



UNIVERSIDADE
LUSÓFONA

Viriatu

Trabalho Final de curso

Relatório Intercalar 1º Semestre

Miguel Lourenço, 22202315, LEI

Vasco Pereira, 22202735, LEI

Orientador: Rui Ribeiro

Entidade Externa: CyberS3c

Departamento de Engenharia Informática da Universidade Lusófona

Centro Universitário de Lisboa

1 de dezembro de 2024

www.ulusofona.pt

Direitos de cópia

*(Viriatu*s), Copyright de *(Miguel Lourenço e Vasco Pereira)*, ULHT.

A Escola de Comunicação, Arquitetura, Artes e Tecnologias da Informação (ECATI) e a Universidade Lusófona de Humanidades e Tecnologias (ULHT) têm o direito, perpétuo e sem limites geográficos, de arquivar e publicar esta dissertação através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, e de a divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

Resumo

Este projeto propõem a criação e desenvolvimento de uma plataforma de gestão de ativos , análise de vulnerabilidades e prevenção de ataques ,em colaboração com a [CyberS3c] que fornecerá os recursos e o apoio técnico para a implementação, Esta implementação ,com foco empresarial , permite a recolha da informação dos vários ativos de uma empresa como switches, routers, PCs entre outros ativos ligados a rede da mesma, permitindo ter uma visão geral dos mesmo , assim como vai permitir a analisar dos dados da rede externa e interna de uma empresa, desta forma a implementação pensada poderá fazer uma análise de vulnerabilidades nesses ativos e uma análise inteligente de prevenção de ataques , garantido assim a integridade dos ativos e da rede da empresa em questão . A colaboração com a [CyberS3c] permite o desenvolvimento de um sistema que reforça a resiliência e a proteção contra ataques maliciosos, unindo o conhecimento teórico com a prática no setor da cibersegurança.

Palavras chave:

- Gestão de Ativos
- Análise de Vulnerabilidades
- Prevenção de Ataques
- Cibersegurança
- Rede Externa/ Interna
- Integridade dos Ativos
- CyberS3c

Abstract

This project proposes the creation and development of a platform for asset management, vulnerability analysis, and attack prevention, in collaboration with [CyberS3c] ,which will provide the resources and technical support for its implementation. This implementation, with a focus on business environments, enables the collection of information about various company assets, such as switches, routers, PCs, and other network-connected devices, offering a comprehensive overview of these assets. Additionally, it will allow the analysis of both the internal and external network data of a company.

This approach aims to conduct vulnerability assessments on these assets and perform intelligent attack prevention analysis, thereby ensuring the integrity of the company's assets and network. The collaboration with [CyberS3c] facilitates the development of a system that strengthens resilience and protection against malicious attacks, bridging theoretical knowledge with practical applications in the field of cybersecurity.

Key-words:

- Asset Management
- Vulnerability Analysis
- Attack Prevention
- Cybersecurity
- External/Internal Network
- Asset Integrity
- CyberS3c

Índice

Resumo	3
Abstract	4
Índice	5
Lista de Figuras	7
Lista de Tabelas	8
Lista de Siglas.....	9
1 Introdução	10
1.1 Enquadramento.....	10
1.2 Motivação e Identificação do Problema.....	10
1.3 Objetivos	11
1.4 Estrutura do Documento.....	12
2 Pertinência e Viabilidade	13
2.1 Pertinência	13
2.2 Viabilidade.....	14
2.3 Análise Comparativa com Soluções Existentes	15
2.3.1 Soluções existentes.....	15
2.4 Proposta de inovação e mais-valias	16
2.5 Identificação de oportunidade de negócio	17
3 Especificação e Modelação.....	19
3.1 Análise de Requisitos.....	19
3.1.1 Enumeração de Requisitos.....	19
3.1.2 Descrição detalhada dos requisitos principais.....	23
3.1.3 Casos de Uso/ <i>User Stories</i>	25
3.2 Modelação.....	26
3.3 Protótipos de Interface	27
4 Solução Proposta	28
4.1 Apresentação	28
4.2 Arquitetura	28
4.3 Tecnologias e Ferramentas Utilizadas	29
4.4 Ambientes de Teste e de Produção.....	30
4.5 Abrangência	30

4.6	Componente.....	30
4.7	Interfaces.....	31
5	Método e Planeamento.....	33
5.1	Planeamento inicial	33
	Bibliografia.....	34

Lista de Figuras

Figura 1	13
Figura 2	15
Figura 3 Use Case Administrador da aplicação	25
Figura 4 Use Case API de detecção de Vulnerabilidades	26
Figura 5 Diagrama Entidade-Relação	26
Figura 6 Mapa Aplicaçional Interface	27
Figura 7 Mapa Aplicaçional API	27
Figura 8 Arquitetura da API	29
Figura 9 Painel de Vulnerabilidades	31
Figura 10 Painel geral de ativos, alertas e eventos	31
Figura 11 Painel de Certificados	32
Figura 12 Painel dos Ativos	32
Figura 13 Gant	33

Lista de Tabelas

Tabela 1 Análise de benchmarking	16
Tabela 2 Requisitos Funcionais	19
Tabela 3 Requisitos Não Funcionais	21

Lista de Siglas

ODS	Objetivos de Desenvolvimento Sustentável
API	Interface de Programação de Aplicações
LEI	Licenciatura em Engenharia Informática
TFC	Trabalho Final de Curso

1 Introdução

1.1 Enquadramento

A cibersegurança é uma das maiores preocupações para as empresas nos dias que ocorrem. A frequência e a sofisticação dos ataques cibernéticos aumentaram exponencialmente nos últimos anos, um único ataque bem-sucedido pode causar interrupções em larga escala afetando infraestruturas críticas como energia, saúde, finanças e transportes. Estima-se que o dano causado por este tipo de ataques ultrapassou os cinco mil milhões de euros para as empresas em 2021 e com base em algumas estimativas este número vai aumentar ao ritmo de 15% por ano. Tendo em conta a recente mudança de paradigma laboral, principalmente após a pandemia da COVID-19, obrigou as empresas a pisar no acelerador da digitalização estando mais dependentes dos dispositivos digitais, sendo a internet o principal canal para trabalhar. O trabalho remoto é hoje uma realidade incontornável, tal como arquiteturas com serviços cloud, e esta realidade aumenta a exposição a ciberataques pois carrega novos riscos e vulnerabilidades obrigando as organizações a reforçarem constantemente as suas defesas. Ao mesmo tempo, surge uma pressão regulatória significativa com diretivas como a [NIS 2] que exige resiliência e conformidade das infraestruturas críticas, esta diretiva de segurança surgiu como resposta a um ambiente digital cada vez mais complexo e vulnerável. A plataforma VIRIATUS, idealizada e desenvolvida pela [CyberS3c], oferece uma solução inovadora para os desafios de cibersegurança das empresas, utilizando a inteligência artificial para monitorar, detetar e mitigar riscos em tempo real além de garantir a conformidade com as normas, como a [NIS 2]. Esta plataforma foi reconhecida com a nomeação para ser finalista da 9ª edição dos Portugal Digital Awards destacando-se como um dos projetos que estão a transformar o paradigma de Portugal. Segundo a análise “A visão das empresas portuguesas sobre os riscos”, que auscultou mais de 130 líderes nacionais, os ataques cibernéticos (46%) são uma das principais preocupações dos gestores mais do que a instabilidade política e a inflação. O VIRIATUS está em constante evolução para oferecer uma plataforma de cibersegurança cada vez mais robusta e adaptada aos desafios modernos. Num futuro próximo, a plataforma integrará um [CISO virtual] baseado em inteligência artificial o que permitirá uma abordagem positiva e preditiva da segurança, proporcionando às empresas uma proteção avançada e alinhada com as exigências regulatórias e ao mesmo tempo que otimiza os processos internos de gestão de cibersegurança.

1.2 Motivação e Identificação do Problema

No momento atual do cenário de cibersegurança, as empresas e organizações enfrentam uma ameaça cada vez mais sofisticada. Ciberataques avançados, como o ransomware e ataques de zero day, multiplicam-se em complexidade e frequência, obrigando as organizações a dar cada vez mais importância em como manter os seus sistemas mais seguros contra esses ataques e em simultâneo atender à pressão regulatória que tende a aumentar com diretivas como [NIS 2], que visa a imposição de requisitos rigorosos de resiliência e conformidade às infraestruturas

consideradas críticas. Cumprir com esta diretiva é fundamental para as empresas e organizações, especialmente para aquelas que operam em setores críticos porque para além de reforçar a proteção das infraestruturas , mitigar riscos operacionais e por consequência financeiros e fortalecer a confiança dos stakeholders, o não cumprimento do [NIS 2] pode levar a sanções financeiras severas e até à suspensão de atividades da empresa, a adesão às diretrizes demonstra compromisso com as normas legais e evita penalizações que podem prejudicar o bom funcionamento das empresas.

Este contexto obriga as empresas a fazerem uma integração de forma eficaz a monitorização e respostas a possíveis ameaças, mantendo a conformidade com as diretivas presentes e sem o comprometimento da agilidade operacional.

