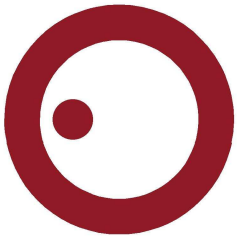


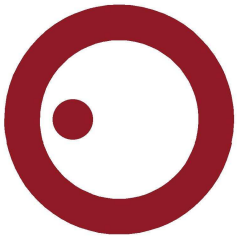
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

AVALIAÇÃO DE FERRAMENTAS DE BREACH AND ATTACK SIMULATION

ESTUDANTE RICARDO JORGE AGUIAR PÊGO

Leiria, setembro de 2023



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

AVALIAÇÃO DE FERRAMENTAS DE BREACH AND ATTACK SIMULATION

ESTUDANTE RICARDO JORGE AGUIAR PÊGO
Número: 2212982

Projeto realizado sob orientação do Professor Carlos Jorge Machado Antunes (carlos.machado@ipleiria.pt).

Leiria, setembro de 2023

AGRADECIMENTOS

Gostaria de expressar a minha sincera gratidão a todas as pessoas que contribuíram para a realização deste projeto final de Mestrado.

Ao meu orientador, professor Carlos Antunes, pela sua constante ajuda e disponibilidade.

Um especial agradecimento à minha família pelo apoio inabalável ao longo destes 24 anos, é graças à educação que providenciaram e aos valores transmitidos que cheguei onde cheguei até ao momento.

Agradeço do fundo do meu coração à minha incrível namorada, pelo apoio, motivação e compreensão. A tua presença ao meu lado foi fundamental para que eu conseguisse superar os desafios e alcançar este marco na minha jornada académica.

Muito obrigado a todos!

RESUMO

O constante surgimento de novas ciberameaças cada vez mais sofisticadas representa um desafio significativo para as organizações. Além dos desafios inerentes às ciberameaças em si, existem outros aspetos que impactam as organizações, principalmente no âmbito financeiro e de profissionais. Isso deve-se à necessidade de aquisição de controlos de segurança para diversos vetores de ataque, bem como à capacidade humana de configurar esses controlos de forma eficaz. Isso torna-se ainda mais complexo devido à constante evolução das infraestruturas de tecnologia, o que pode levar a lacunas nas configurações de segurança.

Nesse contexto, as ferramentas de *Breach and Attack Simulation* (BAS) desempenham um papel crucial. Elas permitem a avaliação contínua da segurança num ambiente corporativo, verificando a eficácia dos controlos de segurança face às ameaças em constante evolução. Estas ferramentas oferecem visibilidade sobre possíveis vulnerabilidades existentes, possibilitando que essas falhas sejam corrigidas antes que ocorra um ciberataque. Isso permite que as organizações adotem uma abordagem proativa na defesa cibernética, em vez de reagir apenas após um incidente ter ocorrido.

O objetivo principal deste projeto consiste em efetuar uma avaliação comparativa das funcionalidades de duas ferramentas de BAS - Cymulate e SafeBreach. A finalidade dessa avaliação é selecionar a ferramenta que melhor atenda aos critérios estabelecidos como resultado da comparação.

Para realizar a avaliação, foram desenvolvidos critérios de comparação e estabelecida uma infraestrutura de testes de pequena escala. Para além disso, foram analisadas de forma aprofundada as ferramentas mencionadas anteriormente, de modo a determinar a ferramenta BAS mais adequada.

ABSTRACT

The constant emergence of new and increasingly sophisticated cyber threats represents a significant challenge for organizations. In addition to the challenges inherent in the cyber threats themselves, there are other aspects that impact organizations, mainly in the financial and professional spheres. This is due to the need to acquire security controls for various attack vectors, as well as the human capacity to configure these controls effectively. This is made even more complex by the constant evolution of technology infrastructures, which can lead to gaps in security configurations.

In this context, BAS tools play a crucial role. They enable the continuous assessment of security in a corporate environment, verifying the effectiveness of security controls in the face of constantly evolving threats. These tools provide visibility into possible existing vulnerabilities, enabling these flaws to be corrected before a cyberattack occurs. This allows organizations to adopt a proactive approach to cyber defence, rather than reacting only after an incident has occurred.

The main objective of this project is to carry out a comparative evaluation of the functionalities of two BAS tools - Cymulate and SafeBreach. The aim of this evaluation is to select the tool that best meets the criteria established as a result of the comparison.

To carry out the evaluation, comparison criteria were developed and a small-scale testing infrastructure was established. In addition, the aforementioned tools were analyzed in depth in order to determine the most suitable BAS tool.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

APT	Advanced Persistent Threat.
ASM	Attack Surface Management.
ASV	Automated Security Validation.
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge.
BAS	Breach and Attack Simulation.
BYOD	Bring Your Own Device.
C&C	Command and Control.
CDR	Content Disarm and Reconstruction.
CEO	Chief Executive Officer.
CERT	Community Emergency Response Team.
CISA	Cybersecurity & Infrastructure Security Agency.
CISO	Chief Information Security Officer.
CNCS	Centro Nacional de Cibersegurança.
CTO	Chief Technology Officer.
CVE	Common Vulnerabilities and Exposures.
DDoS	Distributed Denial of Service.
DLL	Dynamic Link Library.
DLP	Data Loss Prevention.
DNS	Domain Name System.
DoS	Denial of Service.
EDR	Endpoint Detection and Response.

EPP	Endpoint Protection Platform.
FBI	Fereal Bureau of Investigation.
HTTP	Hypertext Transfer Protocol.
IDC	International Data Corporation.
IDF	Israel Defense Forces.
IOC	Indicators of Compromise.
IP	Internet Protocol.
MPS	Mail Protection Service.
PoC	Proof of Concept.
RNCSIRT	Rede Nacional Computer Security Incident Response Team.
SaaS	Software as a Service.
SEG	Secure Email Gateways.
SLA	Service Level Agreement.
SMEX	Scanmail for Exchange.
SO	Sistema Operativo.
SOAR	Security Orchestration, Automation and Response.
TTP	Tactics, Techniques, and Procedures.
URL	Uniform Resource Locator.
WWW	World Wide Web.

1

INTRODUÇÃO

Ao longo deste projeto iremos falar sobre ferramentas BAS. Este é um tipo de método avançado de testes de segurança, cujo objetivo é identificar diferentes vulnerabilidades nos controlos de segurança existentes, simulando as vias e técnicas de ataque suscetíveis de serem utilizadas por agentes maliciosos. Uma simulação de ataque permite às organizações avaliarem os seus controlos de segurança e a sua capacidade de detetar e atenuar as ciberameaças.

As simulações efetuadas de forma regular fornecem informações vitais para ajudar uma organização a medir, gerir e melhorar a capacidade dos seus sistemas para defender-se eficazmente contra ciberataques. Podem também permitir que a organização identifique potenciais vulnerabilidades ou outros problemas numa fase inicial.

Foram selecionadas quatro soluções de BAS, no entanto, ao longo deste projeto são comparadas duas soluções BAS para a finalidade de aquisição, a SafeBreach e a Cymulate.

A SafeBreach é uma empresa de segurança cibernética que oferece uma plataforma para a validação contínua da segurança cibernética corporativa. A sua plataforma proporciona uma abordagem abrangente e automatizada à simulação de ataques cibernéticos, incluindo *phishing*, *malware* e *Advanced Persistent Threats* (APTs).

A Cymulate permite às organizações testarem a sua postura de segurança contra vários cenários de ciberataque e obter um relatório sobre as vulnerabilidades encontradas e a eficácia das soluções de segurança em vigor. Permite às organizações realizarem simulações de ataques cibernéticos, incluindo APTs e ataques direcionados.

Tanto o SafeBreach como o Cymulate são uma solução baseada em *Software as a Service* (SaaS) e oferecem uma vasta gama de características e opções para que as organizações possam personalizar as suas simulações, segundo os seus requisitos específicos. Têm também capacidades de elaborar relatórios que fornecem às organizações informações detalhadas sobre as vulnerabilidades encontradas e a eficácia das

suas medidas de segurança, ajudando as organizações a tomar decisões informadas sobre a sua estratégia e orçamento de segurança cibernética.

1.1 ÂMBITO

A cibersegurança é um tema cada vez mais discutido e necessário. Este tema tem impacto nos indivíduos e nas organizações diariamente. Em Portugal de acordo com o Centro Nacional de Cibersegurança (CNCS) (CNCS, 2022), entre 2009 e 2021 houve um aumento de cerca de 1000% de cibercrimes registados pelas autoridades policiais passando de 2334 para 23409 demonstrando por isso a evolução da cibercriminalidade. Os membros da Rede Nacional *Computer Security Incident Response Team* (RNCSIRT) registaram um total de 46327 incidentes em 2021, sendo que as principais ciberameaças foram o *Phishing/Smishing* e *Ransomware*. Estes dados alarmantes e as ameaças diárias que têm como alvo as organizações representam um esforço de investimento significativo na cibersegurança, que por vezes demonstra-se insuficiente. No entanto, o orçamento não é o único problema, por vezes os erros de configuração e otimização das camadas de defesa fornecem uma falsa sensação de segurança, demonstrando também o mau aproveitamento deste orçamento. Para que o risco destas ameaças sejam menores e se retire o maior proveito possível do investimento efetuado pelas organizações, o uso de ferramentas BAS são de extrema importância. Este tipo de ferramentas espelha a eficácia dos controlos de segurança e os pontos que ainda podem e devem ser melhorados.

1.2 MOTIVAÇÃO E OBJETIVOS

As ferramentas BAS oferecem às empresas, empenhadas na sua cibersegurança, funcionalidades que permitem validar a eficácia dos controlos de segurança implementados, sendo uma componente de elevada importância na estratégia das organizações, isto porque permite uma abordagem proativa à ciberdefesa, dando a capacidade de colmatar as falhas existentes antes dos ataques serem efetuados, possibilitando caminhar para uma ciber-resiliência mais eficaz. O objetivo deste projeto é efetuar a comparação entre ferramentas BAS, explorando as funcionalidades destas ferramentas e a sua capacidade de resposta para os critérios estipulados, concluindo com a seleção de uma das ferramentas. As ferramentas selecionadas foram parcialmente baseadas nos produtos proferidos pela Gartner (Inc., 2023) e, inicialmente, foi escolhido explorar a Pentera, Darktrace Prevent, Picus Security,

Cymulate e a SafeBreach. No entanto, foram excluídas três das cinco escolhas selecionadas:

- A Pentera porque, para além de ser um *Automated Security Validation* (ASV), que se foca no processo de avaliação e verificação automatizada da segurança de *endpoints*, aplicações e redes. Não foi obtida qualquer resposta para um período de experimentação, apesar da insistência;
- A Darktrace Prevent por não se enquadrar nestes testes, dado tratar-se de um *Attack Surface Management* (ASM). Este efetua o processo de identificação, monitorização e gestão contínuas de todos os ativos internos e externos ligados à Internet para potenciais vetores de ataque e exposições (*What is Attack Surface Management ?* 2023);
- A Picus Security porque, embora tenha obtido acesso à ferramenta, não foi uma experiência comparável às restantes, estando possivelmente bastante limitada por se tratar de uma versão experimental.

Desta forma, apenas a Cymulate e SafeBreach vão ser submetidas a avaliação na íntegra. Durante este projeto pretende-se responder a questões como:

- O que é uma ferramenta BAS?
- Quais as equipas de cibersegurança que operam este tipo de ferramentas e onde se posiciona esta ferramenta?
- Quais as funcionalidades das diferentes ferramentas?
- Quais os critérios comparativos para as ferramentas BAS?
- O que é mais valorizado nas ferramentas comparadas?
- Qual é a ferramenta que se enquadra melhor para os critérios descritos?

1.3 ESTRUTURA DO DOCUMENTO

Nesta secção são mencionados os capítulos deste documento e o que cada um consiste:

- Introdução:
  - Informação sobre o âmbito do projeto;
  - Motivação e objetivos que se pretende alcançar com o mesmo;
  - Calendarização do projeto;

- Desenvolvimento:
  - Descrição das três diferentes equipas *blue team*, *red team* e *purple team* e os seus respecivos papéis;
  - Descrição do que se entende por ferramenta BAS, onde também é abordada a infraestrutura de testes criada;
  - Descrição sobre os três vetores de ataque principais;
  - Descrição sobre a *framework* Mitre ATT&CK e os seus benefícios;
  - Explicação sobre os critérios que são usados como forma de comparação das ferramentas BAS;
  - Abordada toda a experiência obtida com as ferramentas do Cymulate e da SafeBreach;
- Conclusão - Análise comparativa entre as ferramentas e concluir sobre qual seria a melhor opção;

1.4 PLANEAMENTO DO PROJETO

Este projeto tem a duração de um ano letivo constituído por dois semestres, traduzindo-se em 10 meses. O planeamento do projeto divide-se em quatro fases:

1. Pesquisa;
2. Implementação;
3. Exploração;
4. Redação;

A fase de pesquisa consistiu na investigação das ferramentas BAS do mercado, e foi selecionado quatro delas para efetuar um *Proof of Concept* (PoC). Durante a fase de implementação, foi preparado o ambiente de testes, efetuada a instalação do agente simulador e configurados os vetores necessários para a execução dos testes. Já na fase de exploração verificou-se e anotou-se os pormenores das diferentes funcionalidades que a ferramenta fornece. Por último foi introduzida toda a informação recolhida e efetuado o objetivo do projeto, que é comparar as ferramentas entre si e concluir qual poderá ser a mais vantajosa para os critérios estipulados à partida. A duração das várias fases foram inseridas num diagrama de Gantt representado na figura 1, e estas foram distribuídas da seguinte forma:

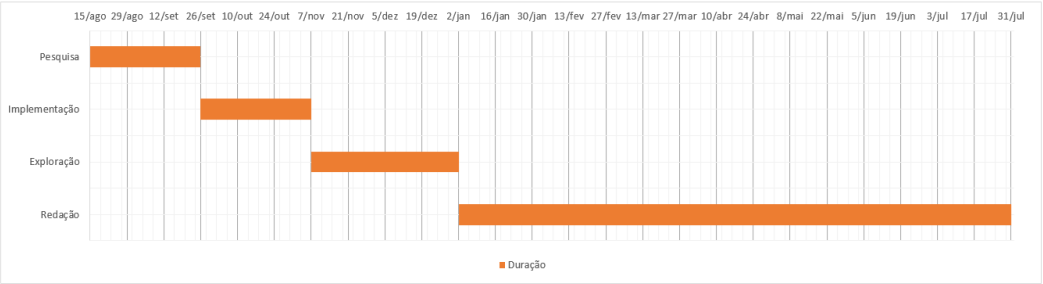


Figura 1: Diagrama de Gantt do planeamento do projeto

2

TRABALHO RELACIONADO

Neste capítulo, é apresentada uma revisão de diversas fontes que abordam o tema das ferramentas BAS e/ou que efetuam comparações entre as soluções Cymulate e SafeBreach. A inclusão dessas fontes diversificadas visa garantir uma abordagem abrangente, capaz de apresentar um panorama completo sobre esta ferramenta e as respetivas soluções.

O objetivo desta análise é fornecer um entendimento geral das funcionalidades e capacidades das ferramentas BAS, além de facultar diferentes pontos de vista relativamente a este tema. Pretende-se assim, identificar critérios que possam ajudar organizações e profissionais de cibersegurança a tomar decisões informadas sobre a seleção da solução mais adequada para as suas necessidades de avaliação e aumento da eficácia dos controlos de segurança.

Para este efeito foram analisados três artigos, relacionados com a ferramenta BAS:

- "Breach Attack and Simulation: A Critical Tool to Test the Efficacy of Security Controls";
- "Top breach and attack simulation use cases";
- "Comparing and Contrasting Cymulate Security Posture Validation Solution with SafeBreach".

De seguida é apresentado o conteúdo destes artigos, onde se apresentam os benefícios deste tipo de ferramenta, de que forma podem ser utilizadas e efetuada uma comparação entre Cymulate e SafeBreach.

2.1 CIBERSEGURANÇA COM BREACH ATTACK AND SIMULATION (BAS): UMA ABORDAGEM PROATIVA PARA PROTEGER AS ORGANIZAÇÕES

O primeiro artigo mencionado foi publicado em 2021 pela IDC (*International Data Corporation*) é abordado o tema de ferramentas BAS e os seus benefícios.

O panorama da cibersegurança enfrenta desafios cada vez mais complexos na defesa contra ameaças. À medida que estas evoluem, os vetores de ataque diversificam-se e os métodos dos agentes maliciosos tornam-se mais sofisticados.

Segundo a IDC, as empresas mundiais investem mais de 100 biliões de dólares em produtos e serviços de segurança para combater as ciberameaças. Para executivos e conselhos administrativos, é crucial demonstrar a eficácia destes gastos. No entanto, quantificar e justificar o montante adequado continua a ser um desafio, especialmente para as equipas de cibersegurança. A procura por recursos adicionais para fortalecer a postura de segurança é dificultada pelo aumento das ameaças cibernéticas, que afetam a reputação e as finanças de empresas em diversos setores.

À medida que as organizações procuram maneiras de evidenciar a eficácia dos investimentos em segurança e das políticas implementadas para lidar com as ameaças, os testes de vulnerabilidade emergem como uma componente vital das práticas de gestão de vulnerabilidades das equipas de segurança.

A maioria das empresas implementou algum tipo de procedimento para administrar as vulnerabilidades presentes no seu ambiente. Após uma avaliação abrangente dos riscos cibernéticos, visando compreender onde estão localizadas as ameaças mais elevadas (ou com maior impacto) para a organização, são feitos investimentos em mecanismos de segurança. Além disso, políticas e processos são desenvolvidos para gerir esses riscos. Os testes de gestão de vulnerabilidades constituem normalmente o próximo passo, visando validar a eficácia dos controlos de segurança implementados para enfrentar os riscos cibernéticos.

Existem várias abordagens de testes que as organizações utilizam como parte das suas práticas de gestão de vulnerabilidades. Quatro das mais comuns estão listadas abaixo:

- Teste de Penetração - É uma abordagem comum de testes usada por empresas para detetar vulnerabilidades em toda a infraestrutura. Um teste de penetração envolve especialistas em segurança altamente qualificados, que utilizam ferramentas e métodos de ataque usados por atacantes reais para alcançar um objetivo específico de comprometimento previamente definido. O teste de penetração abrange redes, aplicações e *endpoints*.
- Red Team - Realiza '*hacking* ético' ao imitar um ator malicioso por via de métodos furtivos, contornando os controlos defensivos e identificando falhas na estratégia de cibersegurança da organização para obter uma compreensão mais aprofundada de como a organização deteta e responde a ataques do

mundo real. Os resultados de um exercício de *red team* ajudam a identificar as melhorias necessárias nos controlos de segurança.

- Blue Team - É uma equipa interna de segurança que se defende contra ataques reais e atividades da *red team*. As *blue teams* devem destacar-se das equipas de segurança convencionais devido à missão de proporcionar uma defesa cibernética constante e contínua contra todas as formas de ciberataques.
- Purple Team - O objetivo desta equipa é alinhar as atividades da *red* e *blue team* e tirar partido das perceções obtidas com estas atividades para proporcionar uma experiência de APT realista e completa, bem como identificar vulnerabilidades prioritárias para a organização.

Apesar de serem comuns nas práticas organizacionais, estas abordagens de teste de vulnerabilidade enfrentam diversos desafios. Em primeiro lugar, tais métodos revestem-se de um carácter profundamente manual e requerem uma considerável alocução de recursos, o que acarreta custos substanciais e uma escassez de pessoal qualificado em várias organizações, no que respeita à realização destes testes. Ainda que os resultados destes testes se revelem essenciais para fundamentar as ações da organização, a sua realização ocorre raramente, em grande medida devido aos custos envolvidos e à ausência dos recursos qualificados supramencionados.

Por fim, todas essas abordagens oferecem uma visão pontual da postura de segurança de uma organização. Visto que o cenário de segurança e as arquiteturas de IT das empresas são fluidos e estão em constante evolução, as abordagens tradicionais de teste de vulnerabilidade geram pouco valor.

Para superar esses desafios, é crucial explorar métodos mais ágeis e automatizados que possam adaptar-se às mudanças contínuas no cenário de ameaças e nas infraestruturas de IT.

Ainda que as ofertas do BAS englobem grande parte dos elementos inerentes aos testes de vulnerabilidade tradicionais, ele distingue-se de forma crucial. As principais funcionalidades de uma ferramenta BAS são as seguintes:

- Simular ataques - Simulação de ameaças reais,
- Visualizar exposições - Identificar pontos de exposição,
- Priorizar - Atribuir uma classificação de criticidade às vulnerabilidades exploráveis,
- Remediar - Corrigir as falhas identificadas.

A discrepância entre uma ferramenta BAS e as abordagens tradicionais residem na implementação de um processo de automação de validação num ambiente corporativo, o qual capacita as equipas de IT e de cibersegurança na deteção de configurações incorretas, erros humanos, falhas de registo e questões básicas de higiene em IT. Com base nestas informações, a equipa de cibersegurança está habilitada a adotar as medidas recomendadas para colmatar as falhas, corrigir as configurações inadequadas e reforçar a gestão de credenciais.

Outro fator distinto de uma ferramenta BAS é a diversidade de modalidades pelas quais um teste de vulnerabilidades pode ser executado. As alternativas de teste englobam testes pontuais, testes contínuos ou testes intermitentes de acordo com intervalos predefinidos. Este panorama proporciona às equipas de segurança uma flexibilidade significativamente alargada na frequência com que podem efetuar testes de vulnerabilidade.

Para concluir, a IDC está convicta de que as ferramentas BAS são um elemento vital na estratégia de cibersegurança de uma empresa, uma vez que proporcionam às organizações um conjunto sólido de características e funcionalidades que não apenas auxiliam a validar a eficácia dos controlos de segurança implementados, como também possibilitam uma abordagem mais proativa à ciberdefesa, recorrendo à automatização de validações. Este panorama tornou-se um tópico recorrente nos serviços de segurança, onde a vontade de atingir a ciber-resiliência assenta na capacidade de monitorizar de forma contínua o ambiente com vista à deteção antecipada de falhas e ameaças, impulsionando assim a prontidão na resolução de questões e minimizando o impacto sobre a organização (*Breach Attack & Simulation: Security Efficacy & BAS | IDC Blog* 2023).

2.2 AVALIAÇÃO DE CIBERSEGURANÇA: CASOS PRÁTICOS DE SIMULAÇÕES DE ATAQUE

O segundo artigo foi publicado em Maio de 2023 na TechTarget, aborda as funcionalidades e casos práticos para uma ferramenta BAS.

Todas as equipas de cibersegurança preocupam-se com a falta de eficácia dos controlos, processos e procedimentos de segurança implementados no bloqueio ou diminuição do impacto de um ataque, bem como com a rapidez com que os seus planos de recuperação (DR) irão manter ou restaurar os sistemas para operações normais. Muitas organizações recorrem a testes de penetração para avaliar a eficácia do seu programa de segurança.

Os testes de penetração são geralmente exercícios pontuais que requerem muitos recursos e fornecem apenas uma imagem instantânea do estado da segurança num momento específico. Para acompanhar os ambientes de IT em constante mudança e o cenário de ameaças em evolução contínua, as equipas de cibersegurança precisam de recorrer a exercícios frequentes para testar consistentemente as defesas de segurança. Isso garante que estas estejam sempre configuradas corretamente e capazes de detetar e responder a qualquer ciberataque.

As simulações podem ser executadas em qualquer momento, no entanto, segundo este artigo, as organizações devem particularmente considerar os seguintes quatro cenários de aplicação essenciais:

- Avaliar, verificar e validar os controlos de segurança - As simulações realizam verificações regulares para assegurar que os atuais controlos de segurança estão devidamente integrados e configurados para detetar e bloquear ataques com sucesso. As frequentes atualizações de *software* e sistemas podem conduzir a desvios de configuração ou erros que resultam em falhas de segurança inesperadas. A natureza iterativa e o âmbito mais abrangente das simulações, em comparação com os testes de penetração, manifestam de uma forma mais fácil a existência de falhas nos controlos de segurança. Não só a eficácia dos controlos de segurança é validada, como também se contribui para melhorar os tempos de resposta a incidentes.
- Aumento da eficácia e eficiência - Uma ferramenta BAS tem a capacidade de melhorar dois indicadores essenciais de segurança: o tempo médio de deteção e o tempo médio de resposta. A prática regular de simulações permite que as equipas de segurança ajustem as suas ferramentas de monitorização e deteção. Além disso, auxilia essas equipas a aprender a responder de maneira mais eficaz a diferentes tipos de ataques, facilitando a atualização dos procedimentos para melhorar tanto a eficácia quanto a rapidez das ações dos responsáveis. As simulações também desempenham um papel importante na verificação de potenciais efeitos adversos nas medidas de segurança decorrentes de atualizações de *patches* e outras alterações no sistema.
- Avaliação do comportamento do utilizador - Os colaboradores frequentemente representam o elo mais vulnerável no contexto de cibersegurança de uma organização, sendo que muitos compromissos de sistemas e dados provêm de erros humanos. Utilizadores podem inadvertidamente auxiliar os atacantes ao carregar em *links* ou anexos maliciosos e ao não seguir estritamente os protocolos de segurança estabelecidos. Os BAS têm a funcionalidade para efetuar

simulações de *phishing* e estas campanhas de *Phishing Awareness* representam um método altamente eficaz para avaliar a resposta dos funcionários face aos ataques deste tipo. Ao serem construídos com base em eventos reais e em campanhas conhecidas, adaptadas para se adequarem às especificidades de cada indivíduo, departamento, empresa ou país. Os resultados do BAS oferecem métricas objetivas para aferir a conformidade com as normas internas de segurança. Além disso, tais simulações permitem avaliar a eficácia da formação atual em cibersegurança e determinar quais colaboradores necessitam de formação adicional.

À medida que as infraestruturas de rede corporativa evoluem para configurações cada vez mais complexas, orientadas para a *cloud*, e o trabalho remoto amplia essa complexidade, as simulações de ataques emergem como um método eficaz e abrangente para avaliar a verdadeira resiliência de uma organização face aos ciberataques. Essas simulações também contribuem para a ampliação do conhecimento, compreensão e eficácia das equipas responsáveis pela deteção, prevenção e resposta a incidentes.

De acordo com o artigo, mesmo com a adoção na utilização de um BAS, os testes de penetração e as atividades das equipas de cibersegurança continuarão a desempenhar um papel fundamental na garantia de uma sólida postura de segurança. Contudo, é vital lembrar que os resultados obtidos a partir de qualquer um destes testes apenas trarão benefícios se forem aplicados e se as vulnerabilidades e fragilidades identificadas forem corrigidas. Em cada ciclo subsequente de simulações, espera-se sempre observar melhorias e progressos positivos.(Cobb, 2023)

2.3 COMPARAÇÃO ENTRE AS FERRAMENTAS CYMULATE E SAFEBREACH

O terceiro artigo mencionado foi publicado em 2017 pela Cymulate, que pela sua natureza está desatualizada e é parcial, efetua comparações entre as funcionalidades da Cymulate e da SafeBreach.

As características em discussão enumeradas neste artigo são:

- Execução com segurança em ambientes de produção – Acreditam que a única forma de saber com certeza se as defesas são eficazes aos agentes maliciosos é testar no ambiente que se pretende proteger. Com vulnerabilidades, agentes maliciosos e outras modificações a acontecer diariamente, não há forma de

um ambiente de testes acompanhar ou visualizar e medir com precisão o risco real.

- Atualizações – Atualização da plataforma com novas ameaças;
- Funciona de forma nativa em todo o ambiente empresarial – Funcionamento em qualquer sistema operativo;
- Integrações – Utilização em qualquer ambiente e integração com controlos de segurança de terceiros;
- Abrangência de ataques – Cobertura total da cadeia de ataques;
- Utilização - Necessidade de formação especializada;
- Informação - Disponibilização de informação para a comunidade;

Passarei agora a transmitir os dados comparativos presentes neste artigo.

A SafeBreach, embora tenha recomendado anteriormente que os testes fossem efetuados apenas em ambientes de testes, desde então mudou de pensamento. Atualmente, assim como a Cymulate, a SafeBreach também valoriza os testes onde eles são mais importantes, em ambientes de produção.

Embora a maioria das soluções tenha algum tipo de alimentação de informações sobre ameaças, a maioria não atualiza as suas ferramentas de teste para as incluir automaticamente. Este é um erro crítico que a Cymulate não cometeu. De facto, um dos maiores pontos positivos da Cymulate é a sua equipa de investigadores que mantêm a solução constantemente atualizada, com novos TTPs (Tactics, Techniques, Procedures) e IoCs (Indicators of Compromise) a serem adicionados diariamente, 24 horas por dia, 7 dias por semana e 365 dias por ano aos modelos de teste.

Embora a SafeBreach tenha um *feed* de informações sobre ameaças e, tal como a Cymulate, agora adicione TTPs e IoCs à sua solução, existem diferenças. A Cymulate adiciona estes não só com base nos avisos do CERT dos EUA, mas também com base em várias atualizações da indústria e fontes de informação. Em alguns casos, esta é uma vantagem crítica para a Cymulate. Por exemplo, ambas as empresas cobriram os ataques ao MS Exchange, mas a Cymulate também se certificou de incluir a variedade de ataques APT e cópias que ocorreram após o ataque inicial.

A Cymulate considerava-se em 2017 a solução mais abrangente, por várias razões:

- Funciona de forma nativa em todo o ambiente empresarial.
- Está ligada a todos os tipos de controlos de segurança de terceiros, como a gestão de vulnerabilidades GRC (Governance Risk and Compliance), SIEM

(Security Incident and Event Management), EDR (Endpoint Detection and Response) e plataformas SOAR.

- Ao mesmo tempo que simula um atacante real, a Cymulate tem a capacidade de encadear testes em toda a cadeia de destruição e de tomada de decisões que lhe permitem chegar a um beco, depois mudar de direção e tentar técnicas alternativas para continuar a testar.

É aqui que os contrastes entre as duas soluções tornam-se maiores. À data de publicação deste artigo pela Cymulate, esta considerava que a SafeBreach, tal como outras soluções antigas, tinham apenas testes individualizados finitos que não funcionam verdadeiramente de forma sequencial em todo o ambiente para o testar, nem tomam decisões para se moverem como atacantes reais.

A melhor forma de a Cymulate ser mais abrangente do que as soluções anteriores, é através da sua cobertura total de toda a cadeia de ataques na área da cibersegurança.

- Reconnaissance - Habilidade de realizar análises na Internet e na Darknet com o propósito de identificar atempadamente informações potencialmente exploráveis por um agente malicioso antes da execução de qualquer ataque;
- Phishing Campaigns - As campanhas de *phishing* visam avaliar a consciencialização dos colaboradores relativamente à segurança, por meio da realização de simulações de ataques de *phishing*. Essas simulações pretendem identificar vulnerabilidades na estrutura organizacional e capacitar os colaboradores a defenderem-se contra tais ataques
- Email Gateway - Avalia as capacidades fundamentais das medidas de segurança do *e-mail*, abrangendo aspetos como a deteção de conteúdo malicioso, identificação precisa do formato e ocultação de ficheiros, identificação de hiperligações maliciosas, deteção de comunicações C2 e prevenção contra o comprometimento de credenciais;
- Web Gateway - Realiza uma avaliação da eficácia das suas capacidades de filtragem dinâmica de URLs, filtragem do conteúdo, deteção de cargas maliciosas e defesa contra *ransomware*. Isso é feito por meio do acesso a endereços Internet Protocol (IP) e URLs reais, os quais estão vinculados a atividades de maliciosas, C2 e outros *sites*;
- Web Application Firewall - Os testes de WAF abrangem diversos cenários, como injeção de SQL, Cross-site scripting (XSS), injeções de comandos e XML, juntamente com outras vulnerabilidades e explorações pertinentes;

- Endpoint - Possibilita implementar e executar simulações de *ransomware*, *trojans*, *worms* e vírus num *endpoint* dedicado, garantindo um ambiente controlado e seguro. Esta abordagem viabiliza testes abrangentes que englobam todos os âmbitos da segurança do *endpoint*, porém não se limitam a: deteção por comportamento malicioso, de vírus e atenuação de vulnerabilidades conhecidas. Adicionalmente, são incluídos um amplo leque de testes que envolvem PowerShell, manipulação de registos, *scripts* e outros cenários de exploração;
- Lateral Movement - A abrangente avaliação de movimentos laterais engloba testes tanto oportunísticos como precisos, recorrendo a mecanismos de credenciais, como Resolução de Nomes Multicast Link-Local (LLMNR) e Serviço de Nomes NetBIOS (NBT-NS), bem como a recolha de dados de DNS, entre outras técnicas. Esta avaliação compreende a obtenção de credenciais do Active Directory (AD), tentativas de acesso SSH/SFTP, exposição à técnica de Kerberoasting e abordagens de força bruta;
- Data Exfiltration - A exfiltração de dados envolve a análise dos fluxos de entrada e saída de informações, como dados de identificação pessoal, cartões de crédito, informações financeiras e dados comerciais confidenciais. O propósito desta avaliação é verificar e assegurar a integridade dos ativos de informação, garantindo a limitação ao ambiente corporativo.

De acordo com o artigo, a SafeBreach demonstra um sólido portfólio de testes de *endpoint*, embora apresente falhas em testar em cadeia e efetuar cadeia de ataques. À semelhante de outras soluções *legacy*, não incorpora testes de reconhecimento crítico, campanhas de *phishing*, Web Application Firewall (WAF) e movimentos laterais. Embora disponha de algumas capacidades relacionadas com Web, correio eletrónico e exfiltração de dados, estas demonstram limitações. Na realidade, a SafeBreach não ostenta uma abordagem integral nem abrangente, conforme se requereria.

A Cymulate é uma plataforma SaaS (Software as a Service), que efetua atualizações automáticas e é gerida de forma automática. A sua implementação requer um único agente por ambiente, não exigindo a aquisição de serviços especializados ou um treino intensivo.

Por outro lado, a gestão e implementação da SafeBreach exigem vários meses de envolvimento com serviços profissionais e formação especializada.

