METODOLOGIA INTEGRATIVA PARA A DETECÇÃO E PREVENÇÃO DE AMEAÇAS UTILIZANDO INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA E SIEM

Alexander André de Souza Vieira e João José Costa Gondim
Pós-graduação Profissional em Engenharia Elétrica – PPEE – Departamento de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília (UnB), Brasília, Brasil, Zip Code 70910-900

RESUMO

As ameaças cibernéticas, como Ameaças Persistentes Avançadas (APTs), evoluíram e superaram as técnicas tradicionais de detecção. Este artigo propõe uma metodologia integrativa para aprimorar a detecção e prevenção de ameaças cibernéticas, com foco na qualidade da Inteligência de Ameaças Cibernéticas (CTI) e na identificação de Táticas, Técnicas e Procedimentos (TTPs). A metodologia inclui, entre outras etapas, o enriquecimento de dados de inteligência e a análise centralizada de eventos de segurança coletados por meio de sensores. Sua eficácia foi demonstrada através da execução de amostras reais de malware, destacando a importância de disponibilizar rapidamente relatórios de segurança, garantindo sua qualidade e sugerindo melhorias na integração e análise de dados para uma detecção mais eficaz.

PALAVRAS-CHAVE

Inteligência de Ameaça Cibernética, Ameaças Persistentes Avançadas, Detecção de Ameaças, SIEM

1. INTRODUÇÃO

Com o avanço contínuo da tecnologia e o aumento da complexidade dos sistemas computacionais, surgem novos desafios e vulnerabilidades em relação à cibersegurança. A evolução das técnicas e ferramentas de ataque acompanhou o progresso dos sistemas, levando os atacantes a adotarem métodos cada vez mais sofisticados e furtivos. Como resultado, muitas ameaças modernas podem passar despercebidas pelos mecanismos tradicionais de segurança (Abu et al. 2018).

Os ataques cibernéticos evoluíram significativamente ao longo dos anos. No passado, os ataques eram geralmente realizados de maneira direta e utilizavam técnicas relativamente simples, que podiam ser identificadas por ferramentas baseadas em assinaturas, que funcionavam de forma rápida e eficaz contra malwares conhecidos (Aslan and Samet, 2020). Contudo, com o surgimento de ameaças mais complexas, como as APTs, os atacantes passaram a empregar técnicas avançadas e encobertas. As APTs são caracterizadas por sua capacidade de infiltrar-se e permanecer ocultas em redes e sistemas por longos períodos, geralmente com o objetivo de roubar dados sensíveis, comprometer a integridade dos sistemas ou causar interrupções de serviço (Wu, 2020; Imperva, 2024).

A natureza dessas ameaças exige uma abordagem de segurança que vá além das técnicas reativas tradicionais. Em resposta a isso, as plataformas de inteligência de ameaças cibernéticas (TIPs) surgiram, utilizando a CTI para aprimorar a detecção, prevenção e resposta aos ataques. A CTI consiste em informações detalhadas sobre ameaças cibernéticas, coletadas e organizadas para fornecer insights valiosos sobre ameaças emergentes e tendências de ataque. Essa inteligência pode ser usada para identificar padrões, antecipar ataques e implementar medidas de defesa mais eficazes (Sagar, 2018).

Para que a CTI seja eficaz, deve atender a várias características fundamentais. Deve ser oportuna, fornecida rapidamente para permitir uma resposta eficaz; relevante, contextualizada para o ambiente específico, de forma que a informação possa ser aplicada de forma prática; abrangente, oferecendo uma visão detalhada dos incidentes; e clara, com informações padronizadas e estruturadas para facilitar a análise e a tomada de decisões (Tounsi and Rais, 2018).

O processo de produção de inteligência nas TIPs segue um ciclo bem definido, que inclui coleta de dados, processamento, análise e disseminação ou implementação dos resultados (Silva, 2020). No entanto, um dos principais desafios enfrentados pelas TIPs é a falta de padronização nos formatos e fontes de dados, o que pode resultar em uma produção de inteligência inconsistente e de baixa qualidade. Além disso, muitas ferramentas TIP concentram-se predominantemente na fase de coleta de dados, negligenciando as etapas subsequentes de análise e disseminação (Sauerwein et al., 2018). Esse foco limitado pode resultar em plataformas que oferecem pouca ou nenhuma melhoria na detecção e resposta a ameaças, tornando-se frequentemente meros repositórios de dados.

