AÉGIS DEFENDER

POWERED BY AVALON TECH

SÃO PAULO – SP

SUMÁRIO

1. INTRODUÇÃO AO AÉGIS DEFENDER

Nos tempos atuais, o cenário de ameaças cibernéticas não para de crescer. Com a expansão dos dispositivos conectados e a integração digital em muitos aspectos de nossas vidas, a segurança tem se apresentado como uma preocupação central. Dentre as diversas ameaças que se destacam, o ransomware é especialmente preocupante. Este tipo de malware, que criptografa os dados do usuário e exige um resgate para sua recuperação, tem causado danos significativos globalmente.

Nesse contexto, apresentamos o Aégis Defender, uma proposta emergente no mundo das ferramentas de Endpoint Detection and Response (EDR), com um enfoque particular na proteção contra ransomwares. Desenvolvido principalmente para o ambiente Windows e com base na versátil linguagem de programação Python, o Aégis Defender integra técnicas promissoras, incluindo aprendizado de máquina e monitoramento em tempo real através do WMI (Windows Management Instrumentation).

O objetivo deste documento é introduzir o Aégis Defender, discutindo suas funcionalidades, pré-requisitos e tecnologias envolvidas, bem como fornecer diretrizes para instalação e uso. É importante salientar que, embora o Aégis Defender apresente qualidades promissoras, reconhecemos que estamos em uma jornada contínua de aprendizado e aprimoramento. Assim, a contribuição da comunidade e de outros stakeholders é fundamental para o progresso deste projeto.

2. CARACTERÍSTICAS PRINCIPAIS DO AÉGIS DEFENDER

À medida que mergulhamos no universo do Aégis Defender, torna-se imperativo entender as características que o diferenciam e o tornam uma ferramenta relevante no combate a ransomwares e outras ameaças cibernéticas. Abaixo, listamos as principais características que definem e moldam sua eficácia:

1. **Enfoque na Detecção em Tempo Real:** Usando o Windows Management Instrumentation (WMI), o Aégis Defender monitora constantemente as atividades no sistema em busca de padrões suspeitos ou atividades que indicam a presença de ransomware, garantindo uma resposta rápida em potenciais situações de comprometimento.

2. **Integração de Aprendizado de Máquina:** O software não depende apenas de assinaturas e regras predefinidas. Utilizando algoritmos de aprendizado de máquina, ele é capaz de adaptar-se a novas ameaças, identificando atividades maliciosas com base em padrões e comportamentos, em vez de apenas assinaturas conhecidas.

3. **Desenvolvimento em Python:** Com uma base em Python, uma das linguagens de programação mais populares e versáteis, o Aégis Defender é altamente customizável. Isso permite atualizações regulares, bem como a possibilidade de integração com outras ferramentas e sistemas.

4. **Módulo de Prevenção Proativa:** Além de detectar ameaças, o Aégis Defender possui um módulo que atua na prevenção, bloqueando automaticamente processos suspeitos e quarentenando arquivos que apresentem risco, minimizando assim o impacto de um possível ataque.

5. **Interface Amigável e Intuitiva:** Com uma interface de usuário claramente estruturada, mesmo aqueles sem um conhecimento profundo em segurança cibernética podem navegar e configurar o software, tornando-o acessível para uma ampla gama de usuários.

6. **Atualizações e Suporte Constantes:** Em um mundo onde as ameaças estão em constante evolução, a capacidade de atualizar e aprimorar regularmente é crucial. O Aégis Defender mantém uma comunicação regular com servidores centrais, recebendo atualizações frequentes para garantir sua relevância contínua. Além disso, uma equipe dedicada está sempre disponível para suporte técnico e orientação.

O **Aégis Defender**, embora promissor em suas funcionalidades, é um projeto em evolução. Acreditamos que o feedback dos usuários e a adaptação contínua são essenciais para atender às crescentes demandas do cenário de segurança cibernética. Estamos comprometidos com essa jornada de aperfeiçoamento, e convidamos a todos para fazer parte deste processo contínuo.

3. PRÉ-REQUISITOS PARA O AÉGIS DEFENDER

Para garantir uma operação suave e eficaz do Aégis Defender, é crucial que certos pré-requisitos sejam atendidos. Estes não só asseguram que o software funcione como o esperado, mas também otimizam a experiência do usuário. Abaixo, detalhamos os principais pré-requisitos para a implementação e uso do Aégis Defender:

1. **Sistema Operacional Compatível:** O Aégis Defender foi projetado para funcionar principalmente em sistemas Windows 10. Uma versão compatível com Windows 11 está em desenvolvimento e será lançada em breve.