A Cymulate optou por retribuir à comunidade, disponibilizando formações técnicas e de gestão de forma gratuita e online. Esta formação é proporcionada num ambiente imparcial, permitindo a evolução das competências por via de cursos e exercícios práticos, abordando uma diversidade de tópicos, desde a gestão de cibersegurança

até aptidões de trabalho em equipa, passando pela estrutura MITRE ATT&CK e muito mais. O programa engloba cursos e laboratórios, caso sejam bem sucedidos, recebem 8 créditos ISC CPE.

Embora um fornecedor estabelecido, o AttackIQ, também ofereça uma sólida gama de cursos online, lamentavelmente, tal não se verifica com a SafeBreach.

Em síntese, de acordo com a Cymulate, ainda que a SafeBreach supere em desempenho a maioria das soluções *legacy*, permanece substancialmente aquém em comparação com a abrangência da oferta proporcionada pela Cymulate.(Moshe, 2022c).

3

DESENVOLVIMENTO

Neste capítulo, são inicialmente apresentadas as diferentes equipas de cibersegurança e conceitos referentes às ferramentas BAS, onde será analisado profundamente duas soluções, da Cymulate e da SafeBreach. É ainda efetuada uma comparação entre ambas, para a seleção da que possui mais benefícios.

3.1 EQUIPAS DE CIBERSEGURANÇA

A *Blue Team*, *Red Team*, e *Purple Team* são equipas de segurança com diferentes papéis e responsabilidades.

A *Blue Team* é responsável pela defesa dos sistemas e redes de uma organização. Esta equipa está encarregue de identificar e mitigar as ameaças à segurança corporativa, e para manter a segurança dos sistemas e dados da organização. Utilizam várias ferramentas e técnicas, tais como sistemas de deteção de intrusão e ferramentas de *Security Information and Event Management* (SIEM), para detetar e responder a incidentes de segurança. Quando um sistema já está numa fase maturada é introduzida uma ferramenta de *Security Orchestration, Automation and Response* (SOAR) (Timonera, 2023).

A *Red Team* é responsável por realizar ataques reais aos sistemas e redes de uma organização, de modo a testar e avaliar a eficácia dos controlos de segurança corporativa. Utilizam várias técnicas, tais como testes de penetração e engenharia social, para identificar e explorar vulnerabilidades nos sistemas e redes da organização (Timonera, 2023).

A *Purple Team* é uma combinação da *Blue Team* e *Red Team*. Esta equipa trabalha em conjunto com as restantes para identificar e mitigar ameaças à segurança do ambiente corporativo, de modo a manter a integridade e a inviolabilidade dos sistemas e dados da organização. A equipa simula ataques reais aos sistemas e redes de uma organização, de modo a testar e avaliar a eficácia dos controlos de segurança da mesma. O principal objetivo da *purple team* é colmatar a lacuna entre a *blue*

team e a *red team*, e melhorar a postura global de segurança corporativa (Timonera, 2023) (Kunal Sehgal, 2023).

Para ajudar nesta tarefa da procura de vulnerabilidades, as equipas *purple team* utilizam ferramentas que ajudam a entender e a automatizar a validação dos controlos de segurança ao longo do tempo, como as ferramentas BAS.

3.2 CONCEITO BAS

Segundo a Gartner, as ferramentas BAS permitem que as organizações obtenham uma compreensão mais profunda das vulnerabilidades da postura de segurança, automatizando o teste de vetores de ameaça, como externos e internos, movimento lateral e exfiltração de dados. O BAS complementa o *red teaming* e os testes de penetração, mas não os pode substituir completamente. O BAS valida a postura de segurança de uma organização, testando a sua capacidade de detetar um conjunto de ataques simulados realizados por plataformas SaaS. Além disso, gera relatórios detalhados sobre as falhas de segurança e dá prioridade aos esforços de correção com base no nível de risco (Inc., 2023).

As funcionalidades gerais deste tipo de ferramentas são:

- Múltiplos Vetores de Ataque, no entanto, esta funcionalidade pode depender do tipo de licenciamento da ferramenta. Poderá ser necessário a aquisição de licenças por vetor;
- Mitre *Adversarial Tactics, Techniques and Common Knowledge* (ATT&CK), é uma *framework* de conhecimento base de táticas e técnicas. As organizações por norma usam esta *framework* para identificar falhas e priorizar mitigações com base no risco associado;
- Testes de forma contínua, isto porque podemos inserir agendamentos de testes com base na regularidade interessada, diária, semanal ou apenas mensal. Para demonstrar esta funcionalidade, na secção 3.7.3 são apresentados conjuntos de testes semanais que foram construídos;
- Integrações com controlos de segurança, de modo a determinar se existe visibilidade para aquele ataque e, caso se aplique, qual a ferramenta que está a efetuar a deteção e/ou mitigação de forma automática.

3.2.1 *Infraestrutura de Testes*

Em termos de infraestrutura, a que está em vigor para o PoC das ferramentas BAS, inclui a utilização de 2 dispositivos, um computador *desktop* que, para este projeto, tem o nome DKT e um *laptop* denominado LTP, ambos contêm o sistema operativo Windows 10 e o agente simulador. Esta infraestrutura está representada na figura 2. O DKT é o ambiente principal que é utilizado para a execução da grande maioria dos testes, sendo que o LTP é utilizado para certas categorias de testes que necessitam de uma máquina secundária, como por exemplo movimento lateral.

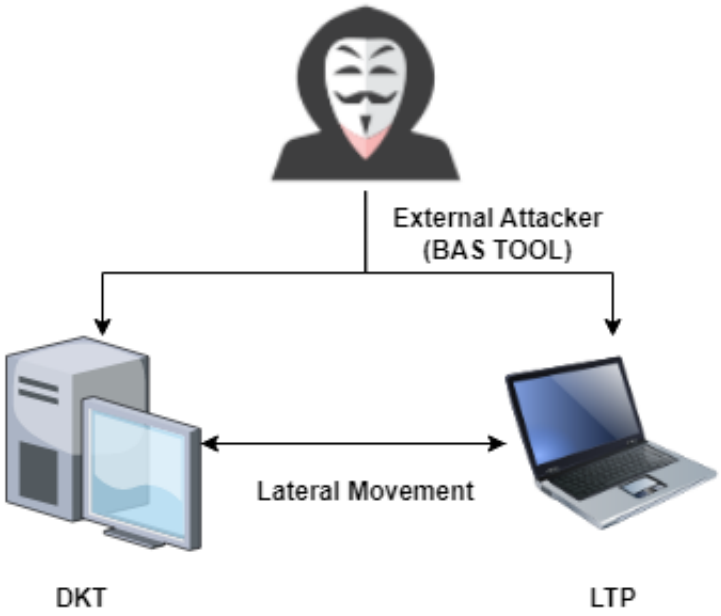


Figura 2: Infraestrutura de testes

Os dispositivos DKT e LTP, de forma a proteger o *endpoint* estão equipados com um *Endpoint Protection Platform* (EPP) da Trend Micro, e um *Endpoint Detection and Response* (EDR) da Crowdstrike.

Um EPP é uma solução implementada em *endpoints*, para evitar ataques de *malware* baseados em ficheiros, detetar atividades maliciosas e fornecer as capacidades de investigação e correção necessárias para responder a alertas e incidentes de segurança dinâmicos(*Definition of Endpoint Protection Platform (EPP) - Gartner Information Technology Glossary* 2023).

Um EDR é uma solução de segurança de *endpoints* de monitorização contínua para detetar e responder a ciberameaças, como *ransomware* e *malware* (Gartner, 2023).

No e-mail, os controlos de segurança são Anubis Networks como primeira camada e, como segunda, Trend *Scanmail for Exchange* (SMEX) dado que se trata de uma *mailbox on-premise*.

A Anubis Networks é uma empresa que possui *Mail Protection Service* (MPS), é simultaneamente uma solução de *Email Security Gateway Appliance* e um serviço de Cloud, que partilham o mesmo sistema central e que possui todas as funcionalidades para proteger adequadamente um ecossistema de correio eletrónico contra ameaças e riscos. (Mailspike, 2023)

A Trend SMEX é uma solução da Trend Micro que impede ataques por e-mail altamente direcionados e *spear phishing* através da utilização de deteção de *exploits* de documentos, *Web Reputation* aprimorado e *sandbox*, como parte da defesa personalizada contra APT. Só o ScanMail bloqueia ameaças tradicionais usando tecnologia de e-mail, arquivos e reputação web, junto à inteligência global de ameaças correlacionada na *cloud*. (*Scanmail for Exchange* 2023)

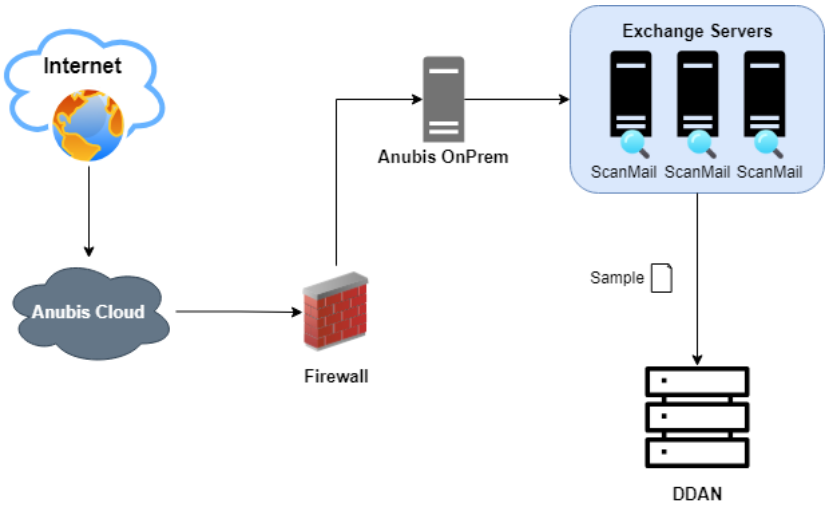


Figura 3: Infraestrutura de e-mail

Relativamente à rede, existe uma *firewall* perimétrica da Palo Alto ligada a uma *firewall* interna para a rede Wifi da Checkpoint. Esta é uma configuração de *firewall* em cadeia que ajuda a tornar a rede corporativa mais resiliente a ciberataques.

3.3 VETORES DE ATAQUE

Nesta secção são mencionados os diferentes métodos, técnicas ou pontos de entrada que os atacantes podem explorar de modo a comprometer a segurança de um sistema ou rede. São a partir dos vetores de ataque que se iniciam as tentativas de explorar vulnerabilidades ou falhas de configuração de segurança num dispositivo ou infraestrutura, para a realização de atividades maliciosas.

3.3.1 *Endpoint*

Um vetor de ataque por via de *endpoint* refere-se ao método utilizado pelos atacantes para comprometer um dispositivo. Este tipo de ataque pode ser refletido através de:

- *Malware* - Os atacantes utilizam *malware*, tais como *infostealers*, *trojans* e *ransomware*, para obterem acesso a informação e/ou controlo sobre um dispositivo;
- Engenharia social - Os atacantes utilizam técnicas de engenharia social, tais como *phishing*, *vishing*, ou *smishing*, para persuadir os utilizadores a revelarem informações sensíveis, tais como credenciais de *login* ou dados pessoais;
- Vulnerabilidades de *software* - Os atacantes exploram vulnerabilidades de segurança de um *software*, sistema operativo, ou *firmware* para obter acesso não autorizado a um dispositivo;
- Acesso físico - Os atacantes podem obter acesso a dispositivos através de meios físicos, tais como roubar um dispositivo ou inserir uma unidade USB com *software* malicioso;

Para proteger os *endpoints* de ataques, é importante manter os *softwares* e o sistema operativo atualizados, utilizar um EPP e EDR, não utilizar redes Wi-Fi públicas, aplicar medidas de segurança físicas, tais como a encriptação do dispositivo, não deixar o computador no carro à vista de todos ou suspender o mesmo após se ausentar do seu posto do trabalho. Para além disso, a educação e a formação dos utilizadores podem ajudar a prevenir ataques de engenharia social, sendo que estas formações são recomendadas de 4 em 4 meses (*How frequently do you run phishing campaigns? | Haekka Blog* 2023). É também cada vez mais importante a existência de uma política anti Bring Your Own Device (BYOD), isto porque os computadores pessoais não estão preparados para ameaças em comparação com os dispositivos corporativos (Lake, 2022).

3.3.2 *Email*

Um vetor de ataque por e-mail refere-se ao método utilizado pelos atacantes para comprometer credenciais ou até mesmo o *endpoint* via email, este também conhecido como ataque de engenharia social. Alguns exemplos de ataque por e-mail:

- *Phishing* - Este é o ataque mais comum, no qual um atacante envia um e-mail que aparenta ser de uma fonte legítima (tal como um banco ou até mesmo a organização para a qual trabalham) e pede ao destinatário que forneça informações sensíveis, tais como credenciais de *login* ou detalhes de cartão de crédito;
- *Spear-phishing* - Semelhante ao *phishing*, mas mais direcionado. Os atacantes pesquisam previamente a vítima para fazer com que o e-mail pareça mais legítimo, aumentando assim as probabilidades de sucesso;
- Anexos de *malwares* - Os atacantes enviam e-mails com anexos maliciosos que, quando abertos, infetam o dispositivo da vítima com *malware*, tais como o *ransomware* ou *spyware*;
- Ataques de *links* - Os atacantes incluem *links* em e-mails que, após interação, levam o utilizador a um *site* falso com aspeto legítimo, mas que foi concebido para roubar as credenciais de *login* ou outras informações sensíveis.

Para mitigação de ataques por email, é importante ser cauteloso ao abrir emails de remetentes desconhecidos, evitar carregar em *links* ou descarregar anexos de e-mails suspeitos, e usar senhas com os critérios recomendados por entidades reconhecidas, como a Microsoft, para além da utilização de autenticação de 2 fatores para as ferramentas corporativas. Além disso, é importante reportar os emails que possam passar pelos controlos de segurança, de modo a que possa ser analisado e adicionado os *Indicators of Compromise* (IoCs) às ferramentas de segurança existentes e/ou verificar métodos por forma a aumentar a eficácia destes mesmos controlos.

3.3.3 *Rede*

Um vetor de ataque de rede é uma técnica utilizada por *hackers* ou criminosos cibernéticos para explorar vulnerabilidades em uma rede, com a finalidade de obter acesso não autorizado a sistemas e informações sensíveis.

Existem vários tipos de vetores de ataque de rede, incluindo:

- Ataques de Denial of Service (DoS) - Envolvem o envio de uma grande quantidade de tráfego para um servidor ou rede para sobrecarregá-los e torná-los indisponíveis;
- Ataques de *phishing* - Envolvem o envio de *e-mails* ou mensagens falsas que parecem legítimas, para obter informações confidenciais do utilizador, como senhas e informações de *login*;
- Ataques de injeção de Structured Query Language (SQL) - Exploram vulnerabilidades em aplicações da *web* para inserir código SQL malicioso numa base de dados e aceder a informações confidenciais;
- Ataques Distributed Denial of Service (DDoS) - Envolvem o uso de vários dispositivos para enviar tráfego malicioso para um servidor ou rede, dificultando a identificação do computador de origem;
- Ataques de acesso remoto - Envolvem a exploração de vulnerabilidades em *software* de acesso remoto para ganhar acesso não autorizado a um sistema.

Estes são apenas alguns exemplos de vetores de ataque de rede. A melhor defesa contra estes ataques é manter software e sistemas atualizados, além de implementar medidas de segurança, como *firewalls* e criptografia de dados.

3.4 MITRE ATT&CK

A Mitre ATT&CK é uma *framework* desenvolvida em 2013 pela Mitre Corporation. Esta *framework* é a base de conhecimento das táticas e técnicas para os *threat hunters*, *blue team* e *red team*. Ajuda a classificar os ataques, a identificar as fases e objetivos dos mesmos e a categorizar o nível de risco da organização. As organizações usam esta *framework* para priorizar mitigações, baseando-se nas diferentes etapas e nas falhas de segurança (*What is the MITRE ATT&CK Framework?* 2023).

O Mitre ATT&CK é composto por 14 táticas, como podemos verificar na tabela 1 (*What is the MITRE ATT&CK Framework?* 2023):

Tática	**Objetivo do Atacantes**
1. Reconnaissance	Recolher informações que possam ser utilizadas para planear operações futuras
2. Resource Development	Estabelecer recursos que possam ser utilizados para apoiar as operações
3. Initial Access	Entrar na rede
4. Execution	Execução de código malicioso
5. Persistence	Manter-se dentro dos sistemas
6. Privilege Escalation	Obter permissões mais elevadas
7. Defense Evasion	Evitar deteção
8. Credential Access	Roubar credenciais
9. Discovery	Descobrir o ambiente
10. Lateral Movement	Acesso a outros sistemas a partir do infetado
11. Collection	Recolha de dados de interesse para os objectivos pretendidos
12. Command and Control	Comunicar com sistemas comprometidos para os controlar
13. Exfiltration	Roubo de dados
14. Impact	Manipular, interromper ou destruir os seus sistemas e dados

Tabela 1: As diferentes táticas da *framework* Mitre ATT&CK.

Dentro destas táticas existem 196 técnicas que possuem 411 sub-técnicas. De seguida, é apresentado na figura 4 um exemplo que demonstra o que isto significa (*Techniques - Enterprise | MITRE ATT&CK® 2023*):

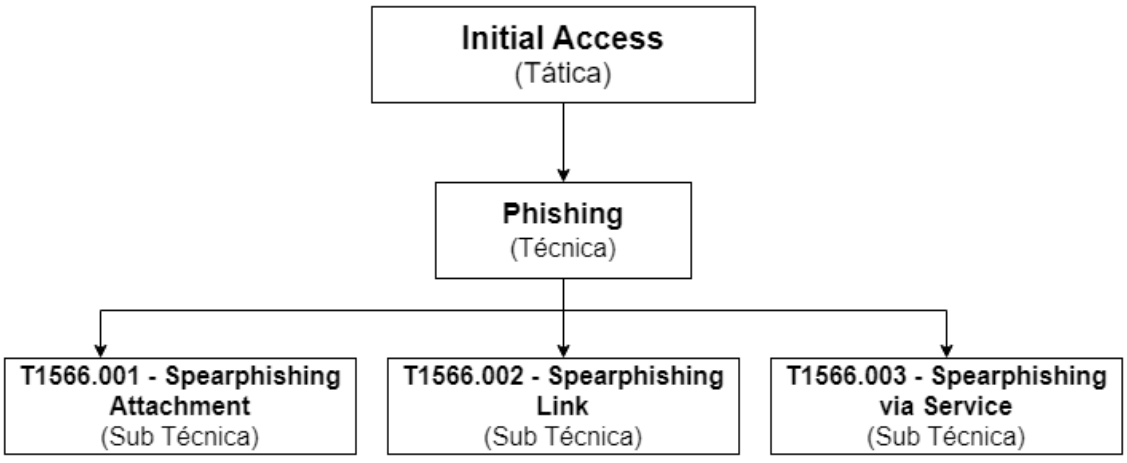


Figura 4: Exemplo de uma opção de ataque

3.4.1 *Benefícios na utilização do Mitre ATT&CK*

O Mitre ATT&CK ajuda as organizações a melhorar a sua postura geral de segurança e a reduzir os riscos. Esta *framework* oferece vários benefícios para as organizações. Um dos principais benefícios é a sua capacidade de manter as organizações atualizadas com as mais recentes ameaças e técnicas de ataque. Oferece também a possibilidade de identificar e priorizar as ameaças mais relevantes dando assim oportunidade às organizações de tomar contramedidas de mitigação de forma eficaz e proativa. Um outro benefício é fornecer um guia de recomendações para mitigação ou deteção de uma potencial ameaça para cada técnica. Isto ajuda as organizações a concentrarem os seus recursos onde são mais necessários, reduzindo o risco de um ataque bem sucedido (*What Is MITRE ATT CK - Definition | VMware Glossary* 2022).

3.5 CRITÉRIOS DE COMPARAÇÃO

Para efetuar a comparação entre as ferramentas selecionadas, foram definidos critérios tendo em consideração as diversas funcionalidades proporcionadas pelas plataformas e a capacidade de suporte das mesmas. Estes encontram-se na tabela 2.

Funcionalidade	**Breve descrição**	**Avaliação**
Vetor de ataque Endpoint	Ataque de escrita e execução de *malware*	1-5
Vetor de ataque Web Browsing	Ataque de *bruteforce*, web shell, controlo remoto e transferência de *exploits*	1-5
Vetor de ataque Email	Ataque de *phishing* e transferência de anexos maliciosos	1-5
Construção de cenários de ataque	Possibilidade de construção de um cenário customizado	1-5
Simulação de APTs	Simulação de ataques avançados persistentes	1-5
Security risk	Classificação do risco de acordo com cada controlo de segurança	1-5
Categorias de cenários de ataque	Apresentação de diferentes categorias de acordo com a industria corporativa, controlos de segurança, entre outros fatores	1-5
Mapeamento na matriz de mitre	De acordo com os testes efetuados, é fornecido um mapeamento dos riscos perante as várias fases da *framework* Mitre ATT&CK e o tipo de ameaças apresentadas	1-5
Medidas de mitigação	Informação fornecida pela plataforma para auxiliar a mitigação das falhas nos controlos de segurança	1-5
Análise detalhada do ataque	Descrição detalhada de todo o processo de ataque e a sua linha temporal	1-5
Reporting	Conteúdo e capacidade de personalização de relatórios e *dashboards*	1-5
Atualização da plataforma	Diferença temporal na introdução de novos IOCs na plataforma	1-5
Capacidade de suporte do parceiro	Capacidade de suporte do parceiro	1-5

Tabela 2: Critérios para comparação das ferramentas BAS selecionadas.

Foi estabelecida uma classificação de 1 a 5 na presente tabela, que consiste em:

- 1- Muito Ineficaz: A ferramenta de BAS é extremamente ineficaz e não fornece uma simulação realista de ataques. Não identifica ameaças significativas e não ajuda a melhorar a postura de segurança;
- 2- Ineficaz: A ferramenta de BAS tem sérias limitações e não oferece uma simulação completa ou precisa de ataques. Pode fornecer resultados inadequados ou imprecisos;

- 3- Moderadamente Eficaz: A ferramenta de BAS é parcialmente eficaz e fornece algumas simulações úteis de ataques, mas ainda pode ser aprimorada para fornecer uma representação mais precisa das ameaças;
- 4- Eficaz: A ferramenta de BAS é eficaz e oferece simulações de ataques que são úteis para identificar vulnerabilidades e melhorar a postura de segurança;
- 5- Altamente Eficaz: A ferramenta de BAS é altamente eficaz e fornece simulações de ataques extremamente precisas e realistas.

Esta tabela servirá como critério para determinar a ferramenta mais adequada com base na pontuação atribuída. Aquela que obtiver a pontuação mais elevada será designada como a escolha preferencial.

3.6 FERRAMENTA CYMULATE

A Cymulate foi fundada por uma equipa de elite de ex-oficiais dos serviços secretos da Israel Defense Forces (IDF) e investigadores cibernéticos líderes, que dedicaram as suas carreiras a capacitar organizações de todo o mundo contra ameaças e a tornar a cibersegurança avançada tão simples e familiar como enviar um e-mail (Moshe, 2023a).

A solução Cymulate BAS conduz com segurança *threat activities*, tácticas, técnicas e procedimentos em ambientes de produção, para validar a eficácia do controlo de segurança (Moshe, 2023d). Esta solução permite assim:

- Validar a resiliência de cibersegurança;
- Racionalizar investimentos;
- Otimizar as operações de segurança e resposta a incidentes;
- Desempenho na cibersegurança.

A segurança é construída com base numa defesa em camadas que necessita de testes contínuos para avaliar se os controlos estão a funcionar eficazmente. O Cymulate BAS testa a deteção e os alertas de ameaças para confirmar que os controlos estão a funcionar corretamente ou, por outro lado, se as ameaças conseguem evitá-los. Cada vetor é pontuado de forma independente e agregado para obter uma pontuação de risco global, com base em estruturas padrão do sector (Moshe, 2023e).

3.6.1 *Processo de Instalação e Configuração do Cymulate*

O processo de instalação é "*user friendly*", ou seja, é de fácil perceção determinar qual o conteúdo necessário para a instalação bem sucedida do mesmo.

São agora apresentadas as etapas deste processo de instalação e as configurações necessárias para realizar as simulações pretendidas.

Em primeiro lugar, efetua-se o *download* do agente simulador para o sistema operativo Windows, tal como é demonstrado na figura 5.

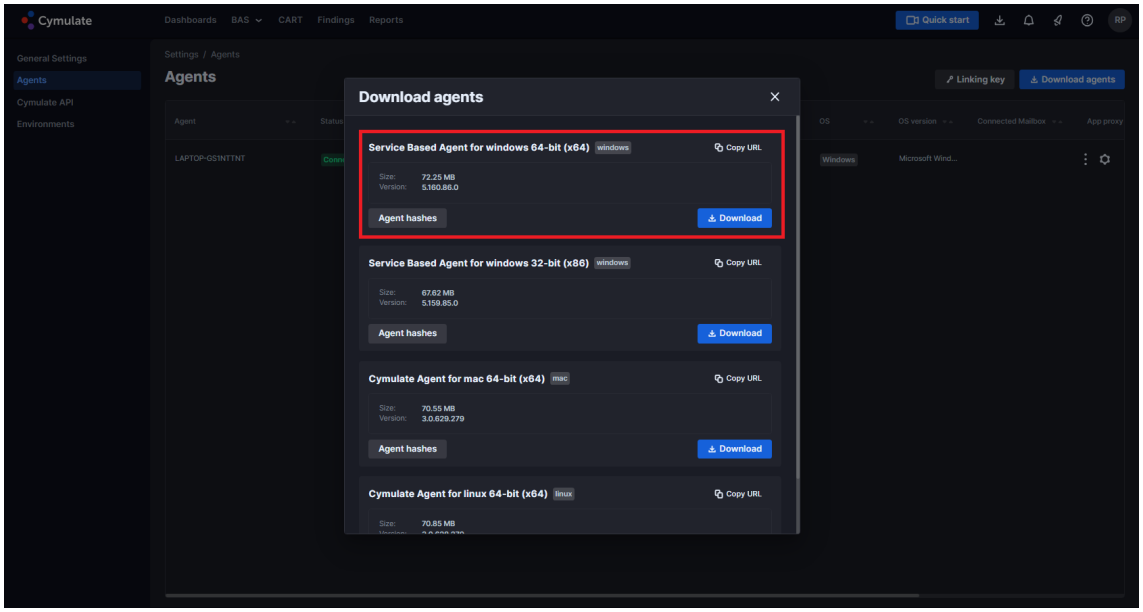


Figura 5: Download do agente simulador do Cymulate

De seguida, é executado o ficheiro que foi descarregado e instalada a ferramenta, seguindo os seguintes passos:

- Passo 1 - O primeiro passo passa por aceitar os termos e condições no contrato da licença do Cymulate, vísivel na figura 6;

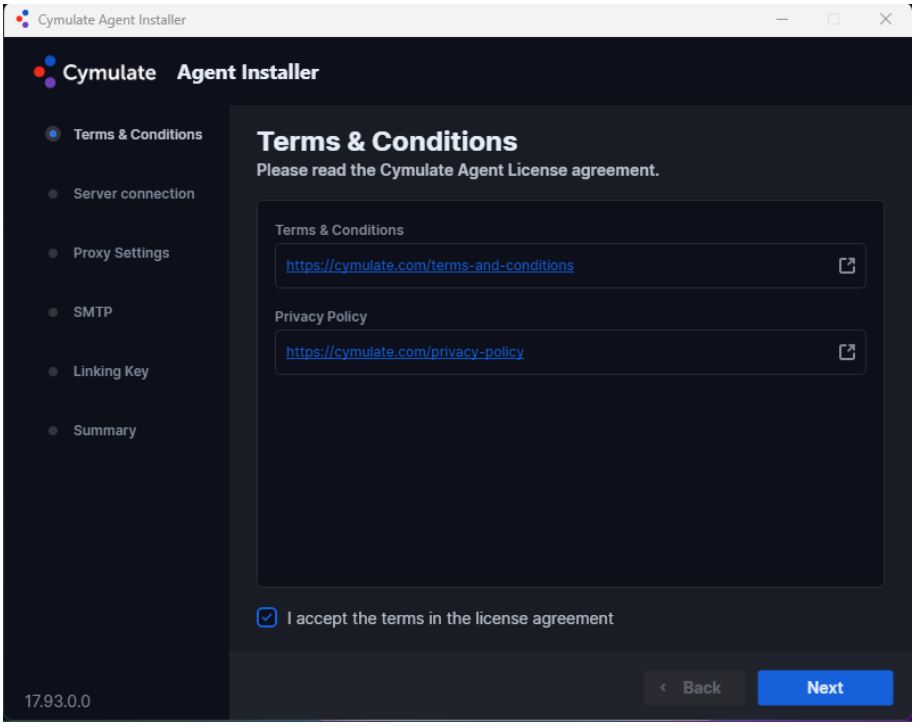


Figura 6: Termos e condições de utilização

- Passo 2 - Inserção do url da plataforma web da Cymulate, demonstrado na figura 7;

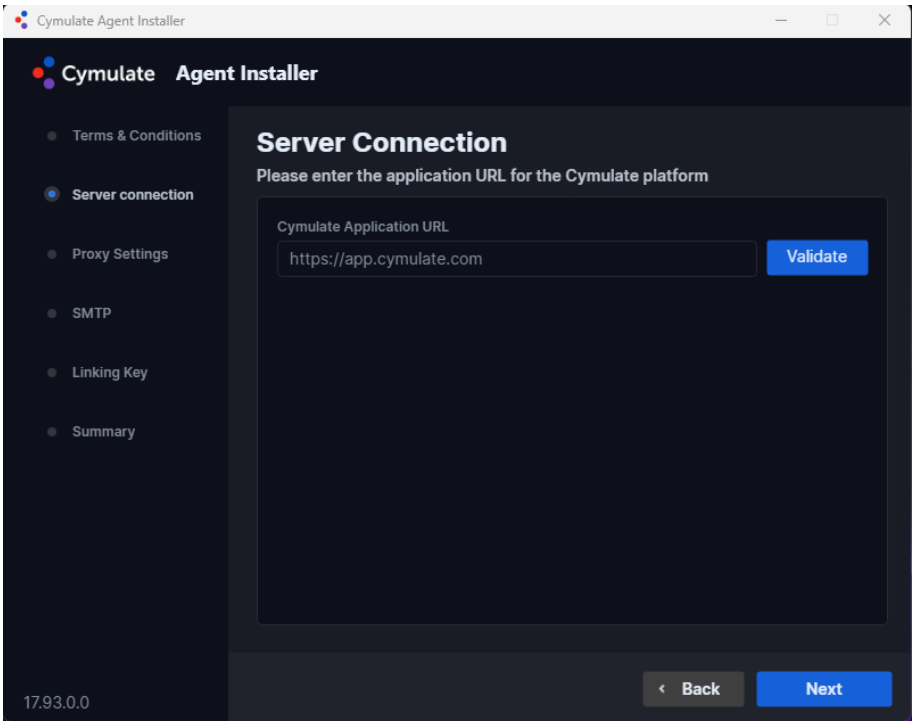


Figura 7: Conexão com o servidor

- Passo 3 - A configuração do *proxy* passa por duas partes, a configuração do *proxy* da aplicação e a configuração do *proxy* relacionado com a navegação web.

