FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS
CURSO DE ENGENHARIA DA COMPUTAÇÃO

César Rafael Sorgato Santos
21907808

SISTEMA CENTRALIZADOR DE LOGS COM VISTA A SEGURANÇA DA INFORMAÇÃO

BRASÍLIA
2023

César Rafael Sorgato Santos

SISTEMA CENTRALIZADOR DE LOGS COM VISTA A SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia da computação do UniCEUB – Centro Universitário de Brasília

Orientador (a)**: Luciano Henrique Duque**

BRASÍLIA
2023

César Rafael Sorgato Santos

SISTEMA CENTRALIZADOR DE LOGS COM VISTA A SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia da computação do UniCEUB – Centro Universitário de Brasília

Orientador (a)**: Luciano Henrique Duque**

Brasília, 2023.

BANCA EXAMINADORA

_____

Nome e titulação.
Orientador (a) : Luciano Duque
Mestre

_____

Nome e titulação.
Examinador (a): Hugo Molina
Especialista

_____

Nome e titulação.
Examinador (a): Nathália Salomão
Especialista

Sistema para centralização de logs com vista a segurança da informação

Centralizer system of logs with a view to information security

César Rafael Sorgato Santos[1], Luciano Henrique Duque[2]

Resumo

Este artigo tem o objetivo de elaborar e desenvolver um SIEM (Security information and event management). A ferramenta terá como objetivo centralizar logs obtidos de soluções de segurança da TrendMicro(empresas fornecedoras de tecnologias de segurança da informação), dessa forma é possível agilizar o processo de visualização dos logs, visto que uma vez que não é necessário acessar diversas soluções, a economia de tempo e rapidez no processo são enormes. Com o SIEM construído, é possível ter uma visão geral de possíveis riscos ou comportamentos anormais no ambiente que possam fornecer alguma brecha para vazamento de dados, dessa forma, os encarregados pela segurança do ambiente digital conseguem fazer uma análise rápida sobre a segurança do ambiente naquele momento e identificar se está acontecendo algum tipo de ataque ou identificar possíveis fatores que levem a um ataque hacker. Além disso, o artigo também vai apresentar todas as ferramentas e linguagens utilizadas para o desenvolvimento do sistema, assim como o seu funcionamento em um ambiente corporativo real.

Palavras-chave: Segurança da informação. SIEM. Log.

Abstract: This article aims to design and develop a SIEM (Security information and event management). The tool will aim to centralize logs obtained from security solutions from TrendMicro (companie that provide information security technologies), in this way it is possible to speed up the process of viewing the logs, since, since it is not necessary to access several solutions, the time savings and speed in the process are enormous. With the SIEM built, it is possible to have an overview of possible risks or abnormal behavior in the environment that may provide some loophole for data leakage, in this way, those in charge of the security of the digital environment can make a quick analysis of the security of the environment in that moment and identify if any type of attack is happening or identify possible factors that lead to a hacker attack. In addition, the article will also present all the tools and languages used for the development of the system, as well as its operation in a real corporate environment.
keywords: Information security. SIEM. Log.

[1] UniCEUB, César Rafael Sorgato Santos
[2] UniCEUB, Luciano Henrique Duque

1 INTRODUÇÃO

A Cyber Segurança está ganhando cada vez mais espaço nas empresas devido ao grande aumento de ataques hacker no mundo inteiro. Segundo a CNN Brasil, foram registrados 31,5 bilhões de tentativas de ataque cibernético nas empresas brasileiras no primeiro semestre de 2022 (CNN Brasil, 2022).

A transformação digital dos negócios já estava em curso, mas a pandemia do coronavírus aconteceu e acelerou ainda mais sua jornada. Diante desse cenário, as reflexões sobre ameaças à segurança da informação precisaram ser otimizadas, passando de um foco em ativos corporativos para ativos pessoais (Nova8, 2022).