2. **Espaço em Disco:** É recomendado ter pelo menos 1 GB de espaço livre no disco rígido para garantir a instalação adequada e a operação do programa, além de espaço adicional para quarentenas e logs.

3. **Memória RAM:** Uma memória RAM mínima de 2 GB é aconselhada para uma performance otimizada. Contudo, 4 GB ou mais é ideal para sistemas que executam várias tarefas simultaneamente.

4. **Conexão com a Internet**: Uma conexão estável e segura é necessária para atualizações regulares, comunicação com os servidores centrais e, se necessário, suporte técnico remoto.

5. **Privilégios de Administrador**: Para a instalação e operação adequadas, é essencial que o usuário tenha direitos de administrador no sistema. Isso garante que o software tenha acesso completo para monitorar, detectar e agir contra ameaças.

6. **Software de Suporte**: Ter um software de firewall ativo e atualizado pode complementar as funcionalidades do Aégis Defender, oferecendo uma camada adicional de segurança.

7. **Política de Backup**: Enquanto o Aégis Defender atua proativamente contra ransomwares, sempre é prudente ter uma política regular de backup de dados. Isso serve como uma rede de segurança em caso de qualquer comprometimento inesperado.

Com esses pré-requisitos em mente, os usuários podem esperar uma interação sem problemas e uma proteção robusta contra ransomwares e outras ameaças cibernéticas. No entanto, é importante lembrar que a segurança cibernética é um esforço contínuo e a conscientização e educação dos usuários são tão vitais quanto as soluções tecnológicas em si.

4. TECNOLOGIAS UTILIZADAS NO AÉGIS DEFENDER

No decorrer do desenvolvimento do projeto "Aégis Defender", a busca contínua pela excelência norteou a seleção e integração de tecnologias avançadas e reconhecidas no campo da cibersegurança. Mesmo com um alicerce sólido, o projeto reconhece a natureza evolutiva da tecnologia e, consequentemente, do Aégis como um produto em constante aperfeiçoamento. Este capítulo oferece uma visão detalhada das tecnologias atualmente incorporadas, sublinhando suas funcionalidades e a motivação para sua inclusão.

4.1 SISTEMA OPERACIONAL

4.1.1 WINDOWS 10

O Windows 10, sendo uma plataforma amplamente adotada no mercado, apresenta-se como a base ideal para o Aégis Defender. As características intrínsecas e APIs deste sistema operacional permitem ao Aégis operar com eficácia e otimização, preparando-o para futuras integrações e melhorias.

4.2 LINGUAGEM DE PROGRAMAÇÃO

4.2.1 PYTHON

A escolha do Python, uma linguagem de alto nível, está fundamentada em sua clareza sintática, legibilidade e vasto ecossistema. Sua adaptabilidade promove facilidade em futuras atualizações e evoluções do Aégis Defender.

4.3 BIBLIOTECAS E PACOTES

4.3.1 BIBLIOTECAS DE INTERAÇÃO COM O SISTEMA: `OS`, `CTYPES`, E `SYS`

Essas ferramentas proporcionam acesso direto às funcionalidades primárias do Windows, tornando possível ao Aégis Defender responder com prontidão às variadas situações emergentes.

4.3.2 INTERFACE DO USUÁRIO: `TKINTER.MESSAGEBOX`

A comunicação eficaz entre o sistema e o usuário é garantida pelo uso de `tkinter.messagebox`, que facilita a apresentação de diálogos e notificações claras.

4.3.3 MONITORAMENTO: `PSUTIL` E `WMI`

`psutil` e `wmi` são vitais para o monitoramento em tempo real das atividades do sistema, assegurando uma identificação atempada e eficaz de comportamentos atípicos.

4.3.4 APRENDIZADO DE MÁQUINA: `SKLEARN`

`sklearn` posiciona o Aégis Defender na vanguarda da detecção de ameaças, permitindo uma resposta adaptativa a novos padrões de ameaças, refletindo a natureza evolutiva do projeto.

4.3.5 GERENCIAMENTO DE DADOS: `JSON`

A escolha pelo formato JSON, facilitada pela biblioteca `json`, prioriza a eficiência e a agilidade na gestão de dados estruturados.

4.4 FRAMEWORKS E APIS

4.4.1 FRAMEWORK WEB: `FLASK`

A interface amigável proporcionada pelo `Flask` reflete o compromisso do projeto em garantir uma experiência do usuário intuitiva e otimizada.

4.4.2 PADRÕES DE SEGURANÇA: MITRE ATT&CK

A adoção do padrão MITRE ATT&CK destaca a orientação do Aégis Defender para alinhar-se às melhores práticas e táticas no domínio da cibersegurança.