Nesta etapa é demonstrada na figura 8a configuração do *proxy* da aplicação, em que é inserido o endereço IP, o porto e as credenciais do utilizador;

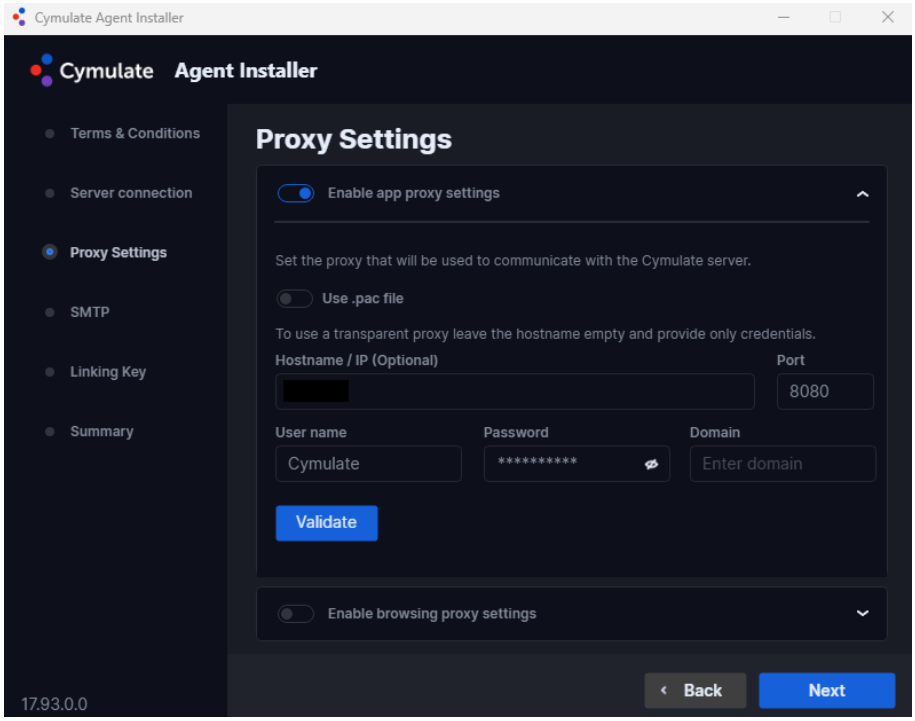


Figura 8: Configuração do *proxy*

- Passo 4 - Na configuração do *proxy* relacionado com a navegação web, são introduzidos os mesmos dados que foram inseridos anteriormente, como observado na figura 9;

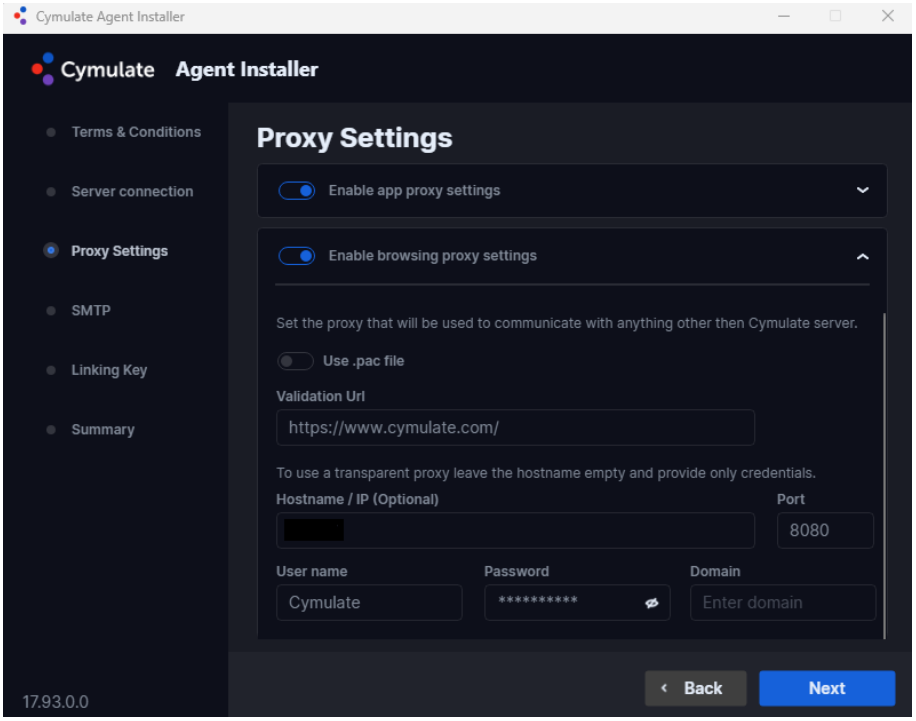


Figura 9: Configuração do *proxy*

- Passo 5 - Neste passo, é configurado o fornecedor de e-mail, sendo este o Exchange cuja versão de servidor é de 2016. Para além disso, foi configurado o *hostname* exchange.mcif.pt e as credenciais para o mesmo, como demonstrado na figura 10;

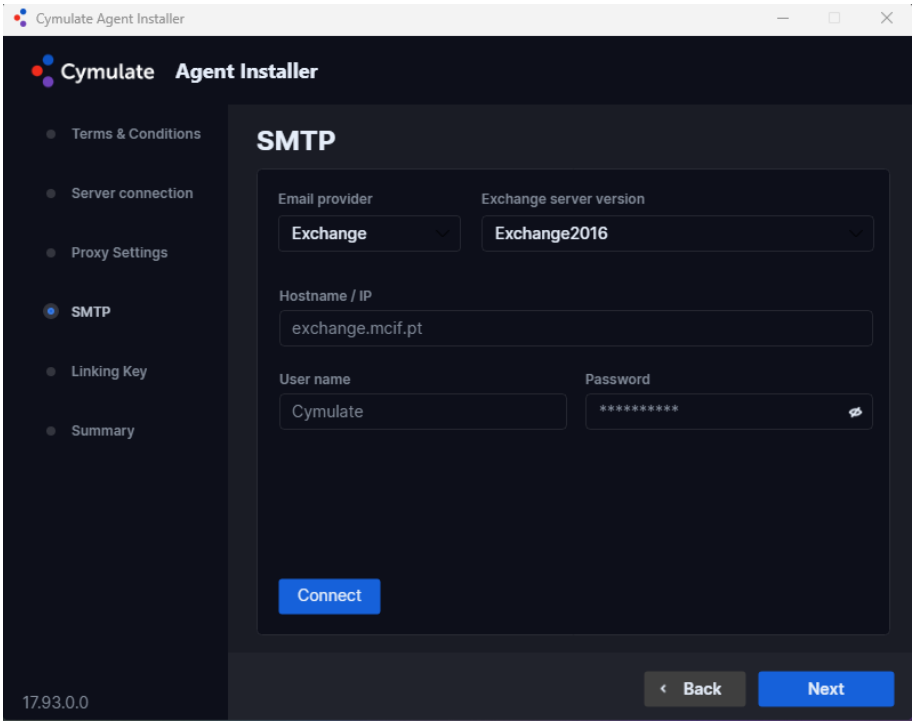


Figura 10: Configuração do vetor de e-mail

- Passo 6 - É necessária uma chave para ligar o agente simulador à plataforma web validada anteriormente. O acesso a esta chave é explicado na figura 12;

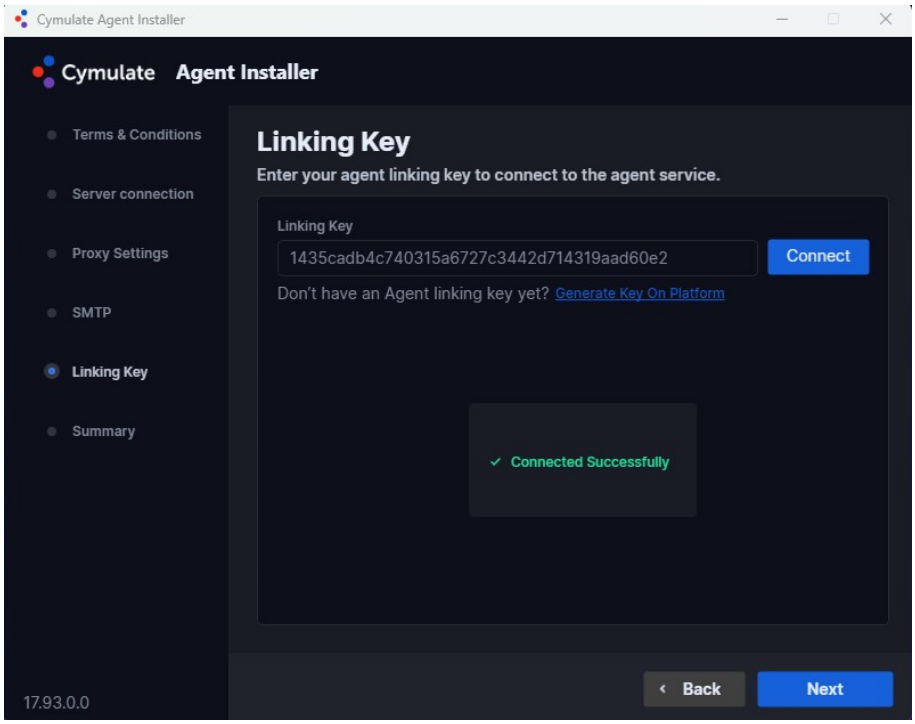


Figura 11: Correlação entre a plataforma e o agente simulador

- Passo 7 - Para o acesso a esta chave é necessário aceder à plataforma web da ferramenta Cymulate. No canto superior direito é possível verificar as iniciais RP, ao premir sobre o mesmo é possível visualizar várias opções, seleciona-se "Settings", de seguida "Agents"e, por fim, "Linking key"estando aqui a informação necessária para a configuração da figura 11;

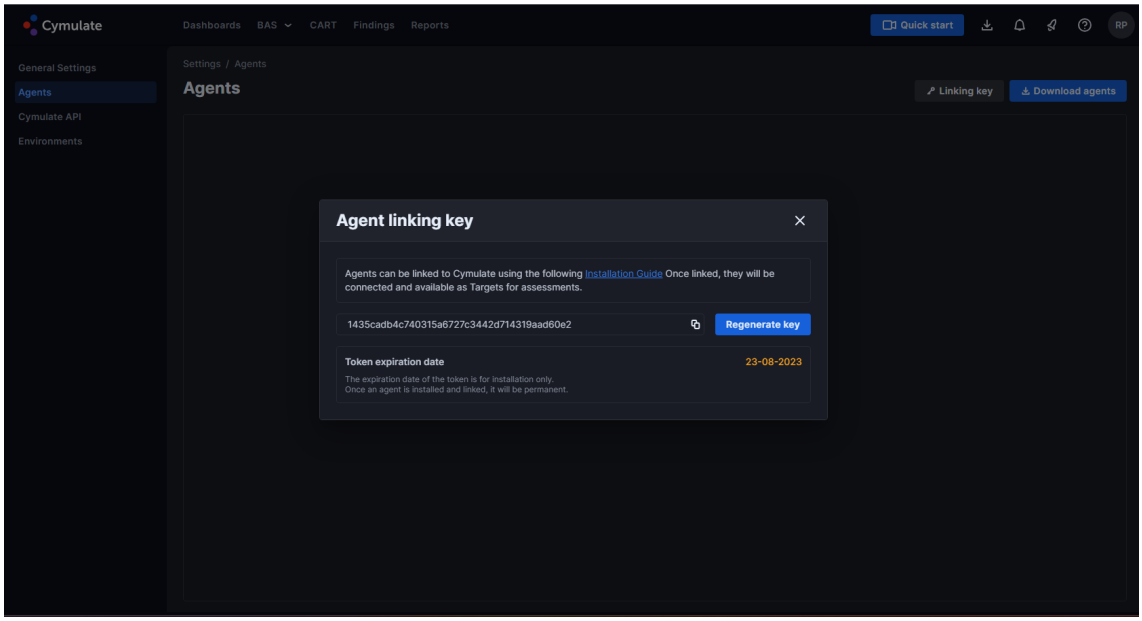


Figura 12: Chave para a dita correlação entre plataforma e simulador

- Passo 8 - Por fim é transmitida a informação do estado das configurações efetuadas até ao momento. Estando satisfeito com as mesmas, é apenas necessário premir "Install", finalizando assim o processo de instalação representado na figura 13.

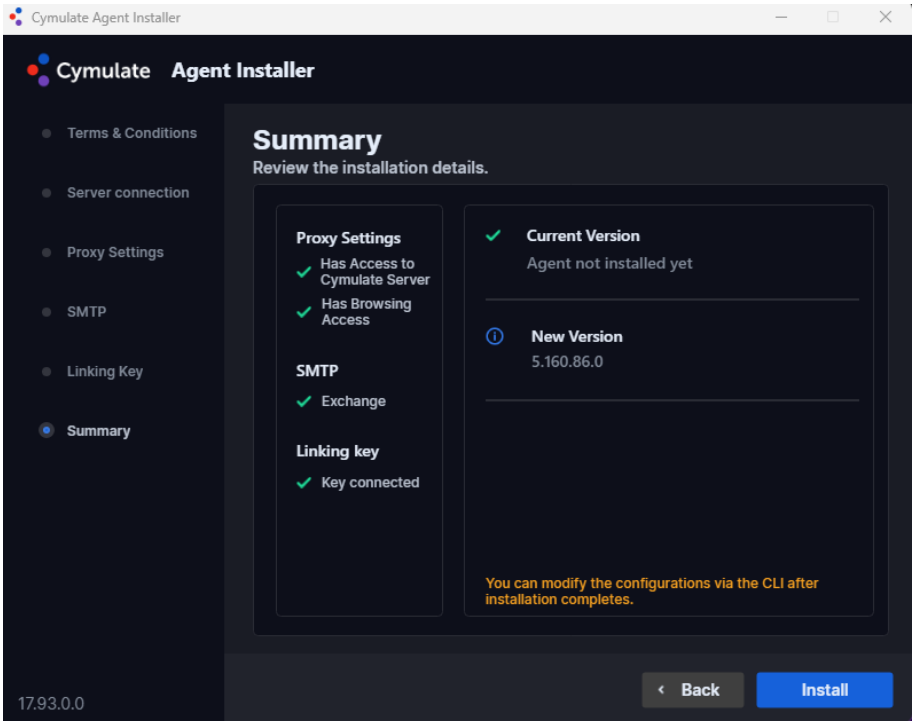


Figura 13: Estado após as anteriores configurações

Após a realização das configurações e a conclusão da instalação, procedeu-se à execução dos testes base da Cymulate, os quais estão identificados como "Free Assessment"em cada um dos vetores, e-mail, web e endpoint.

3.6.2 *Execução dos testes base*

Em primeira instância, foram testados os controlos de segurança do e-mail através da simulação de "Free Assessment", composta por vários tipos de ataques, visíveis na figura 14, tais como:

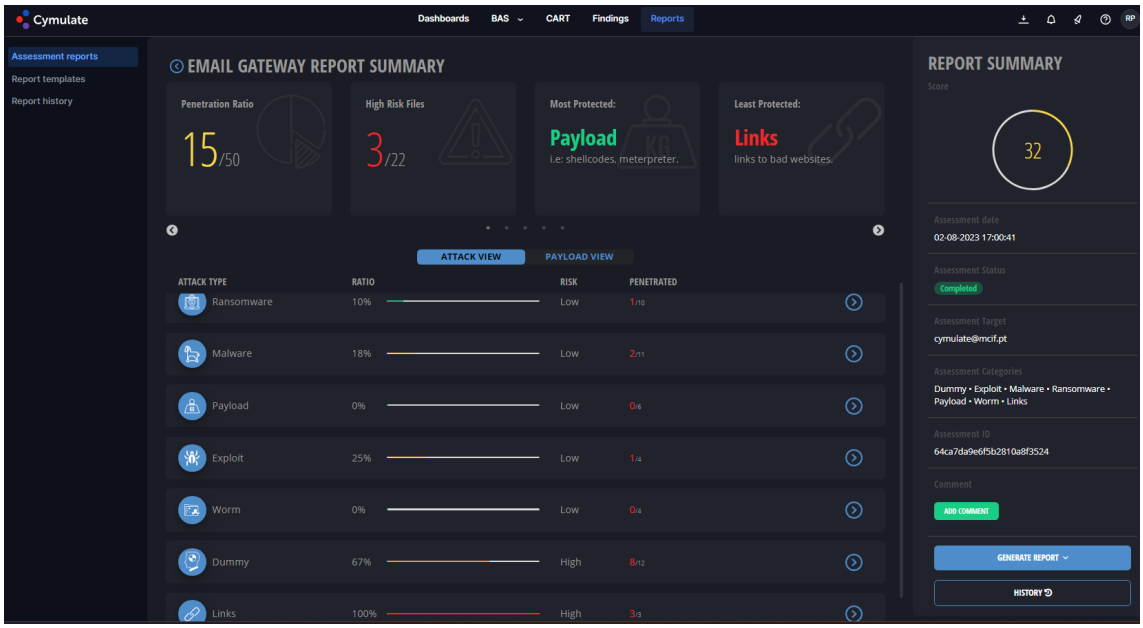


Figura 14: Relatório da simulação efetuada para o vetor de e-mail na solução da Cymulate

- *Ransomware* - Neste ataque 1 dos 10 testes não foi detetado pelos controlos de segurança. Esse ataque implica a utilização de um ficheiro .xla com uma macro incorporada que, uma vez ativada pelo utilizador, realiza automaticamente uma execução de código VBA. O Crypto Ransomware da Cymulate encripta todos os ficheiros do utilizador atual com sessão iniciada, atuando assim como um *ransomware* comum. Não se trata de um *malware* real, pelo que os motores AV baseados em assinaturas não o devem detetar, mas simula a possibilidade de uma verdadeira execução de código malicioso;
- *Malware* - Este ataque envolveu um total de 12 testes em que 2 destes não foram detetados pelos controlos de segurança. O objetivo destes seria abrir um ficheiro Office com macro incorporada que, uma vez ativada pelo utilizador, efetua automaticamente uma execução de código VBA. O *Cymulate's*

Credentials Nagger ataca a interface do utilizador e obriga-o a introduzir o seu nome de utilizador e a sua palavra-passe, forçando *prompts* de autenticação. Quando o utilizador introduz as credenciais corretas, o seu *token* é roubado e pode potencialmente ser utilizado para Movimento Lateral e Acesso a Dados Restritos;

- *Payload* - Todos os 6 testes foram bloqueados, o objetivo era obter informações do dispositivo local, tais como: *usernames*, e-mails e uma *printscreen* do ambiente;
- *Exploit* - Um dos 4 testes não foi bloqueado, este teste era referente à vulnerabilidade exposta no "CVE-2017-8759"(*CVE-2017-8759 : Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely vi* 2018);
- *Worm* - Os 4 testes foram bloqueados pelos controlos de segurança, estes testes consistiam em tentar efetuar movimento lateral;
- *Dummy* - Foram efetuados 12 testes pelo que 8 não foram bloqueados, no entanto, estes não possuíam conteúdo malicioso, o objetivo era verificar se certos tipos de ficheiros eram permitidos. Os 4 testes que realmente possuíam conteúdo malicioso foram bloqueados;
- *Links* - Foi testado o envio de e-mails contendo links maliciosos no corpo do e-mail, 3 dos 3 testes passaram pelos controlos de segurança.

No total, foram realizados 50 testes, dos quais 15 passaram pelos controlos de segurança. Dentro desses 15, 3 foram classificados como de alto risco. A solução concluiu que os controlos de segurança foram mais eficazes contra ataques do tipo *payloads* e menos eficazes contra ataques com *links*. Com base nessas avaliações, a solução atribuiu uma pontuação de risco de 32 em 100 tal como é verificado na figura 15.

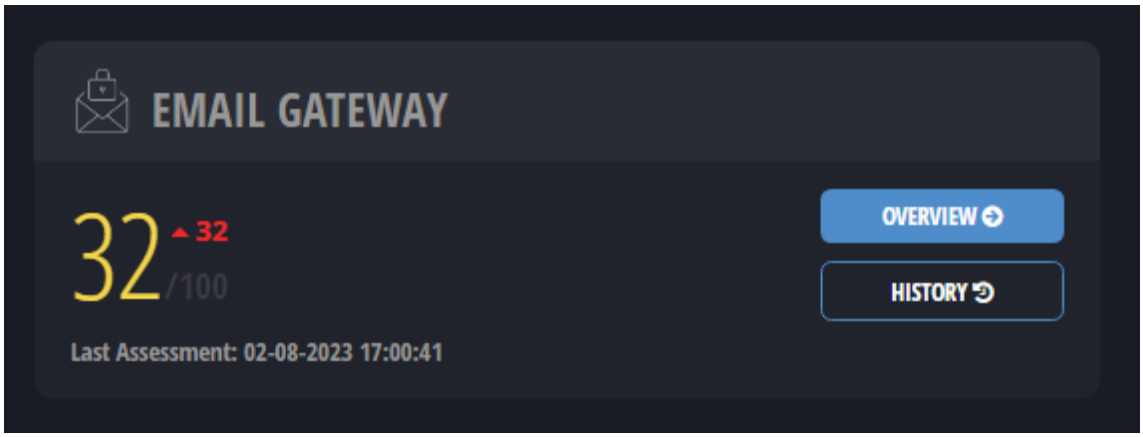


Figura 15: Avaliação do vetor de e-mail na solução da Cymulate

Posto isto foram testados os controlos de segurança da *web*, sendo esta composta por 3 tipos de ataques, como observado na figura 16:

Figura 16: Relatório da simulação efetuada para o vetor de web na solução da Cymulate

- *Phishing* - Foram efetuados 20 testes pelo que 9 não foram bloqueados. Estes testes consistiam na tentativa de acesso a URL's considerados maliciosos por ferramentas de *Threat Intelligence*;
- Command and Control (*C&C*) - Foram efetuados 20 testes pelo que 4 não foram bloqueados. Esses testes envolveram tentativas de ligação a endereços IP identificados como maliciosos por meio de ferramentas de *Threat Intelligence*;

- *Files* - Dos 52 testes efetuados, nenhum foi bloqueado pelos controlos de segurança. Estes testes envolveram *download* de ficheiros, como *malwares* e *ransomwares*.

No total, foram realizados 92 testes, dos quais 65 passaram pelos controlos de segurança. Dentro deste conjunto de 65, 26 foram classificados com um nível de alto risco. A solução concluiu que os controlos de segurança foram mais eficazes contra ataques do tipo *C&C* e menos eficazes contra ataques com ficheiros. Com base nessas avaliações, a solução atribuiu uma pontuação de risco de 55 em 100, tal como se pode verificar na figura 17.

Figura 17: Avaliação do vetor de web na solução da Cymulate

Por último, foram testados os controlos de segurança do *endpoint*. Esses testes consistiram em duas simulações distintas: a primeira identificada por "Free Assessment - Windows"e a segunda por "Free Assessment - Ofuscated - Windows".

A primeira simulação, identificada como "Free Assessment - Windows", consistiu exclusivamente em testes de *ransomware*, como se pode verificar na figura 18.

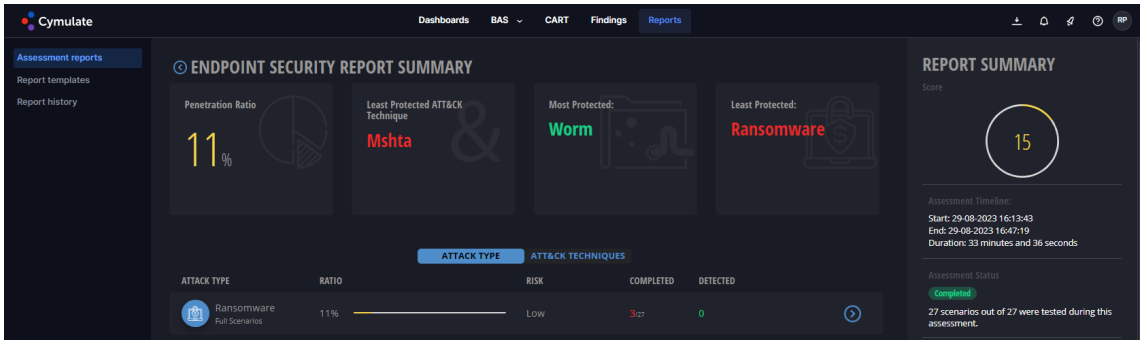


Figura 18: Simulação do "Free Assessment - Windows"efetuada para o vetor de *endpoint* na solução da Cymulate

Dos 27 testes realizados, apenas 3 conseguiram passar pelos controlos de segurança. Com base nessas avaliações, a solução atribuiu uma pontuação de risco de 15 numa escala de 100, conforme ilustrado na figura 19.

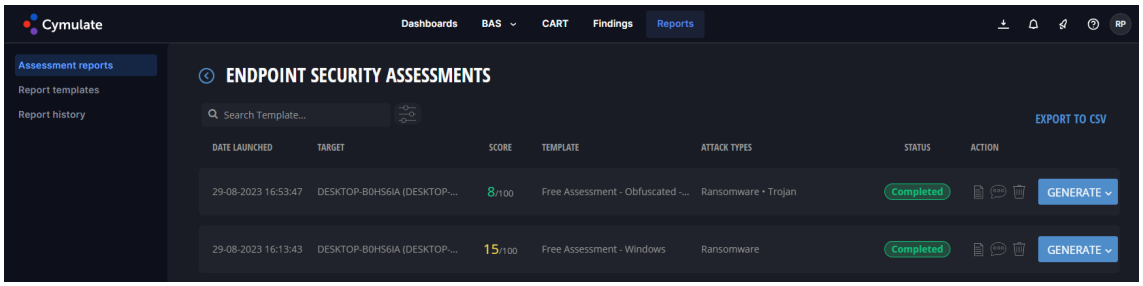


Figura 19: Simulações efetuadas para o vetor de *endpoint* na solução da Cymulate

A segunda simulação, identificada como "Free Assessment - Ofuscated - Windows"consistiu em 2 tipos de ataques, *ransomware* e *trojan*.

No total, foram realizados 26 testes, sendo que nenhum passou pelos controlos de segurança como podemos observar na figura 20.

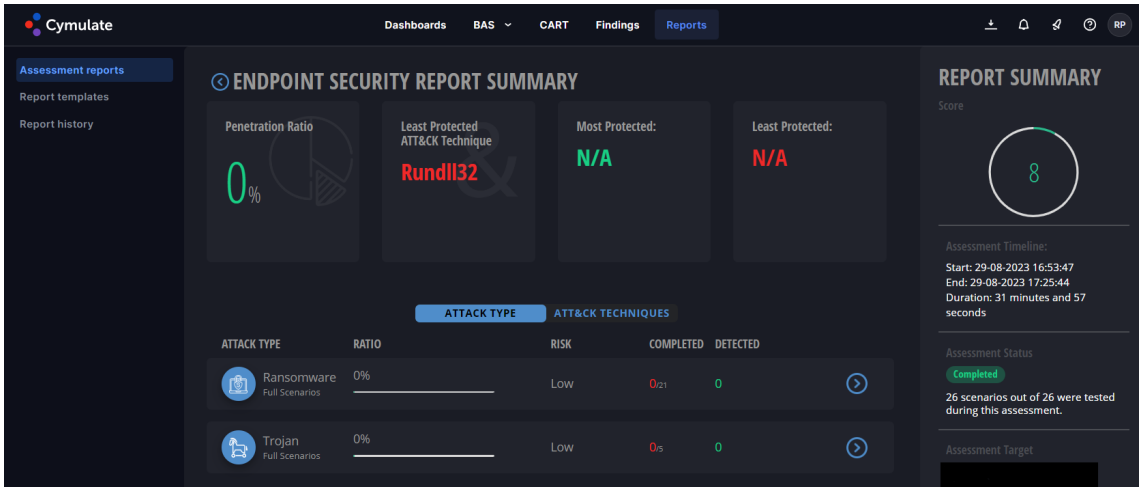


Figura 20: Simulação do "Free Assessment - Ofuscated - Windows"efetuada para o vetor de *endpoint* na solução da Cymulate

Com base nessas avaliações, a solução atribuiu uma pontuação de risco de 10 em 100 tal como é verificado na figura 21.

Figura 21: Avaliação do vetor de *endpoint* na solução da Cymulate

É possível constatar que o vetor *web* é aquele que aparenta estar mais vulnerável, dado que os controlos de segurança existentes necessitam de ajustes nas suas configurações.

3.6.3 *Avaliação contínua - Pilha de testes*

As simulações direcionadas ao *endpoint* e efetuadas a partir dos testes "Cymulate Best Practice", compreendem 2 cenários, tal como podemos verificar através da figura 22:

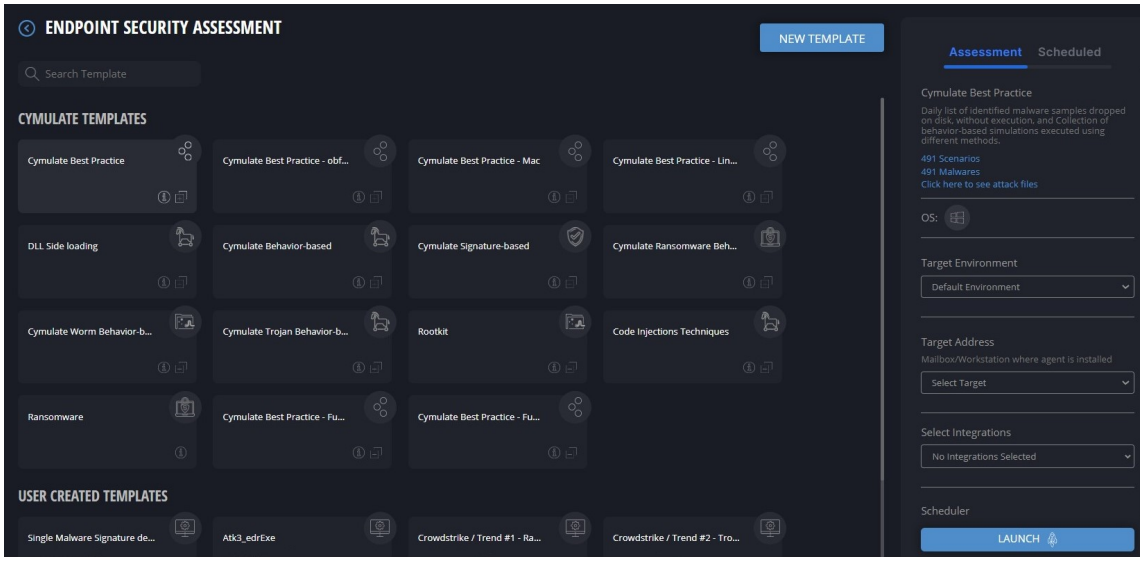


Figura 22: Teste de melhores práticas de acordo com a Cymulate

- Ficheiros - O agente tenta escrever os ficheiros que contêm assinaturas maliciosas conhecidas no disco, no entanto, estes não são executados. O esperado é que estes ficheiros sejam colocados em quarentena pelo controlo de segurança Trend Apex One, sendo que este possui esse propósito.
- Cenários - O agente efetua a execução dos cenários que, por sua vez, realiza ações maliciosas de forma segura. Utilizando o *ransomware* como exemplo da realização destas ações maliciosas de forma segura, o agente cria uma diretoria com ficheiros falsos e tenta encriptá-los. A ação esperada pelo controlo de segurança Crowdstrike é de bloquear esta ação. A função deste é detetar e efetuar ações de mitigação, com base em comportamentos de atividade maliciosa.

De acordo com as configurações de origem do agente, após 120 segundos, se o ficheiro ainda estiver no dispositivo, o processo finaliza, as ações são revertidas e

é considerado um teste sem mitigação. Pode verificar-se o tempo dado através da figura 23.

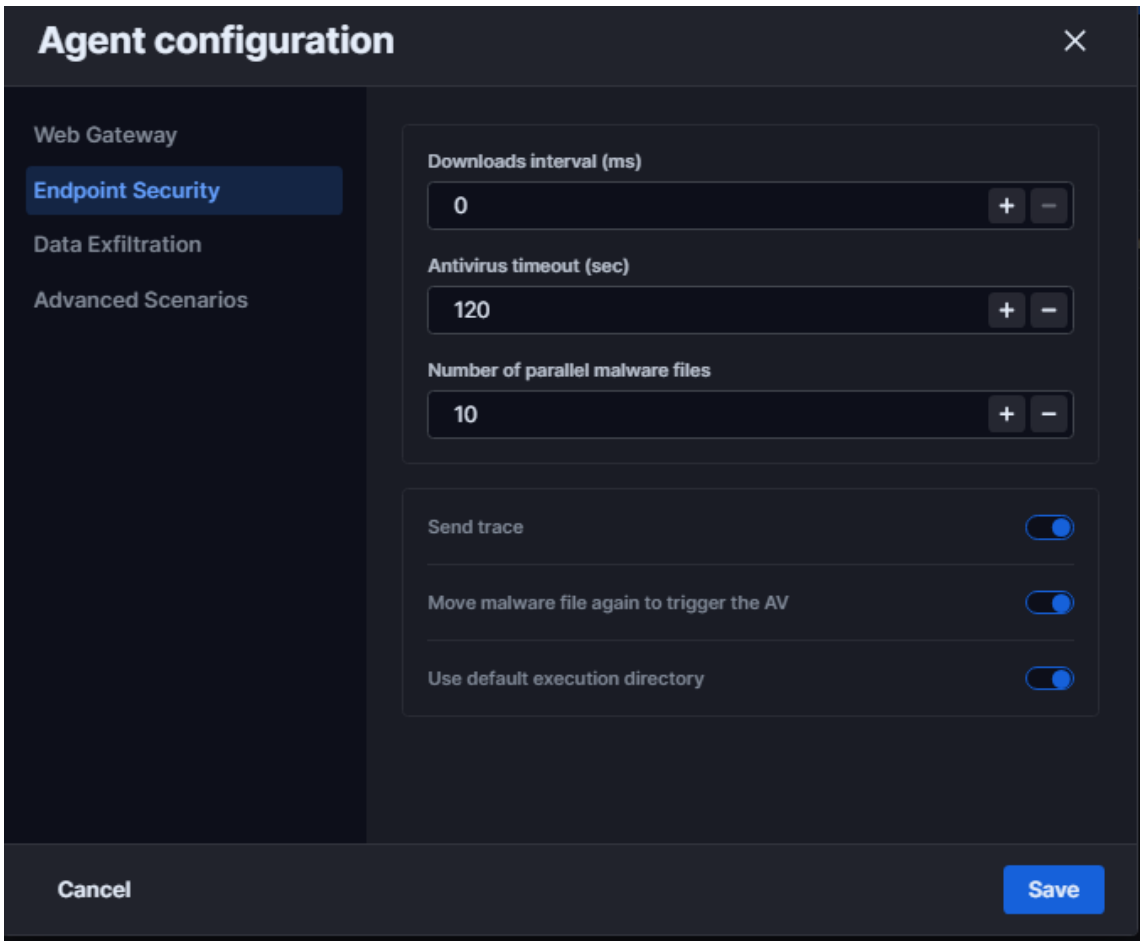


Figura 23: Configurações do Agente segurança do *endpoint*

3.6.4 *Funcionalidades*

A ferramenta Cymulate é uma solução de segurança cibernética projetada para ajudar as organizações a identificar e mitigar potenciais vulnerabilidades no seu ambiente, de forma transversal. Para atingir esses objetivos, a ferramenta constitui diversas funcionalidades, que, de seguida, são apresentadas e explicadas as mesmas, focando no BAS:

- Cenários de ataque;
- Simulação de cenários personalizados;
- *Immediate Threat Intelligence*;

- Relatórios e métricas;
- *Dashboards*;
- Integração com outras ferramentas de segurança (Moshe, 2023f).