No pré-pandemia, a proteção contra ameaças era menos complicada, simplesmente porque a maioria das empresas contava com pelo menos algum tipo de sistema de segurança digital, como filtros web para monitorar e bloquear acessos a sites que possam trazer riscos. O período de isolamento social, porém, mudou esse ambiente (Linx, 2022).

Cada vez mais, os profissionais trabalham remotamente – em casa ou em lugares públicos o nível de segurança tende a ser menor. Além disso, muitos passaram a utilizar seus próprios computadores e celulares, criando um risco extra: as empresas precisaram liberar o acesso de novos equipamentos a seus sistemas, dando margem à exposição das suas plataformas (Linx, 2022).

Devido a essa necessidade de proteger os dados, em 2018 o Brasil aprovou a LGPD (lei geral de proteção de dados) para promover a proteção, dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil (Sepro, 2018).

Por conta da sociedade estar cada vez mais dependente de tecnologia, mais ferramentas e sistemas são desenvolvidos para suprir essa dependência, um dos problemas que acompanha essa demanda tecnológica é o aumento de portas de entrada para ataques cibernéticos. Por conta disso o número de empresas que atuam como prestadoras de serviços e/ou tecnologias de segurança da informação estão aumentando, pois, o número de ataques está aumentando cada vez mais, dessa forma pessoas e empresas precisam proteger cada vez mais seus dados e ativos, movimentando ainda mais esse mercado. Pessoas que optam por soluções de segurança apenas adquirem um antivírus para proteger seu computador, mas grandes corporações tendem adquirir diversas soluções como por exemplo: solução para segurança de email, computadores, servidores e outros, por conta dessa grande variedade de soluções, os analistas de segurança levam muito tempo e ficam com pouca visibilidade de todas soluções, por conta disso outra solução surgiu para resolver esse problema, o SIEM. Ele atua como um centralizador dessas soluções, então os analistas não necessitam entrar de solução em solução e conseguem filtrar somente aquilo que eles realmente necessitam verificar. (César Rafael Sorgato Santos, 2023).

2 REVISÃO BIBLIOGRÁFICA

Há fundamentos necessários para se entender um SIEM, depois de explicá-los, será aborado o tema do SIEM mais afundo.

2.1 Fundamentos de segurança

2.1.1 Segurança da informação

Para melhor entendimento de um SIEM é necessário entender o que é segurança da informação A segurança da informação é aquele conceito por trás da defesa dos dados, detalhes e afins para assegurar que eles estejam acessíveis somente aos seus responsáveis de direito ou as pessoas às quais foram enviados (tecnoblog, 2011).

A segurança da informação é uma grande aliada de empresas, pois é responsável por evitar que qualquer pessoa distribua, de

forma indevida, dados sobre vendas, margem de lucro, concorrentes, entre outras (Canaltech, 2019).

2.1.2 Tríade C.I.D

A segurança da informação tem como base três pilares: confidencialidade, integridade e disponibilidade. Esses aspectos, também conhecidos como CID, devem ser desenvolvidos simultaneamente e são vitais para o estabelecimento da cultura de proteção de dados.

Na Tabela 1, contém os as nomenclaturas da sigla C.I.D e sua descrição.

Tabela 1. Tríade C.I.D

Nomenclatura	Descrição
Confidencialidade	Garante proteção contra acessos indevidos
Integridade	Garante que não haja erros ou alterações não autorizadas nos dados
Disponibilidade	Garante que o serviço e/ou informação não fique indisponível

Fonte: César Rafael Sorgato Santos (2023)

2.2 Soluções de segurança.

Soluções de segurança são softwares/hardwares capazes de impedir ou detectar possíveis riscos ou ameaças, sejam elas internas ou externas tentando chegar ao ambiente (César Rafael Sorgato Santos, 2023).

2.2.1 Antivírus.

Antivírus é um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário (Canaltech, 2014).