Acrescentando a isso as empresas dependem de infraestruturas externas e internas digitais para desempenharem as suas atividades. Por isso, uma gestão eficiente dos ativos e uma identificação rápida das vulnerabilidades tornaram-se um fator crucial para garantir a continuidade do negócio e proteger informação sensível. Neste contexto este projeto propõe então o desenvolvimento de uma plataforma integrada de gestão de ativos, análise de vulnerabilidades e prevenção de ataques , visando atender às necessidades das organizações de uma forma eficaz.

Combinando inovação tecnológica e práticas de cibersegurança, este projeto pretende não apenas criar uma ferramenta com eficiência, mas também ajudar as organizações a dar resposta aos desafios impostos pelas crescentes exigências do mercado e pelas regulamentações em vigor.

1.3 Objetivos

O objetivo principal deste projeto é a integração e desenvolvimento de uma API de Threat Intelligence numa plataforma de cibersegurança para identificar e mitigar ameaças e vulnerabilidades, recebendo dados de fontes externas e gerando relatórios e gráficos para uma melhor visualização do utilizador. A API será integrada para o aprimoramento numa plataforma integrada de cibersegurança que permita às empresas o gerenciamento central dos seus ativos, identificação e prevenção de ataques cibernéticos, assegurando a integridade das infraestruturas digitais e a conformidade com a regulamentação, como a [NIS 2] .

A plataforma é projetada para ser compatível com vários sistemas, como [Sophos] , [Checkpoint] , [Microsoft] e [Fortinet] , garantindo flexibilidade, interoperabilidade e integração perfeita sem a necessidade de as organizações investirem em novas tecnologias. O VIRIATUS oferece ainda uma visão centralizada, com a integração e correlação de informações de várias fontes, como firewalls e endpoints, para oferecer uma visão mais abrangente da postura de segurança da organização, bem como uma visão em tempo real dos ativos de rede, garantindo uma gestão eficiente e atualizada da infraestrutura de TI.

Utilizando Inteligência Artificial (IA), a solução é capaz de realizar a deteção de ameaças avançadas, respondendo de uma forma automatizada a incidentes, criando assim uma análise preditiva de vulnerabilidades. Além disso, facilita a conformidade com normas como

a [NIS 2] , através da geração de relatórios e da monitorização de ativos e incidentes, permitindo que as organizações cumpram os requisitos legais e normativos de forma eficiente. Outro objetivo é a identificação de ameaças e vulnerabilidades em tempo real e a automatização da comunicação a entidades como o CNCS (Centro Nacional de Cibersegurança).

O VIRIATUS já conta com uma primeira versão desenvolvida, sendo o levantamento de novos requisitos para a consolidação e evolução da plataforma, para torná-la ainda mais robusta e apta para enfrentar os desafios do mercado de cibersegurança, um objetivo para este projeto. Combinando inovação tecnológica e práticas avançadas de proteção, o VIRIATUS pretende ser uma ferramenta essencial para fortalecer a resiliência cibernética das organizações.

1.4 Estrutura do Documento

O presente documento estrutura-se da seguinte forma:

- Na 1ª Secção é apresentada a Introdução e enquadramento do projeto
- Na 2ª Secção é apresentada a análise da viabilidade e pertinência do projeto
- Na 3ª Secção é apresentada a Especificação e Modelação do projeto
- Na 4ª Secção é apresentada a Solução Desenvolvida pelo projeto
- Na 5ª Secção é apresentada o Método e Planeamento do projeto

2 Pertinência e Viabilidade

2.1 Pertinência

Este projeto foi desenvolvido para atender à crescente necessidade de proteger as infraestruturas internas e externas das empresas contra ataques cibernéticos, com foco especial em setores críticos como saúde e transportes, onde os custos de recuperação são significativamente mais elevados e as diretivas são muito mais rigorosas. Ao disponibilizar uma solução integrada de gestão de ativos, análise de vulnerabilidades e prevenção de ataques que comprometem a segurança dos ativos das organizações, a plataforma VIRIATUS aborda e oferece uma solução que corresponde aos desafios que as organizações enfrentam no cenário atual de cibersegurança. A plataforma VIRIATUS destaca-se por proporcionar uma abordagem centralizada e automatizada, garantindo uma resposta ágil e eficiente a incidentes, enquanto cumpre com as rigorosas diretivas aplicáveis aos setores críticos. Este impacto a nível positivo é reforçado pela colaboração com a CyberS3c, cuja experiência na área de cibersegurança vai ajudar a garantir que a plataforma detém as melhores práticas do setor e vai responder com eficácia às exigências do mercado.

Estudos recentes, como os realizados pela CyberS3c, demonstram que dois terços das organizações foram alvo de ataques nos últimos 12 meses. Estes dados não sublinham somente a frequência destes ataques, mas também a lacuna existente na capacidade de uma contrarresposta e prevenção das empresas como estará demonstrado na Figura 1. Isto demonstra que métodos tradicionais para prevenir estes ataques já não são suficientemente viáveis, o que leva a que uma plataforma integrada com IA como o VIRIATUS possa ser uma solução para estas organizações, o que valida a pertinência deste projeto.

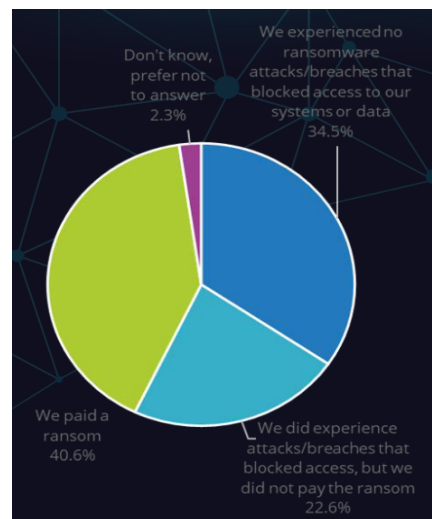


Figura 1

Conforme indicado por [Luís Rato] , NSO da Microsoft Portugal, indica que, do lado de quem ataca, a IA “permite a identificação, de uma forma mais rápida e detalhada, de possíveis vulnerabilidades em sistemas de segurança e tem a capacidade de explorá-las para obter acesso não autorizado a sistemas e dados. A mesma tem sido um recurso para estes agentes na criação de conteúdos fictícios próximos da realidade e controlo da mensagem que se quer transmitir”.

Ao integrar a plataforma com IA é possível a análise automatizada e contínua, mitigação ágil das vulnerabilidades e uma prevenção proativa.

O impacto positivo de uma plataforma como a Viriatus vai além da proteção contra ataques; ela aumenta a confiança operacional, em um cenário onde 60% das pequenas e médias empresas encerram as atividades seis meses após um ataque grave, ferramentas como esta podem ser a diferença entre a resiliência e o fracasso.

2.2 Viabilidade

A viabilidade do projeto é garantir através de uma análise abrangente incluindo fatores técnicos, econômicos, sociais e ambientais assegurando então a sua implementação e não esgotamento enquanto projeto acadêmico. O alinhamento com o ODS, em específico com os ODS 9 [ODS9] (Inovação e infraestruturas) , onde o projeto está diretamente alinhado , propõem uma solução inovadora que reforça a robustez das infraestruturas das empresas , com um papel fundamental para o funcionamento seguro e eficiente das empresas no mundo digital atual . E com o [ODS16] (Paz, Justiça e Instituições Eficazes) , onde o projeto também se alinha ao melhorar a proteção de infraestruturas e prevenção de ataques cibernéticos que podem comprometer e causar instabilidade operacional especialmente em organizações que atuam em áreas críticas , por isso melhorando a proteção de dados e a segurança digital.

No plano técnico, a viabilidade do projeto é reforçada pela experiência da CyberS3c na implementação de uma versão anterior, que já demonstrou a adequação das ferramentas e tecnologias empregadas. Esse histórico, aliado ao suporte técnico especializado e aos recursos fornecidos pela CyberS3c, assegura uma base sólida para a evolução contínua do projeto.

Economicamente, a plataforma irá apresentar-se como uma solução acessível e sustentável, contando com um primeiro plano de subscrição já desenvolvido e precificado pela CyberS3c, o que permitirá tanto a sustentabilidade da plataforma quanto a geração de lucro para a empresa. Além disso, será uma alternativa de custo-benefício para as empresas, pois proporcionará a redução de despesas relacionadas a ciberataques e à prevenção de vulnerabilidades. Conforme demonstrado na Figura 2, que ilustra o crescimento significativo do mercado na área de cibersegurança, a plataforma está bem posicionada para atender à crescente demanda, reforçando sua viabilidade econômica e atratividade para os clientes.