3.6.4.1 *Cenários de ataque*

Dentro do conjunto de funcionalidades do BAS da Cymulate, destacam-se os vários cenários de teste. Cada um desses cenário foi criado para simular uma ampla gama de possíveis ciberataques que as organizações poderiam enfrentar, por forma a testar a deteção e alertas de segurança, com o intuito de confirmar se os controlos estão a funcionar corretamente ou se as ameaças conseguem evitá-los. A plataforma Cymulate oferece avaliações para a validação destes mesmos controlos de segurança, estando equipada com os seguintes cenários, tal como se pode observar na figura 24:

- Email Gateway;
- Web Gateway;
- Endpoint Security;
- Data Loss Prevention;

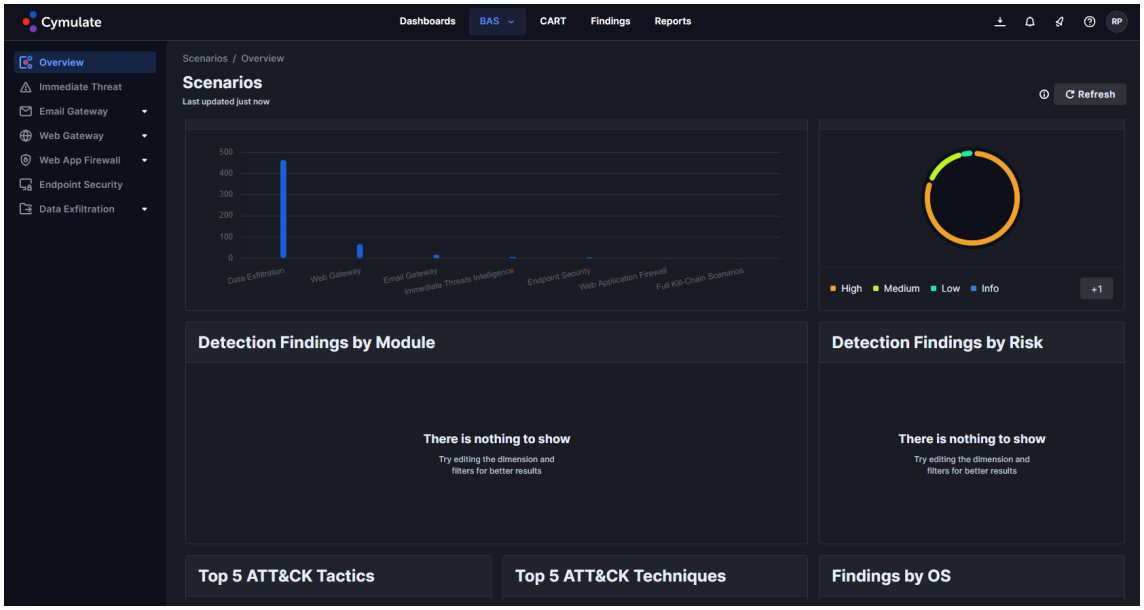


Figura 24: Cenários de avaliação dos controlos de segurança de BAS do Cymulate

EMAIL GATEWAY

O *email* é o método mais utilizado para explorar vulnerabilidades de segurança e comprometer ambientes corporativos. Pesquisas indicam que mais de 75% dos ciberataques em todo o mundo têm origem num email malicioso, e o número desses ataques direcionados continua a aumentar (Moshe, 2021a). Como tem sido testemunhado no passado, campanhas de *phishing* são lançadas através de emails que contêm um anexo ou um *link* malicioso, com o objetivo de roubar informação, infetar com *ransomware* ou estabelecer uma ligação direta aos servidores de Comando e Controlo (C&C) do atacante.

As organizações utilizam diferentes controlos de segurança, tais como Secure Email Gateways (SEGs), Sandbox e Content Disarm and Reconstruction (CDR), para proteger as caixas de email dos colaboradores. No entanto, uma configuração ou implementação incorretas destes sistemas podem levar à falsa suposição de que a organização está segura.

Por estes motivos, o vetor de Email Gateway da Cymulate avalia a segurança do email de uma organização e a exposição potencial a *payloads* maliciosas e *links* enviados por email (Moshe, 2021a). Estes testes estão representados pela figura 25.

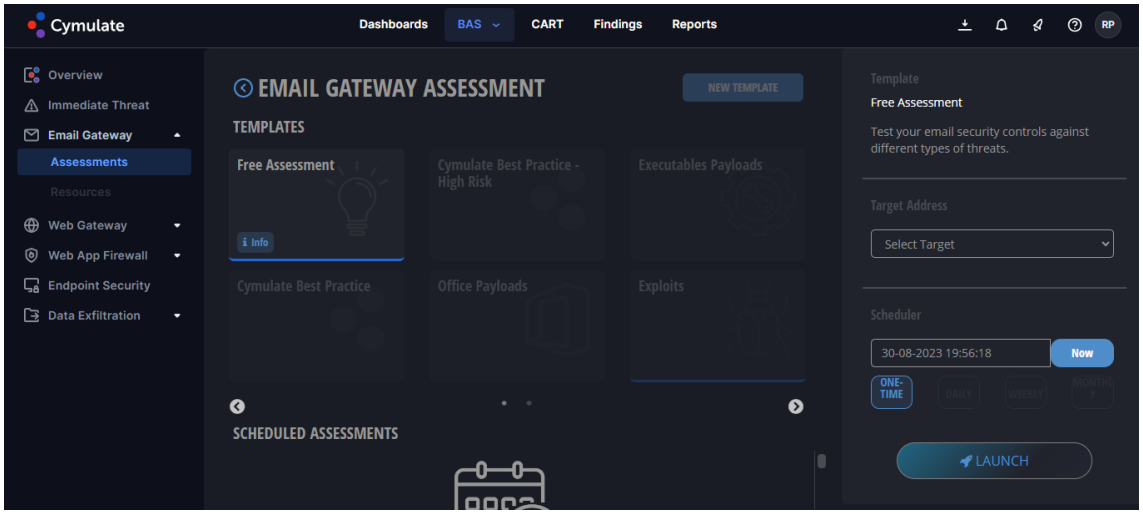


Figura 25: Cenário de Email Gateway da Cymulate

WEB GATEWAY

A *World Wide Web* (WWW) está repleta de *websites* maliciosos e novos são criados todos os dias. Além disso, *websites* legítimos são constantemente comprometidos e usados para espalhar *malware* e outros ataques.

O vetor de *Web Gateway* da Cymulate simula uma série de ataques que desafiam e avaliam a eficácia dos controlos de segurança da web. Este vetor permite medir a exposição de uma organização a uma extensa base de dados continuamente atualizada de *websites* maliciosos, comprometidos e *malware* (Moshe, 2021b). Os testes que representam este vetor são observados através da figura 26.

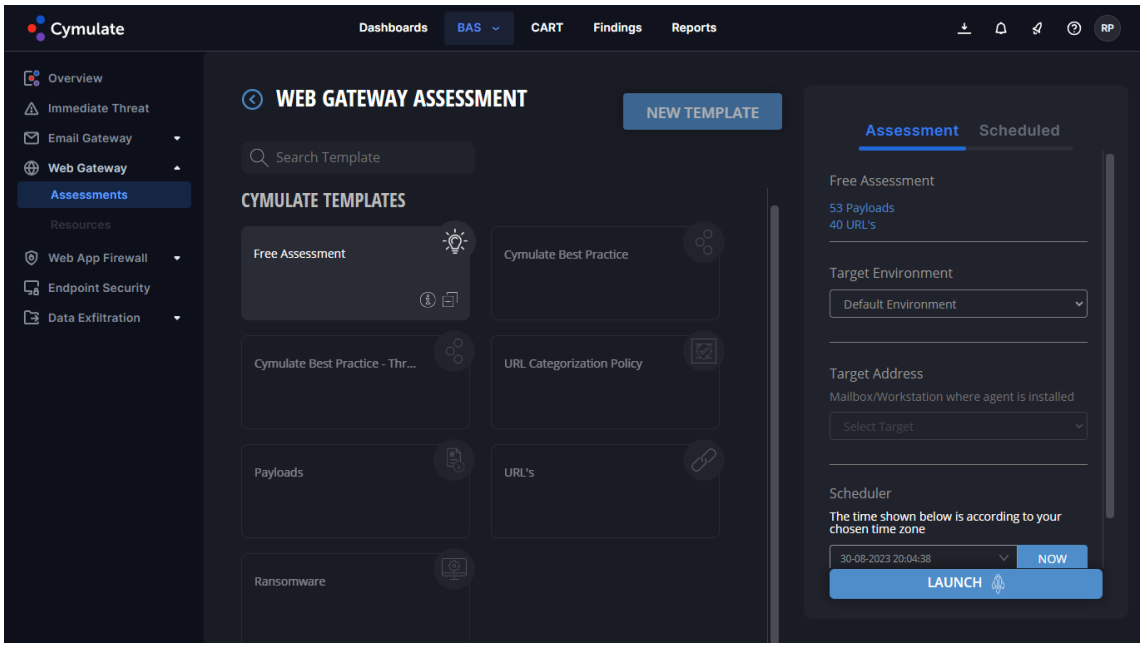


Figura 26: Cenário de Web Gateway da Cymulate

ENDPOINT SECURITY

O vetor de *Endpoint Security* desafia os controlos de segurança do *endpoint* e verifica se estão devidamente ajustados para se defenderem contra ataques baseados em assinaturas e comportamentos. A segurança deste é imperativa para a capacidade de uma organização de mitigar e detetar comportamentos e ameaças maliciosas. As organizações protegem-nos com camadas de defesa, tais como EPP e EDR.

Este vetor da Cymulate permite que as organizações implementem e executem simulações de cenários de ataque completos, como *ransomware* ou a implementação de *Tactics, Techniques, and Procedures* (TTPs) do MITRE ATT&CK num *endpoint* dedicado, de forma controlada e segura (Moshe, 2022b). Os seus testes estão visíveis na figura 27.

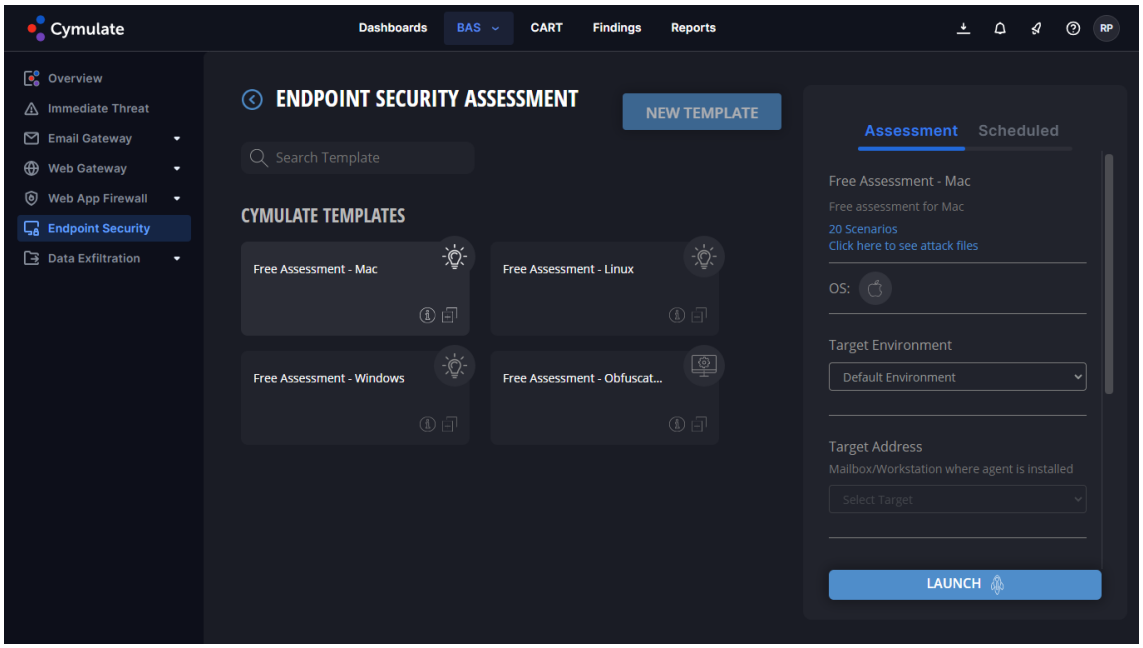


Figura 27: Cenário de Endpoint Security da Cymulate

DATA LOSS PREVENTION

O vetor de Exfiltração de Dados avalia quão bem as suas soluções e controlos de DLP previnem qualquer extração de informações críticas, utilizando múltiplos métodos de extração usados pelos atacantes e por colaboradores que podem não estar cientes de que estão a violar políticas de conformidade e segurança internas. Na figura 28 são apresentados os cenários de testes que este vetor possui.

Por isso, este tem como objetivo colocar à prova os controlos de Data Loss Prevention (DLP) para avaliar a eficácia na prevenção da exposição de informações sensíveis e do roubo de dados críticos. As organizações são obrigadas a cumprir um número crescente de leis e regulamentos que estabelecem diretrizes para a recolha, processamento e proteção de dados pessoais e sensíveis, informações financeiras e registos médicos contra roubo e uso indevido. Além das exigências de conformidade, as violações de dados também podem resultar em enormes impactos financeiros e prejuízos à marca e reputação. A apropriação indevida de propriedade intelectual pode destruir a vantagem competitiva de uma empresa. As organizações dependem da implementação, metodologia e configuração de DLP como última linha de defesa para proteger os seus dados críticos (Moshe, 2022a).

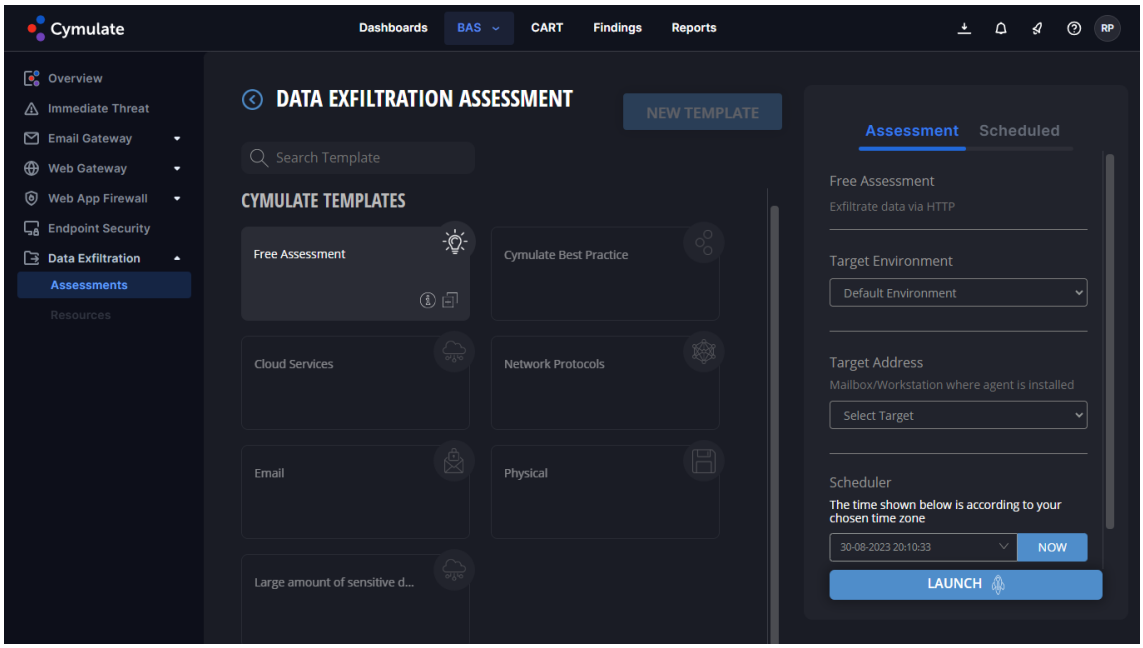


Figura 28: Cenário de Data Exfiltration da Cymulate

3.6.4.2 *Simulação de cenários personalizados*

Além dos *templates* pré-existentes da Cymulate, é possível criar testes de simulações personalizadas. Este processo é exemplificado utilizando o cenário de *Endpoint Security*.

Para criar um novo *template*, é necessário aceder à funcionalidade de cenários do BAS, em seguida selecionar "*Endpoint Security*"e clicar em "*New Template*", como pode ser visto na figura 29.

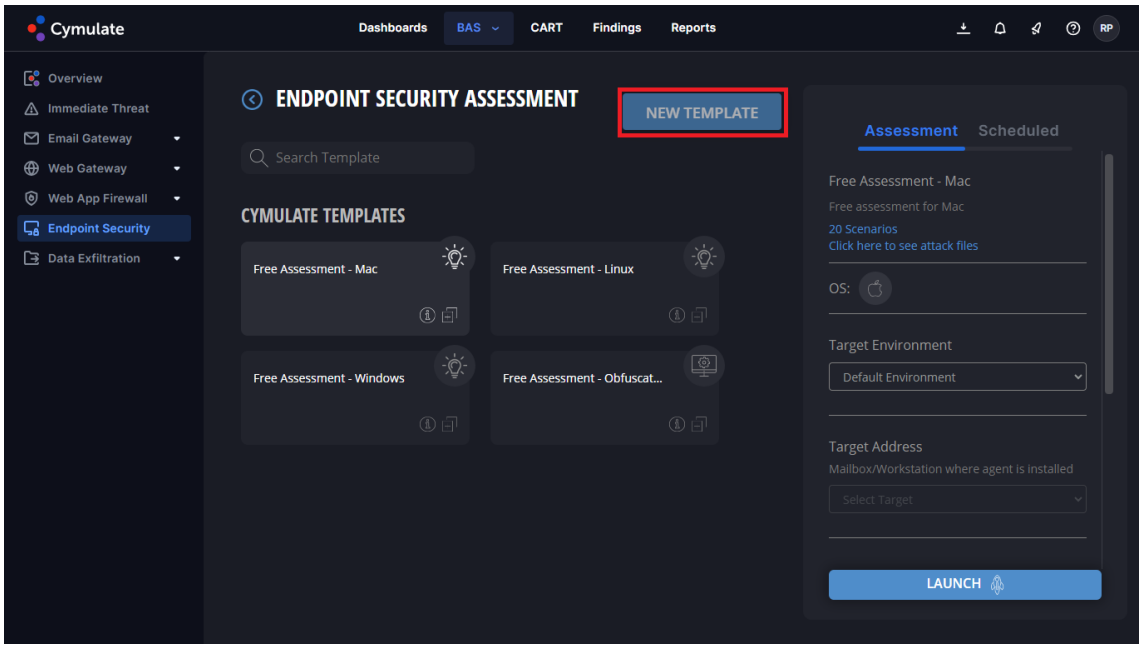


Figura 29: Criação de um novo template de *Endpoint Security* no Cymulate

Posto isto é iniciado um processo de 6 passos. Em primeiro lugar, é questionado o sistema operativo que se deseja testar, existindo as opções de Windows, Mac e Linux, tal como é demonstrado na figura 30.

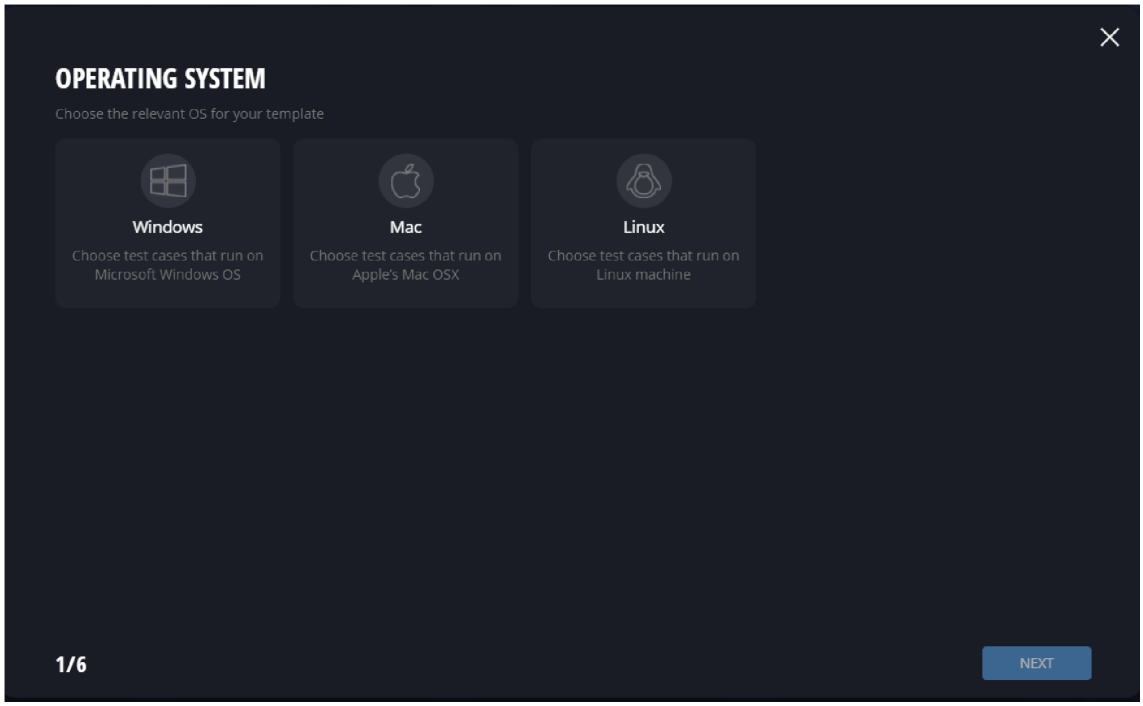


Figura 30: Selecionar o sistema operativo desejado para o novo *template* no Cymulate

Em seguida, é solicitada a escolha do método de entrega do ficheiro malicioso e se desejamos ou não utilizar ofuscação, visível na figura 31.

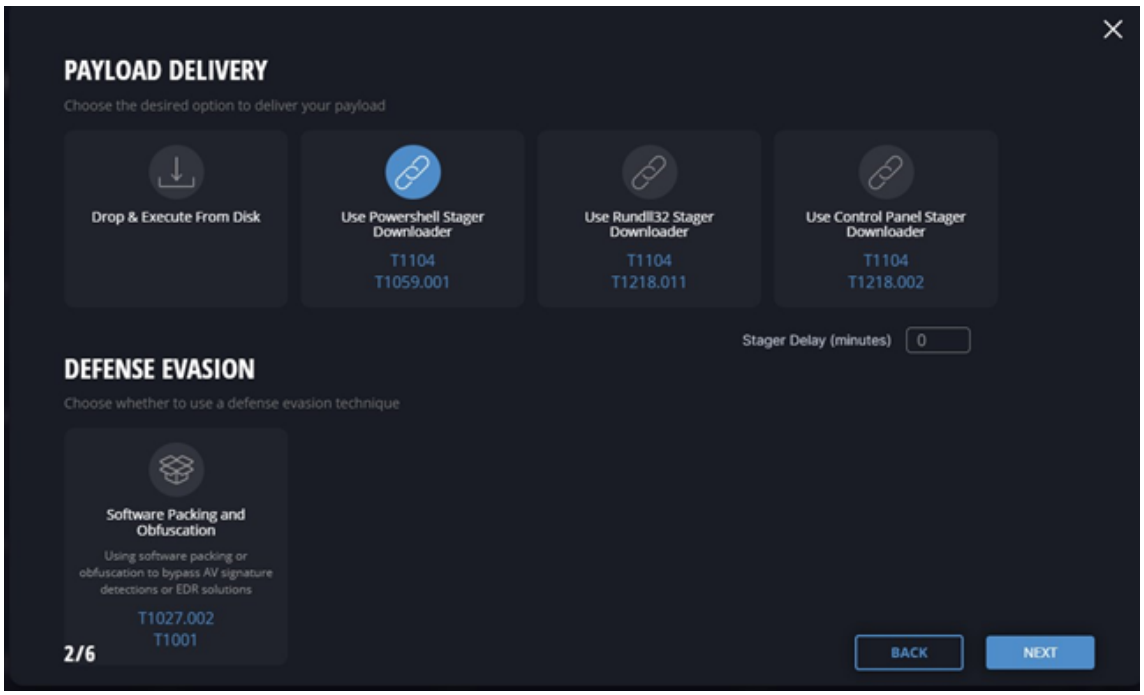


Figura 31: Escolher o método de entrega do ficheiro malicioso e se pretendemos ofuscação para o novo *template* no Cymulate

É analisado e selecionado um ou mais métodos de execução perante as várias opções possíveis, ilustrado na figura 32.

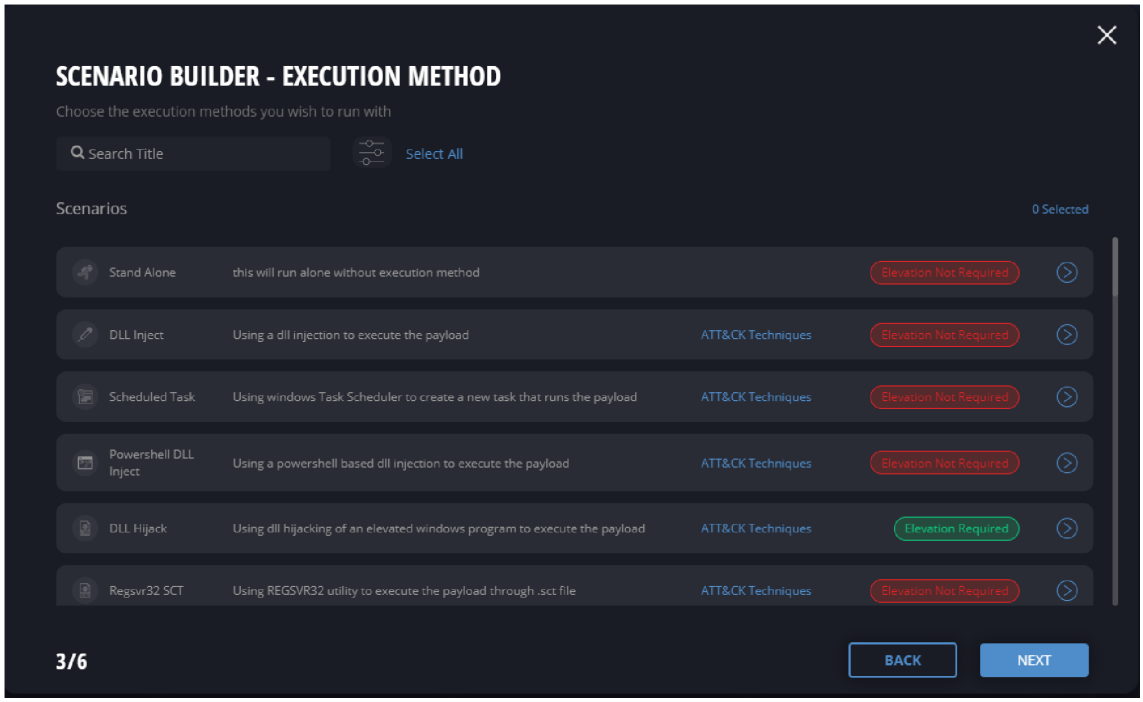


Figura 32: Escolha dos métodos de execução para o novo *template* no Cymulate

De seguida é selecionado um ou mais comportamentos maliciosos para o *template* personalizado, figura 33.

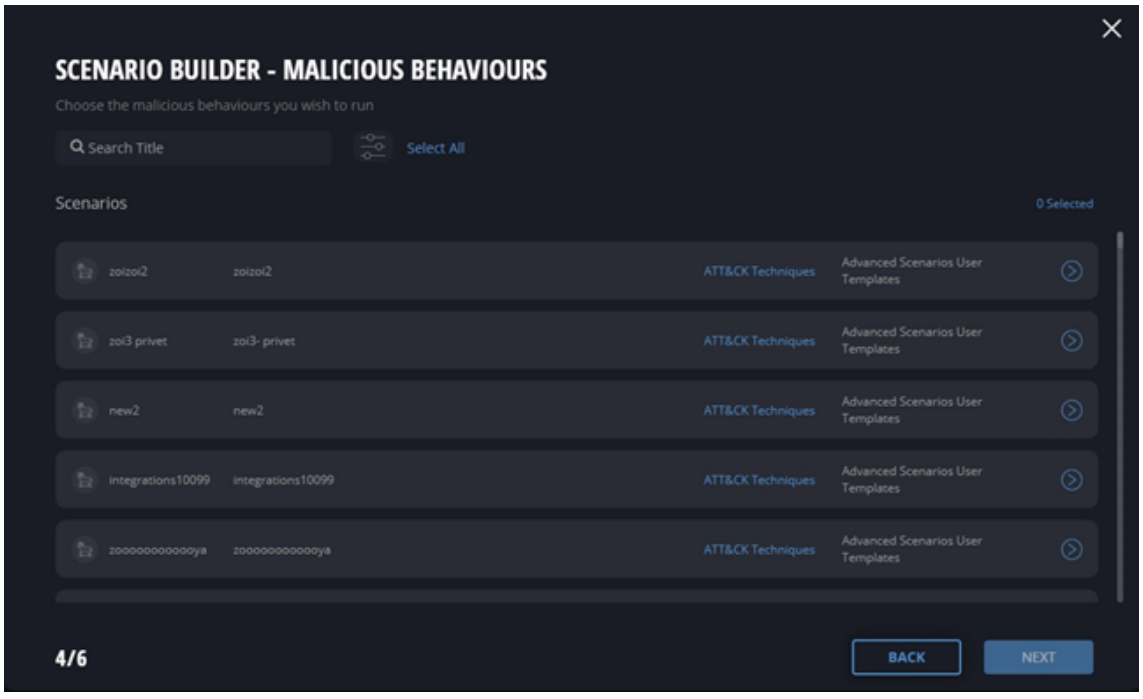


Figura 33: Escolha dos comportamentos maliciosos para o novo *template* no Cymulate

Dentro da base de dados de *malwares*, é escolhido uma ou mais amostras maliciosas para simulação, tal como se pode observar na figura 34.

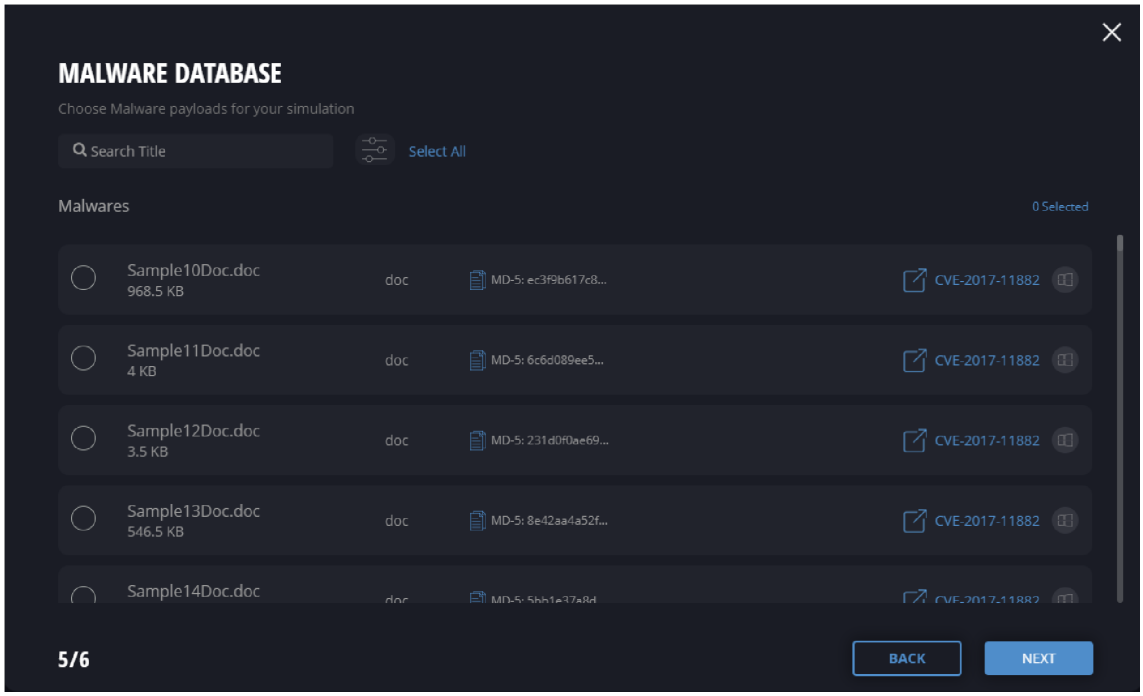


Figura 34: Escolha das amostras maliciosas para simulação para o novo *template* no Cymulate

Por fim, são revistas todas as opções selecionadas anteriormente e é dado um nome ao *template*, de acordo com a figura 35.

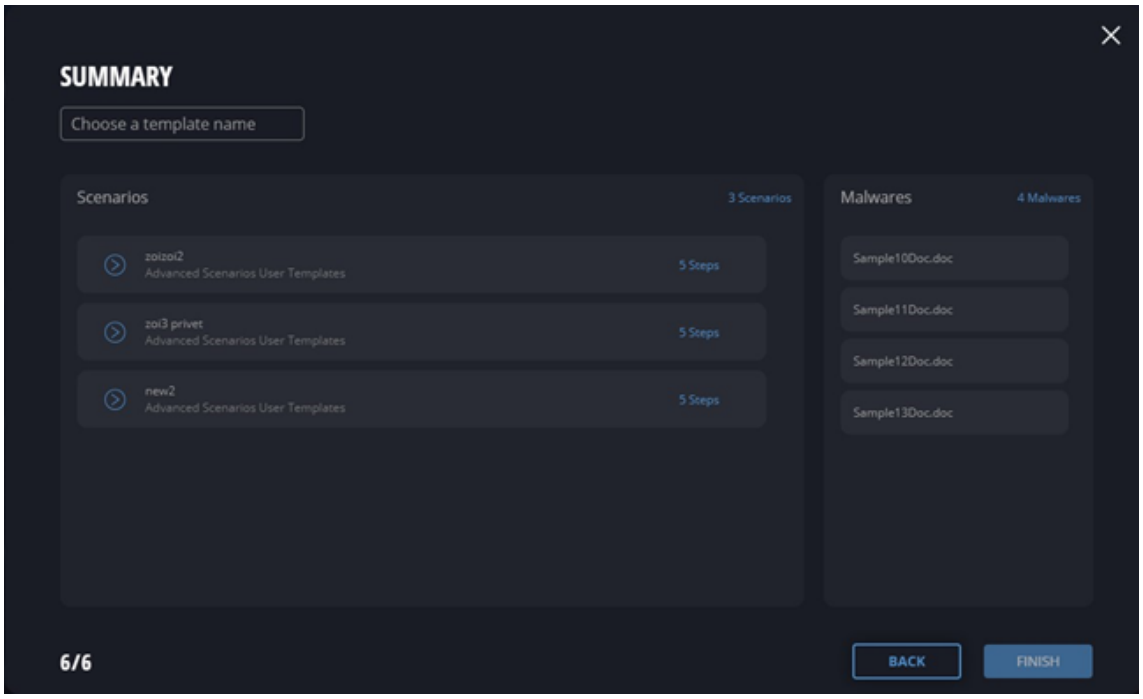


Figura 35: Resumo de todas as opções anteriores para o novo *template* no Cymulate

Este novo *template* fica disponível no cenário de "Endpoint Security"sob "User Created Templates", tal como é visível na figura 29.