Com base no contexto apresentado, este trabalho busca responder às seguintes perguntas de pesquisa:

PP1. Como a integração de fontes de inteligência cibernética pode aprimorar a detecção e prevenção de ameaças avançadas, como APTs, em um ambiente de monitoramento?

PP2. Até que ponto a detecção proativa baseada em TTPs pode ser otimizada através do enriquecimento de dados nas plataformas de inteligência cibernética?

PP3. Como o uso de IoCs nas ferramentas de monitoramento, detecção e alerta pode ser aprimorado para uma detecção mais eficiente de ameaças persistentes?

Este trabalho visa preencher essas lacunas ao desenvolver e avaliar uma metodologia para a detecção e prevenção de ameaças cibernéticas. A metodologia proposta foca no mapeamento de TTPs e na melhoria da qualidade da CTI por meio de um processo de enriquecimento de dados. Ao integrar dados de diversas fontes e melhorar a precisão da detecção, pretendemos oferecer uma solução mais eficaz para enfrentar ameaças cibernéticas modernas e aprimorar a segurança dos sistemas.

O restante deste artigo está organizado da seguinte forma: Na Seção 2, são discutidos os trabalhos relacionados que dão suporte e contextualizam a pesquisa. Na Seção 3, detalhamos a metodologia proposta, explicando as ferramentas e técnicas utilizadas para a detecção e prevenção de ameaças cibernéticas. A Seção 4 foca no estudo de caso, onde implementamos e testamos a metodologia em um ambiente controlado, apresentando os resultados e validações dos testes realizados. Finalmente, na Seção 5, apresentamos nossas conclusões e delineamos direções para trabalhos futuros.

2. TRABALHOS RELACIONADOS

A compreensão e mitigação das Ameaças Persistentes Avançadas (APTs) e o aprimoramento das plataformas de inteligência cibernética são áreas amplamente exploradas pela pesquisa. A seguir, discutimos diversos estudos que contribuíram para o avanço do conhecimento nessas áreas e que são relevantes para o contexto de nossa pesquisa.

O estudo conduzido por Ghafir et al. (2019) explora a exploração de vulnerabilidades por APTs e as limitações dos mecanismos de detecção tradicionais baseados em assinatura. O trabalho introduz uma abordagem inovadora que utiliza correlação de alertas e Modelos Ocultos de Markov (HMMs) para prever estágios das APTs, destacando a importância da análise preditiva e da detecção de anomalias baseada em comportamento para enfrentar ataques cibernéticos sofisticados em múltiplas etapas.

Mahboubi et al. (2024) realizam uma revisão sistemática da evolução das técnicas de "threat-hunting" (caça a ameaças), observando como tecnologias emergentes, como inteligência artificial e aprendizado de máquina, estão sendo integradas para melhorar a detecção de ameaças. Seu estudo oferece uma análise detalhada de como estratégias avançadas de caça a ameaças estão se tornando essenciais na detecção de ameaças ocultas ou em evolução dentro de redes, oferecendo uma perspectiva de como as organizações podem aprimorar suas defesas cibernéticas.

Jin et al. (2024) analisam o impacto do compartilhamento de CTI entre organizações, com foco no volume, na tempestividade e na qualidade dos dados compartilhados. Seus achados revelam que, embora o volume de CTI compartilhado tenha aumentado, a profundidade dos dados compartilhados — como táticas, técnicas e procedimentos (TTPs) — ainda é limitada, resultando frequentemente em inteligência de pouca aplicabilidade. Isso destaca a importância de melhorar tanto a qualidade quanto o escopo do compartilhamento de CTI para aumentar seu valor prático na mitigação de ameaças cibernéticas.

Ainslie et al. (2023) examinam o papel essencial das Plataformas de Inteligência de Ameaças (TIPs) na operacionalização da CTI, enfatizando o potencial das TIPs em transformar dados de ameaças em insights acionáveis. No entanto, os autores observam que as TIPs muitas vezes falham em evoluir, servindo predominantemente como repositórios de dados estáticos em vez de melhorar a detecção e resposta a ameaças em tempo real. Eles ressaltam a necessidade de que as TIPs avancem em padronização de dados e em capacidades analíticas para atender às demandas modernas de cibersegurança e apoiar efetivamente a gestão abrangente de ameaças.