Cybersecurity Global Market Report 2024

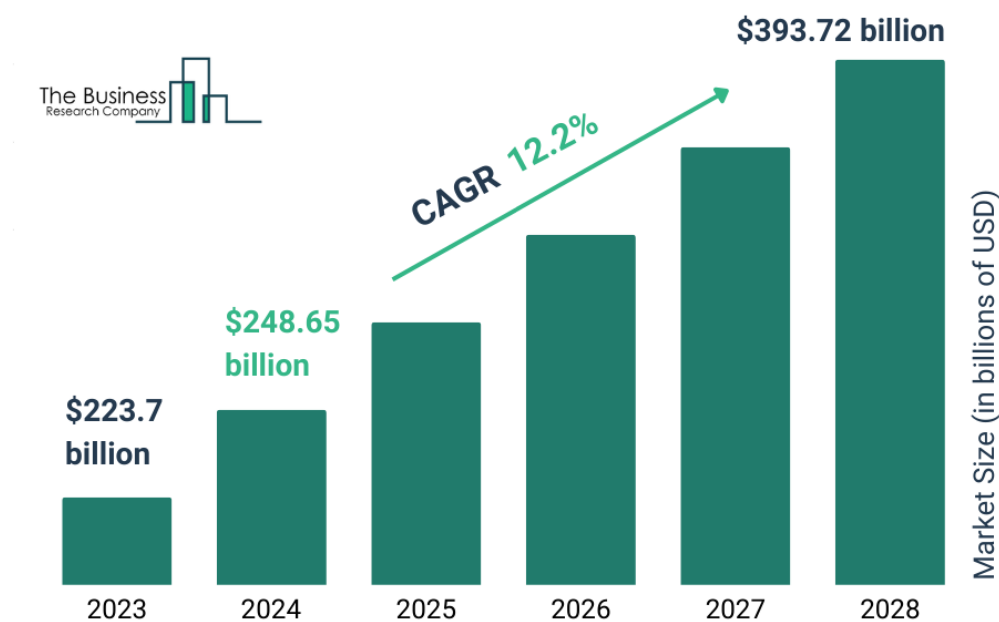


Figura 2

A nível Social, o projeto irá destacar se pela sua ênfase no contexto empresarial, respondendo a necessidades da gestão de ativos, a prevenção de ataques cibernéticos e a geração de relatórios para ir de encontro com as normas como a [NIS 2] e a comunicação de incidentes com entidades como o CNCS.

Desta forma, a plataforma não só se posiciona como uma solução técnica social e economicamente viável, mas também uma ferramenta com potencial para gerar impacto positivo no setor da cibersegurança das empresas.

2.3 Análise Comparativa com Soluções Existentes

2.3.1 Soluções existentes

Para realizarmos uma análise comparativa fundamentada, iremos apresentar abaixo três soluções existentes no mercado, que possuem funcionalidades semelhantes ou complementares ao nosso projeto:

- [Rapid7insightVM]
O Rapid7 é uma ferramenta de gestão de vulnerabilidades que permite a monitorização da rede em tempo real, identificação de riscos e fornecimento de relatórios detalhados com priorização de intervenções. Contém uma interface intuitiva e oferece suporte a diversos ambientes.

- [Checkpoint] [Qualys VMDR]
O Qualys é uma ferramenta abrangente que combina a monitorização de ativos, avaliação de possíveis vulnerabilidades e resposta a incidentes que possam ocorrer, destacando-se pela sua escalabilidade, pois está integrada com serviços de cloud, sendo ideal para empresas de grande dimensão.
- [Tenable.sc]
O Tenable.sc é uma ferramenta que oferece uma gestão personalizada de vulnerabilidades, com destaque para a capacidade de disponibilização de uma visibilidade centralizada e contínua sobre o estado de segurança das infraestruturas da empresa. A plataforma permite avaliações de risco e geração de relatórios para ajudar as empresas a priorizar a mitigação das vulnerabilidades mais críticas para a infraestrutura. Permite também uma análise histórica dos dados, o que, por consequência, possibilita a monitorização da segurança cibernética ao longo do tempo

Tabela 1 Análise de benchmarking

Características	Viriatius	Rapid7	Qualys VMDR	Tenable.sc
Gestão centralizada de ativos	X	X	X	X
Identificação de vulnerabilidades	X	X	X	X
Prevenção de ataques cibernéticos	X			X
Conformidade com NIS2	X			
Relatórios	X	X	X	X
Monitorização contínua	X	X	X	X
Pago	X	X	X	X
Facilidade de implementação	X	X	X	X
Compatibilidade com várias plataformas	X	X	X	X
100% Portuguesa	X			

2.4 Proposta de inovação e mais-valias

A solução apresenta-se como uma solução inovadora na área de segurança cibernética devido à sua gestão centralizada de ativos, à análise de vulnerabilidades e à prevenção de possíveis ataques cibernéticos. O que diferencia a plataforma das restantes soluções é a integração total de ativos, como switches, routers e PCs, facilitando a identificação de riscos e a implementação de medidas preventivas de forma ágil e eficiente.

O foco na conformidade regulatória, como a ([NIS 2]), uma vez que a Plataforma Viriatius é 100% portuguesa, terá um foco na conformidade com as normas da União Europeia aplicadas, por sua vez, em Portugal, automatizando a geração de relatórios, monitorizando os ativos e dando resposta

a incidentes, permitindo que as empresas cumpram as exigências regulatórias. Outro diferencial da aplicação é a utilização de inteligência artificial para detetar ameaças em tempo real e a automatização da comunicação de incidentes com entidades como o Centro Nacional de Cibersegurança (CNCS).

Um elemento adicional na solução, é o desenvolvimento de uma API de Threat Intelligence que permite a integração e coleta de dados provenientes de várias fontes e que são enviados para a plataforma. Estes dados contam com feeds de ameaças e vulnerabilidades que permitem uma maior capacidade de análise preditiva, melhorando a proteção contra ataques antes que eles ocorram, além de permitir uma visão mais abrangente do panorama de ameaças. Do ponto de vista operacional, a API facilita a interoperabilidade entre diferentes ferramentas de segurança já existentes na infraestrutura do cliente, aumentando a eficiência e reduzindo redundâncias permitindo uma maior agilidade na tomada de decisões e maior proteção contra vulnerabilidades e ameaças emergentes.

Enquanto as vantagens, a plataforma oferece várias, em termos de eficiência de operação, otimiza os processos de gestão de ativos e análise de vulnerabilidades, permitindo uma resposta mais rápida a possíveis ameaças. Em termos de impacto social, a plataforma desempenha um papel de grande importância, uma vez que, ao reforçar a segurança das infraestruturas da empresa, contribui para uma maior segurança dos dados das empresas e, por sua vez, contribui para uma sociedade digital mais segura. E, por fim, em termos de sustentabilidade, a plataforma ajuda a garantir uma sustentabilidade das empresas, permitindo que operem as suas infraestruturas de forma mais eficiente e segura. Além disso, tendo um custo-benefício grande, uma vez que reduz os custos que possíveis ataques cibernéticos teriam nessas empresas.

No contexto da parceria, a colaboração com a CyberS3c traz diversas mais-valias. Como empresa especialista em cibersegurança, a CyberS3c fortalece a implementação da solução, fornecendo apoio técnico. Para o parceiro, a solução melhora a oferta de produtos e serviços, mas também contribui para reforçar a imagem da empresa na área de cibersegurança, em particular ao oferecer uma solução em conformidade com as últimas exigências regulatórias. Vai possibilitar também uma entrada num mercado em crescimento, devido à elevada demanda por soluções que resolvam o problema de cibersegurança do setor empresarial.

2.5 Identificação de oportunidade de negócio

O projeto apresenta uma oportunidade de negócio significativa, dado que os ciberataques, se fossem uma economia, representariam a 3ª maior, o que significa uma constante crescente de ameaças cibernéticas. No cenário atual, as empresas estão cada vez mais focadas em melhorar os seus sistemas de cibersegurança, especialmente face às exigências legais. Assim, a exploração comercial deste projeto pode ser realizada de diferentes formas, aproveitando a necessidade crescente do mercado.

Uma das principais oportunidades é oferecer soluções a empresas pequenas e médias, pois estas empresas frequentemente enfrentam desafios em termos de recursos para poder implementar as próprias medidas de segurança cibernética, o que a nossa plataforma visa combater, uma vez que oferece uma solução acessível e escalável, sendo compatível com qualquer equipamento e fabricante, o que reduzirá também os custos de implementação.

Além disso, a disponibilização da plataforma num modelo de subscrição permite às empresas aceder à plataforma e aderir ao plano que vá ao encontro das suas necessidades de utilização, permitindo uma receita recorrente e uma atuação contínua da plataforma.

Já em termos de expansão, a plataforma terá um grande potencial de ser expandida para mercados a nível internacional, especialmente dentro da União Europeia, onde as exigências de conformidade com a regulamentação de segurança cibernética são cada vez mais críticas, fazendo com que haja uma procura crescente por soluções deste tipo.

3 Especificação e Modelação

3.1 Análise de Requisitos

Este Capítulo tem como propósito a análise dos requisitos identificados pelo grupo para o sucesso do projeto. Os requisitos apresentados pretendem resumir as funcionalidades e as necessidades da aplicação. Para o projeto, os requisitos foram levantados ao longo de várias reuniões com o Professor Rui Ribeiro e com a CyberS3c que nos forneceram o material necessário para o desenvolvimento os mesmos.