3.6.4.3 *Immediate Threat Intelligence*

Esta funcionalidade possibilita a validação dos controlos de segurança de uma organização na mitigação de ameaças emergentes e ressurgentes que demonstram estar a propagar-se ativamente pela internet.

O grupo de *threat intelligence* da Cymulate obtém dados de diversas fontes, tais como a *Cybersecurity & Infrastructure Security Agency* (CISA) ou organizações *Community Emergency Response Team* (CERT) de vários países, assim como fontes de *open-source* e *feeds* de ameaças comerciais. Assim que uma ameaça é identificada e confirmada como estando a propagar-se de forma ativa, a equipa desenvolve rapidamente uma simulação de *immediate threat* e disponibiliza-a na plataforma *cloud* da Cymulate. Isto é normalmente realizado num prazo de 24 horas, o que destaca a introdução regular de novas simulações diariamente.

Atualmente, esta funcionalidade contém 1335 simulações e permite que após uma simulação seja publicada, execute de forma automática com os vetores previamente configurados, tal como se pode verificar na figura 36.

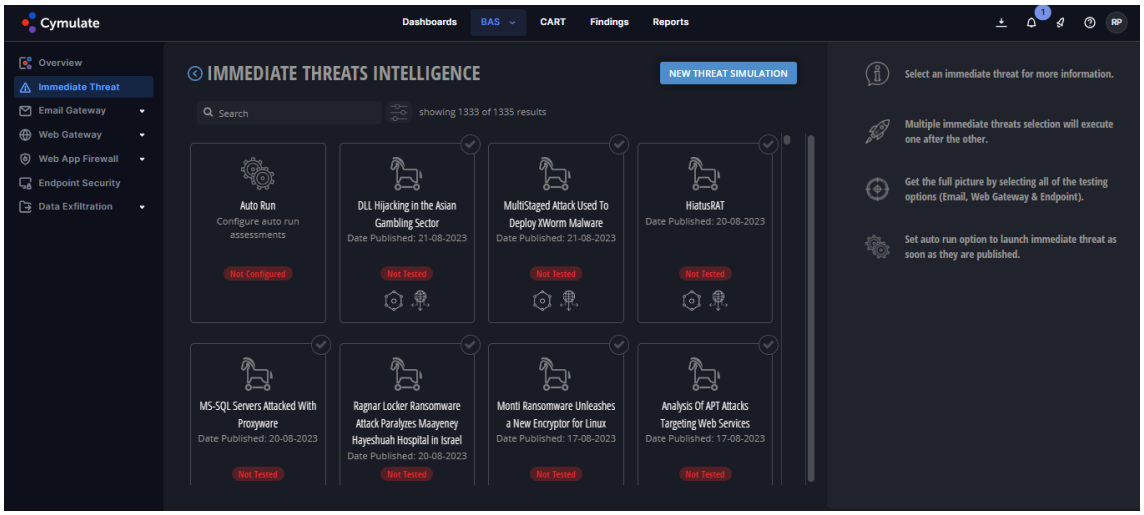


Figura 36: Funcionalidade de Immediate Threat Intelligence do Cymulate

Para demonstrar os testes desta funcionalidade, foi selecionada a simulação mais recente, estando identificada na figura 37 como "DLL HIJACKING IN THE ASIAN GAMBLING SECTOR". A descrição associada a essa simulação é a seguinte: "*hackers* chineses estão a focar-se no setor de apostas de casino no Sudeste Asiático, de acordo com a SentinelLabs e a ESET, que identificaram *malware* suspeito de origem chinesa e infraestrutura associada a uma série de ataques relatados a março de 2023."

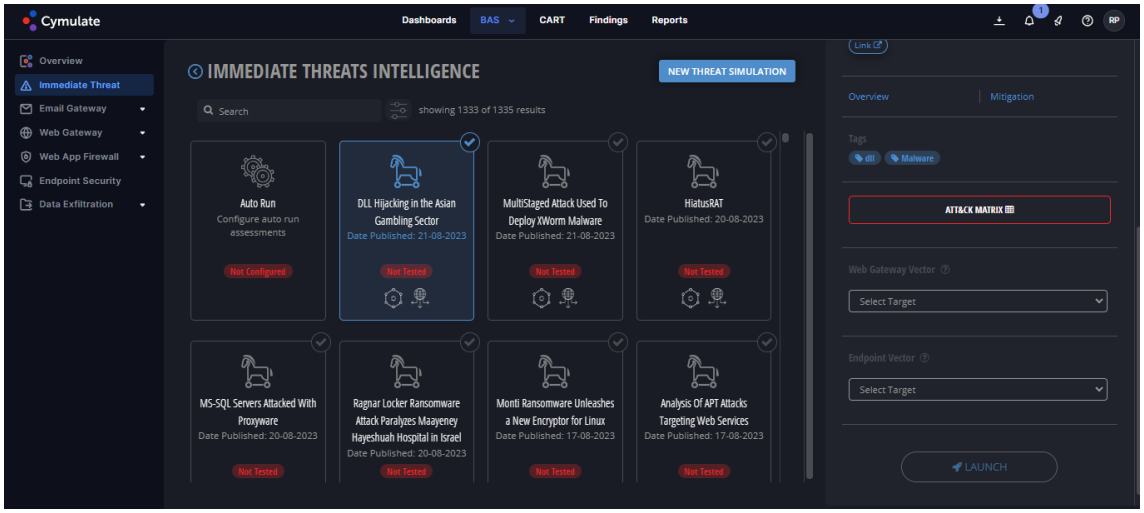


Figura 37: Exemplificação de uma simulação da funcionalidade de *Immediate Threat Intelligence* do Cymulate

Esta simulação tem como referência um artigo da SentinelOne (*Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector* 2023). De forma resumida, o artigo menciona os seguintes pontos:

- A SentinelLabs identificou um *malware* de origem chinesa e uma infraestrutura potencialmente envolvida em operações associadas à China, direcionadas ao setor de jogos de casino no Sudeste Asiático;
- Os atores da ameaça estão a explorar vulnerabilidades de Dynamic Link Library (DLL) *hijacking* em executáveis do Adobe Creative Cloud, Microsoft Edge e McAfee VirusScan para inserir *beacons* do Cobalt Strike;
- Foi observado que *malwares* correlacionados com esta atividade estão a utilizar o certificado digital comprometido para assinarem os seus ficheiros maliciosos, tentando assim transmitir segurança e confiança a quem os executar, este certificado foi emitido para a PMG PTE LTD, um fornecedor sediado em Singapura que oferece serviços da VPN Ivacy;
- Os indicadores apontam para o grupo BRONZE STARLIGHT, no entanto, esta informação permanece pouco clara devido às relações interligadas entre os vários grupos APTs chineses.

3.6.4.4 *Relatórios e métricas*

De seguida são apresentadas funcionalidades de geração de relatórios e a avaliação contínua da postura dos controlos de segurança.

A Cymulate providencia 4 tipos diferentes de relatórios, observável na figura 38:

- Executivo com uma avaliação global - Permitem observar o nível de eficácia dos controlos de segurança para com os diferentes cenários. Neste relatório são apresentados os diferentes vetores de ataque e fornecida uma pontuação para cada um destes. Para além disso é fornecida uma análise com um destaque de tipos de ataques mais relevantes e a quantidade de testes que passaram pelos controlos de segurança de um total de simulações. Para além disso, é demonstrada uma arquitetura de um APT, com os diferentes cenários em conjunto com as suas pontuações de risco e um gráfico de risco comparativo com outras empresas dentro da mesma industria;
- Técnico e/ou executivo por cada cenário - Um relatório executivo apresenta os dados de forma mais simplista e de fácil perceção. Estes dados incluem o nível do risco que os resultados da simulação representam e um resumo das simulações que passaram pelos controlos de segurança por cada tipo de ataques. Quanto aos dados de um relatório técnico, para além da informação fornecida num relatório executivo, este apresenta, de forma singular, cada ameaça que passou pelos controlos de segurança, contendo informação mais específica para

cada um deles, tais como: tipo de ataque, nível de risco, tamanho do ficheiro, descrição da ameaça e sugestões de mitigação;

- Pré-criados - Por padrão, a Cymulate disponibiliza 6 relatórios para diferentes objetivos, tais como: a obtenção de informações importantes sobre a postura global de segurança, monitorização de desvios de segurança, informações importantes sobre o nível de prevenção e deteção, avaliação comparativa entre duas tecnologias EDR e, por último, fornecer uma visão atualizada das lacunas de segurança mais recentes, críticas e de alto risco a serem abordadas pela equipa de segurança da informação nos controlos e políticas de segurança da organização;
- Personalizados - Este tipo de relatório, conforme o próprio nome sugere, oferece a flexibilidade necessária para a criação de relatórios personalizados, seja para um cenário mais específico, como um PoC, ou para um relatório onde se pretenda ter uma base para efeitos regulares.

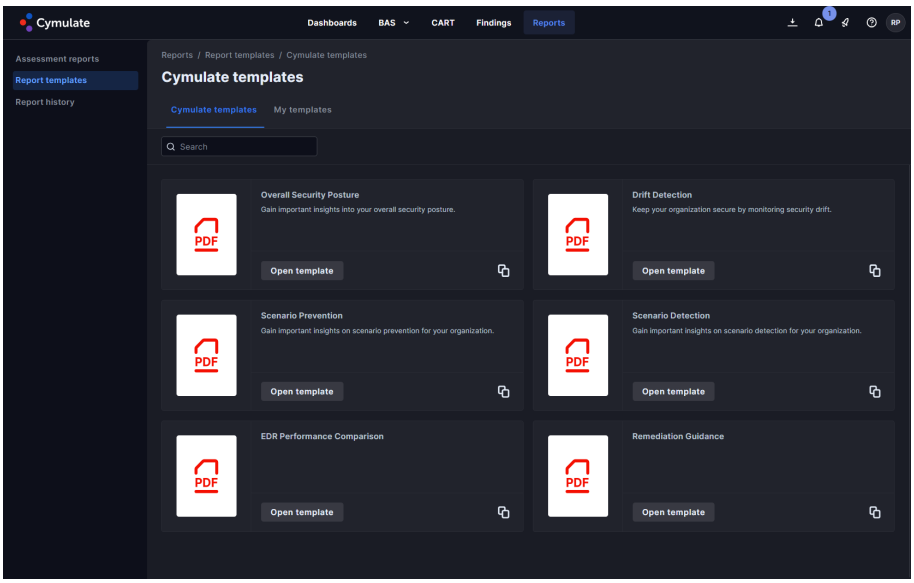


Figura 38: Modelos de relatórios da Cymulate

A escolha do relatório a adotar depende fundamentalmente do objetivo. Para tomar uma decisão informada, é essencial considerar cuidadosamente as metas e propósitos subjacentes à seleção do relatório. Isso implica avaliar a relevância das informações contidas, a profundidade da análise oferecida e a forma como os dados são apresentados. Ao alinhar o objetivo desejado com as características distintas de cada relatório, é possível obter *insights* mais precisos e úteis, que podem orientar ações e estratégias de maneira mais eficaz.

3.6.4.5 *Dashboards*

Apresenta a eficácia dos controlos de segurança contra grupos cibernéticos com intenções maliciosas, bem como contra as ameaças monitoradas pelas agências de resposta a emergências de segurança cibernética dos Estados Unidos.

A solução da Cymulate fornece 9 *dashboards* por padrão:

- Cymulate Dashboard - Oferece uma visão global das avaliações perante os diferentes cenários da ferramenta BAS. É atribuída uma pontuação a cada cenário, variando de 0 a 100, onde 0 representa uma eficácia de segurança perfeita em relação às simulações realizadas, enquanto 100 indica um alto risco de segurança;
- Attack Based Vulnerability Management - Para além de fornecer uma visão global da proteção dos controlos de segurança a vulnerabilidades) este permite efetuar simulações de *immediate threats* relacionadas com cada um destes Common Vulnerabilities and Exposures (CVEs);
- Mitre ATT&CK Heatmap - Permite observar o estado global do ambiente corporativo com a execução das simulações, mediante as diferentes táticas, técnicas e até sub-técnicas;
- Overall Security Posture - Este é um *dashboard* que oferece a visão da postura global de segurança perante as diversas funcionalidades da ferramenta Cymulate;
- Scenario Prevention Overview - Possibilita a análise das tendências de simulação ao longo do tempo, sem mitigações. No contexto desta análise, é verificado das 5 táticas e técnicas de maior destaque na *framework* do Mitre ATT&CK, sem quaisquer ações de mitigação. Além disso, são avaliados os níveis de risco associados aos cenários sem medidas de mitigação. São também identificados os vetores que apresentam as taxas de insucesso mais significativas. Por fim, este fornece uma lista completa das simulações sem terem sido sujeitas a quaisquer medidas de mitigação;
- Scenario Detection Overview - A premissa é semelhante à do painel de controle "Scenario Prevention Overview". No entanto, neste caso, o foco é nas deteções, ao invés das mitigações;
- Drift Detection - O desvio de segurança é o resultado inevitável de um ambiente tecnológico empresarial em constante mudança. Novos utilizadores, aplicações, atualizações, alterações de processos, alterações de infraestruturas

e uma série de outras operações diárias alteram a resiliência da cibersegurança da organização. A atividade de novas ameaças evolui rapidamente, exigindo ajustes e alterações nos controlos para combater adequadamente as novas ameaças. Por esse motivo este fornece a capacidade de identificar alterações, lacunas e desvios das políticas de segurança (Moshe, 2023b);

- Lateral Movement Security Posture - Através deste podemos verificar a postura do ambiente corporativo em relação ao movimento lateral entre *endpoints*.

Para além dos *dashboards* mencionados anteriormente, é possível realizar a criação de *dashboards* personalizados com o intuito de abranger uma ampla gama de cenários. Um exemplo claro dessa possibilidade surge em contextos de PoC que englobem ferramentas de segurança. Nestes cenários, estes *dashboards* possibilitariam a supervisão e avaliação do desempenho das diversas ferramentas, com o objetivo de identificar aquela que mais se destaca em termos de eficácia nos testes que são realizados.

3.6.4.6 *Integração com outras ferramentas de segurança*

A solução Cymulate realiza simulações de ataques com o propósito de avaliar a visibilidade e eficácia dos controlos de segurança. As integrações desempenham um papel crucial nesse objetivo, pois é por meio delas que se identifica qual a ferramenta está a detetar e/ou bloquear as simulações. A Cymulate divide as integrações em várias categorias:

- Vulnerability Management;
- Ticketing System;
- SIEM;
- EDR;
- SOAR;
- Firewall.

VULNERABILITY MANAGEMENT

No complexo cenário da cibersegurança, a identificação e a mitigação de vulnerabilidades são essenciais para manter uma postura defensiva eficaz. A integração da Cymulate com plataformas de gestão de vulnerabilidades, pode ajudar a identificar

vulnerabilidades e a dar-lhes prioridade com base na sua gravidade, enquanto testa e valida os esforços de correção para garantir que os sistemas e aplicações da organização estão seguros. A automatização dos testes de vulnerabilidades pode tornar as equipas de segurança mais eficientes e reduzir a carga sobre as TI para identificar vulnerabilidades e agir rapidamente para reduzir o risco de ataques bem sucedidos (Moshe, 2023c). Atualmente a Cymulate apresenta 5 ferramentas diferentes para integração dentro desta categoria como podemos verificar na figura 39.

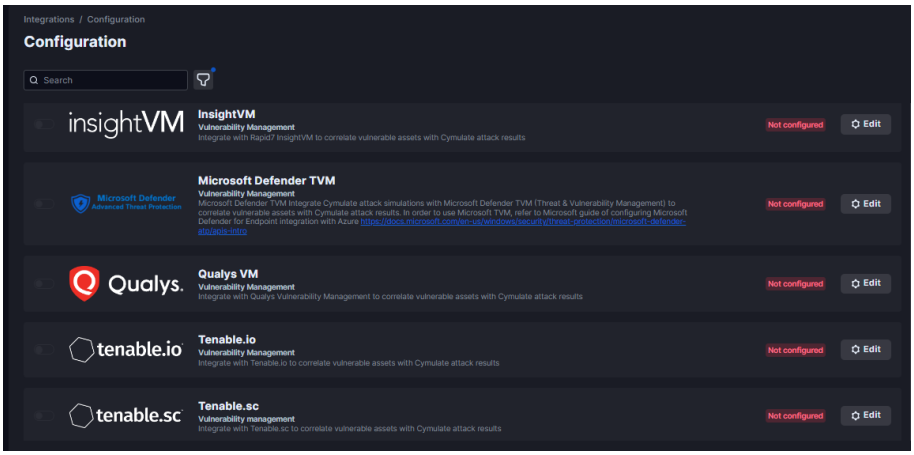


Figura 39: Integrações da Cymulate com ferramentas de gestão de vulnerabilidades

TICKETING SYSTEM

À medida que as organizações enfrentam diversos incidentes de segurança, a capacidade de rastrear e responder a esses eventos de forma eficiente é fundamental. Ao integrar-se com sistemas de *tickets*, a Cymulate ajuda as organizações a melhorar a sua postura de segurança, proporcionando às equipas de segurança uma maior visibilidade e melhores esforços de correção, através da geração automática de *tickets* para problemas de segurança identificados. Com um sistema de emissão de *tickets*, as equipas de segurança podem simplificar os fluxos de trabalho e reduzir o tempo necessário para responder a incidentes de segurança (Moshe, 2023c). Atualmente a ferramenta da Cymulate apenas dá a possibilidade de integração com um único sistema de *tickets*, como se pode verificar na figura 40

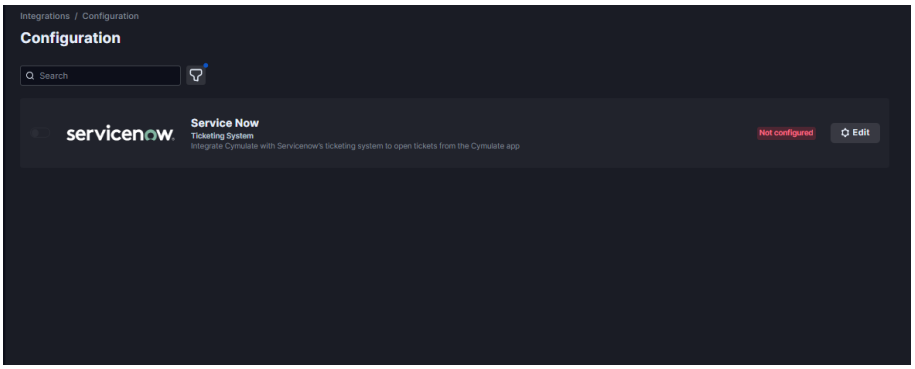


Figura 40: Integrações da Cymulate com sistemas de *tickets*

SIEM

Num ambiente de segurança em constantes mudanças, é importante ter uma visão global e concentrada dos eventos associados à atividade corporativa. A Cymulate, ao integrar-se com sistemas SIEM, concede essa visibilidade de forma precisa, permitindo a análise das simulações com outros dados de segurança. Esta abordagem possibilita afinar a sua configuração para garantir uma melhor cobertura de incidentes, fornecer contexto adicional aos eventos de segurança para priorizar e otimizar os esforços de resposta, para garantir que as ameaças mais críticas sejam abordadas primeiro (Moshe, 2023c). Para a categoria de SIEM, a Cymulate apresenta integrações com 12 ferramentas. Na figura 41, é possível observar algumas das opções.

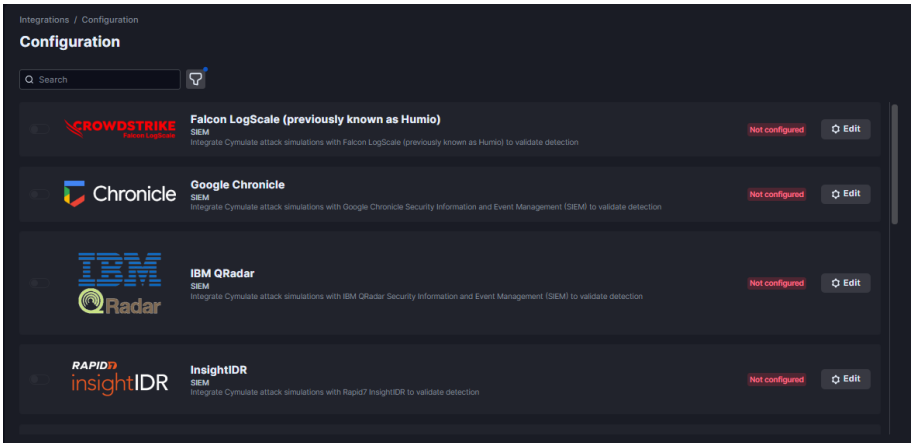


Figura 41: Integrações da Cymulate com o SIEM

EDR

Os *endpoints* constituem pontos críticos de acesso para diversas ameaças cibernéticas. A integração da Cymulate com soluções de EDR permite descobrir lacunas de segurança que podem expor as organizações a ameaças, fornecer informações para priorizar e otimizar os esforços de resposta e dar às organizações uma abordagem mais proativa e abrangente à sua postura de cibersegurança, fornecendo uma maior capacidade defensiva (Moshe, 2023c). Na categoria de EDR, a Cymulate oferece integrações com 13 ferramentas. A figura 42 exibe algumas das opções disponíveis.

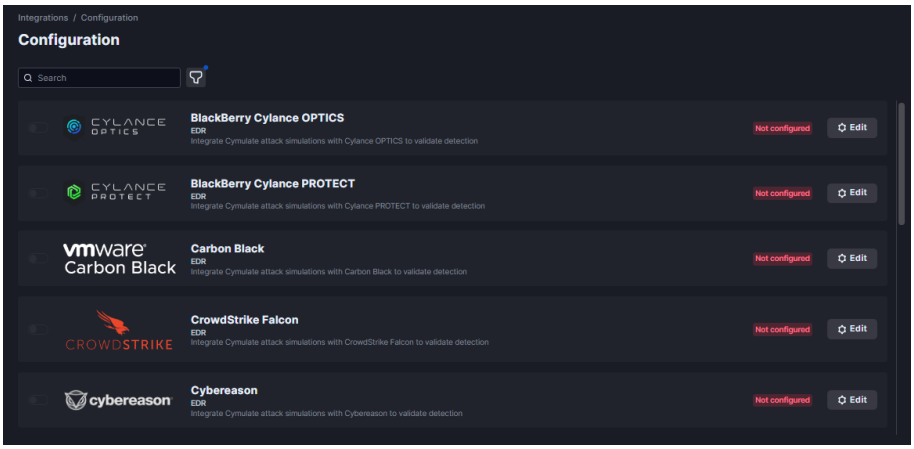


Figura 42: Integrações da Cymulate com o EDR

SOAR

Num contexto em que a rapidez de resposta é necessária, a automação assume um papel crucial na eficácia operacional. A integração da Cymulate com plataformas SOAR possibilita a validação e otimização de desempenho. No âmbito da categoria de SOAR, a Cymulate disponibiliza integração com uma única ferramenta. A figura 43 ilustra a mencionada ferramenta.

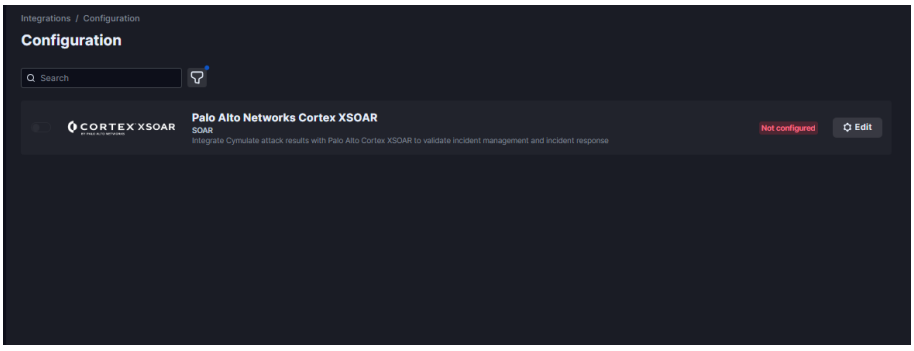


Figura 43: Integrações da Cymulate com o SOAR

FIREWALL

A Cymulate juntamente com os parceiros de sistemas de Firewall, desafiaram a *firewall* da rede de uma organização contra um conjunto abrangente de ataques para validar as definições e políticas de configuração da comunicação de entrada e saída (Moshe, 2023c). Esta integração permite que os resultados apareçam diretamente nos relatórios da Cymulate, para que as organizações possam responder às ameaças mais rapidamente e agilizar a correção dos incidentes. No contexto da categoria de Firewall, a Cymulate oferece integração com uma única ferramenta. A figura 44 retrata a ferramenta em questão.

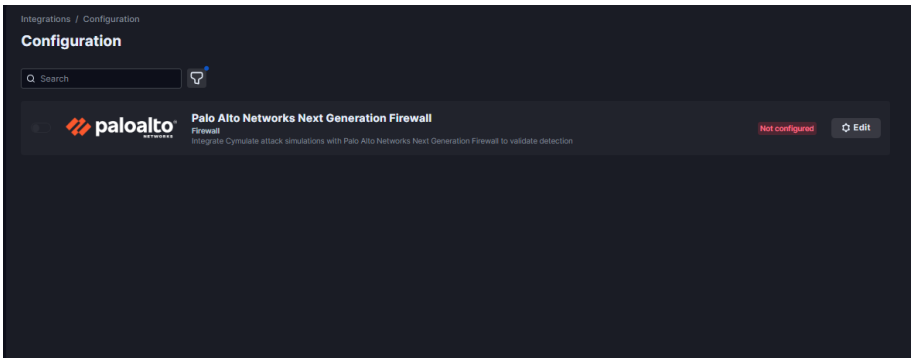


Figura 44: Integrações da Cymulate com a Firewall

As integrações desempenham um papel fundamental na potenciação dos objetivos da solução, uma vez que fornecem informações sobre os controlos de segurança que realizam a mitigação das ameaças, ao mesmo tempo que demonstram a visibilidade das mesmas. Adicionalmente, essas integrações também são responsáveis por efetuar notificações e automações, contribuindo assim para uma abordagem mais completa e eficaz em termos de segurança.

3.6.5 *Prestação de Suporte*

Inicialmente, foi necessário obter apoio para que fosse possível realizar as avaliações gratuitas para cada vetor de ataque. No entanto, não foi uma tarefa simples. Ao ser efetuada, uma das avaliações gratuitas apresentou uma janela informativa que indicava a indisponibilidade de tentativas. Nessa mesma janela, existia um botão para solicitar suporte.

Após um período de tempo considerável, possivelmente algumas semanas, não foi obtida qualquer resposta por parte da equipa de suporte. Perante esta situação, o

problema foi abordado por duas vias distintas. Inicialmente, um contacto através do LinkedIn com um profissional de hierarquia superior da Cymulate. Ao mesmo tempo, foi obtido o contacto de um representante português com o qual já tinha havido interação.

Importa salientar que, num espaço de cerca de 3 dias, obteve-se resposta de ambas as partes. Além disso, não só foi disponibilizada a extensão da versão de avaliação, como também foi concedido acesso às avaliações gratuitas, foram partilhados relatórios e acesso à observação de outras funcionalidades da ferramenta Cymulate. Esta sequência de eventos permitiu retomar o processo e resolver a questão pendente, possibilitando assim a continuação do desenvolvimento deste projeto de mestrado.

3.7 FERRAMENTA SAFEBREACH

A SafeBreach tem a missão de mudar fundamentalmente a forma como as organizações gerem as suas defesas e controlam o risco cibernético. O percurso começou quando o *Chief Executive Officer* (CEO) Guy Bejerano e o *Chief Technology Officer* (CTO) Itzik Kotler se juntaram para partilhar a frustração de que os líderes de segurança podiam gastar uma fortuna em controlos de segurança, mas ainda assim não conseguiam avaliar com confiança o seu nível de preparação contra ameaças específicas. Guy e Itzik começaram rapidamente a trabalhar numa solução para combinar a mentalidade de um CISO com o conjunto de ferramentas de um hacker (*Discover more about SafeBreach* 2023). Em 2014, a SafeBreach nasceu com o lançamento da primeira plataforma de validação de segurança contínua do sector (*Discover more about SafeBreach* 2023).

A solução BAS premiada permite às empresas modernas executar ataques de forma contínua e segura, validar e otimizar a eficácia dos seus controlos de segurança e dar prioridade aos esforços de correção para mitigar as suas falhas mais críticas antes de serem comprometidos. Com o *Hacker's Playbook* - a mais extensa coleção de dados de ataques da indústria - a SafeBreach permite que as organizações se tornem proativas em relação à segurança, com uma abordagem simples que substitui a esperança e o medo por dados do mundo real e ações em tempo real (*Discover more about SafeBreach* 2023).

Tal como a maioria das empresas, a SafeBreach possui investidores, dentro dos quais está uma das maiores empresas de Portugal, a Sonae IM do grupo Sonae (*Discover more about SafeBreach* 2023).

3.7.1 *Processo de Instalação e Configuração da SafeBreach*

Vão ser agora apresentadas as várias etapas do processo de instalação e configurações necessárias para realizar as simulações pretendidas.

Em primeiro lugar, efetua-se o *download* do simulador para o sistema operativo Windows, tal como é apresentado na figura 45.