González-Granadillo et al. (2021) analisam a evolução e o desempenho dos sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM), com foco em sua aplicação em infraestruturas críticas. O estudo revisa ferramentas SIEM comerciais e de código aberto, oferecendo uma avaliação extensa de suas capacidades, limitações e melhorias futuras. Os autores destacam a necessidade de aprimorar a detecção em tempo real, a análise comportamental e a resposta a incidentes para enfrentar as ameaças cibernéticas cada vez mais sofisticadas. Esta pesquisa é particularmente relevante para nosso trabalho, pois delineia as principais tendências e desafios para sistemas SIEM em ambientes complexos, oferecendo um roteiro para desenvolvimento futuro.

Por fim, Leite et al. (2023) propõem uma abordagem automatizada para o uso de CTI durante a resposta a incidentes, mapeando Táticas, Técnicas e Procedimentos (TTPs) em incidentes de rede. A metodologia apresentada permite a criação de padrões de ataque específicos para ameaças identificadas, facilitando a correlação entre eventos de rede e relatórios de CTI. O estudo demonstrou que essa abordagem pode aumentar a precisão da detecção de incidentes e tornar as respostas mais eficientes.

Além desses trabalhos, é importante destacar que a integração e aprimoramento das plataformas TIP e a detecção de APTs continuam sendo áreas de pesquisa ativa. Novas abordagens e tecnologias estão sendo constantemente desenvolvidas para aprimorar a eficácia da inteligência cibernética e a segurança dos sistemas. Este trabalho visa contribuir para essa área de pesquisa ao propor uma metodologia para detecção e prevenção de ameaças cibernéticas que aborda as limitações das abordagens atuais e melhora a precisão da CTI.

3. METODOLOGIA

A metodologia para detecção e resposta a incidentes cibernéticos segue um ciclo estruturado, composto por etapas que integram dados de várias fontes, enriquecem essas informações com inteligência adicional e utilizam essas correlações para identificar e mitigar ameaças. O processo descrito aqui é inspirado na abordagem proposta por Leite et al. em "Actionable Cyber Threat Intelligence for Automated Incident Response" (Leite et al., 2023), mas adaptado a um contexto específico de dados e ferramentas. Na sequência, descrevemos as principais fases de nossa metodologia, representada na Figura *1*.

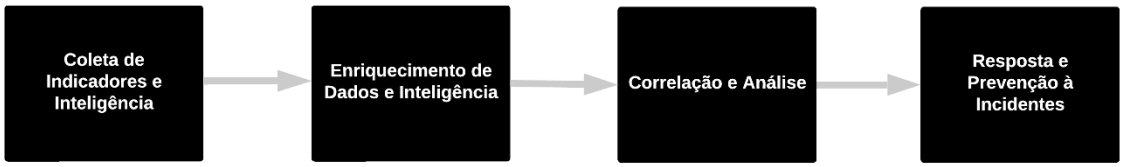

Figura 1. Descrição da Estrutura

3.1 Coleta de Indicadores e Inteligência

A primeira etapa consiste na coleta de dados brutos de múltiplas fontes, tanto internas quanto externas. Essas fontes incluem registros de eventos de segurança, Indicadores de Comprometimento (IoCs), bem como relatórios de inteligência de ameaças cibernéticas. Essa coleta abrange dados estruturados e não estruturados, obtidos de plataformas de Inteligência de Ameaças e de máquinas clientes utilizadas para a execução de malware.

A plataforma de inteligência cibernética é configurada para ser populada com relatórios de segurança estruturados de fontes de inteligência pública. Essa etapa é crítica, pois dados de várias fontes são coletados e consultas são realizadas aos dados disponíveis por meio dos relatórios de ameaças. Sensores são instalados nas máquinas clientes para coletar logs e indicadores, e esses são enviados para uma ferramenta centralizada de gerenciamento de logs.

