerability Detector -** Faz correlação entre pacotes instalados e bases de vulnerabilidades;
- **Log Data Analysis -** Analisa logs de sistemas, aplicações e redes em tempo real, centralizando-os;
- **Security Configuration Assessment (SCA)** - Avalia a conformidade de configurações do sistema com boas práticas e normas de segurança
- **Active Response -** Executa ações automáticas, como bloquear IPs, matar processos ou isolar sistemas comprometidos.

4.3 Desenvolvimento da Solução Proposta

4.3.1 Descrição do cenário proposto para a implementação da solução

Para realizar a avaliação da solução *SOC* Wazuh e, consequentemente, incentivar a Direção da Faculdade de Engenharia a considerar a sua adoção, apresenta-se um cenário (visto na figura 19), que consiste na alteração e redistribuição de determinados equipamentos de rede conforme as suas necessidades operacionais para a implementação da solução.

A construção do cenário foi realizada em um ambiente virtualizado, utilizando uma ferramenta de virtualização. Nesse contexto, foi criado um ambiente virtual capaz de demonstrar o cenário proposto, permitindo a implementação da solução e a execução de eventuais testes. Por não se enquadrar no escopo deste estudo, não serão explorados em profundidade os aspectos referentes à virtualização e/ou à configuração dos serviços apresentados no cenário, excetuando-se o servidor Wazuh.

No senário da solução é possível dividir em quatro (4) diferentes áreas, nomeadamente:

- **Autenticação**

Usada para funcionar como a porta de entrada segura da rede, através de ferramentas como o *FreeRADIUS (802.1X)*, usando protocolos que fazem uso dos **AAA**

(*Authentication, Authorization & Accounting***)** para fazer o controlo de acesso a rede da FEUEM com recurso a switches geríveis e integraveis com o Wazuh, sendo verificavel a identidade do utilizador, avaliado a conformidade do dispositivo e encaminha-o automaticamente para a VLAN apropriada. Este mecanismo garante que apenas equipamentos autorizados e confiáveis acedam à rede da Faculdade, reduzindo drasticamente os riscos de ataques internos.

- **Operação**

Esta área é de responsabilidade dos Analistas *SOC* e dos Técnicos que irão administrar e fazer a supervisão da solução *SOC*. Compete a estes profissionais analisar os dados técnicos produzidos pelo Wazuh e convertê-los em ações práticas de segurança. As suas funções de actuação sendo em: Monitoria contínua dos eventos, Gestão e otimização das regras do Wazuh, Resposta a incidentes detetados pela plataforma e a produção de relatórios de conformidade e auditoria.

No contexto da solução, os playbooks integram-se com as regras e alertas da plataforma, permitindo que sempre que um evento crítico seja gerado, exista um roteiro claro para investigação, validação do alerta, mitigação do risco, documentação do ocorrido e comunicação das ações tomadas. Assim, reforçando a eficiência operacional do SOC e contribuindo para a maturidade dos processos de segurança da organização.

- **Servidor Wazuh**

Com o recurso aos componentes centrais como o Manager, o Indexer e o Dashboard é possível receber e processar dados provenientes dos agentes instalados nos endpoints. A plataforma realiza análises detalhadas, correlaciona eventos, indexa logs e armazena as políticas de segurança definidas.

Os Analistas SOC e os Técnicos acedem ao Dashboard para executar as suas principais funções, incluindo monitoria dos eventos, análise de alertas, gestão de regras, visualização de métricas e acompanhamento do estado geral da infraestrutura.

- **Serviços**

Tendo como elementos centrais os Core Services e o Firewall, ambos operando de forma integrada e desempenhando um papel crítico na infraestrutura, uma vez que são

responsáveis pela gestão de identidade, endereçamento, controlo de acesso, filtragem de pacotes, gestão do tráfego e recolha remota de logs via Syslog.

É feita a segmentação da rede, isolando o tráfego em diferentes sub-redes nomeadamente: Administração, Laboratórios, Estudantes, *Data Center*, Guest e Quarentena, com o objetivo de reduzir a superfície de ataque e impedir a propagação de ameaças. Esta segmentação permite aplicar políticas de segurança direcionadas a grupos específicos, facilitando a gestão e reforçando o controlo da infraestrutura.