4.4.3 INTEGRAÇÕES EXTERNAS: GOOGLE APIS

As APIs do Google permitem que o Aégis Defender expanda suas funcionalidades, reforçando o caráter evolutivo e adaptativo do projeto.

A integração dessas tecnologias exemplifica o empenho do projeto em oferecer um produto de cibersegurança de ponta. Contudo, o Aégis Defender reconhece sua trajetória como uma jornada contínua de aprendizado e inovação.

5. DIRETRIZES DE INSTALAÇÃO DO AÉGIS DEFENDER

A integração bem-sucedida de qualquer aplicativo em um sistema é uma etapa crucial, exigindo diretrizes claras e concisas. O projeto Aégis Defender, mesmo que em um estágio contínuo de desenvolvimento e aperfeiçoamento, visa simplificar tal processo para seus usuários. Abaixo, são apresentados os passos recomendados para uma instalação adequada:

5.1 ACESSO AO PORTAL OFICIAL PARA DOWNLOAD

Reforçamos a importância de obter o software diretamente de sua fonte oficial para garantir sua integridade e autenticidade.

5.1.1 NAVEGAÇÃO ATÉ O WEBSITE

Endereço Eletrônico: O usuário deve acessar Aégis Defender. Esta página foi desenvolvida priorizando uma interface amigável e compatibilidade universal com as versões mais recentes dos navegadores.

5.1.2 IDENTIFICAÇÃO DO LINK PARA DOWNLOAD

Recurso de Download: Na interface principal do site, localiza-se o botão designado para download, usualmente intitulado como "Download" ou "Baixar". A disposição e design do site foram pensados para que tal recurso fosse imediatamente perceptível.

5.1.3 EXECUÇÃO DO DOWNLOAD

Transferência do Arquivo: Ao acionar o botão destinado para download, a transferência do pacote de instalação do software se iniciará. É preciso destacar que a duração deste processo pode variar, dependendo predominantemente da taxa de transmissão da conexão de internet utilizada.

5.1.4 PROCESSO DE INSTALAÇÃO

Diretrizes de Instalação: Uma vez que a transferência do arquivo for finalizada, é essencial que o usuário o localize, execute-o e siga à risca as instruções fornecidas na janela de instalação para garantir a correta configuração do Aégis Defender.

Expressamos nosso sincero agradecimento pela confiança depositada em nosso projeto. Almejamos que sua experiência com o Aégis Defender seja notável e que o software cumpra plenamente suas expectativas.

6. MANUAL DE UTILIZAÇÃO DO AÉGIS DEFENDER

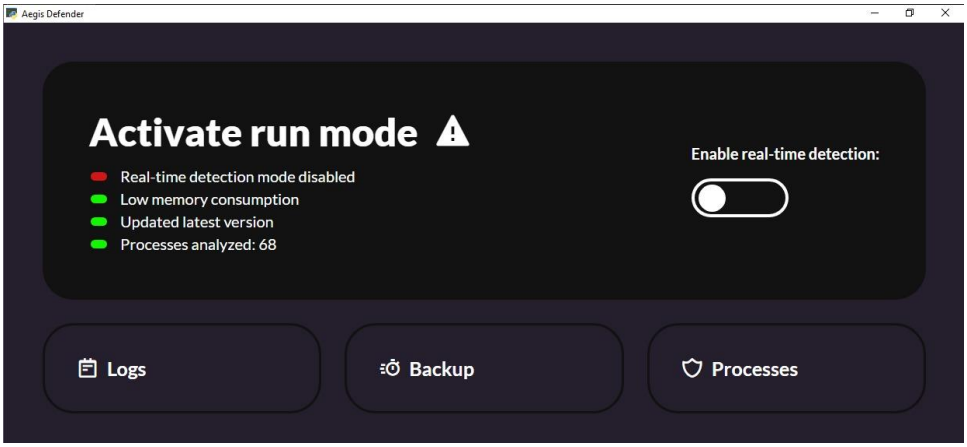
O software Aégis Defender foi projetado com a finalidade de fornecer uma experiência intuitiva para seus usuários, no entanto, como todo software de proteção avançada, é fundamental compreender plenamente suas funcionalidades para maximizar seus benefícios.