3.2 Enriquecimento de Dados e Inteligência

Conforme os relatórios de inteligência são importados para a ferramenta TIP, eles são enriquecidos com dados extraídos de outras fontes de inteligência de código aberto, o que aprimora a contextualização dos eventos e melhora a precisão das potenciais detecções. Entretanto, como a qualidade e autenticidade dos dados usados durante o processo de enriquecimento afetam significativamente a confiabilidade da inteligência resultante, é importante enriquecer os dados de ameaças com feeds verificados ou de alta qualidade, como VirusTotal (VirusTotal, 2024), Hybrid Analysis (Hybrid Analysis, 2024) e AlienVault OTX (Level Blue, 2024). O enriquecimento com feeds de baixa qualidade pode levar a correlações imprecisas, gerando falsos positivos ou falsos negativos. Tais imprecisões podem resultar em respostas a incidentes ineficazes, desperdício de recursos e aumento da vulnerabilidade do sistema.

Os dados brutos recebidos na ferramenta centralizada são processados e enriquecidos com informações adicionais. Esta fase envolve correlacionar os indicadores capturados com Táticas, Técnicas e Procedimentos (TTPs) conhecidos, usando o framework MITRE ATT&CK como referência (MITRE, 2024).

3.3 Correlação e Análise

Nesta etapa, os dados enriquecidos são analisados em busca de padrões de comportamento malicioso e TTPs que correspondam a ameaças conhecidas. Essa análise utiliza uma abordagem baseada em inteligência de ameaças para correlacionar eventos de segurança com ataques previamente documentados. O processo envolve regras predefinidas que utilizam técnicas de correspondência de padrões, especificamente expressões regulares (regex), para buscar ocorrências específicas de ações dentro dos logs coletados. Essas ações são então mapeadas para os TTPs correspondentes, permitindo a identificação de potenciais ameaças com base nos comportamentos observados e facilitando a detecção proativa de ameaças, correlacionando os indicadores observados com táticas conhecidas de adversários.

Assim, os TTPs que foram correlacionados a um indicador são comparados com a base de informações de ataques e ameaças cibernéticas obtida dos relatórios de segurança. Se TTPs originados de um indicador forem encontrados entre os TTPs listados anteriormente nos relatórios, uma segunda verificação é realizada, onde o indicador suspeito é comparado com uma lista de indicadores relacionados aos TTPs identificados.

3.4 Resposta e Prevenção a Incidentes

A fase final envolve ações de resposta com base nas correlações encontradas. Incidentes detectados podem ser priorizados de acordo com o nível de ameaça e criticidade, permitindo uma resposta mais ágil e eficiente. De acordo com os TTPs e indicadores encontrados, regras de bloqueio podem ser criadas na ferramenta centralizada de gerenciamento de logs para prevenir novas ocorrências, bem como encerrar casos em andamento em tempo real.

4. ESTUDO DE CASO

O estudo de caso da metodologia proposta envolveu a configuração e utilização de várias ferramentas para a detecção de ameaças cibernéticas. A solução está representada na Figura *2*, e as principais etapas da implementação são descritas na sequência:

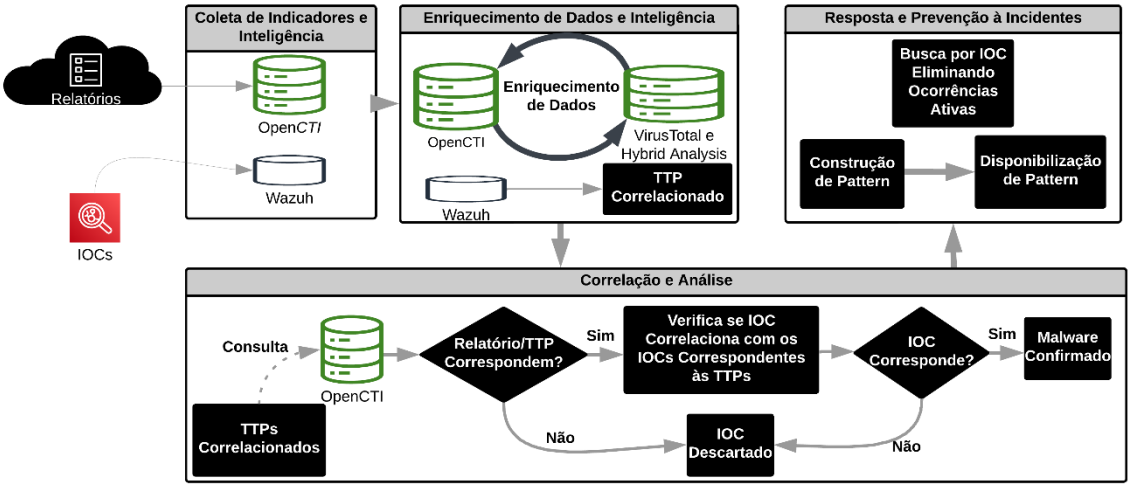

Figura 2. Fluxo da solução proposta

4.1 Configuracão do OpenCTI

Como ferramenta TIP para armazenamento e gerenciamento de relatórios de inteligência de ameaças cibernéticas, foi escolhida a plataforma OpenCTI (Filigran, 2024). Esta plataforma de código aberto é projetada para estruturar, armazenar e visualizar tanto informações técnicas quanto não técnicas sobre ameaças cibernéticas, permitindo o gerenciamento eficiente do conhecimento de inteligência cibernética e observáveis. Aproximadamente 1.500 relatórios foram importados do banco de dados AlienVault OTX.

Como fontes adicionais de informação para enriquecer os relatórios de CTI (Figura *3*), foi configurada a integração com VirusTotal e Hybrid Analysis via conectores no OpenCTI. À medida que os relatórios foram adicionados ao banco de dados do OpenCTI, consultas foram realizadas às outras duas fontes para coletar informações relevantes e correlacionadas. Essas informações foram então adicionadas aos relatórios no OpenCTI, enriquecendo os relatórios iniciais para melhorar a precisão da detecção e fornecer um contexto mais profundo sobre as ameaças.

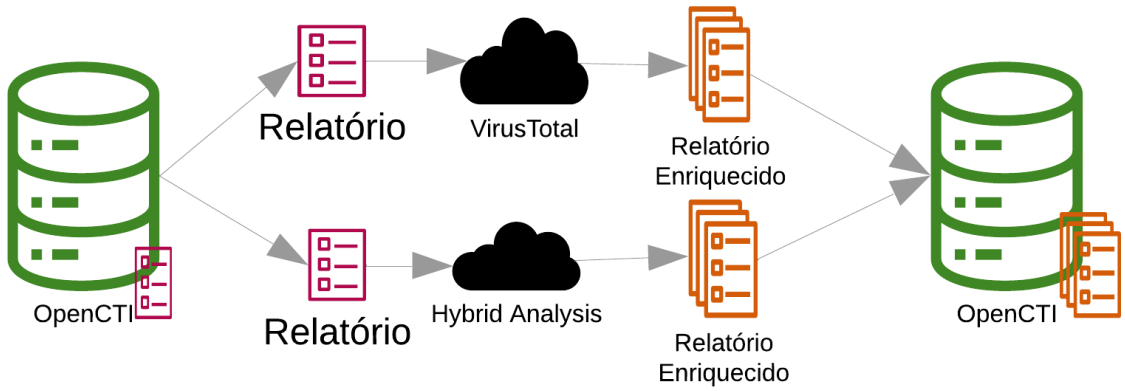

Figura 3. Processo de enriquecimento

4.2 Instalação e Configuração do Wazuh

A plataforma centralizada de logs utilizada foi o Wazuh, uma ferramenta de código aberto que combina funcionalidades de SIEM (Gerenciamento de Informações e Eventos de Segurança) e XDR (Detecção e Resposta Estendidas) (Wazuh, 2024), realizando atividades de monitoramento, detecção e alerta. O Wazuh foi instalado em um servidor Linux executando o sistema operacional Ubuntu. Sua função principal é coletar, correlacionar e analisar logs de endpoints, proporcionando uma visão consolidada e em tempo real da segurança da rede. Sensores do Wazuh foram instalados em máquinas virtuais configuradas com Windows 10 para capturar eventos e logs dos endpoints. Para aprimorar a coleta de dados, o Sysmon foi configurado conforme as recomendações de Hartong (2023), o que permitiu a coleta de logs detalhados do sistema.

4.3 Coleta e Análise de Amostras de Malware

Para a obtenção de amostras de malware, foi utilizado o repositório Malware Bazaar, mantido pela Abuse. Esse repositório é uma fonte valiosa de amostras de malware que são compartilhadas com a comunidade de segurança da informação (Malware Bazaar, 2024). As amostras obtidas foram usadas para testar a eficácia da metodologia proposta na identificação de ameaças. O malware usado para validar a metodologia foi o Agent Tesla. As amostras foram executadas nas máquinas virtuais, e, conforme os logs de segurança eram gerados, os sensores instalados nas máquinas encaminhavam as informações correspondentes para o Wazuh, que automaticamente as interpretava e fornecia os TTPs associados aos eventos ocorridos durante a execução do malware.