A sub-rede de Quarentena foi destinada a dispositivos considerados comprometidos ou não conformes, funcionando como uma camada de contenção para ameaças internas. Nesta arquitetura, o Firewall assume a responsabilidade de controlar rigorosamente o fluxo de comunicação entre a rede interna e a rede externa, garantindo que apenas tráfego autorizado e seguro seja permitido.

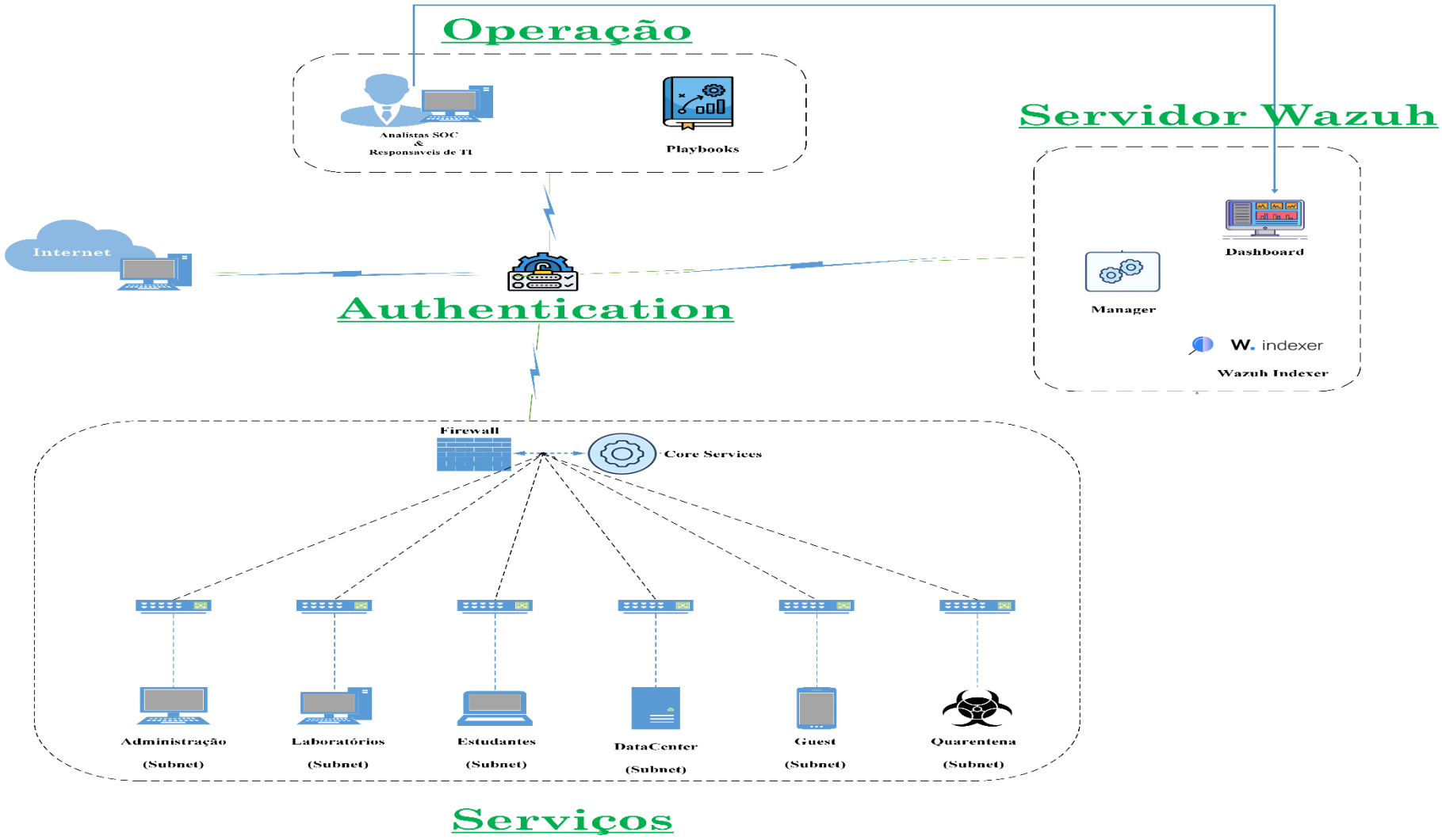

Figura 16: Cenario proposto para a implementação da solução.