2.2.2 Cloud Security.

O Cloud Security ou Segurança na Nuvem, refere-se às tecnologias, políticas, controles e serviços que protegem os dados, aplicativos e infraestrutura da nuvem contra ameaças (Introduce, 2022).

2.2.3 Gerenciador de vulnerabilidades.

O gerenciador de vulnerabilidades permite identificar, priorizar e responder a problemas de software e configurações incorretas que podem ser explorados por invasores, causar a liberação acidental de dados confidenciais ou interromper as operações de negócio (Servicenow, 2023).

2.2.4 SIEM.

As ferramentas SIEM coletam, agregam e analisam volumes de dados de aplicativos, dispositivos, servidores e usuários de uma organização em tempo real para que as equipes de segurança possam detectar e bloquear ataques. As ferramentas SIEM usam regras predeterminadas para ajudar as equipes de segurança a definir ameaças e gerar alertas (Microsoft, 2023).

.

2.3 LGPD

A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes (MPF, 2023).

Com a vinda da LGPD, basicamente todas empresas devem começar a se preocupar com a segurança, pois qualquer vazamento pode acabar acarretando com a

paralisação da empresa e ainda por cima, uma multa (César Rafael Sorgato Santos, 2023).

Fica evidente que para ficar de acordo com a LGPD e não acontecer nenhum imprevisto, as empresas precisam começar a adquirir soluções de segurança, caso contrário, um acesso indevido é algo simples de acontecer (César Rafael Sorgato Santos, 2023).

2.4 Tipos de ataques

Riscos no mundo digital estão presentes em todas as organizações e nem sempre estão sob o controle direto de uma equipe de de TI. Um ataque cibernético é realizado por hackers com a finalidade de interromper, desativar, destruir ou controlar, de forma maliciosa, um ambiente/infraestrutura de computação (33giga, 2022).

2.4.1 Ransomware

Ataque de ransoware foi um dos ciberataques que mais cresceu com a migração dos colaboradores para o modelo de trabalho remoto. Na prática, o ransomware bloqueia o acesso a todos os arquivos do servidor atacado. Os hackers só liberam novamente o acesso após o pagamento do valor de resgate, normalmente cobrado em bitcoins, determinado pelo sequestrador (33giga, 2022).

2.4.2 Cavalo de Tróia

Este é um tipo de malware popular que só funciona com “autorização” do usuário. Basta que a pessoa execute algum anexo de e-mail de remetente suspeito ou desconhecido, ou então, faça um download suspeito, contendo o vírus camuflado, e pronto: o Cavalo de Troia está instalado. Com isso, os hackers podem roubar informações pessoais e interromper funções no computador (33giga, 2022).

2.4.3 Phishing

Consiste em um ataque cibernético no qual os hackers levam os usuários a entregarem informações sigilosas, incluindo senhas, dados bancários e CPF. Via de regra, este tipo de cibercrime direciona o usuário para um site idêntico ao verdadeiro de uma agência bancária, por exemplo.Assim, nessa página falsa, que funciona como uma “isca”, os hackers “pescam” os dados dos usuários. Esse é um dos ataques cibernéticos mais populares.

2.4.4 Spyware

Spyware ou software espião, ataca computadores ou dispositivos móveis para coletar informações sobre seus usuário. Atua pegando informações sobre sites acessados, histórico de navegação e pode inclusive ter acesso a câmera de um celular ou notebook. Entretanto, hoje em dia, alguns dispositivos já vêm com bloqueio físico para impedir este tipo de ação (ilustradev, 2022).

2.4.5 Spoofing

O ataque cibernético spoofing consiste na falsificação de endereços de IP, de DNS e de e-mails. Assim, o cibercriminoso pode se passar pela empresa para roubar informações de clientes, usuários e funcionários, por exemplos (sigmatelecom, 2022).

2.5 Funções SIEM

Um SIEM tem diversas funções, a depender da solução pode conter mais ou menos ferramentas (César Rafael Sorgato Santos, 2023).