6.1 FUNCIONALIDADES DO SOFTWARE

6.1.1 DETECÇÃO EM TEMPO REAL

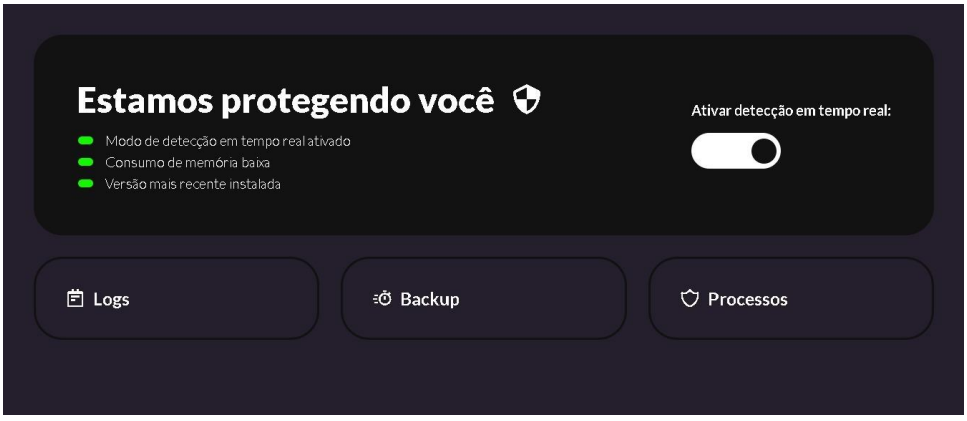
Procedimento: Para acionar esta funcionalidade, após inicializar o programa, localize e selecione o botão designado "Iniciar Detecção em Tempo Real".

Representação gráfica - modo desativado



Descrição: Esta funcionalidade permite ao Aégis Defender monitorar e identificar, em tempo real, qualquer irregularidade ou ameaça potencial, proporcionando uma camada adicional de proteção para seu sistema.

Representação gráfica - modo ativado



Recomendação: Para garantir uma defesa proativa e contínua contra ameaças cibernéticas, sugere-se manter essa funcionalidade sempre ativa.

6.1.2 REGISTRO DE ATIVIDADES (LOGS)

Status Atual: Esta funcionalidade está em fase de desenvolvimento e será disponibilizada em versões futuras do software.

6.1.3 BACKUP

Status Atual: Esta ferramenta ainda está em processo de desenvolvimento. Ao ser finalizada, proporcionará aos usuários a capacidade de realizar cópias de segurança de seus dados essenciais.

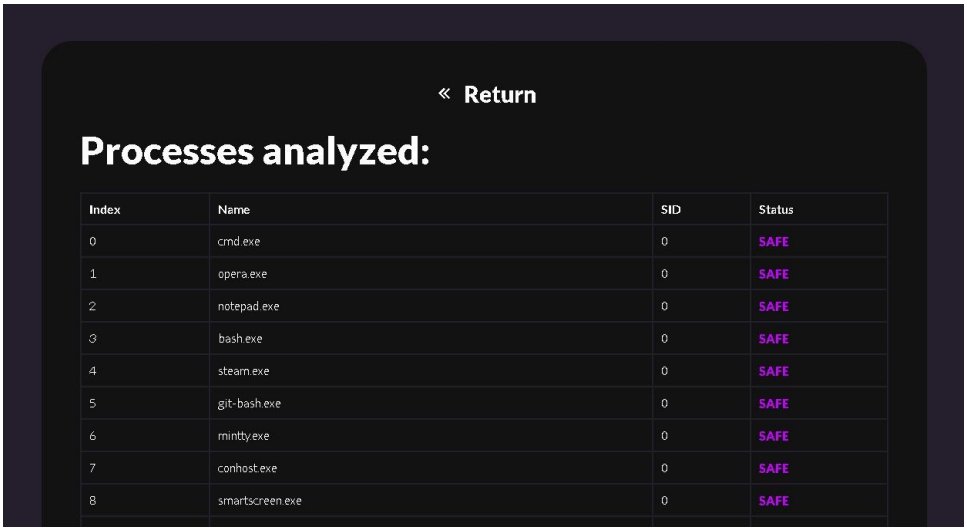
6.1.4 MONITORAMENTO DE PROCESSOS

Procedimento: Para acessar, dirija-se à opção "Processos" no menu principal. Uma lista detalhada dos processos ativos no sistema será apresentada.

Descrição: Este recurso permite a identificação e gestão de todos os processos em curso, oferecendo ao usuário uma visão detalhada do que ocorre em seu sistema.

Orientação: Em caso de identificação de um processo desconhecido ou que desperte suspeitas, é prudente proceder com sua análise ou finalização, visando assegurar a integridade do sistema.

Representação gráfica - processos



7. AVALIAÇÕES E TESTES

O comprometimento do projeto Aégis Defender com a qualidade e eficácia é demonstrado através de sua rigorosa metodologia de testes e avaliações.