Fonte: Elaborado pelo autor

4.3.2 Procedimentos de implementação

No eventual caso da FEUEM decidir proceder com a implementação da proposta do *SIEM/SOC* o Wazuh para monitoramento e resposta a incidentes de segurança detalhar-se-há um processo estruturado, e adequado para seu funcionamento. O autor faz a sua divisão em pontos chave, sendo esses:

- Planeamento: Definindo a Monitoria de logs, Deteção de intrusões, Gestão de vulnerabilidades, Controlo de acesso à rede (*NAC*), e Segmentação da rede em sub-redes / VLANs como os requisitos funcionais necessários;
- Recursos Humanos e Capacitação: A FEUEM necessitará de equipa técnica que deva possuir conhecimento sólido em administração de sistemas Linux/Windows, redes, segurança da informação e gestão de incidentes. Será imperativo investir em capacitação contínua através de certificações, workshops internos e participação em comunidades técnicas. Sendo essencial funções como **Gestor do SOC, Analista de Segurança Niveis 1, 2 e 3,** e também **Gestor de Segurança.**
- Recursos de Infraestrutura: Sabendo que a proposta tem em conta a realidade da infraestrutura actual, ou seja, dos recursos computacionais que a FEUEM possui de momento existe necessidade de especificar tais recursos que seriam disponibilizados para suportar a solução, sendo os seguintes:
  - ☑ Um servidor físico dedicado, com a capacidade de processamento e armazenamento definidos como requisitos do Wazuh;
  - ☑ Uma base de dados otimizada para carga de media de logs.
  - ☑ Salas dedicadas para a monitoria e uso do *SOC*.

Também é muito importante ter em conta a avaliação dos recursos computacionais vendo a capacidade dos switches e roteadores para suportar tráfego de logs, ver existência de VLANs para segmentação segura da rede, verificar políticas de firewall e filtragem de tráfego, e por ultimo garantir a conectividade com servidores Windows, Linux e dispositivos IoT.

5. Capitulo V - Discussao de Resultados

5.1. Revisão de Literatura

A revisão da literatura teve como objetivo, inicialmente, caracterizar a segurança cibernética em infraestruturas de redes corporativas, destacando os principais mecanismos de proteção, tais como: *IDS/IPS*, *SOAR*, *EDR*, *XDR* e *Playbooks*. Foi realizada uma descrição detalhada do modo de operação dessas soluções, apresentando ainda pontos fortes e limitações de cada uma.

O estudo concentrou-se, de forma particular, nos Centros de Operações de Segurança (*SOC*), nas suas arquiteturas e nos componentes que os constituem, analisando os diferentes modelos existentes. Esta investigação serviu como alicerce para o desenvolvimento do trabalho.

De maneira geral, tais mecanismos são essenciais para assegurar a proteção da informação no ambiente digital de organizações e instituições. No entanto, é importante reconhecer que eles não representam a solução absoluta para todos os problemas de segurança em redes corporativas. Sendo assim, torna-se fundamental adotar uma estratégia de proteção em múltiplas camadas.

Todos estes conceitos, abordados de forma estruturada na revisão teórica, mostraram-se determinantes para a execução do processo de monitoria e protecção da rede. Sem este conhecimento prévio, a proposta técnica não teria sido feita de forma rigorosa e não teria qualidade cientifca.

6. Capitulo VI - Considerações Finais

6.1. Conclusões

Ao longo do desenvolvimento deste trabalho de pesquisa, criar proposta viável de implementação de um Centro de Operações de Segurança para a Faculdade de Engenharia, com o objectivo de lidar com o problema de falta segurança cibérnetica, prevenir a perda de dados sensíveis e assegurar maior eficiência operacional.

Durante o processo, foi possível compreender profundamente os desafios enfrentados no contexto actual, caracterizado pela ausência de segurança, falta de planos elaborados em relação a segurança cibernética e infraestrutura robusta suficiente para suportar uma implantação de um *SOC* de grande escala. Essa realidade revelou-se vulnerável a falhas, dificultando a identificação rápida de incidentes de segurança, bem como o controlo de acessos e a proteção das informações sensíveis.