2.5.1 Agregação de dados

Os dados são coletados e monitorados de aplicativos, redes, servidores e bancos de dados (computerweekly, 2023).

2.5.2 Alertas

Se um incidente de segurança for detectado, as ferramentas SIEM podem notificar os usuários (computerweekly, 2023).

2.5.3 Automação

Alguns softwares SIEM também podem incluir funções automatizadas, como análise automatizada de incidentes de segurança e respostas automatizadas a incidentes (computerweekly, 2023).

2.5.4 Correlação

A correlação refere-se à ferramenta que encontra atributos semelhantes entre eventos diferentes (computerweekly, 2023).

3 METODOLOGIA DO TRABALHO

Este trabalho restringe-se ao ambiente que está sendo configurado, dessa forma nem todas suas funções seriam utilizaveis em outros ambientes, pois depende muito de configurações de rede e das soluções de segurança utilizadas.

3.1 Informações sobre o ambiente

O ambiente conta com mais de 80 de computadores, contas de emails e servidores, sendo todos sistemas operacionais windows e emails da microsoft 365.

3.2 Softwares utilizados

Pycharm (IDE para programação python), Visual Studio Code (IDE para programação web), XAMPP (hospedagem local de servidor web) e MySQL-Server (hospedagem de banco de dados local).

3.3 Linguagens utilizadas

Python para programação back-end, onde vai realizar a chamada pela API das soluções de seguranças e encaminhar para o banco de dados. HTML, CSS e JS para o front-end, onde teremos a parte visual do site.

3.4 Soluções utilizadas

Para o projeto funcionar é necessário adquirir os dados de alguma origem, nesse caso será utilizada as ferramentas da Trend micro (apex one, cloud app e email security) e Desktop Mannager.

3.4.1 Apex one

Ferramenta que entrega segurança para computadores, capaz de agir como anti-virus e firewall.

3.4.2 Cloud app

Solução para bloquear ameaças de aplicações em nuvem, como por exemplo: Email, one drive e sharepoint.

3.4.3 Email security

Gerenciador de email, capaz de aplicar soluções anti-spam e anti-virus.

3.4.4 Desktop mannager

Centralizador e gerenciador de de computadores.

4 DESENVOLVIMENTO

4.1 Instalação

O primeiro passo para começar a desenvolver o projeto é a instalação dos softwares de forma padrão (Visual Studio code, pycharm, xampp e mysql-server).

4.2 Desenvolvimento Python

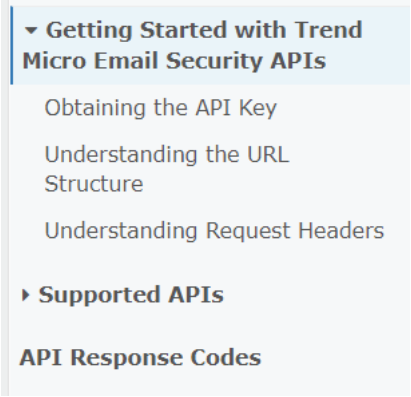
Feito a instalação, é necessário primeiro desenvolver o cógido python, pois com ele

vamos fazer a aquisição dos dados na trend e no desktop mannager para inserir em um banco de dados, que no caso será o mysql.

4.2.1 Requisisão API

O primeiro passo no desenvolvimento do código python é a aquisição dos dados pelas API's das soluções, então foi necessário consultar a documentação no site oficial das soluções para entender como as utilizar.

Figura 1. Documentação de API utilizada

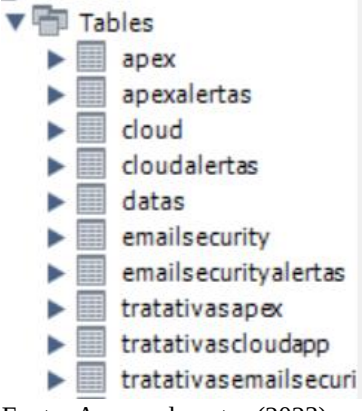


Fonte: Acervo do autor (2023)

4.2.2 Criação do banco de dados

Após finalizar a requisição dos dados já é possível verificar quais campos serão utilizados para desenvolver o banco de dados, a criação desse banco de dados é toda feita no python através de bibliotecas específicas para esse fim.