4.4 Validação e Resultados

Durante a execução de uma amostra aleatória do Agent Tesla, os logs gerados nas estações clientes foram enviados pelos sensores para a ferramenta Wazuh. Automaticamente, o Wazuh verificou os logs recebidos em busca da presença de táticas, técnicas e procedimentos conhecidos, e correlacionou os TTPs observados durante a execução do malware, gerando a lista l_{TTPs}. Com a lista l_{TTPs}em mãos, foi realizada uma busca no banco de dados de relatórios do OpenCTI, listando todos os relatórios que continham pelo menos um dos TTPs mencionados anteriormente, o que gerou a lista l_{Rep}, contendo aproximadamente 640 relatórios. Após a criação da lista l_{Rep}, os relatórios nela contidos foram classificados com base no número de TTPs associados, produzindo o ranking R_1:

$$R_1 = f\,(L_{Rep})$$

Aqui, a função f serve como um mecanismo de pontuação que classifica os relatórios em l_{Rep} de acordo com quantos TTPs da lista observada l_{TTPs} eles compartilham. Quanto mais TTPs um relatório compartilha com o comportamento observado, maior é sua pontuação. Isso permite a identificação e priorização de relatórios que fornecem as informações mais relevantes sobre a ameaça observada. Dessa forma, a função f ajuda a otimizar o processo de investigação, concentrando a atenção nos relatórios com maior probabilidade de conter detalhes úteis sobre a ameaça observada.

Era esperado que os relatórios presentes em R_1 tivessem referências diretas ao Agent Tesla. No entanto, ao analisar os principais relatórios em R_1, ou seja, aqueles que tinham mais TTPs associados à execução do malware, verificamos que nenhum deles mencionava o Agent Tesla. Formalmente, definimos A_1 como o conjunto de relatórios que mencionam o Agent Tesla, e observamos que este conjunto estava vazio:

$$A_1 = \{r \in R_1 : r \text{ menciona Agent Tesla}\} = \emptyset$$

A segunda abordagem envolveu a verificação dos Indicadores de Comprometimento (IoCs) presentes nos relatórios da lista L_{Rep}. Um IoC é definido como um dado ou evidência que sugere uma possível violação de segurança em um sistema, e ajuda os profissionais de segurança a identificar atividades suspeitas e responder a possíveis ameaças buscando padrões como endereços IP maliciosos, hashes de arquivos, nomes de domínios ou comportamentos anômalos na rede. Todos os IoCs foram pesquisados no Wazuh durante o período de

execução do malware, mas também não foram encontradas correlações. Formalmente, a correlação C_1 entre os IoCs I_1 e os logs do Wazuh foi nula:

$$C_1 = \{i \in I_1 : i \text{ corresponde aos logs do Wazuh}\} = \emptyset$$

Essa falta de correlação levantou questões sobre a atualidade e relevância dos relatórios analisados. Finalmente, foi realizada uma segunda validação com uma versão diferente do Agent Tesla, que sabíamos estar referenciada em um dos relatórios existentes no OpenCTI. Os mesmos passos foram repetidos, onde a lista de TTPs observados durante a execução do malware l_{TTPs2}foi gerada, depois os relatórios que faziam referência a esses TTPs foram listados, gerando a lista L_{Rep2}, e os relatórios foram classificados usando R_2. Desta vez, o relatório correspondente ao malware executado foi encontrado no ranking R_2. Assim, agora definimos A_2 como o conjunto de relatórios que mencionam o Agent Tesla, e observamos que este conjunto não estava mais vazio:

$$R_2 = f\,(L_{Rep2})$$
$$A_2 = \{r \in R_2 : r \text{ menciona Agent Tesla}\} \neq \emptyset$$

Por fim, os IoCs presentes nos relatórios da lista L_{Rep2} também foram verificados e, conforme esperado, o IoC da versão executada do malware apareceu nos relatórios anteriores. Assim, a nova correlação C_2 indicou uma correspondência positiva:

$$C_2 = \{i \in I_2 : i \text{ corresponde aos logs do Wazuh }\} \neq \emptyset$$

4.5 Discussão

Na primeira tentativa de validação da metodologia, onde uma amostra aleatória do Agent Tesla foi executada, foi possível correlacionar os TTPs detectados com os relatórios disponíveis. No entanto, não foi possível atribuir a sequência de TTPs a um malware específico. Isso foi alcançado na segunda tentativa de validação da metodologia, onde, entre os TTPs listados durante a execução do Agent Tesla, os TTPs identificados puderam ser correlacionados com os relatórios disponíveis, bem como um segundo fator de verificação, no qual também foi observada a correlação dos IoCs com os relatórios.