O presente estudo teve como objectivo principal propor a proposta de uma solução *SOC* na infraestrutura de rede da FEUEM. Para alcançar esse objectivo, foram realizadas etapas de análise e descrição das lacunas na infraestrutura de rede, complementadas por entrevistas e questionários, de modo a avaliar o estado atual da segurança e identificar os principais constrangimentos enfrentados pela instituição. Fez-se uma análise comparativa profunda entre as soluções, onde das opções a escolhida seria a que apresentasse o melhor custo/beneficio e melhor que adequasse as condições e realidade da instituição em causa.

Em síntese, concluiu-se que a adoção de soluções *SOC* possui grande potencial para beneficiar significativamente instituições não apenas como a FEUEM, mas também organizações de diferentes dimensões e estruturas, em especial as instituições moçambicanas, permitindo-lhes obter uma visão abrangente e em tempo real das suas infraestruturas de rede, de forma a detetar e mitigar ataques cibernéticos cada vez mais sofisticados e organizados.

6.2. Recomendações

O facto de *SOC* serem utilizados em várias partes do mundo por várias organizações para reduzir a probabilidade e o impacto de ameaças cibernéticas, monitorando a infraestrutura digital de uma organização, identificando e respondendo a incidentes de segurança e gerenciando a postura de segurança geral. O trabalho surgiu na tentativa de solucionar os problemas que advêm da falta do mesmo, porém foram identificadas algumas limitações. Dessa forma recomenda-se aos futuros utilizadores e tecnicos o seguinte:

- Implementação e capacitação de uma equipe de TI para gerir, e monitorar o *SOC*;
- Criação de planos formais de continuidade de negócios;
- Melhoria da infra-estrutura, tornado a mais robusta;
- Promover uma cultura de segurança em todas camadas academicas e administrativas (através de campanhas, workshops, e formações periódicas)
- Avaliação periódica da eficácia do *SOC*;
- Mais investimento em pesquisa e inovação na área de cibersegurança

6.2. Constrangimentos

Durante a realização do projecto constituíram constrangimentos os seguintes aspectos:

- Limitações na gestão do tempo, devido à necessidade de conciliar a pesquisa científica com as tarefas do estágio profissional;
- Insuficiência de apoio institucional no que se refere à disponibilização de recursos computacionais adequados para a realização dos testes de modo a gerar relatórios mais concisos;
- Baixo desempenho do equipamento utilizado nos testes, o que comprometeu a eficiência e a rapidez na execução das experiências.

Bibliografia

Baddi , Y., Almaiah, M., Almomani, O., & Maleh, Y. (2025). *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence.* Boca Raton: CRC Press.

Basta, A., Basta, N., Anwar, W., & Essar, M. I. (2025). *Open-Source Security Operation Center.* New Jersey: Jonh Wiley & Sons.

ENISA. (2022). *Padrões de gestão de risco.* Atenas: European Union For Cybersecurity.

Gil, A. C. (2022). *Como Elaborar Projetos de Pesquisa.* São Paulo: atlas.

Islam, R. (Junho de 2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture*, pp. 136-144.

ISO. (2018). *Gestão de riscos — Diretrizes.* Geneva: International Organization for Standardization.

ISO. (2019). *Segurança e resiliência — Sistemas de gestão de continuidade de negócios.* Geneva: International Organization for Standardization.

ISO/IEC. (2022). *Gestão de Segurança de Informação.* Geneva: International Organization for Standardization.

Lakatos, E. M., & Marconi, M. (2021). *Fundamentos de Metodologia Científica.* São Paulo: atlas.

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (12 de Março de 2024). ybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS.One*, pp. 100-175.

Mughal, A. A. (Março de 2023). Building and Securing the Modern Security Operations Center. *International Journal of Business Intelligence and Big Data Analytics*.

Muniz, J., McIntyre, G., & AlFardan, N. (s.d.). *Security Operations Center, Bulding, Operating and Maintaining your SOC.* Indianopolis: Cisco Press.