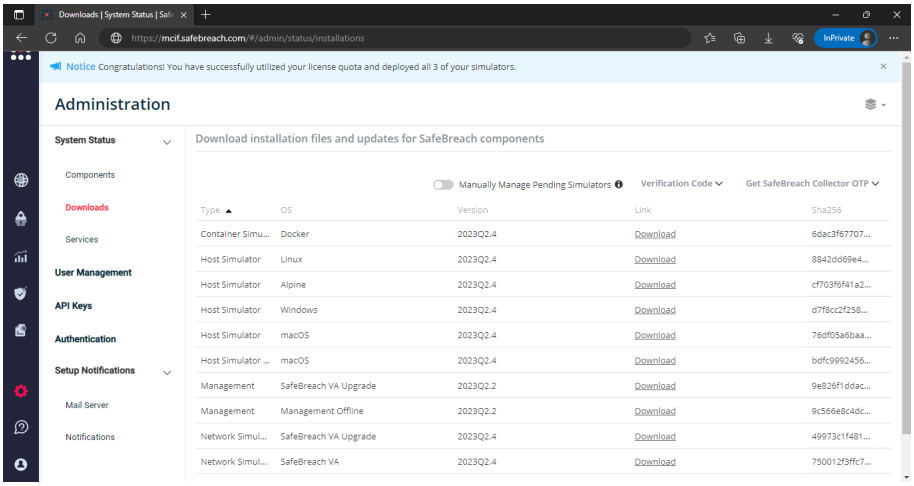


Figura 45: Download do agente simulador da SafeBreach

De seguida, é executado o ficheiro que foi descarregado e a instalação é efetuada seguindo os seguintes passos:

- Passo 1 - Início da instalação do simulador da SafeBreach, conforme apresentado na figura 46;

Figura 46: Bem vindo, instalação do simulador da SafeBreach

- Passo 2 - Para prosseguir com a instalação é necessário aceitar os termos e condições do contrato da licença da SafeBreach, presentes na figura 47;

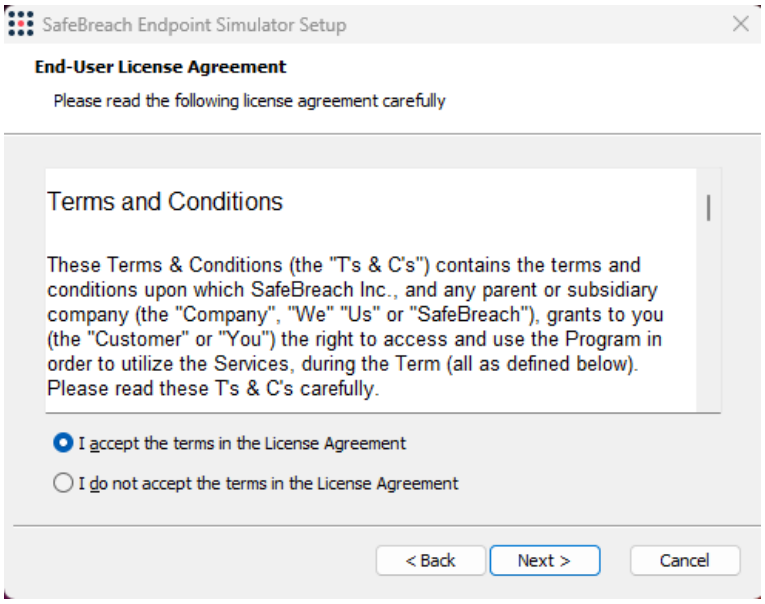


Figura 47: Aceitar os Termos e Condições da SafeBreach

- Passo 3 - É selecionada a pasta para a instalação da ferramenta, conforme é apresentado na figura 48;

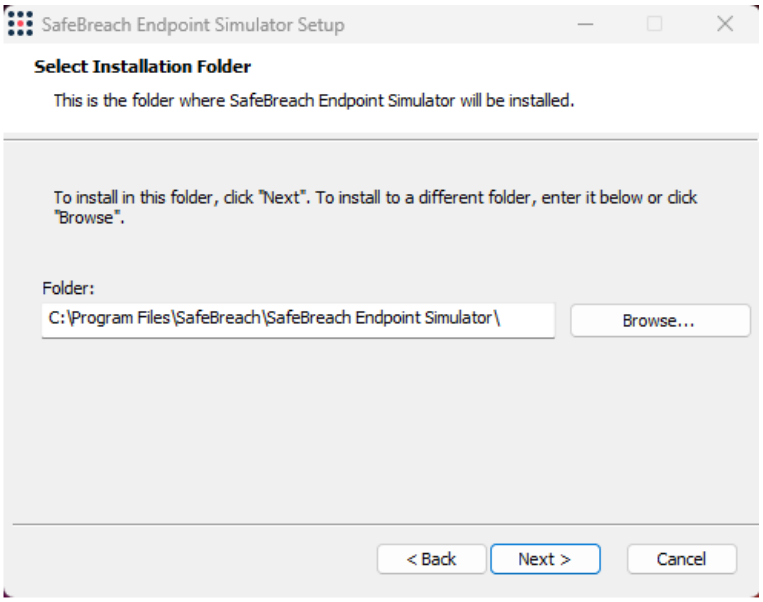


Figura 48: Selecionar pasta de instalação

- Passo 4 - Através do passo 5 e 6 é possível preencher os pontos obrigatórios do passo 4, visíveis na figura 49, como podem verificar no URL do passo seguinte é visível que o "*SafeBreach Management URL*"é mcif.safebreach.com, no passo 6 conseguimos demonstrar onde podemos obter o "*Verification Code*";

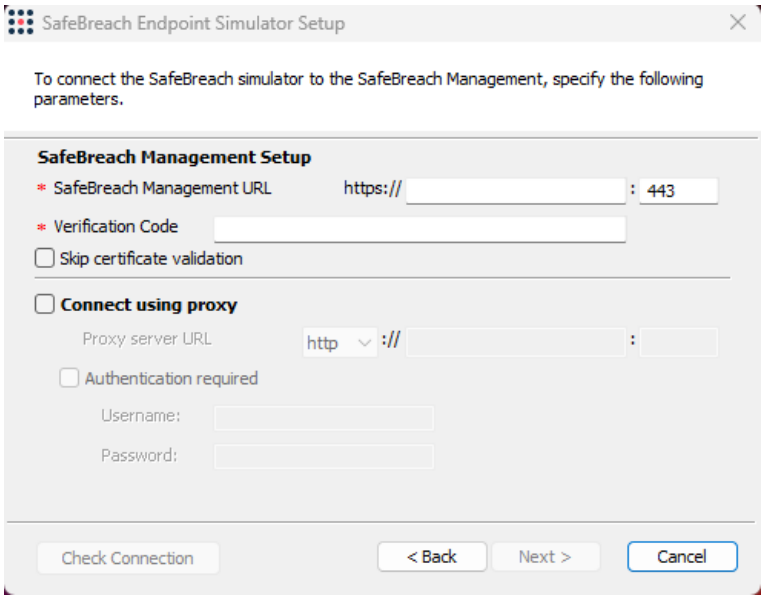


Figura 49: Domínio da consola e código de verificação

- Passo 5 - Para obtermos o código de verificação necessário para o passo anterior, é necessário aceder à plataforma com uma conta com o *role* de administração, de seguida acede-se às definições e seleciona-se a opção de administração, tal como é demonstrado na figura 50;

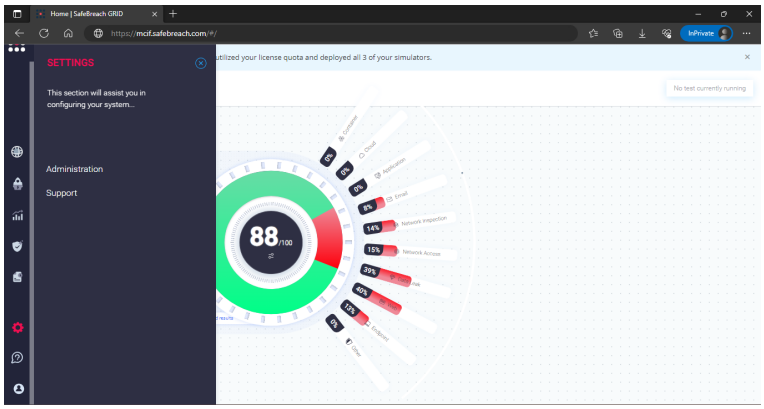


Figura 50: Opção de Administração

- Passo 6 - Como se pode observar na figura 51, o código de verificação é adquirido ao selecionar *"Verification Code"*, podendo voltar a ser gerado as vezes forem necessárias e copiado de forma fácil;

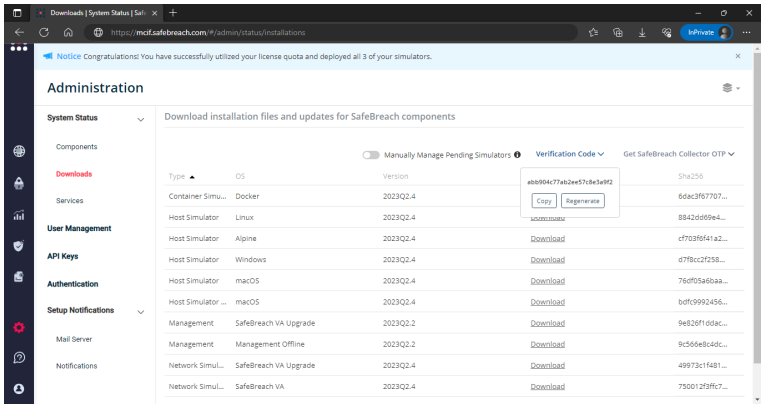


Figura 51: Código de Verificação

- Passo 7 - Por fim, é só carregar na opção de instalar para instalar e finalizar o processo, tal como foi efetuado na figura 52;

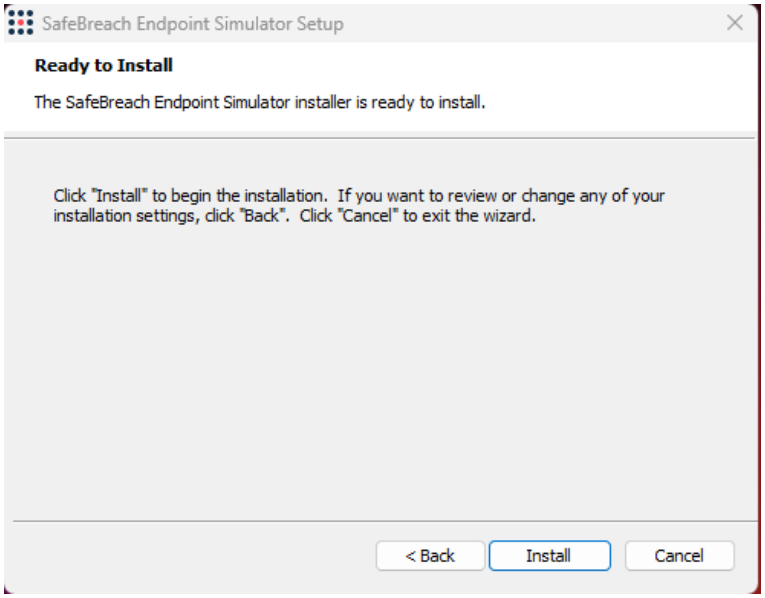


Figura 52: Instalar

Depois da instalação, e considerando que se pretende testar 3 vetores de ataque - *endpoint*, *network* e e-mail - foi realizada a configuração do email na plataforma da SafeBreach. Dado que se vai usar um e-mail *on premise*, é selecionado como "*Connection type*"o Exchange. Para além disso foi inserido o servidor do exchange designado por exchange.mcif.pt à escuta no porto 993 (IMAPS - Internet Message Access Protocol over SSL). Posto isto, são inseridos os dados da conta de email - endereço de email e password - e selecionado o simulador pretendido, que, para esta configuração, foi escolhido o DKT, terminando assim o processo de configuração, tal como é visível na figura 53.

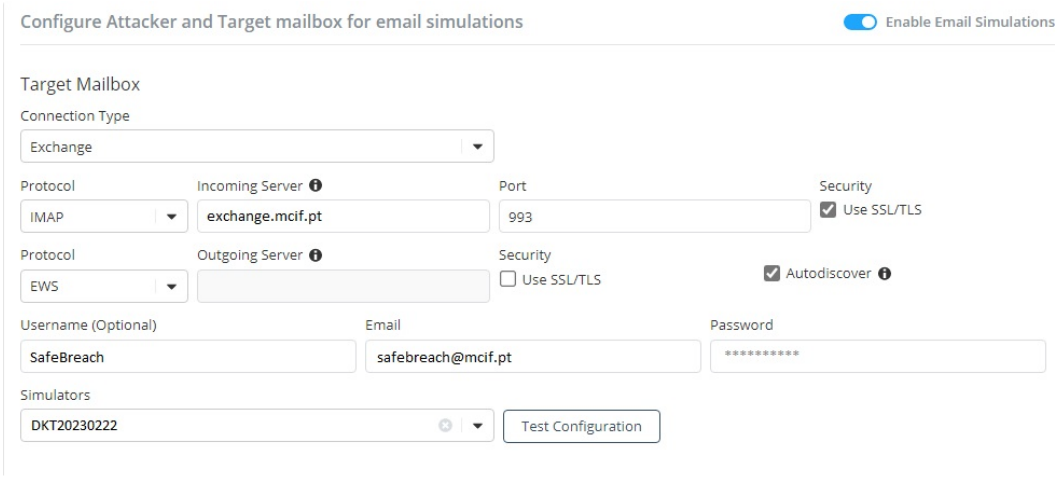


Figura 53: Configuração do email para testes na SafeBreach

Foi necessário efetuar adicionar um *proxy* para certas simulações com as configurações visíveis na figura 54.

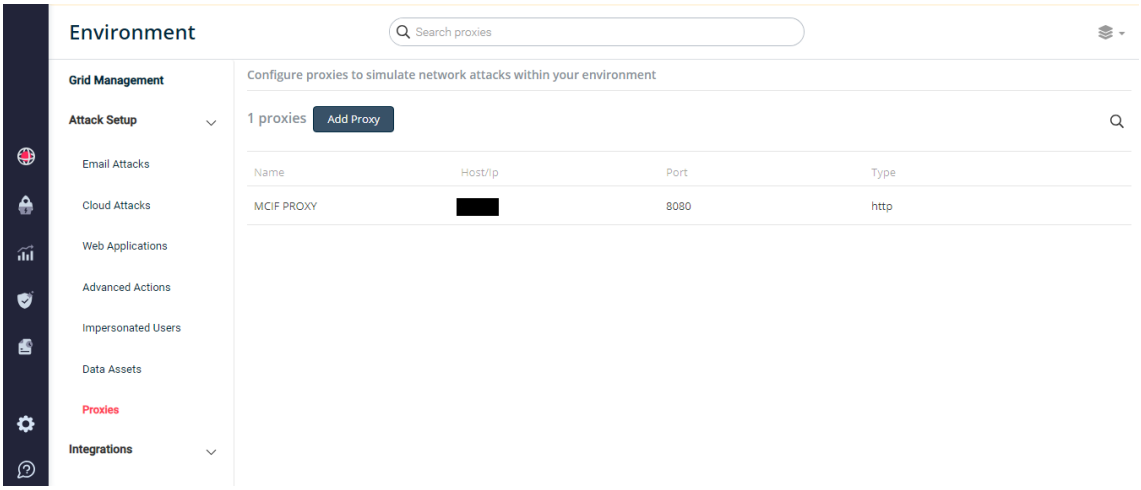


Figura 54: Adicionar o *proxy*

3.7.2 *Execução dos testes base*

Após se realizar a instalação e as configurações, foram efetuados os testes base recomendados pela SafeBreach, de modo a verificar, de modo geral, o estado da eficácia dos controlos de segurança e os pontos de falha a serem melhorados. Estes testes são compostos por 5 passos, sendo estes os seguintes:

- Step 1 - Fortify your Network Perimeter: Este cenário irá executar ataques de infiltração contra as defesas de perímetro, com uma variedade de ameaças que se espera que sejam bloqueadas pelo perímetro da rede.

Como é verificado na figura 55, observa-se uma taxa de sucesso de 79 em 100 na eficácia dos controlos de segurança, havendo sido bloqueadas 3000 das 3788 simulações realizadas. Das 788 simulações que não resultaram em bloqueio, os controlos demonstraram uma eficácia reduzida nas situações em que o tipo de ataque estava associado a:

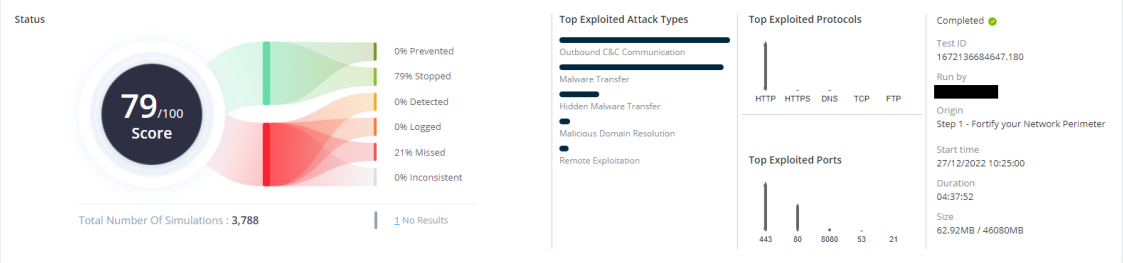


Figura 55: Resultado do teste "Step 1 - Fortify your Network Perimeter"

  - Malicious Domain Resolution - A proporção de simulações que não foram bloqueadas pelos controlos de segurança atingiu 50%, o que corresponde a 7 dos 14 executados. Este cenário poderia ser explorado por possíveis invasores para atividades de *phishing*, disseminação de *malware* e o estabelecimento de servidores de C2 para *botnets*;
  - Outbound C&C Communcation - "A taxa de sucesso nos testes alcançou os 36%, correspondendo a 332 casos dos 930 testes totais realizados. Esse contexto viabilizaria a capacidade dos agressores para enviar comandos, transferir informações e manter o controlo sobre o sistema comprometido.

- Step 2 - Validate your Endpoint Protection: Este cenário executa vários ataques aos *endpoints* para validar a resiliência da proteção dos mesmos contra diferentes tipos de ameaças.

  Conforme evidenciado na figura 56, constata-se uma taxa de eficácia dos controlos de segurança de 85 em 100, devido ao facto de 631 em 742 simulações terem sido bloqueadas. Das 111 simulações que não foram, os controlos revelaram menor eficácia nas simulações cujo tipo de ataque está relacionado com:

  - System Information Dump and Data Collection - A percentagem que não foi bloqueada totalizou 93%, o que equivale a 13 testes dos 14 realizados. Isto possibilitaria que potenciais atacantes obtivessem dados do sistema e realizassem ações como *scan* de redes, obtenção de credenciais entre outros métodos dentro deste âmbito.

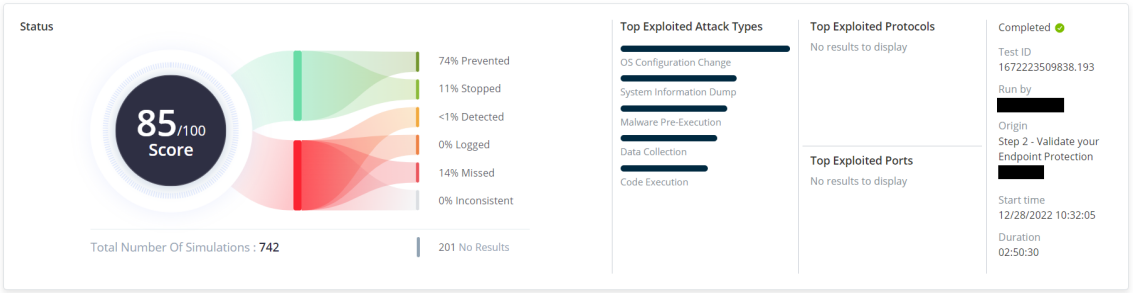


Figura 56: Resultado do teste "Step 2 - Validate your Endpoint Protection"

– OS Configuration Change - A proporção de testes bem-sucedidos atingiu 78%, o que corresponde a 29 de um total de 37 testes efetuados. Este cenário abriria espaço para a manipulação das configurações do sistema operativo, permitindo a execução de ações como a criação de utilizadores, a ocultação de ficheiros, a obtenção de privilégios, entre outras possibilidades.

- Step 3 - Defend Against Internal Network Propagation: Este cenário conduz ataques e comportamentos que utilizam o acesso à rede interna para realizar atividades maliciosas. Este cenário irá ajudar a identificar áreas onde a execução de protocolos e políticas de segurança mais rigorosas podem ajudar a reduzir o risco de movimento lateral.

  De acordo com a representação apresentada na figura 57, é possível verificar que a efetividade dos mecanismos de segurança apresentou uma taxa de 2 em 100. Tal resultado advém do bloqueio de 148 simulações num total de 5220. Das simulações não bloqueadas, foi observada uma menor eficácia dos controlos em situações que envolvem os seguintes tipos de ataques:

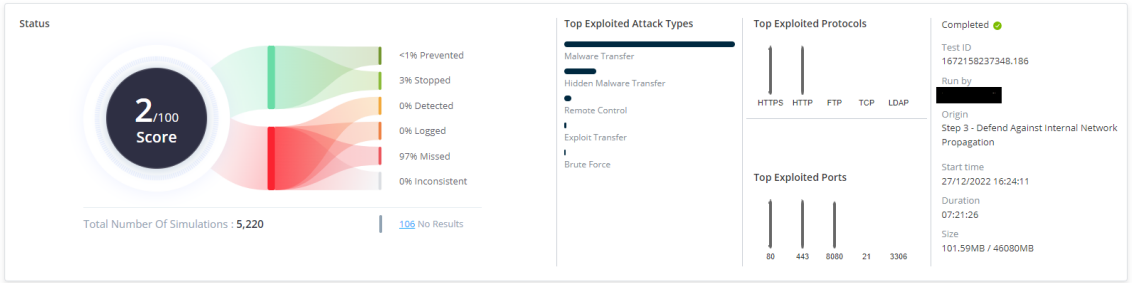


Figura 57: Resultado do teste "Step 3 - Defend Against Internal Network Propagation"

– Remote Exploitation - A totalidade das tentativas não bloqueadas correspondeu a 100%, ou seja, 2 num total de 2 testes efetuados. Nesse contexto, potenciais atacantes poderiam explorar a vulnerabilidade CVE-2020-1350. Essa vulnerabilidade permite o envio de uma *query* de Domain

Name System (DNS) especialmente concebida para um servidor DNS vulnerável, podendo resultar na execução de código com privilégios de SYSTEM, que por sua vez, comprometeria integralmente o servidor.

– Malware Transfer - A percentagem de tentativas não bloqueadas alcançou 99%, representando 4031 testes não bloqueados de um total de 4068. Esse cenário denota a facilidade na transferência de *malwares* para os dispositivos-alvo via HTTP/S.

- Step 4 - Optimize Outbound Egress Filtering: Este cenário testa a política de *egress* de rede, executando vários comportamentos e atividades maliciosas em torno dos canais de comunicação e exfiltrando dados sensíveis.

  Conforme ilustrado na representação exibida na figura 58, é possível constatar que a eficácia dos mecanismos de segurança demonstrou uma taxa de sucesso de 56 em 100. Esse desfecho resulta do bloqueio de 262 simulações, de um total de 466. Dentro das simulações não bloqueadas, foi notada uma reduzida eficiência dos controlos em cenários que abarcam os seguintes tipos de ataques:

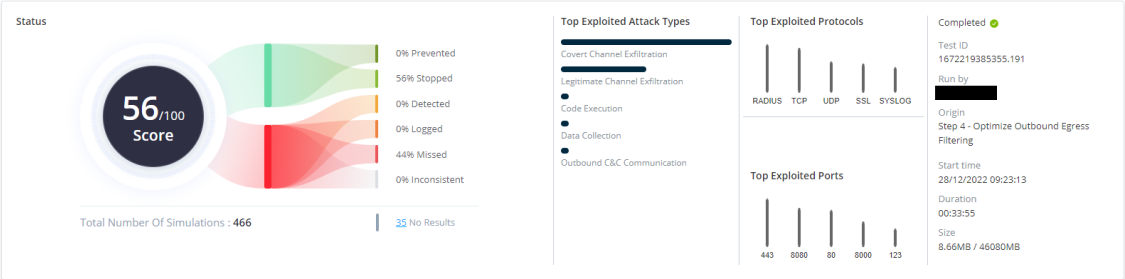


Figura 58: Resultado do teste "Step 4 - Optimize Outbound Egress Filtering";

– Legitimate Channel Exfiltration - A totalidade das investidas não bloqueadas alcançou 51%, correspondendo a 62 num total de 122 testes conduzidos. Nesse contexto, potenciais atacantes teriam a capacidade de realizar a exfiltração de informações através de canais legítimos, evitando assim a deteção.

– Covert Channel Exfiltration - A proporção de tentativas não bloqueadas atingiu 41%, representando 193 de um total de 329. Dessa forma, os atacantes conseguem transmitir informações de um sistema comprometido para um destino externo sem levantar suspeitas. Isso envolve a exploração de vias de comunicação não convencionais ou o uso de vias de comunicação legítimas de formas não convencionais.

- Step 5 - Run The 3 Latest Known Threats: Este cenário valida a postura de segurança contra os 3 ataques mais recentemente conhecidos. O *Service Level Agreement* (SLA) de 24 horas da SafeBreach garante uma rápida cobertura para alertas da US-CERT e alertas do *Fereal Bureau of Investigation* (FBI).

Faltando a análise ao vetor de e-mail, foi criado um cenário personalizado para a avaliação destes controlos de segurança. Este cenário compreendia 2448 simulações, refletindo a totalidade de simulações existentes para este vetor.

Como ilustrado na representação exibida na figura 59, é possível constatar que a eficácia dos mecanismos de segurança demonstrou uma taxa de sucesso de 98 em 100. Esse resultado é o produto do bloqueio de 49 simulações, de um total de 2.448.

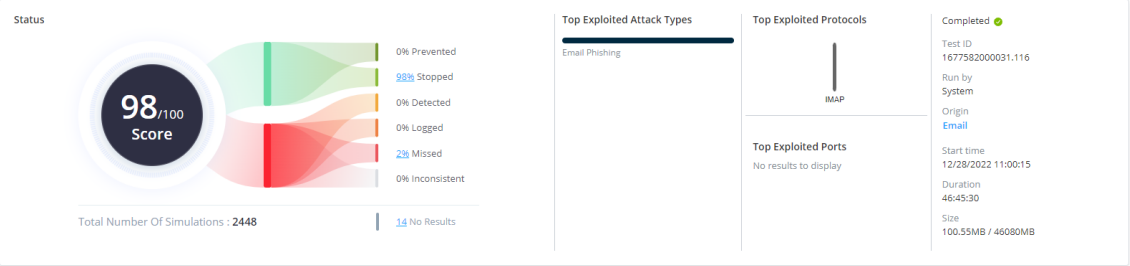


Figura 59: Resultado do cenário personalizado para o vetor de *e-mail*

Todos estes passos permitem identificar falhas nos controlos de segurança e com a finalidade de corrigi-las, fornecendo total visibilidade para os processos do lado do atacante e do alvo, tal como é possível observar nos registos apresentados na Apêndice A, provenientes da plataforma.

Após avaliação dos resultados dos testes base, foi detetado que havia um controlo abaixo da eficácia pretendida, nomeadamente o da rede. Para remediar esta situação foi adicionado bloqueio de acesso a certos tipos de categorizações de *websites* na *firewall*. Nas imagens abaixo podemos ver o antes e o depois da implementação destas melhorias, figura 60 e figura 61 respetivamente.

Esta configuração fez aumentar a eficácia em 15 pontos numa escala de 0 a 100, em que 0 significa que não bloqueou nenhuma ameaça e 100 que bloqueou todas as ameaças testadas, passando assim de uma eficácia de 65 na primeira avaliação para 80 após ter sido aplicada as melhorias supramencionadas.

Figura 60: Antes de aplicar as configurações na *firewall*

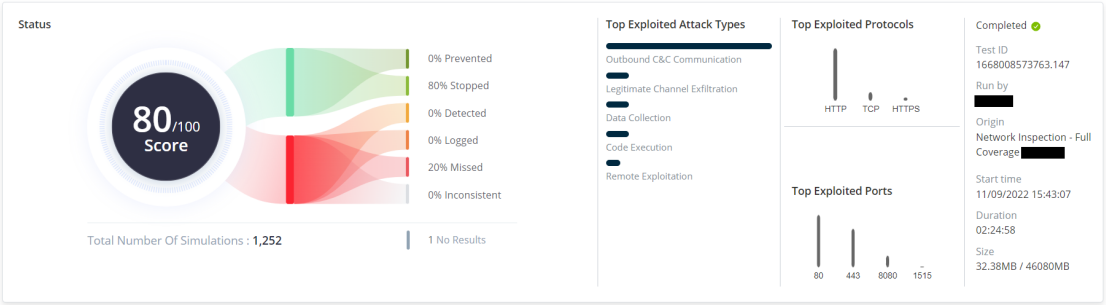


Figura 61: Depois de aplicar as configurações na *firewall*

3.7.3 *Avaliação contínua - Pilha de testes*

Para que haja uma avaliação contínua da eficácia dos controlos de segurança, foi criado um conjunto de testes semanais listados abaixo:

- Segunda-Feira:
  - Endpoint - Antivirus(signature) Full Coverage
  - Endpoint - Behavioral
  - Endpoint - Full Coverage
- Terça-Feira:
  - Endpoint - Next-Gent AV(pre-execution) Full Coverage
  - Email
  - Network Access - Full Coverage

  - Step 3 - Defend Against Internal Network
- Quarta-Feira:
  - Data Leak - Full Coverage
  - Company field (Energia, Telecomunicações, Defesa, etc...)
  - Step 4 - Optimize Outbound Egress Filtering
- Quinta-Feira:
  - Ransomware - Full Kill Chain Coverage
  - Step 2 - Validate your Endpoint Protection
- Sexta-Feira:
  - Step 1 - Fortify your Network Perimeter
  - Step 5 - Run The Latest Known Threat

É possível que se levantem questões acerca do motivo pelo qual estes testes não foram agrupados por controlo de segurança ou organizados por ordem. De seguida, são apresentados os 2 fatores que levaram a esta organização.

O primeiro fator relaciona-se com o facto de este conjunto de testes diários ter sido selecionado de modo a iniciar e terminar dentro do horário de trabalho. Supõe-se que exista um operador de prevenção após o horário de trabalho, no qual, em determinados cenários de teste, o sistema de monitorização e alarme de segurança seja acionado. No entanto, é importante salientar que esses cenários específicos têm o potencial de gerar o que é conhecido como um "falso positivo".

Dessa forma, para evitar que o operador de prevenção seja acordado desnecessariamente e para garantir que o tempo de trabalho seja otimizado, esta abordagem visa assegurar uma gestão eficiente dos recursos e a correta identificação de situações de segurança que exigem intervenção imediata.

O segundo fator está relacionado com a duração dos testes. Por norma, quanto mais simulações forem incluídas, maior será a duração do teste. Para fins de referência, um exemplo é o teste "Step 1 - Fortify your Network Perimeter", que contém 4,427 simulações e tem a duração aproximada de 7 horas e 23 minutos, enquanto o teste "Step 4 - Optimize Outbound Egress Filtering", com 480 simulações, tem a duração de cerca de 1 hora e 6 minutos.

Esta abordagem tem como objetivo principal garantir a realização dos testes de segurança e otimizar eficazmente o tempo disponível, evitando interrupções desnecessárias ou intervalos de tempo sem a execução de testes.

3.7.4 *Funcionalidades*

A ferramenta SafeBreach é uma solução de segurança cibernética projetada para ajudar as organizações a identificar e mitigar potenciais vulnerabilidades no seu ambiente, de forma transversal. Para atingir esses objetivos, a ferramenta constitui diversas funcionalidades, que, de seguida, são apresentadas e explicadas:

- Cenários de ataque;
- Simulação de cenários personalizados;
- *Threat Intelligence*;
- *Breach Studio*;
- *Vulnerability Management*;
- Relatórios e métricas;
- *Dashboards*;
- Integração com outras ferramentas de segurança.

De seguida, são explicadas detalhadamente cada uma destas funcionalidades.

3.7.4.1 *Cenários de ataque*

Os cenários da SafeBreach incluem uma coleção de cenários para avaliar as defesas da organização contra ciberataques e satisfazer as necessidades de validação dos controlos de segurança existentes (*Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach* 2022).

A coleção de cenários predefinidos da SafeBreach baseiam-se nas melhores práticas e vêm com funcionalidades incorporadas para permitir personalizar cenários e configurá-los conforme as necessidades.

Cada cenário inclui uma série de ataques organizados em etapas que simulam a progressão de uma ameaça numa organização.

Ao ter os ataques organizados em cenários, é mais rápido e fácil validar a ciber-defesa contra ameaças conhecidas, aproveitando as capacidades e o conhecimento da SafeBreach, em vez de ter de criar as próprias combinações de ataques. Cada cenário vem com os ataques apropriados já envolvidos em etapas lógicas e prontos para serem configurados para o ambiente corporativo.

Quando se escolhe um cenário para validar as suas defesas contra uma ameaça, uma consideração fundamental é selecionar os ativos que se pretende proteger/testar. Ao configurar-se o cenário (por exemplo, com simuladores e *proxies*), está a definir-se quais as secções da rede e quais os ativos a verificar, quanto à proteção contra as ameaças representadas no cenário.

Esta funcionalidade contém várias categorias, de modo a satisfazer as necessidades de validação dos diferentes controlos de segurança. De seguida, é apresentada a tabela 3 com a descrição das diferentes categorias:

Categorias	**Breve descrição**
Getting Started	Este cenário serve para criar uma linha de base inicial a partir da qual se pode começar a avaliar a eficácia dos controlos de segurança. Os cenários centram-se em todos os vetores para fornecer uma visão holística da sua postura de segurança.
Known threat series	As ameaças conhecidas referem-se a campanhas e elementos de ataque que foram divulgados como avisos ao público por organizações como a CISA (*Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach* 2022).
Endpoint Security	Validar a cobertura e a eficácia da postura das defesas de segurança dos *endpoints* do ambiente corporativo.
Network Security	Validar os controlos de segurança da rede e da *web* em relação a vários tipos de ataques, incluindo movimento lateral, comunicação C&C e exploração de aplicações.
Email Security	Validar as defesas contra *phishing* por via de anexos, infiltração e outros tipos de ataques de *email*.
Data Security	Validar as defesas contra a exfiltração de dados através de uma grande variedade de portas, protocolos e aplicações.
Cloud Security	Validação da postura de segurança na *cloud* e nos *containers*.
Threat Groups	Os *threat groups* são definidos por conjuntos de atividades e metodologias de intrusão relacionadas que são seguidas por um nome comum na comunidade de segurança (*Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach* 2022).
Baseline scenarios	Os cenários de base fornecem uma referência da postura de segurança esperada para vários tipos de atividade no seu ambiente.
Industry	Este cenário são para ataques específicos de um determinado sector.
Enviroment	Obtenha uma visibilidade precisa da eficiência dos controlos de segurança, executando ataques que correspondem aos componentes e arquitetura específicos do seu ambiente.
Mitre ATT&CK	A estrutura MITRE ATT&CK é uma base de conhecimento das táticas e técnicas dos adversários baseada em observações do mundo real, que pode ser utilizada como base para avaliar a postura de segurança e a prontidão face a várias metodologias de ataque (*Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach* 2022).

Tabela 3: Diferentes categorias de cenários disponibilizados pela SafeBreach e a sua descrição.

3.7.4.2 *Simulação de cenários personalizados*

Para além das categorias apresentadas anteriormente e disponibilizadas pela plataforma, ainda existe a possibilidade de efetuar 2 tipos de diferentes cenários:

1. Configuração cenários já existentes com as alterações desejadas;
2. Criação de um cenário de raiz para um objetivo mais focado;

Em primeiro lugar, é necessário detalhar o que é demonstrado num cenário de testes, na figura 62 são apresentados estes mesmos detalhes. Cada cenário é composto por um ou mais passos, cada um dos quais contém uma ou mais simulações de ataques.

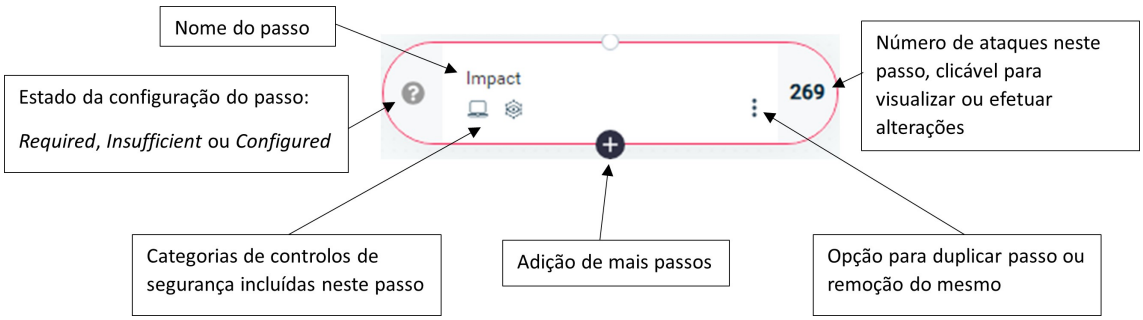


Figura 62: Informação apresentada num passo de um determinado teste;

O cenário pode ser configurado para adicionar um tempo de espera entre passos. O utilizador insere a duração desejada de intervalo de tempo. Após o passo anterior terminar, o teste aguardará o tempo especificado antes de iniciar o passo seguinte. É importante frisar que esta configuração não é transversal a todos os passos do teste.

Para um teste apresentar-se como configurado, é necessário identificar os elementos exigidos, na figura 63 é apresentado os 3 estados de um passo.

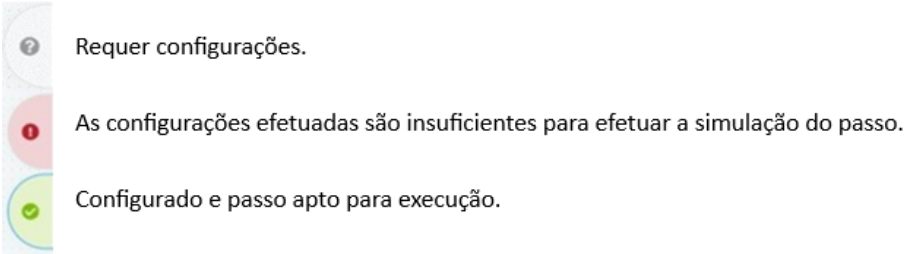


Figura 63: Informação dos vários estados dos passos;

No teste observável na figura 66, foi adicionado o simulador DKT como atacante e alvo. Após ter efetuado esta operação, é verificado pelo estado dos passos que foram

efetuadas todas as configurações necessárias à execução deste teste. É relevante referir que, por vezes, existem cenários que também exige a adição de um *proxy* ou *data assets* que estão correlacionados com os simuladores.