Os requisitos são definidos em dois grupos:

- **Requisitos Funcionais** – Descrição das funções que oferecem valor aos utilizadores
- **Requisitos Não Funcionais**– Definem restrições sobre o projeto ou a execução, tais como requisitos de desempenho, segurança.

3.1.1 Enumeração de Requisitos

Tabela 2 Requisitos Funcionais

ID do Requisito	Descrição do Requisito	Prioridade/Impacto
REQ-01-A aplicação deverá permitir a integração de uma API para verificação de falhas, vulnerabilidades e possíveis ataques.	A aplicação deverá ser capaz de fazer integração de uma API que realize a verificação contínua de falhas de segurança, vulnerabilidades e de possíveis ataques, cruzando dados de diversas fontes para identificar ameaças.	Alta/Alto
REQ-02- A API deverá ser capaz de integrar fontes públicas de Threat Intelligence	A API deverá ser capaz de integrar fontes públicas de Threat Intelligence, como VirusTotal , AlienVault OTX e AbuseIPDB, para coletar informações sobre indicadores de compromisso (IoCs) e dados de ameaças reportados pelo globo .	Alta/Médio
REQ-03-A API deverá ser capaz de integrar dados sobre phishing	A API deverá ser capaz de integrar dados sobre phishing, detetando	Alta/Médio

	domínios maliciosos e URLs a partir de fontes como PhishTank e MalwareBazaar.	
REQ-04 -A API deverá ser capaz de integrar APIs que reportam dados sobre malware	A API deverá ser capaz de integrar APIs que reportam dados sobre malware, permitindo a identificação de novas ameaças e amostras de malware para análise forense e preventiva	Alta/Alto
REQ-05 -A API deverá comunicar-se e recolher informações de fontes que reportam vulnerabilidades	A API deverá processar informações de fontes que reportam vulnerabilidades, como a NVD e Exploit Database, para detectar vulnerabilidades críticas exploits em sistemas e CVES	Alta/Alto
REQ-06 -A API deverá ser capaz de verificar credenciais e dados comprometidos através de fontes e APIs integradas.	A API deverá ser capaz de verificar credenciais e dados comprometidos através de fontes externas, como Have I Been Pwned, Dehashed e Leak-Lookup, identificando fugas de dados, como emails e contas comprometidas, associadas a utilizadores da empresa	Alta/Médio
REQ-07 -A API deverá ser capaz de integrar ferramentas de navegação e análise de rede da empresa	A API deverá integrar ferramentas de navegação e análise, como Shodan e a Censys, permitindo a identificação de dispositivos com vulnerabilidades na rede externa ou interna da empresa e facilitando assim o mapeamento de possíveis vulnerabilidades.	Alta/Médio
REQ-11 A API deverá ser capaz de correlacionar e cruzar os dados recebidos.	A API deverá ser capaz de detetar padrões, conexões e tendências tal como por exemplo cruzar logs de eventos, identificar IoCs para transformar dados em informações úteis e fornecer análises profundas e	Alta/Médio

	importantes sobre ameaças e vulnerabilidades	
REQ-12 A API deverá gerar relatórios sobre possíveis ameaças e vulnerabilidades	A API deverá ser capaz de criar relatórios com informações das ameaças e vulnerabilidades encontradas. Estes relatórios vão conter gráficos, resumos e estatísticas das ameaças para ajudar na comunicação com stakeholders e tomadas de decisão ao nível da segurança das organizações oferecendo insights mais profundos	Alta/Médio
REQ-13 A API deverá conter endpoints para disponibilizar IoCs (Indicadores de Comprometimento)	A API deverá conter endpoints que estejam disponíveis para disponibilizar indicadores de comprometimento como hashes de arquivos maliciosos, IPs suspeitos, processos suspeitos num determinado ativo	Alta/Médio
REQ-14 A API deverá conter endpoints para disponibilizar relatórios de ameaças em tempo real	A API deverá disponibilizar endpoints que forneçam relatórios atualizados em tempo real sobre atividades suspeitas, eventos correlacionados e IoCs recentes	Alta/Médio

Tabela 3 Requisitos Não Funcionais

ID do Requisito	Descrição do Requisito	Prioridade/Impacto
REQ-08 -A API deverá ter uma base estável para futuras expansões.	A API deverá ser desenvolvida com uma arquitetura escalável, suportando por isso a futura adição de novas integrações sem comprometer o desempenho da mesma e por sua vez da aplicação.	Alta/Médio

<p>REQ-09-A API deverá suportar, de forma estável, o grande volume de dados recebidos</p>	<p>A API deverá ser capaz de processar e suportar grandes volumes de dados , garantindo a estabilidade da aplicação mesmo em cenários de alta demanda de informação e assegurando assim a continuidade da mesma</p>	<p>Alta/Alto</p>
<p>REQ-010-A API deverá ser capaz de normalizar os dados recebidos de diversas plataformas.</p>	<p>A API deverá ser capaz de normalizar os dados recolhidos de diferentes pontos de informação, convertendo as informações para um formato padronizado. Esta normalização facilitará a correlação e análise cruzada entre os dados de diversas fontes</p>	<p>Alta/Médio</p>
<p>REQ-15 A API deverá incluir um guia de instalação detalhado</p>	<p>A API deverá fornecer um guia detalhado dos passos para a instalação da mesma, bem como um manual de configuração para o correto funcionamento da API, este guia deve retratar passo a passo a instalação inicial e a resolução de problemas comuns</p>	<p>Média/Médio</p>
<p>REQ-16 A API deverá conter um guia de utilização completo</p>	<p>Para o correto uso da API, esta deverá incluir um manual de utilização que descreva por completo as funcionalidades da API , os exemplos dos endpoints e melhores práticas</p>	<p>Média/Médio</p>
<p>REQ-17 A API deverá garantir que apenas utilizadores autorizados podem aceder às funcionalidades</p>	<p>A API deverá implementar um sistema de autenticação robusto e seguro que assegure que somente utilizadores que tenham determinado tipo de permissões possam usar as suas funcionalidades</p>	<p>Alta/Alto</p>

REQ-18 Implementar limites de requisições por IP ou chave de API para evitar ataques de Denial of Service	A API deverá conter mecanismos que permitem que haja um controlo de requisições por IP ou chave de API para que o serviço esteja sempre disponível evitando ataques de Denial of Service	Alta/Alto
REQ-19 A API deverá conter mecanismos de bloqueio temporário em casos de múltiplas tentativas falhadas de autenticação	A API deverá conseguir identificar múltiplas tentativas falhadas de autenticação e bloquear temporariamente o IP ou o utilizador para bloquear ataques BruteForce	Alta/Alto

3.1.2 Descrição detalhada dos requisitos principais

Neste Ponto iremos descrever com maior exatidão os requisitos que consideramos mais importantes indicando dependências, objetivos e critérios de aceitação, completando a descrição feita dos mesmo no ponto anterior, sendo então esta descrição dispostas imediatamente abaixo:

[REQ-01] Integração de API para Verificação de Falhas, Vulnerabilidades e Ataques

Este requisito tem um objetivo principal de garantir que a aplicação consiga integrar uma API dedicada à deteção de falhas, vulnerabilidades e possíveis ataques. A API deverá ser capaz de identificar vulnerabilidades, possíveis ataques e gerar relatórios, permitindo assim uma resposta proativa a ameaças. Tendo como Dependências o acesso às APIs de Threat Intelligence e integração de sistemas externos de segurança e sendo os seus critérios de aceitação que a API deve identificar e reportar vulnerabilidades com precisão e deve gerar relatórios automáticos em tempo real

[REQ-02] Integração de Fontes Públicas de Threat Intelligence

O sucesso deste requisito depende da conectividade segura com fontes externas de Threat Intelligence, como VirusTotal, AlienVault OTX e AbuseIPDB. A qualidade dos dados recebidos deverá a todo o momento ser validada. O objetivo é fornecimento de informações atualizadas sobre ameaças emergentes, aumentando assim a sua capacidade de deteção e neutralização dos mesmos por parte da empresa. Para ser aceite, a API deverá integrar com sucesso todas as 4 fontes distintas e conseguir correlacionar os dados recebidos. Este requisito suporta diretamente o processo de análise de ameaças, fornecendo dados essenciais para a tomada de decisões estratégicas em segurança.

[REQ-04] Integração de Dados sobre Malware

O sucesso deste requisito depende da interação com plataformas especializadas na recolha de dados sobre Malwares, como o MalwareBazaar. O objetivo é identificar e analisar malwares conhecidos por essas plataformas. A aceitação desta funcionalidade exige que a API recolha dados com sucesso da MalwareBazaar e com isso seja capaz de identificar diferentes tipos de malware que possam afetar a empresa.

[REQ-05] Comunicação com Fontes de Vulnerabilidades

O sucesso deste requisito depende da integração com duas bases de dados, a National Vulnerability Database (NVD) que armazena vulnerabilidades e a Exploit Database que armazenam exploits conhecidos e detalhados. O principal objetivo é identificar vulnerabilidades conhecidas, permitindo assim a implementação de medidas de correção de uma forma mais eficaz. Para ser aceite, a API deverá integrar com sucesso A National Vulnerability Database e Exploit Database, recolher e reportar vulnerabilidades. Esta funcionalidade apoia o processo de gestão de vulnerabilidades da empresa, permitindo assim um combate mais rápido dos riscos identificados.