Assim, a metodologia proposta demonstra ser eficaz na identificação de TTPs e na correlação deles com relatórios, desempenhando o papel de um sistema de recomendação, ao sugerir possíveis caminhos de investigação onde a sequência de TTPs utilizados poderia potencialmente ser atribuída a um malware específico. Os resultados observados na segunda tentativa de validação indicam que, dependendo da tempestividade na detecção dos TTPs e da correlação com os relatórios, a convergência de uma investigação pode ser acelerada, levando a uma atribuição mais rápida da entidade maliciosa. Portanto, a metodologia apresentada tem o potencial de ir além da escalabilidade no processo de detecção e identificação de TTPs, possivelmente levando à atribuição. No entanto, isso depende da qualidade e especificidade dos relatórios carregados na TIP.

5. CONCLUSÃO E TRABALHOS FUTUROS

A integração de fontes de inteligência cibernética no contexto de sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM) demonstrou ser uma abordagem eficaz para melhorar a detecção e prevenção de ameaças cibernéticas avançadas. A pesquisa demonstrou que a combinação de diferentes fontes, como relatórios de Inteligência de Ameaças Cibernéticas (CTI) e Indicadores de Comprometimento (IoCs), proporcionou melhorias substanciais na capacidade de identificar padrões de ataque e correlacionar comportamentos maliciosos. No entanto, essa integração requer um esforço contínuo para garantir a qualidade, relevância e tempestividade dos dados coletados, a fim de maximizar sua eficácia.

O processo de enriquecimento de dados mostrou-se particularmente eficaz na detecção proativa de ameaças, especialmente ao correlacionar Táticas, Técnicas e Procedimentos (TTPs) com eventos de segurança. A pesquisa demonstrou que, ao adicionar camadas adicionais de contexto aos TTPs conhecidos, foi possível melhorar significativamente a precisão da detecção e acelerar as respostas a incidentes. No entanto, esse processo de enriquecimento ainda depende amplamente de intervenções manuais, sugerindo que pesquisas futuras devem focar na automação dessa etapa para aumentar a escalabilidade e eficiência do sistema.

Além disso, a análise dos IoCs mostrou-se eficaz na detecção de malware avançado, como o Agent Tesla, mas a volatilidade desses indicadores, como endereços IP e domínios, pode limitar sua utilidade a longo prazo. A pesquisa indicou que, para maximizar a eficiência de ferramentas como o Wazuh, é crucial que os IoCs sejam continuamente atualizados em tempo real para garantir sua tempestividade, e que os relatórios de segurança sejam criados e disponibilizados rapidamente para a comunidade de segurança.

Para trabalhos futuros, recomenda-se explorar métodos mais automatizados para integrar fontes de inteligência cibernética com sistemas SIEM, com foco particular na automação dos processos de enriquecimento, validação e correlação de dados. A automação dessas tarefas ajudará a garantir que a inteligência de ameaças permaneça oportuna e precisa, uma vez que a qualidade e autenticidade dos dados continuarão a desempenhar um papel fundamental na eficácia dos sistemas de detecção de ameaças; informações não confiáveis podem prejudicar significativamente as medidas de defesa proativas, levando a correlações imprecisas, falsos positivos ou falsos negativos. Além disso, o desenvolvimento de um framework universal de padronização para o compartilhamento de dados entre plataformas TIP e SIEM apresenta uma via promissora para futuras pesquisas.

Outra área que merece atenção é o uso de algoritmos de aprendizado de máquina para automatizar o processo de enriquecimento de dados, permitindo que modelos de inteligência artificial aprendam com grandes volumes de dados históricos de TTPs e forneçam insights em tempo real. Isso não só poderia melhorar a detecção de ameaças conhecidas, mas também antecipar ataques futuros, aprimorando a segurança preventiva.