Munteanu, A.-R. (12 de Dezembro de 2024). Business Continuity Planning Case Study. *SEA - Pratical Aplication of Science*, pp. 193-201.

NIST. (2018). *Estrutura de Gestão de Riscos para Sistemas de Informação e Organizações: Uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade.* Gaithersburg, MD: National Institute of Standards and Technology.

NIST. (2024). *Cybersecurity Framework 2.0.* Gaithersburg, MD: National Institute of Standards and Technology.

Rehman, R. (2021). *Cybersecurity Arm Wrestling: Winning the perpetual fight against crime by building a modern Security Operations Center.*

Shahjee, D., & Ware, N. (08 de Março de 2022). Integrated Network and Security Operation Center: A Systematic Analysis. *IEEE*, pp. 216-353.

Stallings, W. (2023). *Cryptography and Network Security.* Reino Unido: Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security.* Boston: Cengage Learning.

ANEXOS

Anexo 1: Especificações do Host e das Máquinas Virtuais

Sistema Operativo	**Windows 11 Home**
Arquitectura do Sistema	**64 bits**
Processador	**Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 4 Core(s)**
RAM	**16 GB**
Hard Disk Drive (HDD)	**500GB + 1T**

Tabela A1- 1: Especificações do Host.

Sistema Operativo	**Linux – Debian**
Arquitectura do Sistema	**64 bits (Open Virtualization Appliance)**
RAM	**8 GiB**
Processadores	**4 vCPU**
Hard Disk Drive (HDD)	**50 GB**
Network Adapters	**Subnet Management**
	Subnet Servers
	Subnet Students
	Subnet Quarentene
	Subnet Labs

Tabela A1- 2: Especificações da máquina virtual Wazuh

Anexo 2: Careacterização da função do Core Services e Firewall

Serviço Essencial	Função na Rede	Tipo de Log Monitorizado pelo Wazuh
AD/LDAP	Autenticação centralizada de usuários e gestão de políticas.	Tentativas de login falhadas, criação/eliminação de contas de usuário, alterações de privilégios de administrador.
RADIUS	Autoriza o acesso à rede (via 802.1X/NAC) de dispositivos e usuários.	Acessos bem-sucedidos ou negados, logouts inesperados, flooding de pedidos de autenticação.
DHCP	Atribuição dinâmica de endereços IP a dispositivos.	Atribuição de IPs a dispositivos não autorizados, logs de starvation (esgotamento de IPs).
DNS	Resolução de nomes de domínio para endereços IP.	Tentativas de resolução para domínios maliciosos (phishing/C2) e falhas no serviço.

Tabela A2- 1: Carateristicas do Core Services

Categoria	Função na Solução	Detalhe de Implementação	Integração com o Wazuh
Controlo de Perímetro	Separação de Redes. Define a fronteira entre a Rede Interna (Campus Net) e a Rede Externa (Internet).	Aplica regras para bloquear ou permitir tráfego de entrada e saída, protegendo o Datacenter e os Core Services de	Envia logs de conexão/bloqueio para o Wazuh Manager via Syslog, permitindo a deteção de varreduras de porta (port scans)

		ameaças externas.	e ataques DDoS vindos da Internet.
Segmentação Interna	Controlo de Fluxo. Regula o tráfego entre as diferentes sub-redes internas.	Impede que o tráfego da sub-rede de Estudantes aceda diretamente à sub-rede de Administração ou Servidores Críticos sem autorização (isolamento de tráfego).	Os logs de tentativas de acesso não autorizadas entre sub-redes são analisados pelo Wazuh para identificar movimentação lateral de um atacante.
Quarentena	Contenção de Ameaças. É a política de segurança que direciona os dispositivos não conformes/comprometidos para a sub-rede de Quarentena.	O Network Access Control (NAC) ou o Switch (com base em regras) instrui a Firewall a aplicar regras de isolamento a um endpoint detetado como infetado.	O Wazuh pode ser configurado para acionar comandos de resposta automática na Firewall para isolar imediatamente um dispositivo que gere um alerta crítico (Resposta a Incidentes).