[REQ-09]: Suporte a Grande Volume de Dados

O sucesso deste requisito exige uma infraestrutura estável e robusta, capaz de suportar elevados volumes de dados. A API deverá por isso incorporar mecanismos de otimização do desempenho para garantir que seja estável. O objetivo da mesma é assegurar o seu funcionamento de forma eficiente, mesmo ao processar grandes quantidades de dados provenientes das diferentes fontes que vai integrar. A aceitação deste requisito vai ser validada através de testes de desempenho que vão simular cenários de um elevado número de dados, onde a API deverá manter estabilidade e eficiência. Esta capacidade é fundamental para uma continua monitorização e uma análise de dados das diversas fontes em larga escala.

[REQ-11]

O sucesso deste requisito exige a implementação de algoritmos para análise e correlação dos dados. A integração eficaz com diversas fontes externas de dados é uma dependência crítica para o bom funcionamento. O objetivo é correlacionar a informações de diferentes origens, identificando padrões e tendências que permitam transformar dados em informações uteis para edificar vulnerabilidades nas empresas. O critério de aceitação será que A API deverá demonstrar a capacidade de cruzar informações provenientes das diversas fontes que estão integradas, gerando análises relevantes.

[REQ-12] Geração de Relatórios sobre Ameaças

O sucesso deste requisito depende da capacidade de processar de dados e da posterior geração automática de relatórios, vai ser por isso necessário a implementação de templates padronizados. O objetivo é fornecer relatórios detalhados sobre vulnerabilidades e possíveis ameaças, facilitando assim a tomada de decisões estratégicas. A aceitação vai ser validada com

o sucesso em gerar relatórios claros e precisos e que correspondam aos dados necessários para as empresas.

[REQ-17]

O sucesso deste requisito depende da implementação de formas de autorização e autenticação de acesso a API, assim como políticas para a gestão utilizadores autorizados. O objetivo da API é garantir que apenas os utilizadores autorizados possam ter acesso aos endpoints, protegendo assim informações sensíveis contra tentativas de acessos não autorizados. Para ser aceite, a API deverá demonstrar controlo do acesso a mesma de forma eficaz e seguro. Esta funcionalidade esta em conformidade com regulamentações de proteção de dados impostas pela União Europeia.

3.1.3 Casos de Uso/*User Stories*

Nesta seção, são apresentados cenários de utilização real da solução desenvolvida, esta representação permite contextualizar os requisitos descritos nos pontos anteriores e também compreender melhor o seu impacto. Serão abordados casos de uso em forma de diagramas de casos de uso que vão estar disponíveis nas imagens imediatamente abaixo e que refletem situações práticas, facilitando a compreensão do contexto de aplicação da API e das funcionalidades associadas

Neste contexto definimos dois Atores como sendo:

- Administrador
- API

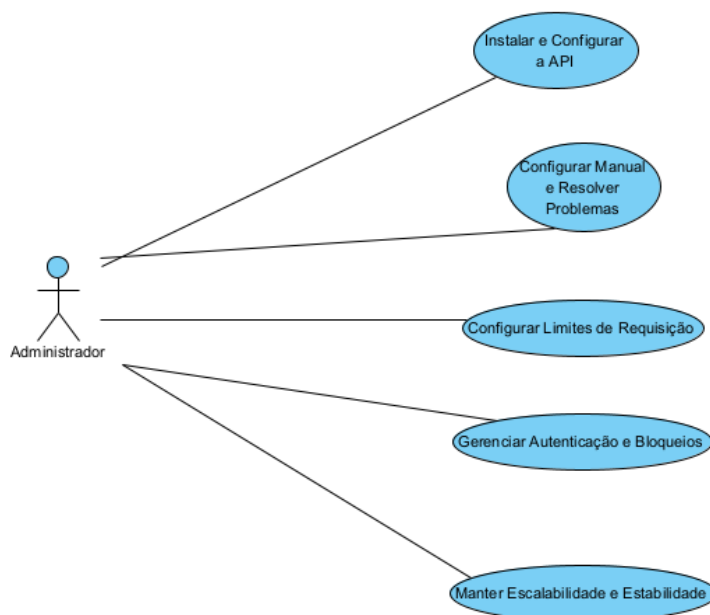


Figura 3 Use Case Administrador da aplicação

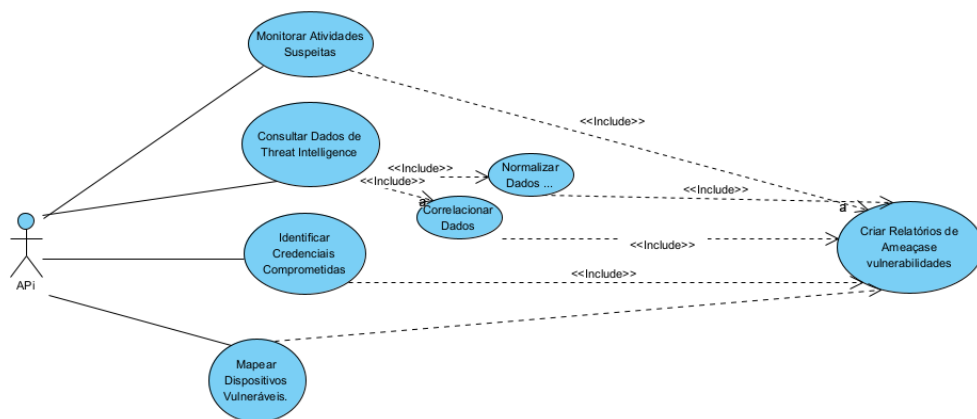


Figura 4 Use Case API de detecção de Vulnerabilidades

3.2 Modelação

Neste capítulo, com a Figura 5 Diagrama Entidade-Relação, será apresentado o diagrama de entidade-relação do nosso projeto que representa a estrutura da base de dados da aplicação. O modelo foi desenvolvido de forma a garantir que os dados estejam organizados e normalizados, cumprindo a Terceira Forma Normal.

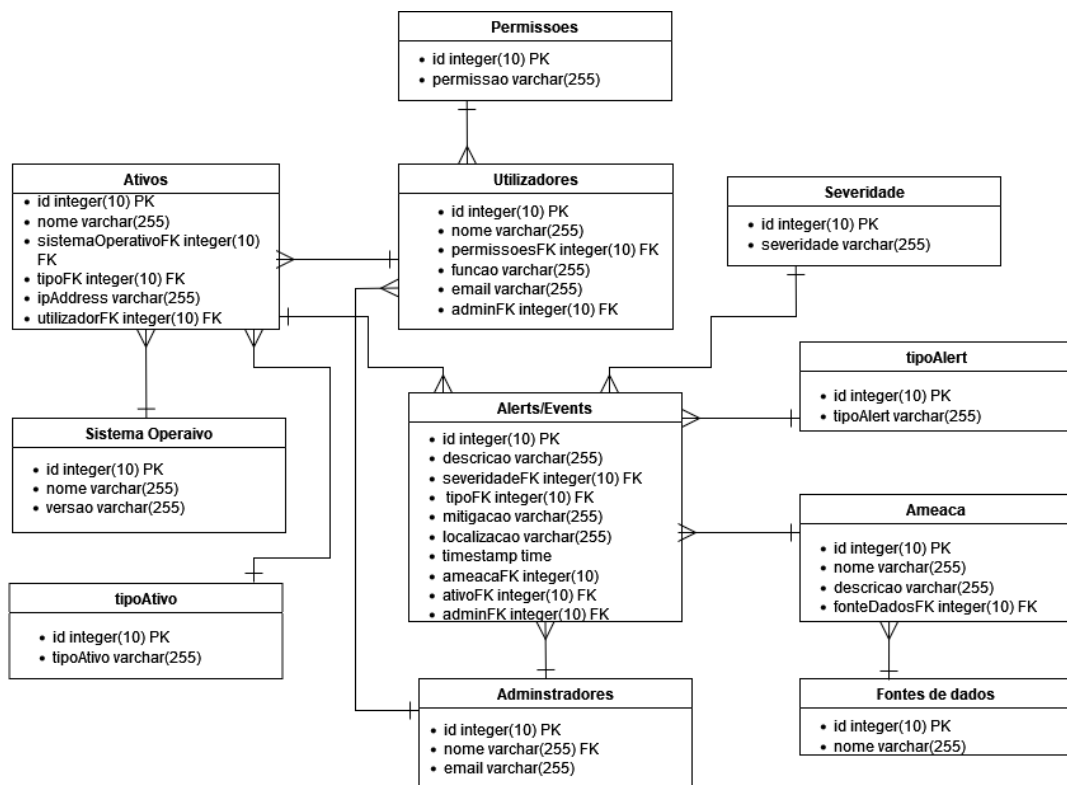


Figura 5 Diagrama Entidade-Relação

3.3 Protótipos de Interface

Neste capítulo, com a Figura 6 Mapa Aplicacional Interface e Figura 7 Mapa Aplicacional API, serão apresentados os mapas aplicacionais da API e da interface, onde o Viriatus comunicará com a API. Estes mapas refletem os ecrãs da aplicação e ilustram a forma como a navegação ocorre entre eles, bem como a interação que é esperada entre os diferentes componentes.