Finalmente, é crucial desenvolver mecanismos mais dinâmicos e automatizados para atualização e correlação de IoCs. Ferramentas que monitoram continuamente a validade dos IoCs em tempo real e os correlacionam automaticamente com os logs do sistema, como o Wazuh, aumentarão as taxas de detecção de malware, especialmente quando combinadas com análise comportamental. Assim, pesquisas futuras podem focar na implementação de soluções que tornem esses processos mais ágeis, garantindo uma detecção de ameaças mais eficaz e escalável, ao mesmo tempo em que abordam o desafio de atribuição.

REFERÊNCIAS

Abu, M., Selamat, S., Ariffin, A., & Yusof, R., (2018). Cyber threat intelligence – issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10, pp. 371–379. [Online]. Available: https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A., (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers Security, vol. 132, p. 103352. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823002626

Aslan, A. & Samet, R., (2020). A comprehensive review on malware detection approaches. IEEE Access, vol. 8, pp. 6249–6271.

Filigran, (2024). Opencti documentation space. OpenCTI Documentation. Accessed on: August 24, 2024. [Online]. Available: https://docs.opencti.io/latest/

Ghafir, I., Kyriakopoulos, K. G., Lambotharan, S., Aparicio-Navarro, F. J., Assadhan, B., Binsalleeh, H., & Diab, D. M., (2019). Hidden markov models and alert correlations for the prediction of advanced persistent threats. IEEE Access, vol. 7, pp. 99508–99520.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R., (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. Sensors, vol. 21, no. 14. [Online]. Available: https://www.mdpi.com/1424-8220/21/14/4759

Hybrid Analysis, (2024). Public knowledge base. Free Automated Malware Analysis. Accessed on: October 5, 2024. [Online]. Available: https://www.hybrid-analysis.com/knowledge-base

Imperva, (2024). Advanced persistent threat (apt). Advanced persistent threat (APT). Accessed on: August 21, 2024. [Online]. Available: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., & Kim, H., (2024). Sharing cyber threat intelligence: Does it really help?

Leite, C., den Hartog, J., dos Santos, D. R., & Constante, E., (2023). Actionable cyber threat intelligence for automated incident response. Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavik, Iceland, November 30–December 2, 2022, Proceedings. Berlin, Heidelberg: Springer-Verlag, pp. 368–385. [Online]. Available: https://doi.org/10.1007/978-3-031-22295-5_20

Level Blue, (2024). The world's first truly open threat intelligence community. Level Blue - Open Threat Exchange. Accessed on: October 5, 2024. [Online]. Available: https://otx.alienvault.com

Mahboubi, A., Luong, K., Aboutorab, H. T., Bui, G., Jarrad, M., Bahutair, S., Camtepe, B., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H., (2024). Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications, vol. 232, p. 104004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804524001814

MalwareBazaar, (2024). Malwarebazaar database. MalwareBazaar by Abuse. Accessed on: August 24, 2024. [Online]. Available: https://bazaar.abuse.ch

MITRE ATT&CK, (2024). Matrix - enterprise. Enterprise Matrix. Accessed on: September 9, 2024. [Online]. Available: https://attack.mitre.org/matrices/enterprise/

Hartong, O., (2023). A sysmon configuration repository for everybody to customise. sysmon-modular. Accessed on: September 1, 2024. [Online]. Available: https://github.com/olafhartong/sysmon-modular

Sagar, S., (2018). Developing proactive cyber threat intelligence from the online hacker community: A computational design science approach. The University of Arizona. [Online]. Available: http://hdl.handle.net/10150/628454

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R., (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. The 13th International Conference on Wirtschaftsinformatik, pp. 837–851. [Online]. Available: https://wi2017.ch/images/wi2017-0188.pdf

Silva, A., (2020). Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto. Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília. [Online]. Available: https://repositorio.unb.br/handle/10482/40541

Tounsi, W. & Rais, H., (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers Security, vol. 72, pp. 212–233. [Online]. Available: https://doi.org/10.1016/j.cose.2017.09.001

VirusTotal, (2024). Reports. VTDoc. Accessed on: October 5, 2024. [Online]. Available: https://docs.virustotal.com/docs/results-reports

Wazuh, (2024). The open source security platform. Accessed on: August 25, 2024. [Online]. Available: https://wazuh.com

Wu, J., (2020). New approaches to cyber defense. Cyberspace mimic defense, [S.l.]: Springer, pp. 113–157.