Tabela A2- 2: Papeis do Firewall na Solução

Anexo 3: Descrição da Situação Actual do Departamento De Electrotecnia (DEEL)

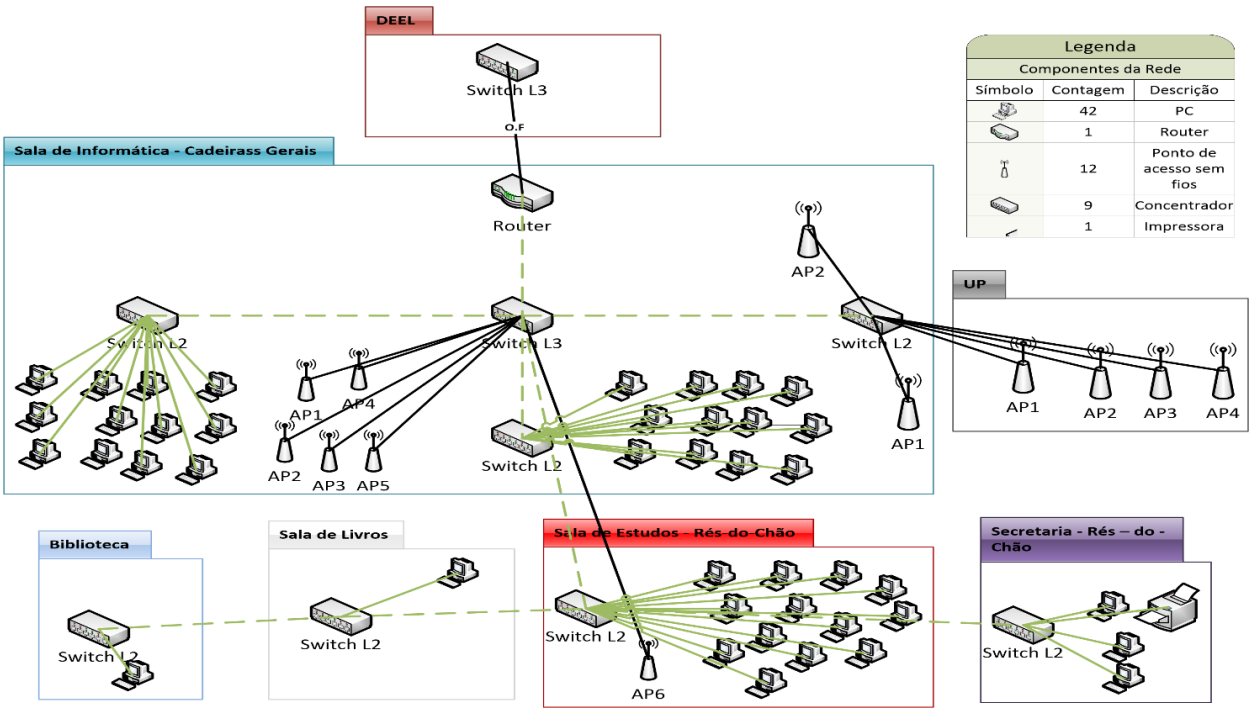

Figura A3- 1: Topologia da DEEL

1. **Rés do Chão**
   - Um Switch da CISCO com capacidade de 1Gbps;
   - Três AcessPoints da Microtic.
2. **Primeiro Piso**
   - Um Switch L2 com capacidade de 100Mbps da Cisco na secretaria;
   - Quatro AccessPoints conectados ao Switch L3 do Data Center;
   - Três Computadores de mesa conectados ao Switch L2 da Secretaria;
   - Uma Impressora Conectado ao Switch da secretaria.
3. **Segundo Piso**
   - Três Switch's L2 no bastidor da sala de informática;
   - Vinte e cinco computadores de mesa conectados aos Switch's na sala de informática;
   - Cinco AccessPoints conectados ao Switch L3 do Data Center, que fazem a destribuição do sinal pelas salas e pelo corredor.

Anexo 4: Descrição das Sub-redes propostas para a FEUEM

Como mencionado anteriormente na descrição do cenário da solução, a rede foi segmentada para permitir um controlo mais eficaz de usuários e dispositivos, otimizar a coleta de logs e a monitoria dos equipamentos, reduzir falsos positivos e melhorar o desempenho geral da rede

A seguir, apresenta-se a proposta recomendada pelo autor para a separação das sub-redes no local de implementação.