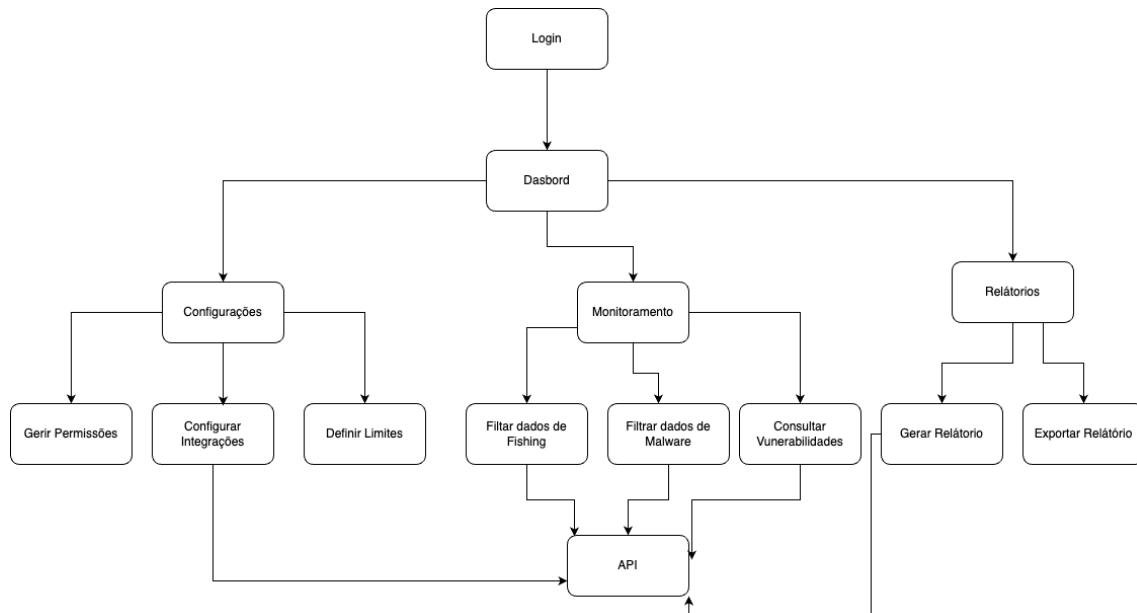


Figura 6 Mapa Aplicacional Interface

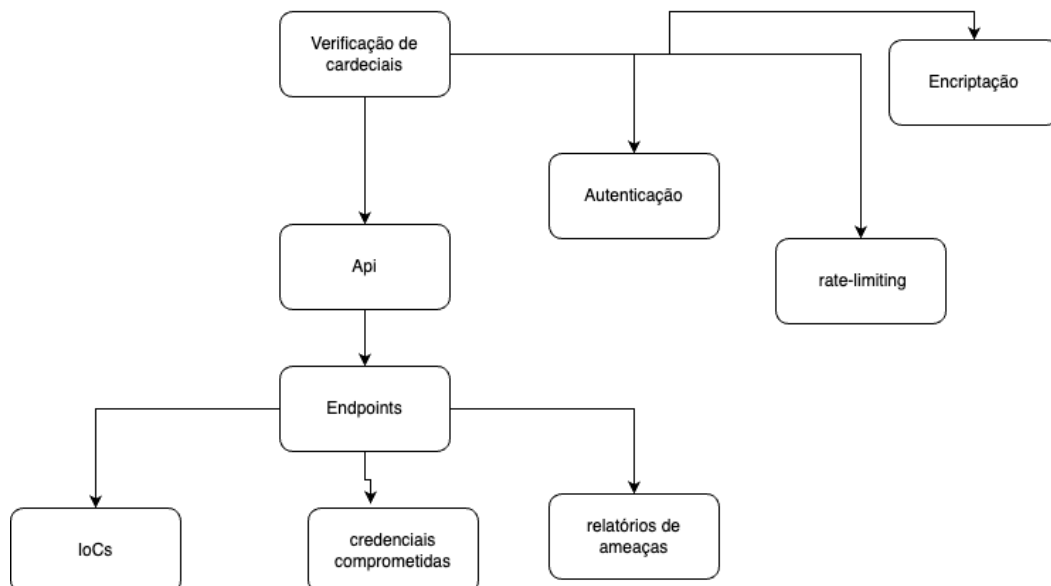


Figura 7 Mapa Aplicacional API

4 Solução Proposta

4.1 Apresentação

A nossa solução proposta visa o aprimoramento da plataforma VIRIATUS, desenvolvida pela CyberS3c, através de uma API que fornece uma solução abrangente para a gestão de ameaças cibernéticas e proteção de ativos, centralizando e organizando dados sobre vulnerabilidades e IoCs correlacionando esses dados de modo a ampliar a compreensão sobre ataques e ameaças. Através disto é possível para as organizações mitigar os seus riscos, oferecendo decisões mais informadas, de forma proativa garantindo segurança e escalabilidade. Espera-se conseguir oferecer uma abordagem eficaz e simples para conseguir facilitar todas as tarefas relacionadas com a plataforma VIRIATUS.

No subcapítulo 4.2 será abordado a Arquitetura utilizada para a resolução da plataforma e tecnologias a utilizar no desenvolvimento do TFC e a fundamentação das principais opções na construção da solução. No subcapítulo 4.3 é uma breve descrição das tecnologias e ferramentas utilizadas e a sua justificação de uso. Já no ponto 4.4 é descrito o ambiente produtivo da solução a desenvolver, indicando os recursos necessários à exploração produtiva da solução. No subcapítulo 4.5 verifica-se todas as cadeiras que são necessárias ao projeto e o porquê de as mesmas serem aplicadas a este Projeto. No ponto 4.6 é detalhado cada um dos componentes, realçando aspetos técnicos de sua implementação. E por último, no 4.7 é abordado o mapa aplicacional composto por screenshots dos ecrãs mais importantes da solução.

4.2 Arquitetura

A imagem abaixo ilustra a arquitetura da API que será integrada ao projeto. É importante notar que esta arquitetura se refere exclusivamente à estrutura e funcionamento da API, e não à arquitetura geral do projeto em si. A API servirá como um componente essencial para a comunicação entre os sistemas, mas não reflete a totalidade da arquitetura do projeto como um todo.

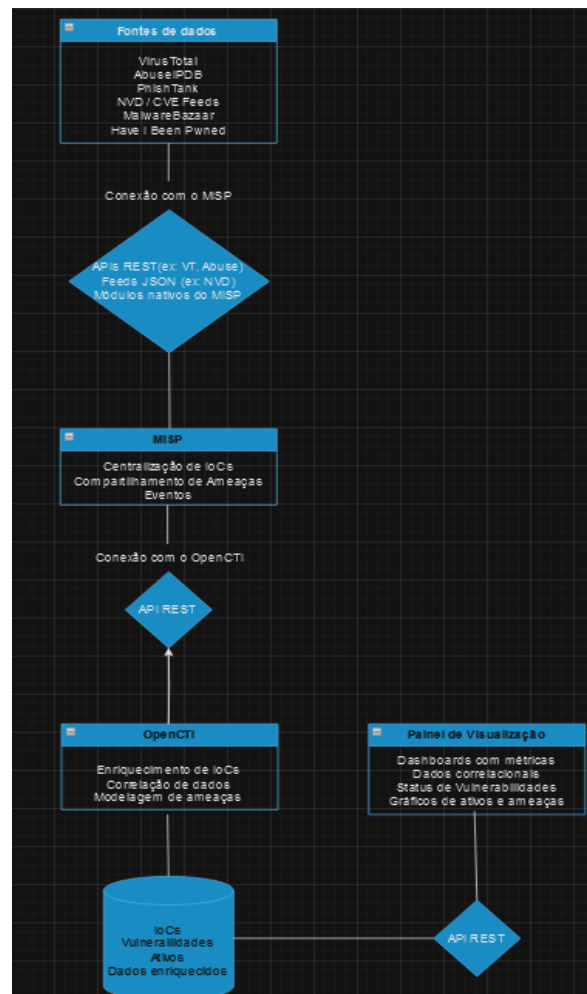


Figura 8 Arquitetura da API

4.3 Tecnologias e Ferramentas Utilizadas

Python - Python é uma linguagem de programação de alto nível, conhecida pela sua simplicidade e legibilidade. Ela é versátil, usada para diversos fins como desenvolvimento web, ciência de dados, inteligência artificial e automação. Esta linguagem tem uma vasta abundância de bibliotecas e Framework o que facilita a criação de APIs REST com rapidez e segurança o que preenche os nossos requisitos.

SGBDS (ainda a definir) - Um SGBD é o conjunto de programas de computador (softwares) responsáveis pelo gerenciamento de bases de dados. O principal objetivo é retirar da aplicação cliente a responsabilidade de gerenciar o acesso, manipulação e organização dos dados.