Figura 2. Estrutura do banco de dados

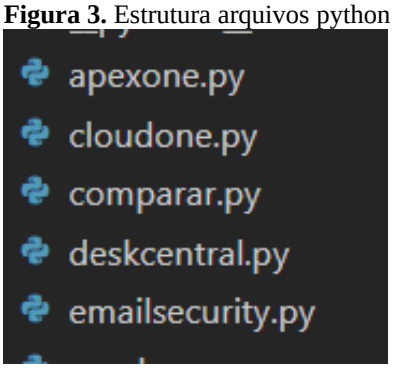


Fonte: Acervo do autor (2023)

4.2.3 Finalização do código Python

Com o banco de dados criado e mapeado os dados das API's, já é possível fazer todo o código python. Primeiramente é criado o banco de dados e suas tabelas, em seguida é realizado a requisição das API's, e todo o processo é finalizado com esses dados sendo enviados para o banco de dados.

Figura 3. Estrutura arquivos python



Fonte: Acervo do autor (2023)

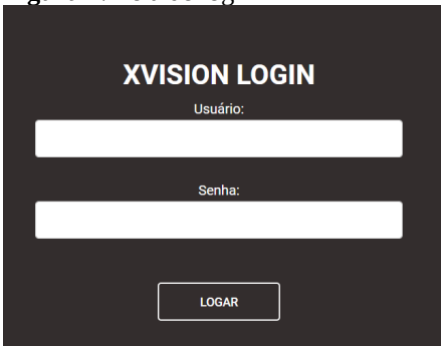
4.3 Desenvolvimento Web

Depois de finalizar o código python já está finalizado todo o banco de dados e suas informações, agora tem que demonstrar essas informações em uma aplicação web.

4.3.1 Página de login

O primeiro passo para o desenvolvimento web é a página de login, pois como a aplicação vai apresentar dados sensíveis, é necessário que contenha alguns fatores de segurança.

Figura 4. Tela de login



Fonte: Acervo do autor (2023)

4.3.2 Tabelas

Com a segurança aplicada, agora já é possível começar a desenvolver as tabelas onde serão alocados as informações do banco de dados, as tabelas são feitas com os frameworks bootstrap e jquery, porém para adquirir os dados, será utilizado o PHP, que vai realizar a consulta sql e popular as tabelas.

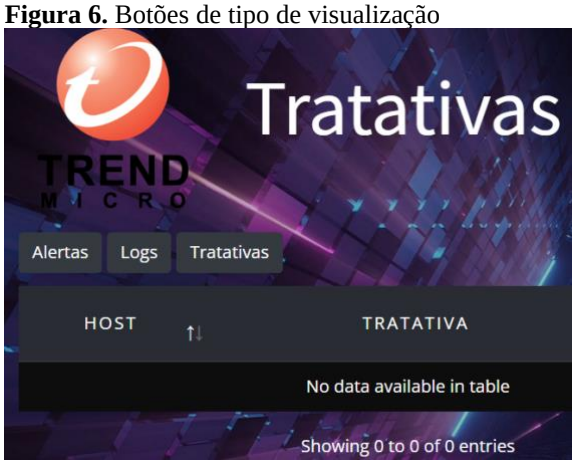
Figura 5. Tabela em branco

Fonte: Acervo do autor (2023)

4.3.3 Botões de tipo de visualização

Após finalizar as tabelas, alguns botões serão necessários para alternar as tabelas que serão mostradas, pois cada solução de segurança vai ter 3 abas: alertas (vai mostrar a quantidade de alertas que um host possui), logs (mostra o detalhe de cada alerta do host) e tratativas (mostra a informação que o usuário registrar).