Sub-rede	Nome	Finalidade
10.10.1.0/24	**Administração**	PCs de Funcionários, Estações de trabalho, material administrativo
10.10.2.0/24	**Laboratórios**	Computadores de laboratórios
10.10.3.0/24	**Estudantes**	Acesso apenas à internet
10.10.4.0/24	**Servidores**	Wazuh, AD/LDAP, DNS, DHCP, serviços internos
10.10.5.0/24	**Guest**	Rede isolada, com acesso apenas à Internet e sem comunicação com qualquer outra sub-rede interna.
10.10.6.0/24	**Quarentena**	Dispositivos inseguros, não conformes ou suspeitos

Tabela A4- 1: Descrição das sub-redes propostas a FEUEM

Anexo 5: Invetário do equipamento actual da FEUEM

Localização Física			Dispositivo											
Edifício / Departamento	Piso	Compartimento	Roteador		Switch		Access Point		Computador	Impressora	Servidor	Conversor	Firewall	Observação
			Quantidade	Marca e modelo	Quantidade	Marca e modelo	Quantidade	Marca e Nome	Quantidade	Quantidade	Quantidade	Quantidade	Quantidade	
Bloco Administrativo	RC	Administração	0		1		0		1	1	0	0	0	O Switch da administração é da camada 3
		DTIC	0		3		1		4	1	0	0	0	
		DPM	0		0		1		9	2	0	0	0	
		UP	0		1		3		7	1	0	0	0	
		UGEA	0		0		1		5	1	0	0	0	
		Lab. Estruturas	0		0		1		2	1	0	0	0	
		R. Académico	0		0		1		7	1	0	0	0	
	1º	Gab. Do Director	0		0		1		2	1	0	0	0	
		Corredor da Dir	0		0		1		0	0	0	0	0	
		Sala de reunião	0		0		1		1	0	0	0	0	
	Subtotal		0		5		11		39	9	0	0	0	
Cadeiras Gerais	RC	Secretaria	0		1		1		3	1	0	0	0	A Sala 2 (De mestrados) pertence ao edifício/departamento de Pós-Graduação.
		Sala de estudos	0		1		1		0	0	0	0	0	
		Sala de formações	0		0		0		10	0	0	0	0	
		Salas administrativas	0		0		0		4	0	0	0	0	
	1º	Sala de informática	1		4		1		25	0	0	0	0	
		Sala 2 (De mestrados)	0		1		0		20	0	0	0	0	
		Salas de Aulas e corredor	0		0		6		0	0	0	0	0	
		Anfiteatro	0		0		1		0	0	0	0	0	
		Biblioteca	0		0		1		1	0	0	0	0	
	Subtotal		1		7		11		63	1	0	0	0	
Pós-Graduados	RC	Pós-Graduados	0		1		1		0	0	0	0	0	O sinal da sala Pós-Graduados provém directamente do backbone e o da RH provém do LAB de Alta Tensão, pois esta sala (RH) pertence ao Bloco Administrativo.
		Sala de Mestrados	1		1		3		25	0	0	0	0	
		RH	0		2		0		3	2	0	0	0	
	Subtotal		1		4		4		28	2	0	0	0	
Lab. De Alta Tensão			0		1		3		0	0	0	0	0	O sinal provém do Bloco Administrativo mas o edifício pertence ao DEEL.
CEEI			0		2		2		0	0	0	0	0	Pertence ao DEEL
EQ	RC	Sala 0	0		4		0		0	0	0	0	0	Existe um switch da camada 3, o que recebe o Sinal
	RC, 1º e 2º	Laboratórios	0		0		9		0	0	0	0	0	
	1º	Secretaria	0		1		1		4	2	0	0	0	
		Salas dos docentes	0		1		3		0	0	0	0	0	
	2º	Sala de Informtica	0		1		1		17	0	0	0	0	
		Sala de Informática de Mestrados	0		1		1		20	0	0	0	0	
		Salas de Aulas	0		0		3		0	0	0	0	0	
	Subtotal		0		8		18		41	2	0	0	0	
EC	RC	Laboratório	0		1		3		0	0	0	0	0	
	1º	Sala de Informática	0		2		3		16	0	0	0	0	
	Subtotal		0		3		6		16	0	0	0	0	
EM	RC	Oficinas	0		0		5		0	0	0	0	0	
	1º	Lab. Info de Mestrados	0		2		1		12	1	0	0	0	Pertence à Pós-Graduação.
		Laboratorio	1		3		1		0	0	0	0	0	
		Salas de Aulas	0		0		3		0	0	0	0	0	
	2º	Sala de Informática	0		2		1		0	0	1	0	0	
		Sala de Lab.	0		1		1		1	0	0		0	
		Salas de aulas	0		0		2		0	0	0	0	0	
		Gabinete	0		2		0		1	1	0	1	0	
	Subtotal		1		10		14		14	2	1	1	0	
DEEL	RC	Sala Máquinas Electricas	0		0		2		0	0	0	0	0	
		Sala de formações	0		0		3		10	0	0	0	0	
	RC | Data Center	Huawei	1		2		0		0	0	1	0	2	Serve apenas no DEEL. O servidor possui 8 discos de 4 TB cada. Dois (2) Storages de 5 discos (4 TB cada).
		Backbone	3		3		0		0	0	1	2	0	Apenas um roteador funciona. Tem também a Starlink mas não sendo usando. Um Storage de 6 TB. Controlador de WI-FI.
		Mestrados dos Petrolio	0		2		0		0	0	0	0	1	Tem um RTN 905 (Radio Transponder Network).
	1º	Secretaria	0		1				4	1	0	0	0	
		Salas de Aulas	0		0		4		0	0	0	0	0	
	2º	Sala Lab. Informática	0		3		1		25	0	0	0	0	
		Salas/Lab. de Aulas	0		0		4		1	1	0	0	0	
	Subtotal		4		11		14		40	2	2	2	3	
Total			7		51		83		241	18	3	3	3	