MISP - O MISP é uma solução de software de código aberto para coletar, armazenar, distribuir e compartilhar indicadores de segurança cibernética e ameaças relacionadas à análise de incidentes de segurança cibernética e análise de malware. O MISP foi projetado por e para analistas de incidentes, profissionais de segurança e de TI, ou especialistas em engenharia reversa de malware, com o objetivo de apoiar suas operações diárias, permitindo o compartilhamento eficiente de informações estruturadas.

OpenCTI - O OpenCTI é uma plataforma de código aberto que permite às organizações gerir seus conhecimentos e observáveis de inteligência sobre ameaças cibernéticas. Foi criada para estruturar, armazenar, organizar e visualizar informações técnicas e não

técnicas sobre ameaças cibernéticas. Além disso, o OpenCTI pode ser integrado com outras ferramentas e aplicações, como o MISP.

4.4 Ambientes de Teste e de Produção

A solução de Threat Intelligence para integração da plataforma VIRIATUS, será implementada em dois tipos de ambientes diferentes : ambiente de teste e um ambiente de produção. O ambiente de teste será usado para validação, desenvolvimento e integração de novas funcionalidades antes de passar para o ambiente de produção, já este que é configurado para suportar com operação contínua garantindo disponibilidade e desempenho. Estes dois tipos de ambientes são essenciais para garantir uma solução robusta e segura com capacidade de escalabilidade, reduzindo riscos operacionais, e integração contínua.

4.5 Abrangência

Nome das Disciplinas Associadas:

- Bases de Dados
- Engenharia de Software
- Fundamentos de Programação
- Inteligência Artificial
- Interação Humano-Máquina
- Linguagens de Programação I
- Linguagens de Programação II
- Engenharia de Requisitos e Testes
- Sistema de Informação na Nuvem

4.6 Componente

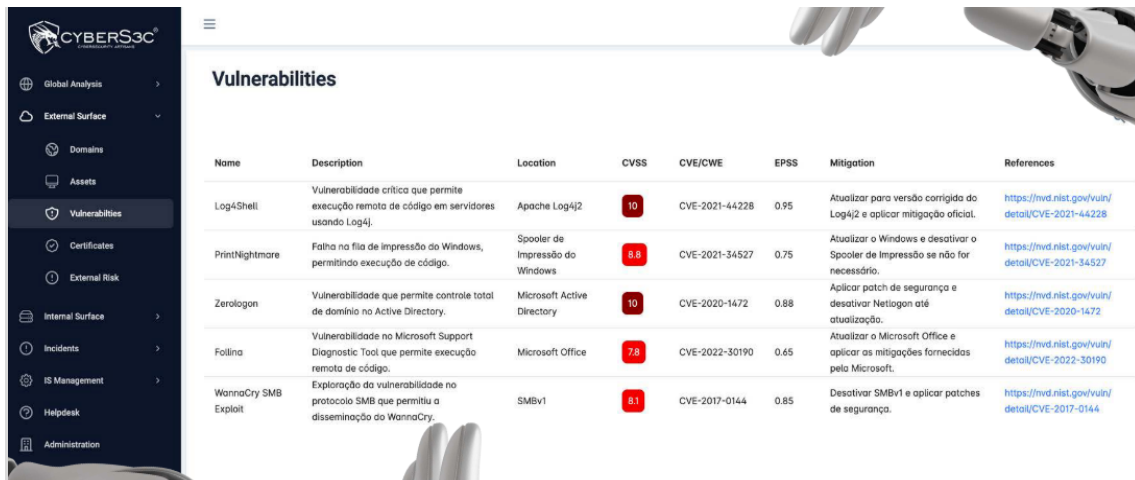
4.6.1 API CENTRAL - A API centraliza todas as funcionalidades do serviço que vamos implementar permitindo a integração com a plataforma, utilizando uma linguagem simples como Python e com a ajuda de algumas frameworks para aumentar a simplicidade, eficiência e agilidade de alguns processos. Esta API oferece também protocolos de segurança e um alto nível de desempenho para garantir respostas rápidas para requisições frequentes.

4.6.1 Módulo de Corelacionamento de Dados – Este módulo responsável por processar e correlacionar dados, de várias fontes externas, como vulnerabilidades e IoCs para gerar insights mais profundos e robustos.

4.6.3 Painel de Gestão (Fronted) – Esta componente é essencial para oferecer uma interface amigável e interativa para uma melhor visualização por parte dos utilizadores da plataforma, e um melhor controlo das funcionalidades do serviço.

Esses componentes trabalham de forma integrada, permitindo que a solução seja robusta, escalável e eficaz no gerenciamento e mitigação de ameaças cibernéticas, atendendo aos objetivos propostos pela plataforma VIRIATUS.

4.7 Interfaces



Name	Description	Location	CVSS	CVE/CWE	EPSS	Mitigation	References
Log4Shell	Vulnerabilidade crítica que permite execução remota de código em servidores usando Log4j.	Apache Log4j2	10	CVE-2021-44228	0.95	Atualizar para versão corrigida do Log4j2 e aplicar mitigação oficial.	https://nvd.nist.gov/vuln/detail/CVE-2021-44228
PrintNightmare	Falha na fila de impressão do Windows, permitindo execução de código.	Spooler de Impressão do Windows	8.8	CVE-2021-34527	0.75	Atualizar o Windows e desativar o Spooler de Impressão se não for necessário.	https://nvd.nist.gov/vuln/detail/CVE-2021-34527
Zerologon	Vulnerabilidade que permite controle total de domínio no Active Directory.	Microsoft Active Directory	10	CVE-2020-1472	0.88	Aplicar patch de segurança e desativar Netlogon até atualização.	https://nvd.nist.gov/vuln/detail/CVE-2020-1472
Follina	Vulnerabilidade no Microsoft Support Diagnostic Tool que permite execução remota de código.	Microsoft Office	7.8	CVE-2022-30190	0.65	Atualizar o Microsoft Office e aplicar as mitigações fornecidas pela Microsoft.	https://nvd.nist.gov/vuln/detail/CVE-2022-30190
WannaCry SMB Exploit	Exploração da vulnerabilidade no protocolo SMB que permitiu a disseminação do WannaCry.	SMBv1	9.1	CVE-2017-0144	0.85	Desativar SMBv1 e aplicar patches de segurança.	https://nvd.nist.gov/vuln/detail/CVE-2017-0144