7.1 RESISTÊNCIA A RANSOMWARES

Em nossos testes, o Aégis Defender foi submetido a diversos cenários de ataque, inclusive àqueles propiciados pelos ransomwares mais prevalentes no cenário atual, como Wannacry e Jigsaw. A performance destacada frente a tais ameaças endossa a efetividade da solução proposta.

7.2 CONTINUIDADE NA AVALIAÇÃO DE SEGURANÇA

O Aégis Defender não é apenas submetido a testes pontuais. Há um compromisso contínuo com a avaliação de sua performance, garantindo que, a cada atualização, o software mantenha-se atualizado frente às ameaças emergentes.

7.3 COMPROMETIMENTO COM A EXCELÊNCIA

A equipe por trás do Aégis Defender busca, incessantemente, a excelência. Isto é refletido na dedicação à realização de testes meticulosos e na busca constante pelo aprimoramento da ferramenta, visando proporcionar aos usuários a melhor proteção possível.

8. AUTORES

O software Aégis Defender é resultado da colaboração e dedicação de profissionais comprometidos com a excelência e inovação em segurança cibernética. A seguir, apresentamos os arquitetos por trás deste renomado projeto:

8.1 JÚLIA BARBOZA BRUNELLI

Contato Profissional:

- Perfil GitHub
- Perfil LinkedIn

8.2 NICHOLAS CALEGARI SANCHES

Contato Profissional:

- Perfil GitHub
- Perfil LinkedIn

8.3 RENAN DIAS DA COSTA SILVA

Contato Profissional:

- Perfil GitHub
- PerfilLinkedIn

A sinergia entre os membros da equipe é claramente refletida no sucesso e robustez do Aégis Defender. Cada integrante, com sua expertise e dedicação, consolidou este projeto como uma referência no panorama atual de segurança cibernética.

9. AGRADECIMENTOS

Em meio ao contínuo avanço do universo digital, os desafios relacionados à segurança cibernética ampliam-se, tornando-se cada vez mais complexos e multifacetados. O desenvolvimento do Aégis Defender, situado nesse intricado contexto, foi possível graças à confluência de talento, dedicação e uma profícua colaboração interdisciplinar. Diante dessa realidade, sentimo-nos compelidos a expressar nossa sincera gratidão a todos aqueles que trilharam conosco este caminho.

9.1 PROFESSORES DA FIAP

Nossa jornada acadêmica na FIAP proporcionou um ecossistema propício ao desenvolvimento de ideias inovadoras e ao estímulo do pensamento crítico. Gostaríamos de agradecer aos docentes que, armados de vasto conhecimento e experiência, nos guiaram com maestria, esculpindo assim os pilares teóricos e aplicados que sustentam o Aégis Defender.

9.2 PRIDE SECURITY

Em um setor tão volátil e competitivo como o da segurança cibernética, investir e acreditar no potencial de jovens inovadores é uma atitude audaz e meritória. A Pride Security desempenhou um papel crucial, não somente ao lançar-nos um desafio, mas integrando-se efetivamente em nossa trajetória de aprendizado e maturação.

9.3 AVALON TECH

Nossa parceria com a Avalon Tech revelou-se fundamental para materializar o conceito do Aégis Defender no software que é hoje. Nossos mais sinceros agradecimentos pelo inestimável apoio e confiança depositada em nosso projeto.

A saga do Aégis Defender atesta o quão impactante pode ser a união de esforços. Portanto, expressamos, com genuína humildade e reverência, nosso reconhecimento a cada entidade e indivíduo que depositou em nós seu apoio e confiança. Este é apenas o prólogo de uma jornada que, almejamos, fará notáveis contribuições ao mundo da segurança cibernética.

10. ASSISTÊNCIA E SUPORTE TÉCNICO

Canais de Comunicação: Estamos comprometidos em oferecer um suporte eficiente e ágil aos usuários do Aégis. Se você encontrar dificuldades, tiver dúvidas sobre a aplicação ou precisar de orientação técnica:

1. Página de Contato: A primeira opção é visitar a nossa página de contato no site da Avalon Tech, onde disponibilizamos um formulário para dúvidas e sugestões.

2. E-mail: Para um suporte mais direto, não hesite em nos enviar um e-mail. A nossa equipe de suporte técnico está sempre pronta para auxiliar e responderá sua mensagem o mais breve possível.

3. Documentação: Recomendamos também a consulta à nossa documentação extensiva, onde muitas questões comuns são abordadas e esclarecidas.

Esperamos que estas vias de comunicação facilitem sua experiência com o Aégis e garantam a resolução de qualquer inquietação ou obstáculo que possa surgir.