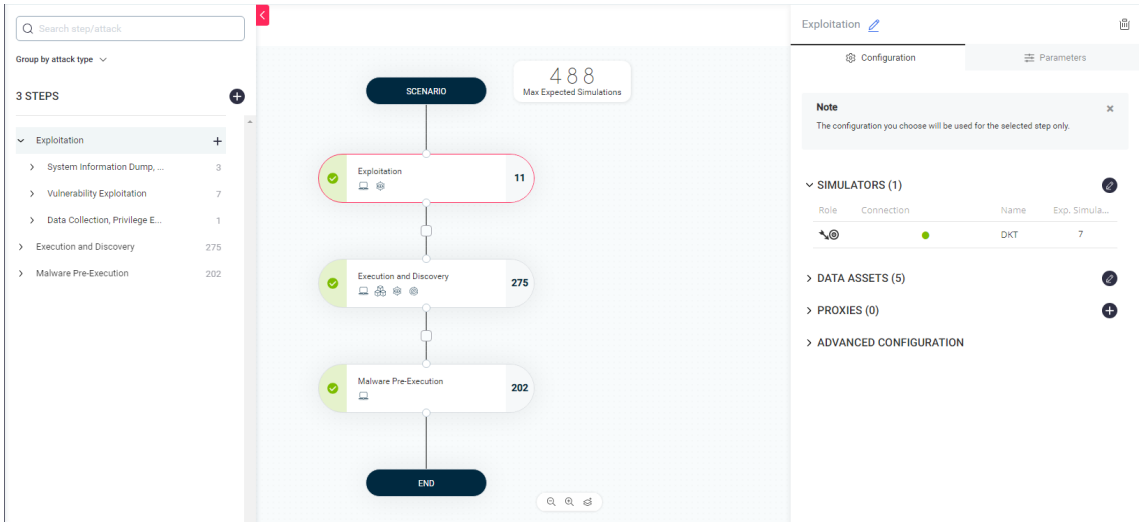


Figura 64: Teste válido para execução;

Posto isto o único passo em falta é a execução do teste. Após conclusão, é necessário avaliar a eficácia dos controlos de segurança em relação a cada ataque. Isso pode ser feito analisando as falhas que são exploradas por cada ataque e os controlos de segurança que podem ser usados/implementados para mitigar.

Relativamente ao ponto "Criação de um cenário de raiz para um determinado objetivo", irei aproveitar a secção seguinte para abordar este tema, uma vez que estão interligados.

VALIDAÇÃO DOS CONTROLOS DE SEGURANÇA

A essência desta ferramenta é validar a efetividade dos controlos de segurança implementados dentro de uma organização.

Por norma, para efetuar estas validações, são usados os cenários definidos pela plataforma. No entanto, para certos casos, como PoCs ou novas ameaças, são criados cenários personalizados de raiz.

Num cenário que se pretenda criar um teste de raiz, é necessário primeiro identificar o objetivo do teste. Neste caso, como um cenário hipotético, considere-se que a finalidade é avaliar a eficácia dos controlos de segurança em relação ao *ransomware* Locky. Para isso, é necessário encontrar todos os ataques relacionados com este *ransomware*. Isso pode ser feito através de uma pesquisa na funcionalidade SafeBreach

Playbook, tal como é visível na figura 65, que contém 7313 ataques, equivalentes a 26.918 métodos de compromisso.

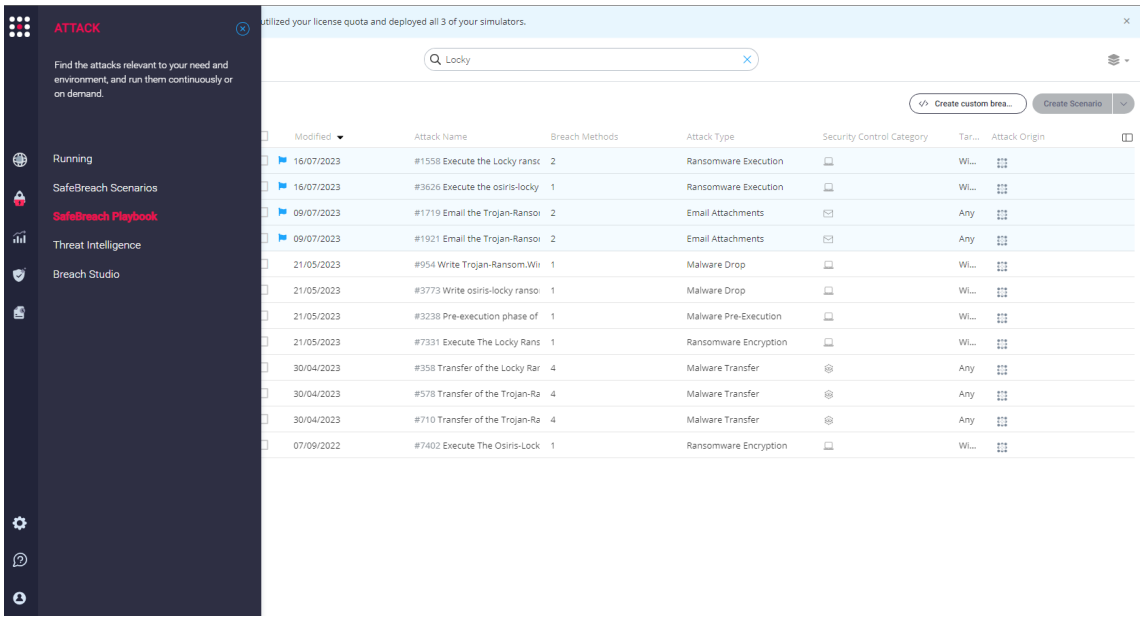


Figura 65: Ataques relacionados com o *ransomware* Locky

Ao pesquisar pelo *ransomware* Locky, são identificados 12 ataques como podemos observar na figura 65. No entanto, como se pode verificar, estes estão divididos em diferentes tipos de ataques. A próxima etapa passa por dividir estes ataques em vários passos.

Após uma avaliação cuidadosa dos testes, foi decidido dividi-los em 4 passos, apresentado na figura 66:

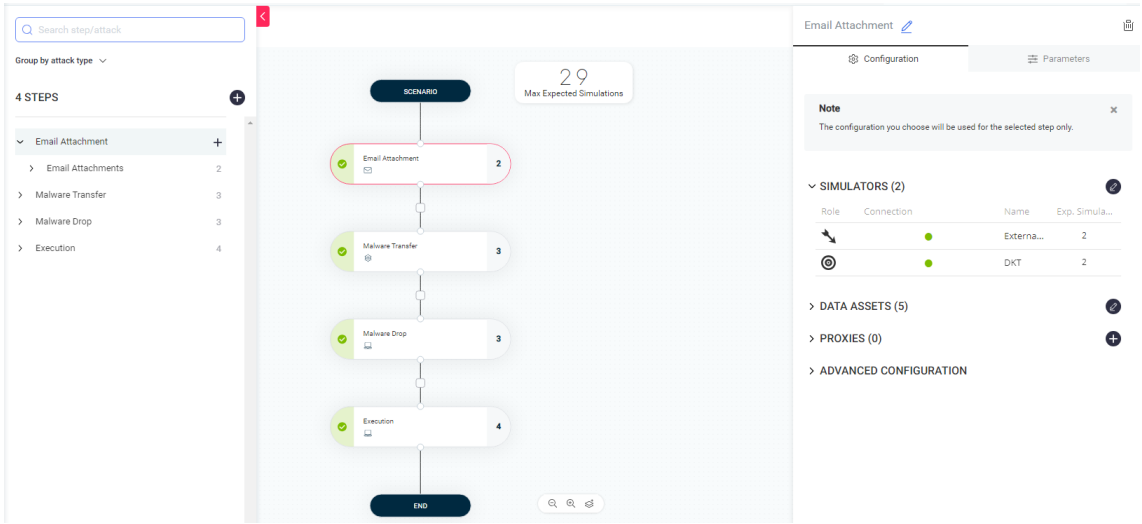


Figura 66: Teste válido para execução

1. Email Attachment - Avalia os controlos de segurança de e-mail mencionados anteriormente, Anubis e Trend SMEX;
2. Malware Transfer - Este passo avalia a resposta das *firewalls*, tanto a perimétrica como a interna;
3. Malware Drop - Para este passo o controlo de segurança a ser avaliado é o EPP;
4. Execution - O último passo está a avaliar o comportamento do EDR;

Este teste é uma forma valiosa de avaliar a eficácia dos vários controlos de segurança em relação ao *ransomware* Locky. Os resultados do teste são depois usados para recomendar ações de melhoria na segurança corporativa, com o objetivo de mitigar e, por consequência, prevenir de forma proativa qualquer ataque com a utilização deste *ransomware*.

3.7.4.3 *Threat Intelligence*

A *Threat Intelligence* é uma das funcionalidades fornecidas pela ferramenta da SafeBreach, representada na figura 67.

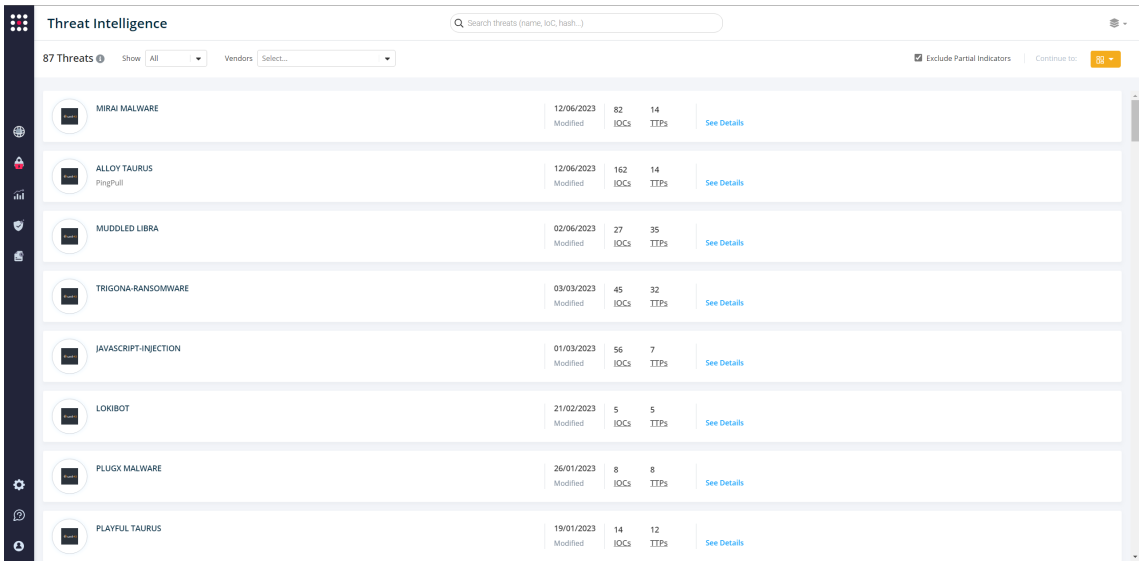


Figura 67: Funcionalidade de *Threat Intelligence*

A *Threat Intelligence* é constituída por dados recolhidos, processados e analisados de modo a compreender os motivos, os alvos e os comportamentos de um determinado ataque. Estes dados são cruciais para adaptar proativamente os controlos de segurança e evitar futuros ataques. Permite tomar decisões de segurança mais rápidas, mais informadas e baseadas em dados concretos, com o objetivo de mudar

a postura de reativo para proativo, na luta contra as ameaças emergentes (*What is Cyber Threat Intelligence? [Beginner's Guide]* 2023).

Atualmente a SafeBreach contém 5 fontes de informação para esta funcionalidade, identificadas na figura 68:

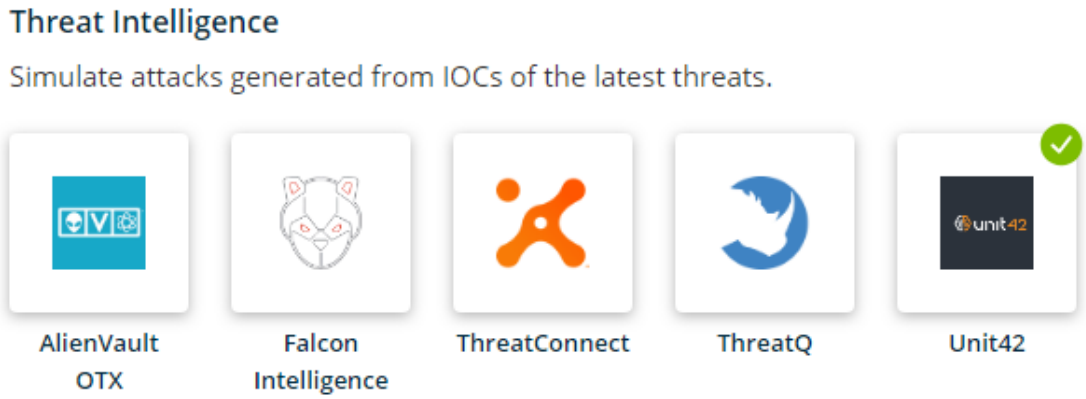


Figura 68: Fontes de *Threat Intelligence*

- AlienVault OTX;
- Falcon Intelligence;
- ThreatConnect;
- ThreatQ;
- Unit42;

Esta ferramenta, por padrão, já inclui a integração com o Unit42, providenciando assim 87 ameaças em constante atualização.

3.7.4.4 *Breach Studio*

A funcionalidade *Breach Studio*, representada na figura 69, permite o desenvolvimento de metodologias de comprometimento personalizadas.

É possível encontrar na documentação da SafeBreach, amostras em código Python para exfiltração e infiltração (transferência de *malware*). São também apresentados 3 grupos de componentes: gerais, *endpoint* e rede. Cada grupo possui vários componentes que podem ser usados em *scripts* de *breaches* personalizadas. Por fim, é referida a utilização da API SafeBreach que permite aos utilizadores automatizar várias tarefas, sem a necessidade de aceder à consola de gestão SafeBreach.

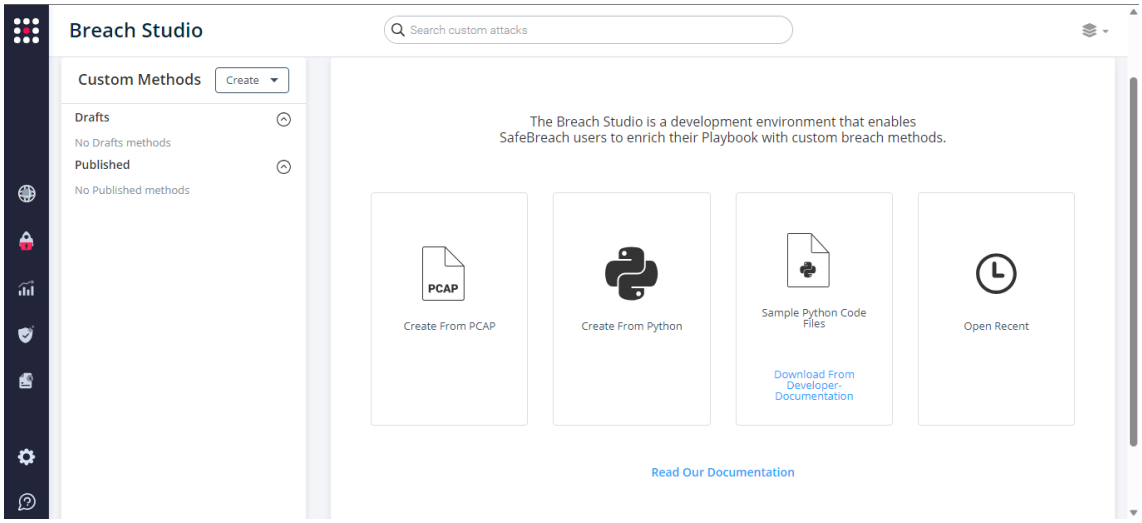


Figura 69: Local de criação de metodologias de comprometimento personalizadas

Esta secção explica e demonstra os principais serviços e *endpoints* da API que podem ser utilizados ao desenvolver integrações com o SafeBreach.

3.7.4.5 *Vulnerability Management*

A funcionalidade de gestão de vulnerabilidades da SafeBreach tem como finalidade priorizar a remediação de vulnerabilidades exploráveis através de *patches*.

Esta funcionalidade é capaz de integrar com as ferramentas topo de mercado, tal como ilustrado na figura 70, permitindo às organizações gerirem de forma eficaz as suas vulnerabilidades e a otimização dos seus recursos de segurança.

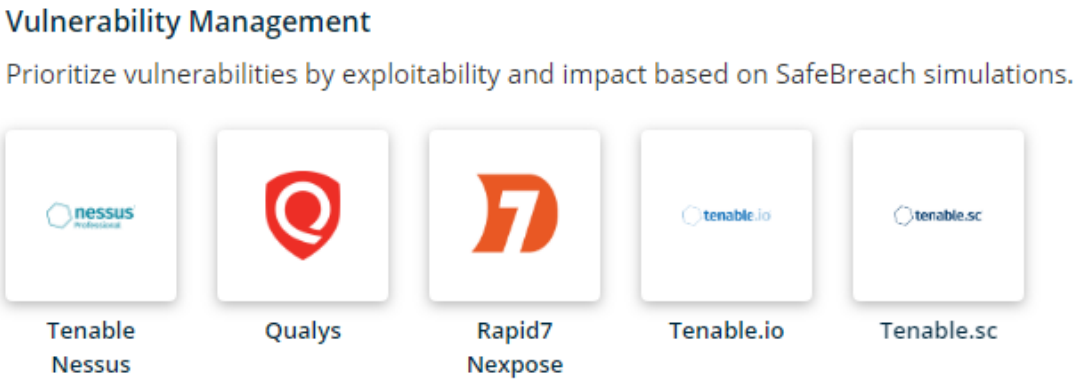


Figura 70: Integração com ferramentas de *Vulnerability Management*

Esta funcionalidade é apoiada por 3 pontos fundamentais:

- Correlação de vulnerabilidades - Correlacionamento dos dados do *scan* de uma ferramenta de gestão de vulnerabilidades e *threat intelligence* com os resultados da simulação de ataques para desenvolver uma compreensão global da superfície de ataque;
- Avaliação de desempenho e priorização - Avaliar os controlos de segurança e identificar quaisquer vulnerabilidades que possam ser exploradas por atacantes. Estas vulnerabilidades devem ser priorizadas com base no seu nível de acessibilidade, probabilidade de exploração e potencial impacto. Por fim, deve-se corrigir essas vulnerabilidades o mais rápido possível para mitigar o risco e reduzir a superfície de ataque;
- Remediar, testar novamente e relatório - Primeiro, é necessário identificar as vulnerabilidades que representam o maior risco para a organização. De seguida, é efetuada a correção dessas vulnerabilidades e realizada novas simulações de ataque para garantir que as correções foram eficazes. Por fim, é fornecido a visibilidade e a informação que os *stakeholders* necessitam para formular planos de segurança a longo prazo, com o auxilio de *dashboards* personalizáveis (*Risk Based Vulnerability Management | SafeBreach* 2023).

Através do painel de controlo apresentado na figura 71 é possível definir a importância para ativos que possuam uma trajetória de ataque a partir de um atacante externo, com os seguintes critérios:

- Criticidade da vulnerabilidade;
- Superfície de ataque;
- Exposição crítica;
- Acesso externo;
- Exposição direta;
- Acesso crítico;

Para cada um destes critérios, podem ser definidas 4 graus de importância:

- Extreme;
- Major;
- Moderate;
- Minimal;

A definição destes critérios irá depender do planeamento definido pelos elementos responsáveis pelas tomadas de decisões.

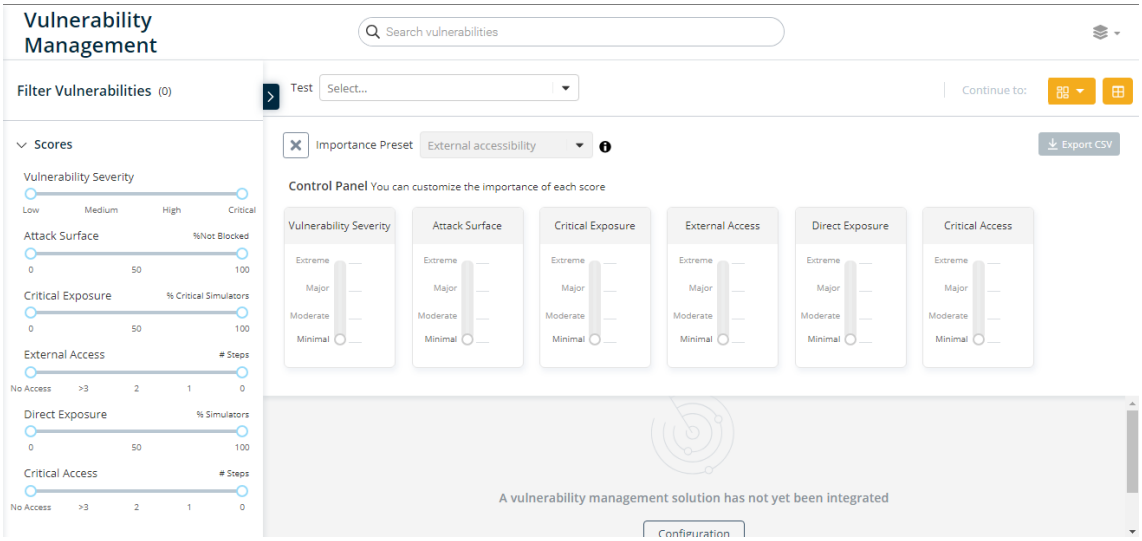


Figura 71: Funcionalidade de priorização de *scans* provenientes de um *Vulnerability Management*

3.7.4.6 *Relatórios e métricas*

De seguida, é descrita a funcionalidade dos relatórios e a avaliação contínua da postura dos controlos de segurança.

A SafeBreach providencia uma variedade de relatórios tendo estes diferentes objetivos:

- Security Risk - Este relatório apresentado na figura 72 é destinado aos executivos de uma organização empresa, por forma a tomarem decisões fundamentadas;

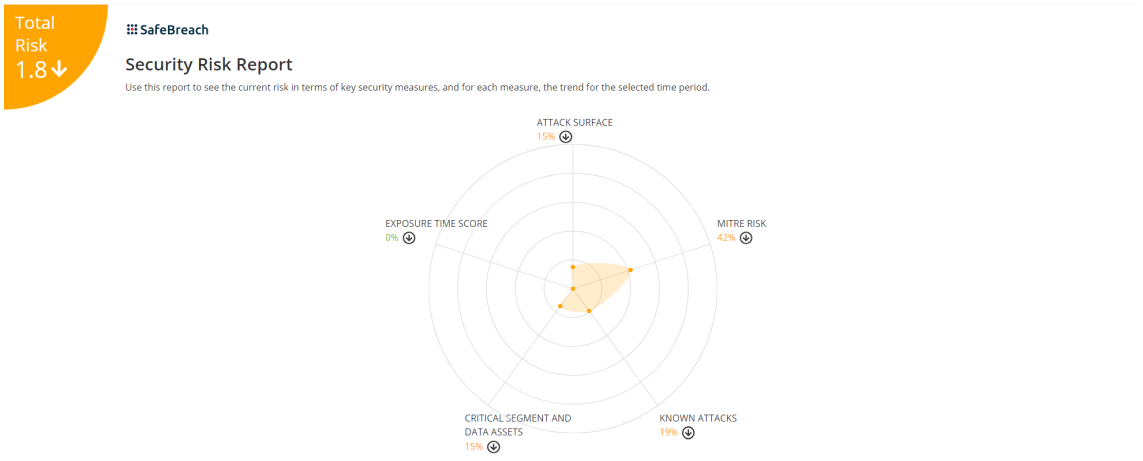


Figura 72: Relatório de risco de segurança

- Mitre ATT&CK Risk - O relatório visível na figura **??** analisa os riscos de segurança cibernética de uma organização com base na *framework* do MITRE ATT&CK, identificando as táticas que são mais suscetíveis de serem exploradas por agentes maliciosos;

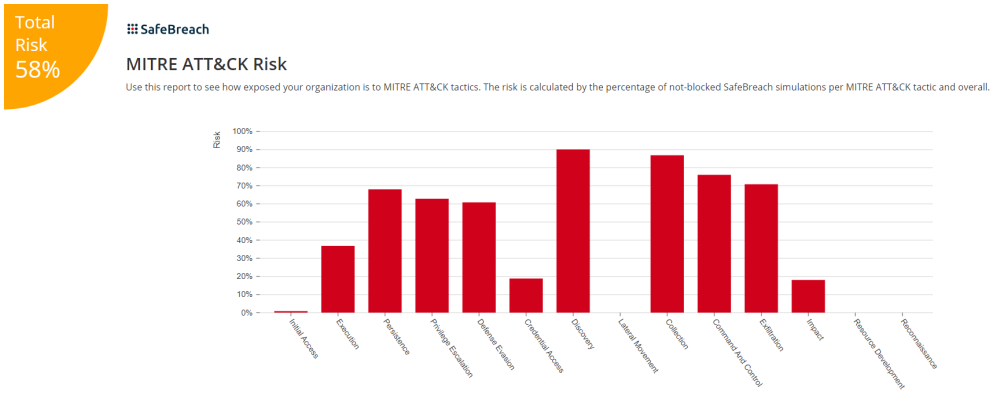


Figura 73: Relatório do risco com base no Mitre ATT&CK

- Security Posture Threat Groups - Assim como o relatório anterior, o relatório presente na figura **??** apresenta as táticas mais suscetíveis de serem exploradas por *threat groups*, além disso, identifica quais desses grupos teriam mais sucesso num ataque à infraestrutura corporativa;

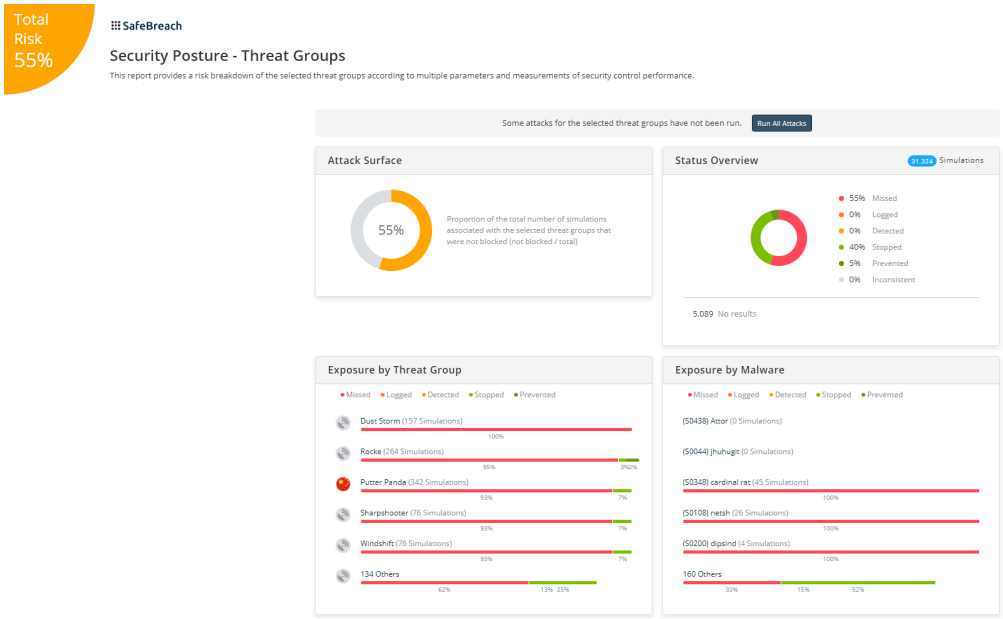


Figura 74: Relatório da postura de segurança contra *Threat Groups*

- Known Threats Series - O relatório observado na figura **??** apresenta dados sobre o risco das diferentes fases de *Threat Series* conhecidas, identificando os controlos de segurança que devem mitigar a ameaça;

!h

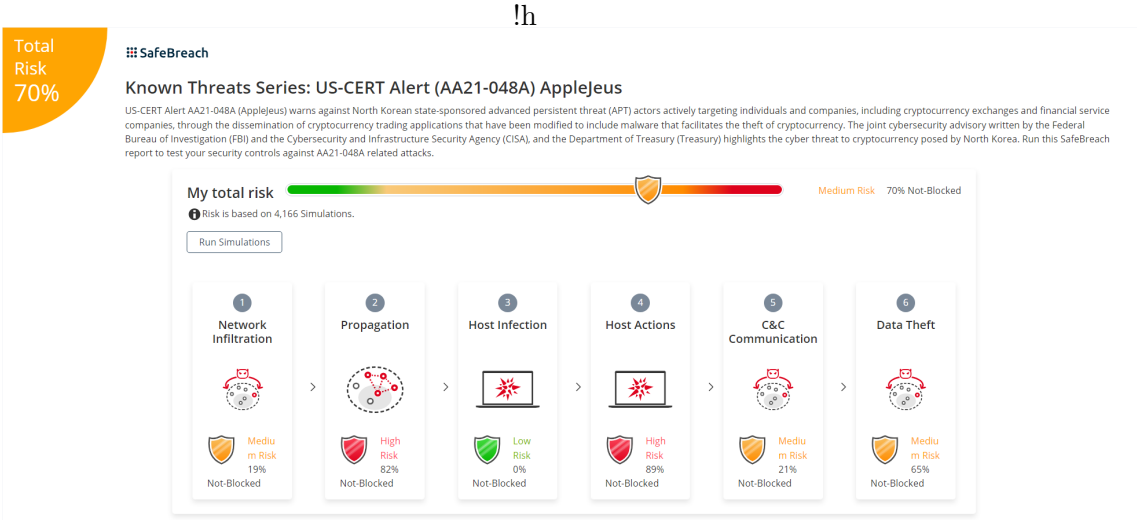


Figura 75: Relatório sobre *threat series* conhecidas

- Insights Summary - Este relatório apresentado na figura 76 é o mais importante numa perspetiva de implementação de mitigações, pois apresenta uma lista de sugestões de remediações. No entanto, importa referir que, em alguns casos, a lista apresenta sugestões por vezes genéricas e não são substanciais de forma a fornecer assistência na mitigação, como podemos observar na figura 77;

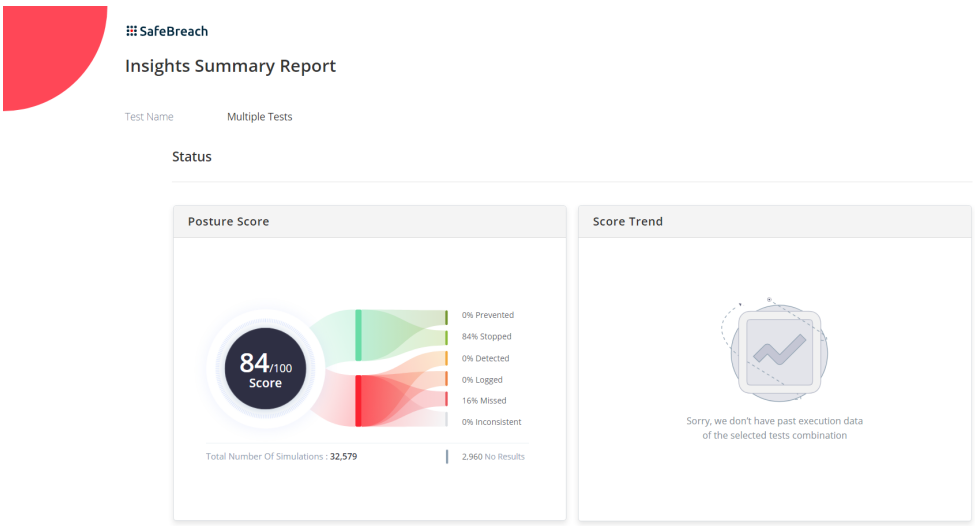


Figura 76: Relatório que contém maior nível de detalhe em relação aos testes

Em suma, a decisão sobre qual o relatório escolher tem, como base, o objetivo que se pretende alcançar.

3.7.4.7 *Dashboards*

A solução da SafeBreach fornece 7 *dashboards* por padrão:

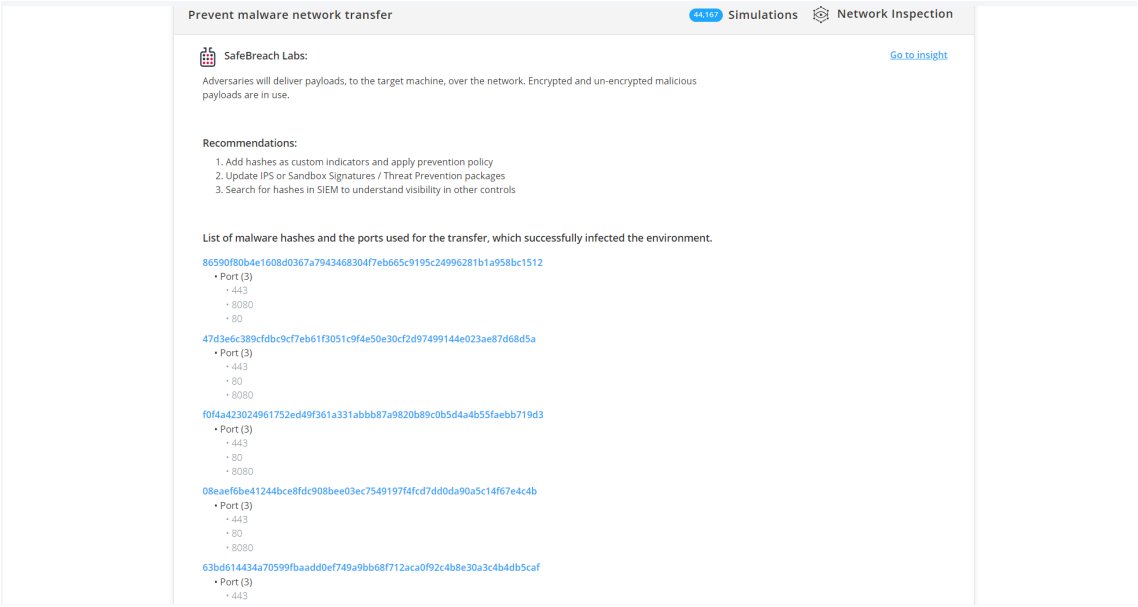


Figura 77: Detalhes relativamente à mitigação a ser implementada

- Security Posture - Apresenta a eficácia controlos de segurança contra grupos cibernéticos com intenções maliciosas, bem como contra as ameaças monitorizadas pelas agências de resposta a emergências de segurança cibernética dos Estados Unidos (US-CERTs);
- Threat Assessment - Demonstra o estado de eficácia dos controlos perante exfiltração, filtração, a nível do *host* e perante a *framework* MITRE;
- Security Control Effectiveness - Evidencia a efetividade das diversas categorias de controlos de segurança e das ferramentas integradas. Além disso, oferece uma visão abrangente do estado global dos controlos de segurança, abrangendo tanto os integrados, como os não integrados;
- Security Test Analysis - Dá ênfase aos ataques que não foram bloqueados por alvo, com o intuito de ser realizada uma análise aprofundada;
- Executive View - Como o próprio nome indica, é para ser utilizada num ambiente executivo de forma a facilitar o entendimento do estado atual da cibersegurança corporativa;
- Impersonated Users Breakdown - Fornece informações acerca da eficácia dos controlos a determinadas ações realizadas por um utilizador específico, no caso de comprometimento das suas credenciais;
- Ransomware Challenge - Demonstra com detalhe dos ataques nas várias fases de um *ransomware*, infiltração, propagação e exfiltração.