Figura 6. Botões de tipo de visualização



Fonte: Acervo do autor (2023)

4.3.4 Botões das soluções

Agora é necessário botões para alternar entre as soluções de segurança, que nesse caso são: apex, cloudapp e emailsecurity. Cada botão vai deixar visível somente a tabela que o usuário desejar.

Figura 7. Botões das soluções

Fonte: Acervo do autor (2023)

4.3.5 Botões de exportar

Os ultimos botões necessários são os de exportar, que vai permitir exportar todos os dados da tabela no tipo de formato desejado. Esses botões são importantes pois facilitam na elaboração de um relatório de conformidade.

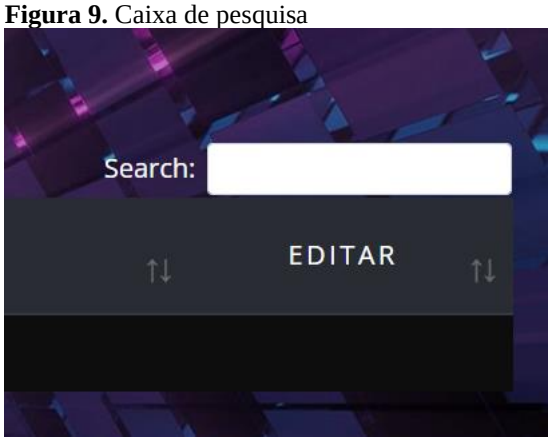
Figura 8. Botões de exportar

Fonte: Acervo do autor (2023)

4.3.6 Caixa de pesquisa

A depender do número de dados recebidos das API's, é provável que seja difícil localizar alguma informação, então foi inserido uma caixa de pesquisa, essa caixa faz uma pesquisa em todas as colunas da tabela, facilitando encontrar qualquer tipo de informação.

Figura 9. Caixa de pesquisa



Fonte: Acervo do autor (2023)

4.3.7 Informações de datas

Outro dado importante na página é a data da última atualização das informações, pois dessa forma é possível identificar se a aplicação está funcionando direito e de quando são as informações obtidas.

A data do log mais antigo também é interessante mostrar, pois assim tem como identificar o periodo das informações demonstradas.

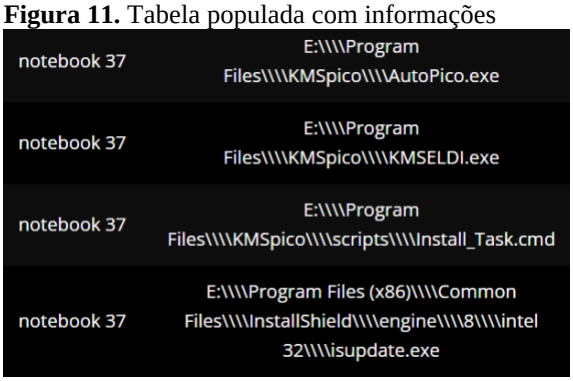
Figura 10. Informações de datas

Fonte: Acervo do autor (2023)

4.3.8 Aquisição das informações

Com a tabela pronta, já pode ser feita a aquisição das informações para popular a tabela. O PHP vai se encarregar de pegar essas informações e encaminhar para as tabelas.

Figura 11. Tabela populada com informações

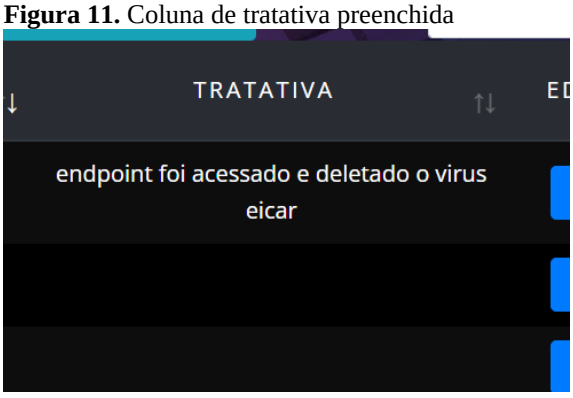


Fonte: Acervo do autor (2023)

4.3.9 Tratativas

O último passo relevante para finalizar o desenvolvimento da aplicação WEB são as tratativas, que nada mais são do que informações registradas pelo operador do sistema, onde ele pode registrar alguma informação sobre o que foi feito em relação ao alerta.