Figura 9 Painel de Vulnerabilidades

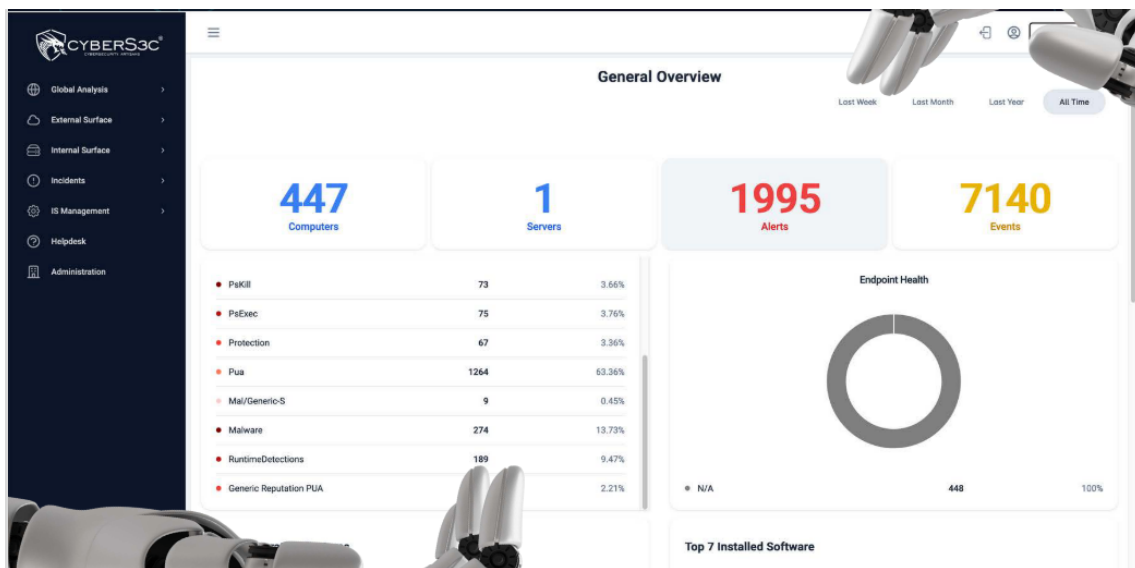


Figura 10 Painel geral de ativos, alertas e eventos

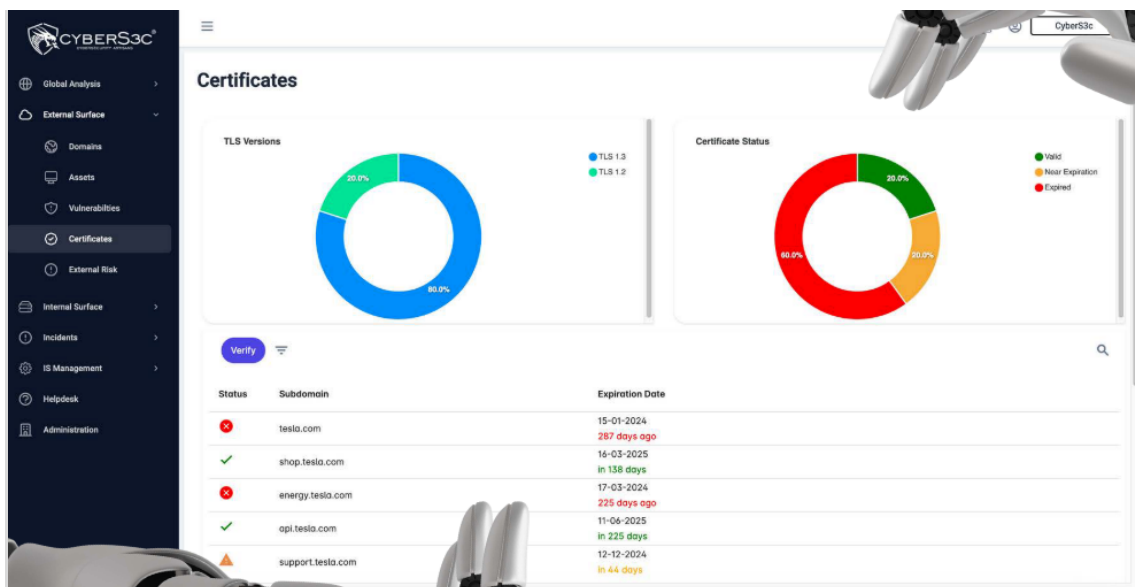


Figura 11 Painel de Certificados

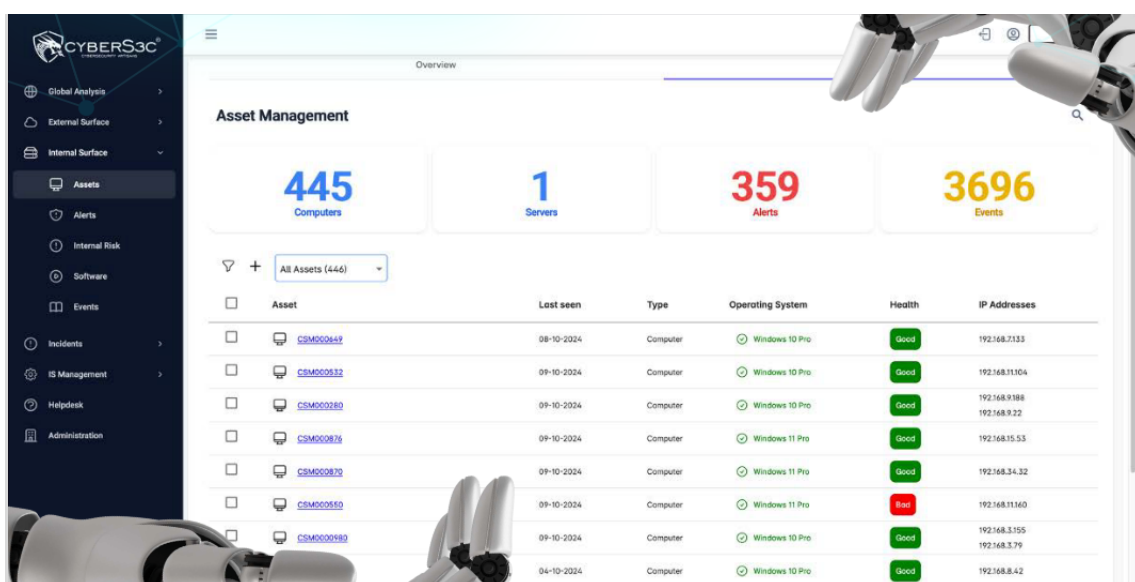


Figura 12 Painel dos Ativos

5 Método e Planeamento

5.1 Planeamento inicial

O plano de trabalho e o cronograma proposto para o Trabalho Final de Curso foram realizados em formato Gant, utilizando a aplicação [ProjectLibre] para o planeamento do trabalho. Além disso, foi utilizado o [Redmine] para a gestão das tarefas atribuídas semanalmente pela CyberS3c, permitindo um desenvolvimento contínuo do projeto, onde numa entrega futura vai substituir o Gant inicial.

A dificuldade inicial do projeto foi a compreensão do mesmo, uma vez que trabalhar num projeto com uma empresa introduz alguma complexidade até se alcançar o alinhamento necessário. Entender e instalar as tecnologias iniciais foi um processo complicado, sobretudo porque nunca tínhamos tido contacto prévio com a área de segurança cibernética.

Lista de Entregáveis:

- Entrega do Relatório Intercalar 1.º Semestre
- Entrega do Relatório Intercalar 2.º Semestre
- Entrega do Relatório Final
- Entrega do Projeto

Lista de Tarefas:

Para uma melhor compreensão do planeamento, segue abaixo uma Figura 13 Gant que apresenta o mesmo, elaborada no [ProjectLibre], representando o planeamento provisório e inicial definido por nós em colaboração com a CyberS3c.

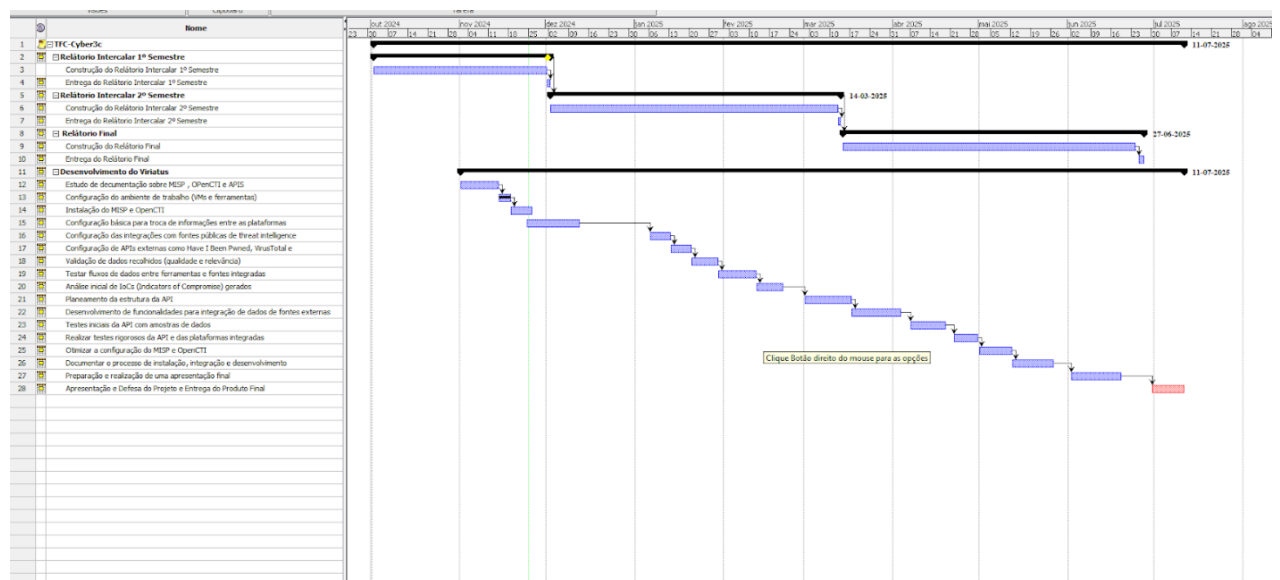


Figura 13 Gant

Bibliografia

[Rapid7insightVM] <https://www.rapid7.com/>, acedido em Nov.2024.

[Qualys VMDR] <https://www.qualys.com/>, acedido em Nov.2024.

[Tenable.sc] <https://www.tenable.com/>, acedido em Nov.2024.

[CyberS3c] <https://www.cybers3c.pt/sobre-nos/>, acedido em Nov.2024.

[NIS 2] <https://www.cncs.gov.pt/pt/diretiva-sri-2-nis-2/> , acedido em Nov.2024

[CISO virtual] <https://fieldeffect.com/blog/what-is-a-virtual-ciso>, acedido em Nov.2024

[Sophos] <https://fieldeffect.com/blog/what-is-a-virtual-ciso>, acedido em Nov.2024

[Checkpoint] <https://www.checkpoint.com/pt/>, acedido em Nov.2024

[Microsoft] <https://www.microsoft.com/pt-pt>, acedido em Nov.2024

[Fortinet] <https://www.fortinet.com/br>, acedido em Nov.2024

[ProjectLibre] <https://www.projectlibre.com/products>, acedido em Nov.2024

[Redmine] <https://www.redmine.org/>, acedido em Nov.2024

[ODS9] <https://ods.pt/objectivos/9-inovacao-e-infraestruturas/>, acedido em Nov.2024

[ODS16] <https://ods.pt/objectivos/16-paz-e-justica/> ,acedido em Nov.2024

[Luís Rato] <https://www.itsecurity.pt/news/analysis/como-a-inteligencia-artificial-impacta-a-ciberseguranca> ,acedido em Nov.2024