Adicionalmente, é viável integrar *dashboards* personalizados para abranger uma variedade de cenários de interesse. Um exemplo disso pode ser encontrado em situações de PoC que envolvam ferramentas de segurança. Nesses casos, tais *dashboards* possibilitariam a monitorização e a avaliação do desempenho das diferentes ferramentas, com o objetivo de identificar aquela que se destaca mais em termos de eficácia nos testes personalizados realizados.

3.7.4.8 *Integração com outras ferramentas de segurança*

Como já tinha sido abordado anteriormente, a ferramenta SafeBreach simula ataques de modo a avaliar visibilidade e a eficácia dos controlos de segurança. Dessa forma, as integrações vão ao encontro desse objetivo, dado que é através delas que se identifica qual a ferramenta que está a detetar e/ou a prevenir as simulações de ataque. Para demonstrar esse efeito, a figura 78 apresenta alguns dados estatísticos.

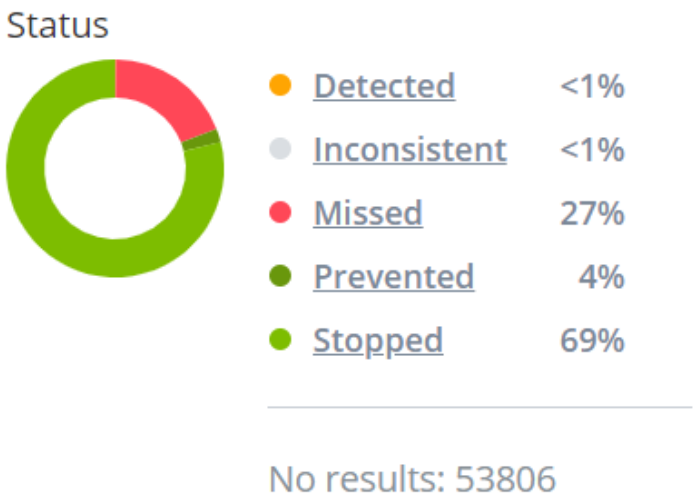


Figura 78: Estado dos resultados das simulações

Através da figura 78, é possível verificar que existem 5 estados diferentes:

- Detected - Detetado por um controlo segurança integrado com a ferramenta da SafeBreach, no entanto, não houve qualquer ação de mitigação durante a simulação;
- Inconsistent - Mitigado, porém a simulação deu como terminado com sucesso;
- Missed - Não foi detetado, nem foi efetuada qualquer ação de mitigação;
- Prevented - Foi mitigado através de um controlo de segurança integrado com a ferramenta da SafeBreach;

- Stopped - Foi mitigado, contudo, não identifica qual o controlo de segurança que realizou a ação de mitigação;
- No Results - Por motivos de requisitos não foi possível efetuar a simulação.

Com base nos dados apresentados na figura 78, é notória uma visibilidade relativamente baixa, abrangendo apenas cerca de 0,5% das simulações totais, o que equivale a 2.690 simulações das 541.254 realizadas até o momento. Porém, a explicação para este fenómeno é simples, dado que a única integração com impacto direto sobre esses dados foi a do Crowdstrike (EDR).

De modo a ser obtida uma maior visibilidade sobre as simulações que são efetuadas, é necessário efetuar integrações, algumas delas visíveis na figura 79, com 2 elementos chave, o SIEM e os controlos de segurança, isto porque os controlos de segurança são quem efetuam as mitigações e deteções, e o SIEM é onde se gere e correlacionam os vários eventos dentro de uma organização.

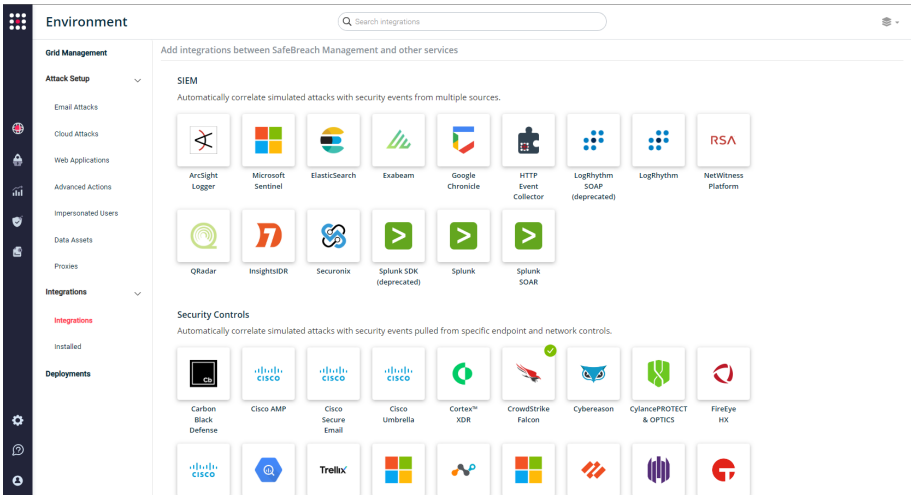


Figura 79: Integrações da ferramenta SafeBreach

No que diz respeito ao SIEM, apesar de estar disponível para integração, não foi possível montar um cenário em que incluísse este tipo de ferramenta de segurança.

Relativamente aos controlos de segurança, era necessário efetuar a integração com a Trend Apex Central, dado que é neste que se encontra a visibilidade central das várias ferramentas da Trend Micro, e a Anubis, que representa a primeira camada defensiva no vetor de e-mail. No entanto, estas integrações não foram efetuadas dado que não estavam disponíveis na plataforma da SafeBreach, como se pode verificar na figura 80.

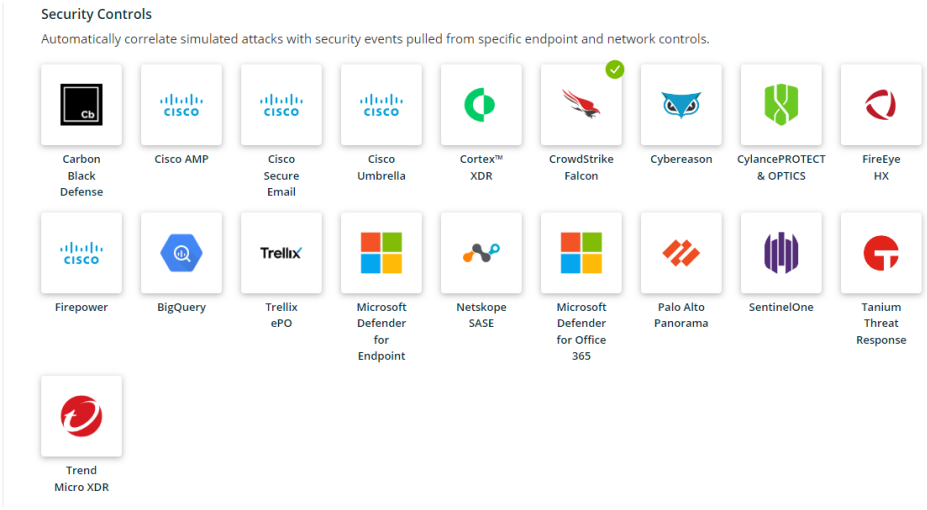


Figura 80: Listagem das integrações com controlos de segurança

Outras integrações possíveis são de:

- WorkFlow and Automation - Receção de notificações sobre eventos do sistema e criação de incidentes para ações de correção automatizadas, na figura **??**, podemos observar os parceiros;

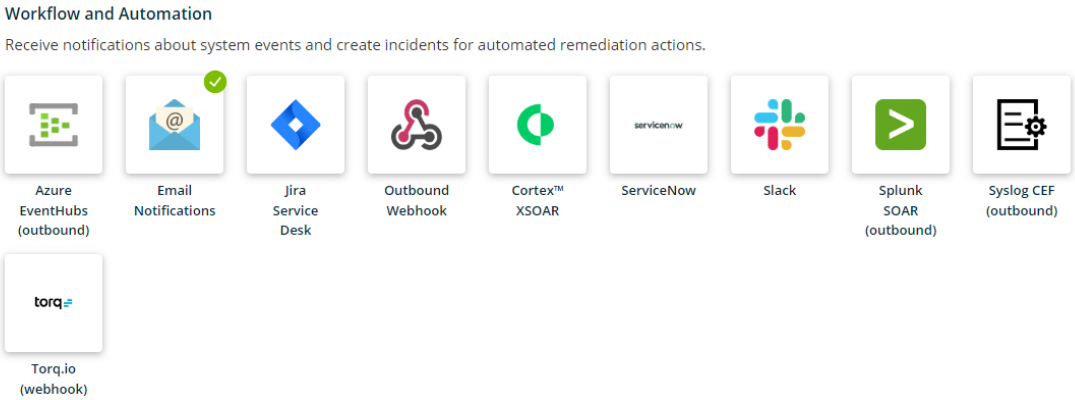


Figura 81: Integração para automatizações de processos

  A integração atualmente ativa dentro deste grupo é a notificação por e-mail. O objetivo destas notificações é informar o término de simulações e um resumo do resultado final das mesmas.

- File Provider - Criação automática de ataques a partir de indicadores de ameaças que envolvam ficheiros maliciosos, na figura 82 verificamos que apenas possui uma opção.

As integrações permitem melhorar o intuito da solução, visto que estas fornecem informação sobre os controlos de segurança que efetuam a mitigação das ameaças

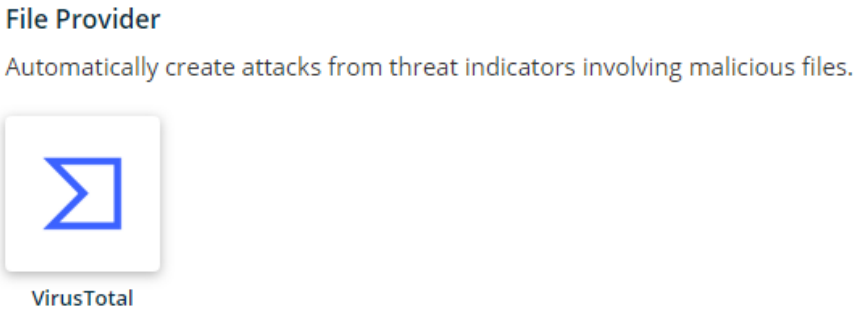


Figura 82: Integração para a criação automática de ataques

e demonstram a visibilidade das mesmas, para além disso, efetua notificações e automatizações.

3.7.5 *Prestação de Suporte*

A prestação de suporte foi realizada nos primeiros meses de implementação da ferramenta no ambiente corporativo e continuou posteriormente. Nesta primeira instância, o suporte envolveu um guia pelas diversas funcionalidades da ferramenta. Mais tarde, tornou-se uma oportunidade para reportar duas falhas identificadas: uma na plataforma, específica na secção dos *dashboards*, e outra relacionada ao agente simulador.

O erro com a *dashboard* originava a partir do momento em que se tentava efetuar a agenda do envio de um determinado relatório em formato PDF. Após configurar as opções necessárias e selecionar "Set"para concluir o processo, uma mensagem de erro era exibida após alguns segundos. O caso foi encaminhado para o suporte técnico e, após cerca de uma semana, o problema foi resolvido.

Quanto à situação do agente de simulação, após atualizar para uma versão mais recente, este inicializava normalmente. Entretanto, em breves momentos, constatou-se que o agente não havia realizado qualquer atualização, e o simulador se desconectava, impossibilitando a reconexão. Inicialmente, tentou-se resolver o problema colocando novas imagens corporativas nos dispositivos em questão, considerando a possibilidade de interferência de alguma das diversas simulações no sistema. No entanto, após essa solução, o comportamento repetiu-se.

Foi decidido aguardar o lançamento de uma nova versão do agente, porém, essa tentativa não foi bem-sucedida, e o problema persistiu. Como medida subsequente, foi necessário desinstalar e reinstalar a SafeBreach no dispositivo afetado, mas entretanto, mais uma vez, não foi possível resolver o problema.

Dado esse cenário, foi realizado contacto com o suporte técnico, que sugeriu repetir a última operação descrita anteriormente. Até o momento, o problema não voltou a suceder e o agente de simulação está a operar normalmente.

3.8 APRESENTAÇÃO DE RESULTADOS

A tabela 4 mostra a pontuação de cada uma das soluções analisadas, são usados os fatores mencionados na secção 3.5, os valores contidos na mesma, são um reflexo dos resultados que serão aqui descritos.

Iniciando pela instalação das ferramentas, ambas revelaram-se intuitivas e de fácil configuração. No entanto, a instalação da SafeBreach foi mais rápida do que a da Cymulate.

Os resultados da avaliação inicial revelaram que o controlo de segurança de rede alcançou uma eficácia de 65 em 100 por parte da SafeBreach, enquanto a Cymulate obteve uma eficácia de 45 em 100.

No que diz respeito ao controlo de segurança de *endpoint*, a SafeBreach demonstrou uma eficácia de 85 em 100, enquanto a Cymulate obteve uma pontuação ligeiramente superior, com uma eficácia de 90 em 100.

No controlo de segurança de e-mail, a SafeBreach obteve uma eficácia quase de excelência de 98 em 100, enquanto a Cymulate alcançou uma eficácia de 68 em 100.

Quanto aos resultados da personalização de cenários, observou-se que a Cymulate permite apenas a personalização por vetor, enquanto a SafeBreach oferece a flexibilidade de personalização de cenários, com a criação com conjuntos de vetores.

No âmbito da análise detalhada das simulações, a SafeBreach sobressaiu em comparação com a Cymulate, uma vez que detalha o processo da simulação desde o seu início até à conclusão da execução. Esta abordagem permite uma análise técnica mais aprofundada, tornando mais simples a implementação de medidas de mitigação. É relevante salientar que as medidas oferecidas por ambas as ferramentas possuem um caráter genérico, o que significa que não oferecem um suporte relevante no processo de mitigação.

A *threat intelligence* oferecida pela Cymulate destaca-se em relação à SafeBreach, devido à sua ampla variedade de fontes de informações, expandindo a sua capacidade de recolha, análise e publicação de simulações de ameaças. Enquanto a SafeBreach se restringe à integração padrão da Unit42 e a outras fontes externas que podem ser adicionadas posteriormente. A simulação de APTs está integrada no cenário de

Immediate threats da Cymulate, ao contrário da SafeBreach, onde está integrado no cenário de "*Threat Groups*".

No que diz respeito aos relatórios e métricas, ambos oferecem um conjunto abrangente de opções, adequadas ao que se pretende. No entanto, é importante destacar que a Cymulate permite a personalização dos relatórios, o que a distingue nesse aspeto.

No que toca aos *dashboards*, ambas as ferramentas proporcionam uma ampla gama de opções que se adequam às necessidades particulares, com a flexibilidade adicional da personalização dos mesmos.

Na *framework* Mitre ATT&CK, um ponto a destacar na solução da Cymulate é a sua capacidade de exibir as subtécnicas utilizadas, uma funcionalidade que não está presente na solução da SafeBreach.

A integração com outras ferramentas em ambas as soluções são equiparáveis, assim como a prestação de suporte e a regularidade das atualizações das suas plataformas.

Funcionalidade	**Cymulate**	**SafeBreach**
Vetor de ataque Endpoint	4	5
Vetor de ataque Web Browsing	4	5
Vetor de ataque Email	4	5
Construção de cenários de ataque	2	5
Threat Intelligence e Simulação de APTs	5	4
Risco de segurança	4	3
Categorias de cenários de ataque	3	5
Mapeamento na matriz de mitre	5	4
Medidas de mitigação	3	3
Análise detalhada do ataque	1	5
Reporting	5	4
Atualização da plataforma	5	4
Capacidade de suporte do parceiro	5	5
Total	50	57

Tabela 4: Comparação das ferramentas BAS selecionadas.

4

CONCLUSÕES

No decorrer desta análise comparativa entre duas ferramentas BAS, Cymulate e SafeBreach, foi possível explorar as suas funcionalidades, de modo a efetuar uma avaliação dos pontos fortes e as limitações de ambas as soluções. Sendo a cibersegurança um dos pilares mais críticos para as organizações atualmente, a escolha da ferramenta ideal pode fazer a diferença na capacidade de uma empresa em proteger os seus ativos e dados críticos. Após uma análise abrangente, é possível identificar algumas conclusões-chave que podem orientar a decisão na seleção da ferramenta mais adequada às necessidades de segurança específicas de uma organização.

Numa abordagem à avaliação dos resultados, a SafeBreach demonstrou ser superior nos vetores de ataque dado conter diversos cenários para os diferentes vetores, possuir cenários focados para as várias indústrias, além de fornecer a coleção de ataques mais abrangentes. Esta também permite a criação de cenários personalizados, com os diferentes vetores de ataque integrados, algo que a Cymulate não possui, como foi possível observar no tópico 3.6.4.2. A sua análise das simulações efetuadas são mais detalhadas, fornecendo toda a informação do processo de simulação, permitindo uma análise mais técnica da falha de segurança, como já foi demonstrado anteriormente.

No entanto, a Cymulate é superior ao nível de *Threat Intelligence*, devido ao facto de possuir uma maior coleção de ataques, mais fontes de informação e ser atualizada diariamente. A sua análise através da *framework* da Mitre disponibiliza a possibilidade de ativar a visualização das sub-técnicas de uma forma ampla permitindo uma análise mais detalhada, ao contrário da SafeBreach que necessita de interagir técnica a técnica para visualizar as sub-técnicas. Além disso, esta ferramenta possibilita a personalização de relatórios ao gosto do utilizador ou por necessidades específicas.

Com base nas considerações apresentadas, na minha opinião, embora ambas as ferramentas tenham pontos fortes e limitações, a minha escolha recai sobre a ferramenta SafeBreach, devido aos pontos mencionados anteriormente, que, na minha perspetiva, conseguem compensar as suas desvantagens.

Para trabalhos futuros, uma hipótese passa pela comparação da SafeBreach com outro BAS presente no mercado. Dado que a escolha foi feita a favor da SafeBreach,

seria também extremamente interessante demonstrar esta ferramenta num ambiente corporativo, de modo a comprovar aumento da eficácia dos controlos de segurança, para mitigar qualquer vulnerabilidade existente e justificar os investimentos avultados efetuados pela organização.

BIBLIOGRAFIA

Breach Attack & Simulation: Security Efficacy & BAS | IDC Blog (ago. de 2023). [Online; accessed 17. Aug. 2023]. URL: https://blogs.idc.com/2021/04/29/breach-attack-and-simulation-a-critical-tool-to-test-the-efficacy-of-security-controls.

Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector (ago. de 2023). [Online; accessed 23. Aug. 2023]. URL: https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector.

CNCS (set. de 2022). [Online; accessed 18. Sep. 2023]. URL: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf.

Cobb, Michael (mai. de 2023). «Top breach and attack simulation use cases». Em: *Security*. URL: https://www.techtarget.com/searchsecurity/tip/Top-breach-and-attack-simulation-use-cases.

CVE-2017-8759 : Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely vi (jan. de 2018). [Online; accessed 19. Aug. 2023]. URL: https://www.cvedetails.com/cve/CVE-2017-8759.

Definition of Endpoint Protection Platform (EPP) - Gartner Information Technology Glossary (set. de 2023). [Online; accessed 18. Sep. 2023]. URL: https://www.gartner.com/en/information-technology/glossary/endpoint-protection-platform-epp.

Discover more about SafeBreach (ago. de 2023). [Online; accessed 19. Aug. 2023]. URL: https://www.safebreach.com/about-safebreach.

Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach (jan. de 2022). [Online; accessed 25. Sep. 2023]. URL: https://www.safebreach.com/resources/enhancing-user-experience-with-safebreach-scenarios-and-simplified-navigation.

Enhancing User Experience with SafeBreach Scenarios and Simplified Navigation - SafeBreach (jan. de 2022). [Online; accessed 19. Aug. 2023]. URL: https://www.safebreach.com/resources/enhancing-user-experience-with-safebreach-scenarios-and-simplified-navigation.

Gartner (set. de 2023). *Best Endpoint Detection and Response (EDR) Solutions Reviews 2023 | Gartner Peer Insights*. [Online; accessed 18. Sep. 2023]. URL:

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

How frequently do you run phishing campaigns? | Haekka Blog (ago. de 2023). [Online; accessed 18. Aug. 2023]. URL: https://www.haekka.com/blog/how-frequently-do-you-run-phishing-campaigns.

Inc. (ago. de 2023). *Breach and Attack Simulation (BAS) Tools*. [Online; accessed 18. Aug. 2023]. URL: https://www.gartner.com/reviews/market/breach-and-attack-simulation-bas-tools.

Kunal Sehgal, Nikolaos Thymianis (2023). *Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization*. Packt Publishing. ISBN: 1801072477; 9781801072472.

Lake, Kate (nov. de 2022). «Does BYOD Fit Into a Zero Trust Security Strategy? - JumpCloud». Em: *JumpCloud*. URL: https://jumpcloud.com/blog/byod-zero-trust-security-strategy.

Mailspike, Anubisnetworks | (set. de 2023). *EMAIL SECURITY SERVICE FOR ENTERPRISES*. [Online; accessed 18. Sep. 2023]. URL: https://www.anubisnetworks.com/email-protection-service-for-enterprises.

Moshe, Tal (nov. de 2021a). «Email Gateway». Em: *Cymulate*. URL: https://cymulate.com/email-gateway.

— (nov. de 2021b). «Web Gateway». Em: *Cymulate*. URL: https://cymulate.com/web-gateway.

— (abr. de 2022a). «Data Exfiltration». Em: *Cymulate*. URL: https://cymulate.com/data-exfiltration.

— (abr. de 2022b). «Endpoint Security». Em: *Cymulate*. URL: https://cymulate.com/endpoint-security.

— (abr. de 2022c). «SafeBreach vs Cymulate». Em: *Cymulate*. URL: https://cymulate.com/blog/safebreach-vs-cymulate.

— (ago. de 2023a). «About us - Learn about Cymulate». Em: *Cymulate*. URL: https://cymulate.com/about-us.

— (mai. de 2023b). «Drift Detection & xn–Control-6z6c – Minimize Risk». Em: *Cymulate*. URL: https://cymulate.com/drift-detection.

— (jun. de 2023c). «Technology Alliances». Em: *Cymulate*. URL: https://cymulate.com/technology-alliances.

— (jul. de 2023d). «What is Breach and Attack Simulation?» Em: *Cymulate*. URL: https://cymulate.com/breach-and-attack-simulation.

— (jul. de 2023e). «What is Breach and Attack Simulation?» Em: *Cymulate*. URL: https://cymulate.com/breach-and-attack-simulation.

— (jul. de 2023f). «What is Breach and Attack Simulation?» Em: *Cymulate*. URL: https://cymulate.com/breach-and-attack-simulation.

Risk Based Vulnerability Management | SafeBreach (ago. de 2023). [Online; accessed 18. Aug. 2023]. URL: https://www.safebreach.com/risk-based-vulnerability-management.

Scanmail for Exchange (set. de 2023). [Online; accessed 18. Sep. 2023]. URL: https://www.trendmicro.com/pt_br/business/products/user-protection/sps/email-and-collaboration/scanmail-for-exchange.html.

Techniques - Enterprise | MITRE ATT&CK® (ago. de 2023). [Online; accessed 19. Aug. 2023]. URL: https://attack.mitre.org/techniques/enterprise.

Timonera, Kaye (fev. de 2023). «Red Team vs Blue Team vs Purple Team: Differences Explained». Em: *eSecurity Planet*. URL: https://www.esecurityplanet.com/networks/red-team-vs-blue-team-vs-purple-team.

What is Attack Surface Management ? (Set. de 2023). [Online; accessed 20. Sep. 2023]. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-attack-surface-management.

What is Cyber Threat Intelligence? [Beginner's Guide] (ago. de 2023). [Online; accessed 18. Aug. 2023]. URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence.

What Is MITRE ATT CK - Definition | VMware Glossary (nov. de 2022). [Online; accessed 19. Aug. 2023]. URL: https://www.vmware.com/br/topics/glossary/content/mitre-attack.html.

What is the MITRE ATT&CK Framework? (Ago. de 2023). [Online; accessed 19. Aug. 2023]. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework.

APÊNDICES

A

APÊNDICE A

```
2023-06-29 04:35:13.602 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 347: Starting new task action, timeout=29.962025316455694 (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:13.615 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 366: Generated tempdir for simulation: 'C:\WINDOWS\TEMP\sb-sim-temp-lsv_pnfw\sb_504269_bs_iirdlt0q' (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:14.172 - INFO     7504: safebreach_simulator.running.run_manager_utils - run_manager_utils.py: 290: Copied executable path: C:\Program Files\SafeBreach\SafeBreach Endpoint Simulator\app\currentVersion\simulation\sbsimulation_sb_504269_bs_475876.exe (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:14.173 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 1218: Running task executable '['C:\\Program Files\\SafeBreach\\SafeBreach Endpoint Simulator\\app\\currentVersion\\simulation\\sbsimulation_sb_504269_bs_475876.exe', 'sb_504269_bs']' (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:17.740 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 1229: Process was started PID=20708 (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:17.745 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 413: Creating process tree (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:17.769 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 1240: Sent args over communication pipe (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:17.771 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 456: Finished run action flow (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:17.774 - INFO     7504: safebreach_simulator.running.run_manager - run_manager.py: 630: Waiting for task action to finish for '60' seconds (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:22.668 - INFO     20708: safebreach_simulation.simulation - simulation.py: 228: Running task action (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:24.017 - INFO     20708: safebreach_simulation.task_action_runner - task_action_runner.py: 191: Running action TASK_ACTION_ID=417968697090428323 (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:24.020 - WARNING 7504: safebreach_simulator.running.run_manager - run_manager.py: 826: Simulation started after '6' seconds (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)

2023-06-29 04:35:24.020 - INFO     20708: safebreach_simulation.task_action_runner - task_action_runner.py: 83: Running pythonect string as 'NT AUTHORITY\SYSTEM' (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
```

```
26
27 2023-06-29 04:35:24.024 - INFO     7504: safebreach_simulator.running.run_manager -
     run_manager.py: 630: Waiting for task action to finish for '39.962025316455694'
     seconds (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID
     =113, ACCOUNT_ID=##########)
28
29 2023-06-29 04:35:24.054 - DEBUG    20708: simulation-steps - __init__.py: 172: enter
     framework.filters.codec.base64_decode: {'id': '33861d85-3ece-444b-9cf3-ccb518cc88d8
     ', 'operation': 'enter', 'level': '0', 'component': '
     framework.filters.codec.base64_decode', 'status': 'None'} (JOB_ID=504269, TASK_ID
     =475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
30
31 2023-06-29 04:35:24.057 - DEBUG    20708: simulation-steps - __init__.py: 172: leave
     framework.filters.codec.base64_decode: {'id': '33861d85-3ece-444b-9cf3-ccb518cc88d8
     ', 'operation': 'leave', 'level': '0', 'component': '
     framework.filters.codec.base64_decode', 'status': 'success'} (JOB_ID=504269, TASK_ID
     =475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
32
33 2023-06-29 04:35:24.061 - DEBUG    20708: simulation-steps - __init__.py: 172: enter
     framework.filters.codec.hex_encode: {'id': '6d48da58-8a36-46a5-9d11-553ec7e73387', '
     operation': 'enter', 'level': '0', 'component': 'framework.filters.codec.hex_encode
     ', 'status': 'None'} (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
     =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
34
35 2023-06-29 04:35:24.064 - DEBUG    20708: simulation-steps - __init__.py: 172: leave
     framework.filters.codec.hex_encode: {'id': '6d48da58-8a36-46a5-9d11-553ec7e73387', '
     operation': 'leave', 'level': '0', 'component': 'framework.filters.codec.hex_encode
     ', 'status': 'success'} (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
     =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
36
37 2023-06-29 04:35:24.101 - DEBUG    20708: simulation-steps - __init__.py: 172: enter
     framework.network.irc.client.send_data: {'id': 'ffb47e0f-94eb-402c-99bf-8945839f63b3
     ', 'operation': 'enter', 'level': '0', 'component': '
     framework.network.irc.client.send_data', 'status': 'None'} (JOB_ID=504269, TASK_ID
     =475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
38
39 2023-06-29 04:35:24.103 - DEBUG    20708: simulation-steps - __init__.py: 591: Waiting for
      event: {'subject': 'EVENT_Default'} (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
     =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
40
41 2023-06-29 04:35:24.106 - DEBUG    20708: simulation-steps - __init__.py: 594: Done
     waiting for event: {'subject': 'EVENT_Default'} (JOB_ID=504269, TASK_ID=475876,
     TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
42
43 2023-06-29 04:35:24.112 - INFO     20708: simulation-steps - socket_wrapper.py: 161:
     Connect socket: {'address': "('mcifp01cloudsim01.safebreach.net', 80)"} (JOB_ID
     =504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID
     =##########)
44
45 2023-06-29 04:35:24.160 - INFO     20708: simulation-steps - client.py: 105: Client
     started: {'protocol': 'IRC', 'host_name': 'mcifp01cloudsim01.safebreach.net', 'port
     ': '80'} (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID
     =113, ACCOUNT_ID=##########)
46
47 2023-06-29 04:35:52.637 - INFO     20708: safebreach_simulation.simulation - simulation.py
     : 177: Reached timeout TIMEOUT=29.962025316455694 (JOB_ID=504269, TASK_ID=475876,
     TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
48
49 2023-06-29 04:36:03.997 - WARNING 7504: safebreach_simulator.running.run_manager -
     run_manager.py: 659: Task process has not finished in the given time timeout=39 (
     JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113,
     ACCOUNT_ID=##########)
50
51 2023-06-29 04:36:03.999 - WARNING 7504: safebreach_simulator.running.run_manager -
     run_manager.py: 669: Simulation timed out after '39' seconds (JOB_ID=504269, TASK_ID
     =475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
52
53 2023-06-29 04:36:04.001 - INFO     7504: safebreach_simulator.running.run_manager -
     run_manager.py: 511: Stopping task action (code=TIMEOUT), details: Task action timed
      out after 39/30 seconds (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
     =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
54
```

```
55 2023-06-29 04:36:04.003 - INFO     7504: safebreach_simulator.running.run_manager -
       run_manager.py: 986: Handling task action finish RESULT_TYPE: FAILURE, RESULT_CODE:
       TIMEOUT (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID
       =113, ACCOUNT_ID=##########)
56
57 2023-06-29 04:36:04.543 - INFO     7504: safebreach_simulator.running.run_manager -
       run_manager.py: 1188: Task process has finished with code 1 (JOB_ID=504269, TASK_ID
       =475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
58
59 2023-06-29 04:36:04.557 - INFO     7504: safebreach_simulator.running.run_manager -
       run_manager.py: 1258: Task executable copy deleted: C:\Program Files\SafeBreach\
       SafeBreach Endpoint Simulator\app\currentVersion\simulation\
       sbsimulation_sb_504269_bs_475876.exe (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
       =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
60
61 2023-06-29 04:36:04.558 - INFO     7504:
       safebreach_simulator.storage.post_actions.PostActionsManager - post_actions.py: 151:
        Running post actions with (JOB_ID=504269, TASK_ID=475876, CLEANUP_TIME=None) (
       JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113,
       ACCOUNT_ID=##########)
62
63 2023-06-29 04:36:04.560 - INFO     7504:
       safebreach_simulator.storage.post_actions.PostActionsManager - post_actions.py: 164:
        Found '0' post actions to run (JOB_ID=504269, TASK_ID=475876, TASK_ACTION_ID
       =417968697090428323, MOVE_ID=113, ACCOUNT_ID=##########)
64
65 2023-06-29 04:36:04.561 - INFO     7504:
       safebreach_simulator.storage.post_actions.PostActionsManager - post_actions.py: 177:
        Finished running post actions (JOB_ID=504269, TASK_ID=475876) (JOB_ID=504269,
       TASK_ID=475876, TASK_ACTION_ID=417968697090428323, MOVE_ID=113, ACCOUNT_ID
       =##########)
```

D E C L A R A Ç Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Avaliação de ferramentas de Breach and Attack Simulation"*, é original e foi realizado por Estudante Ricardo Jorge Aguiar Pêgo (2212982) sob orientação de Professor Carlos Jorge Machado Antunes (carlos.machado@ipleiria.pt).

Leiria, setembro de 2023

Assinado por: **RICARDO JORGE AGUIAR PÊGO**
Num. de Identificação: BI15373536
Data: 2023.12.12 23.38.59 GMT Standard Time

CHAVE MÓVEL

Estudante Ricardo Jorge Aguiar Pêgo