Figura 11. Coluna de tratativa preenchida



Fonte: Acervo do autor (2023)

5 APRESENTAÇÃO DOS RESULTADOS

Após todo o desenvolvimento ser concluído, o sistema já está pronto para ser utilizado no ambiente.

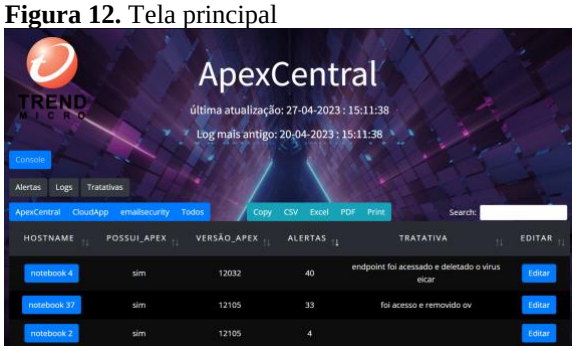
5.1.1 Python

O primeiro passo para começar a utilizar o sistema é colocar o código python em execução, pois eles são os dados que serão mostrados no sistema.

5.1.2 Tela principal

Com o python rodando em background, o sistema já estará funcionando, basta acessar a url do sistema, que nesse caso será “http://localhost/threatdb/index.php”. Agora basta utilizar o sistema.

Figura 12. Tela principal



Fonte: Acervo do autor (2023)

5.1.3 Alertas individuais

Na tela de alertas é possível selecionar um dos notebooks apenas clicando em seu nome, dessa forma é possível verificar todos os alertas gerados para esse notebook e qual ação foi tomada.

Figura 13. Alertas individuais

Fonte: Acervo do autor (2023)

5.1.4 Tratativas

Todo alerta tem um campo tratativa onde é inserido um texto (caso necessário) pelo operador. Esse campo vai receber alguma informação sobre o que foi feito em relação a esse alerta, como por exemplo: foi verificado que o notebook realmente apresentava um virus, mas já foi removido.

Figura 14. Tratativas

Fonte: Acervo do autor (2023)

5.1.5 Exportar

Acima da tabela temos os botões de exportar, esses botões exportam os dados da tabela de diversas formas (CSV, excel, pdf, imagem e texto), essa função facilita na geração de relatórios de compliance.

Figura 15. Exportar

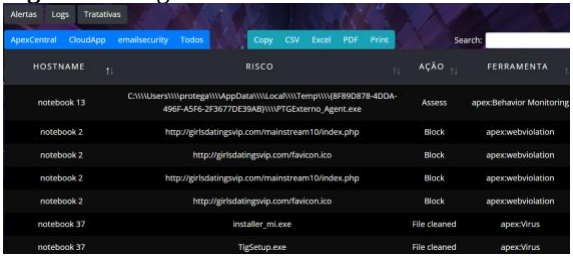
	A	B	C	D	E
1	Exported data				
2	**Hostname**	**Possui_Apex**	**Versão_Apex**	**Alertas**	**Tratativa**
3	notebook 4	sim	12032	40	endpoint foi acessado e deletado o virus eicar
4	notebook 37	sim	12105	33	foi acesso e removido ov
5	notebook 2	sim	12105	4	
6	notebook 66	sim	12105	2	
7	notebook 86	sim	12105	2	
8	notebook 5	sim	12105	1	
9	notebook 13	sim	12105	1	
10	notebook 67	sim	12105	1	
11	notebook 1	sim	6755	0	
12	notebook 3	sim	12105	0	
13	notebook 6	sim	12105	0	
14	notebook 7	sim	12105	0	
15	notebook 8	sim	12105	0	

Fonte: Acervo do autor (2023)

5.1.6 Logs

Ao apertar o botão logs, é possível ver os logs de todas máquinas/emails de uma vez só, caso seja necessário fazer uma análise mais rápida.