Legenda

1. **CEI:** Centro de Eletrónica e instrumentacão
2. **DEEL:** Departamento de Engenharia Electrotécnica
3. **DTIC:** Departamento de Tecnologia de Informacão e Comunicacão
4. **DPM:** Departamento de Património e Manutencão
5. **UP:** Centro de Estudos de Informática
6. **UGEA:**
7. **RC:** Rés do Chão
8. **EM:** Engenharia Mecanica
9. **EQ:** Engenharia Química
10. **EC:** Engenharia Civil

Anexo 6. Inquéritos : Guião de Entrevista

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Entrevista

1. Quais activos existem na infra-estrutura de rede Institucional?
2. Em relação ao sinal que vem da ISP (CIUEM), existe uma redundância?
3. Quais são activos considerados críticos na infra-estrutura de rede Institucional (FEUEM)?
4. É usada alguma Politica de Segurança? Se sim quais politicas de seguranças são usadas?
5. Qual é a maior dificuldade ou barreira para a melhoria da segurança cibernética na Faculdade de Engenharias?
6. Na sua opinião, o acesso à rede da instituição é segura?
7. Quando ocorrido algum problema de rede ou de segurança, sabe-se a quem reportar? E como normalmente são resolvidos ou solucionados tais problemas?
8. Na sua experiência, como classificaria o desempenho da rede Institucional, e com base em que pontos?

Anexo 7. Inquéritos : Guião de Questionario

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Questionario

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

1. A instituição possui um inventário atualizado de todos os dispositivos (laptops, servidores, IoT) que se conectam à rede?
2. Alguma vez teve problemas ao conectar o computador a uma tomada/porta RJ45 ou Wifi no recinto da FEUEM?
3. Existe uma equipa de TI dedicada monitoria ativamente dos ativos da FEUEM?
4. Actualmente, quais dos seguintes Mecanismos de Segurança são usados:
   - 4.1. Firewall
   - 4.2. Antivírus
   - 4.3. Network Access Control
   - 4.4. Sistema de Detecção de Intrusão
   - 4.5. Virtual Private Network
5. A FEUEM possui um plano de Respostas a incidentes de Segurança?

Questão	1	2	3	4.1	4.2	4.3	4.4	4.5	5
Sim	☑	☑			☑				
Não			✘	✘		✘	✘	✘	✘