Figura 16. Logs



Fonte: Acervo do autor (2023)

5.1.7 Tratativas

Ao apertar o botão de tratativas, é possível ver todas as tratativas atribuidas aos emails/máquinas.

Figura 17. Tratativas

Fonte: Acervo do autor (2023)

5.1.8 Soluções

Existem 3 soluções para escolher, apexcentral, cloudapp e emailsecurity. Ao clicar no botão de uma dessas 3 soluções, ficam visiveis os logs dessa solução.

Figura 18. Soluções

Fonte: Acervo do autor (2023)

5.1.9 Console

Por último, o botão “console”, ao pressionar o botão uma nova página será aberta e redirecionada ao site da solução de segurança selecionada, facilitando o acesso a página oficial dos logs para uma análise mais profunda se necessário.

Figura 19. Console

Fonte: Acervo do autor (2023)

6 CONSIDERAÇÕES FINAIS

O projeto tinha como objetivo reduzir o tempo de análise e facilitar o desenvolvimento de relatórios, visto que as soluções originais onde são gerados os logs possuem tais defeitos, o objetivo foi atingido da forma esperada, causando uma redução significativa nas análises de compliance, como é possível verificar na tabela 1.

Tabela 1. Tempo de análise do Apex

Quantidade de vezes que a foi feito análise	Diretamente da ferramenta	SIEM
1x	4:40 minutos	1 minuto
10x no dia	46 minutos	10 minutos
50x na semana	3 horas e 50 minutos	50 minutos
200x no mês	15 horas e 30 minutos	3 horas e 20 minutos

A solução é simples porém bastante eficaz, com seu grande ganho de tempo, os analistas de segurança recebem mais tempo para focar em outras soluções ou serviços que necessitam realizar.

REFERÊNCIAS

CABLE NEWS NETWORK. Anuário estatístico de acidentes de origem elétrica. São Paulo: CNN Brasil, 2020.

NOVA8. Como o crescimento da digitalização aumenta a necessidade de segurança de sistemas?. São Paulo: Nova8, 2022.

LINX. Por que a segurança digital precisa ser uma prioridade do varejo?. São Paulo: Linx, 2022.

SERPRO. O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. Distrito Federal: Serpro, 2018.

TECHNOBLOG. O que é segurança da informação?. São Paulo: Technoblog, 2011.

CANALTECH. O que é segurança da informação?. São Paulo: Canaltech, 2019.

CANALTECH. O que é antivírus?. São Paulo: Canaltech, 2014.

INTRODUCE. O que é Cloud Security?. Rio Grande do Sul: Introduce, 2022.

SERVICENOW. O que é gerenciamento de vulnerabilidades?. California: Servicenow, 2023.

MICROSOFT. O que é SIEM?. Washington: Microsoft, 2023.

MINISTÉRIO PÚBLICO FEDERAL. Lei Geral de Proteção de Dados Pessoais (LGPD). Distrito Federal: MPF, 2023.

33GIGA. Os 8 tipos mais comuns de ataques hackers. São Paulo: 33Giga, 2022.

ILUSTRADEV. 15 Tipos De Ataques Hackers: Ataque Cibernético. São Paulo: IlustraDev, 2022.

SIGMATELECOM. Conheça os 11 tipos mais comuns de ataques cibernéticos a empresas e descubra como se proteger. Paraná: SigmaTelecom, 2022.

COMPUTERWEEKLY. SIEM ou gerenciamento de eventos e informações de segurança. São Paulo: ComputerWeekly, 2023.