DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM

Alexander André de Souza Vieira

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM

Alexander André de Souza Vieira

Orientador: Prof. Dr. João José Costa Gondim, FT/UnB

Publicação: PPEE.MP.085

Brasília - DF, MARÇO - 2025

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM

Alexander André de Souza Vieira

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. João José Costa Gondim, Dr., FT/UnB _____
Orientador

Prof. Robson de Oliveira Albuquerque, Dr., FT/UnB _____
Examinador Interno

Prof. Cristoffer Leite da Silva, Ph.D, TU/e _____
Examinador Externo

Prof. Fábio Lúcio Lopes de Mendonça, Dr., FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

VIEIRA, ALEXANDER ANDRÉ DE SOUZA
Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM [Distrito Federal] 2025.
xvi, 54 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Publicação: PPEE.MP.085
Departamento de Engenharia Elétrica

1. Inteligência de Ameaça Cibernética	2. Ameaças Persistentes Avançadas
3. Detecção de Ameaças	4. SIEM
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

VIEIRA, A. A. DE S. (2025). *Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM*. Dissertação de Mestrado ProfissionalPPEE.MP.085, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 54 p.

CESSÃO DE DIREITOS

AUTOR: Alexander André de Souza Vieira
TÍTULO: Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM.
GRAU: Mestre em Engenharia Elétrica ANO: 2025

Alexander André de Souza Vieira
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

AGRADECIMENTOS

Gostaria de agradecer imensamente ao meu orientador, Prof. Dr. João Gondim, que sempre esteve disposto a ajudar, e tornou todo esse processo acadêmico mais com suas orientações descontraídas.

Agradeço à minha esposa, Antonia Taiza, por me apoiar nos momentos difíceis, incentivar o crescimento e evolução constante, além de lidar com inúmeras variações de humor decorrentes dos prazos a serem cumpridos.

Agradeço aos meus familiares, especialmente à minha mãe e irmã, por me proporcionarem o apoio e a estrutura que tornaram possível o meu desenvolvimento educacional.

Agradeço também aos meus amigos, que iniciaram essa trajetória antes de mim e me incentivaram a realizar o curso de mestrado.

Por fim, expresso minha gratidão a todos aqueles que, de forma direta ou indireta, caminharam ao meu lado e, de alguma forma, influenciaram no desenvolvimento deste trabalho.

RESUMO

As ameaças cibernéticas evoluíram a ponto de superar as táticas de segurança tradicionais, impulsionadas por tecnologias cada vez mais sofisticadas e adversários avançados, como as Ameaças Persistentes Avançadas (*APTs*). Para enfrentar esses desafios, este trabalho propõe uma metodologia integrativa que aprimora a detecção de ameaças, combinando Inteligência de Ameaça Cibernética (*CTI*) de alta qualidade através do enriquecimento de dados de inteligência, identificação de Táticas, Técnicas e Procedimentos (*TTPs*) e análise centralizada de eventos. Um diferencial desta pesquisa é o "*Toolkit* para Análise e Correlacionamento de *TTPs*", desenvolvido para automatizar a correlação entre indicadores (*IoCs*), relatórios de *CTI* e registros de sistemas de monitoramento, tornando o processo de investigação mais ágil e reduzindo o tempo de resposta a incidentes. A eficácia da proposta foi validada com amostras reais de *malware*, evidenciando a importância de relatórios de segurança atualizados, do enriquecimento de dados e da rápida integração das informações para alcançar maior eficiência na detecção e mitigação de ameaças.

ABSTRACT

Cyber threats have evolved evolved and surpassed traditional security tactics, propelled by increasingly sophisticated technologies and advanced adversaries, such as Advanced Persistent Threats (APTs). To address these challenges, this work proposes an integrative methodology that enhances threat detection by combining high-quality Cyber Threat Intelligence (CTI) through data enrichment, the identification of Tactics, Techniques, and Procedures (TTPs), and centralized event analysis. A key differentiator of this research is the "Toolkit for TTP Analysis and Correlation," developed to automate the correlation among Indicators of Compromise (IoCs), CTI reports, and monitoring system logs, making the investigation process more agile and reducing incident response times. The effectiveness of the proposed approach was validated through real malware samples, underscoring the importance of timely security reports, data enrichment, and rapid information integration to achieve greater efficiency in threat detection and mitigation.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

AI	*Artificial Intelligence*.
APT	*Advanced Persistent Threat*.
C2	*Command and Control*.
CDB	*Constant Database*.
CIF	*Collective Intelligence Framework*.
CRITs	*Collaborative Research into Threats*.
CSV	*Comma-separated Value*.
CTI	*Cyber Threat Intelligence*.
CVE	*Common Vulnerabilities and Exposures*.
CybOX	*Cyber Observable eXpression*.
EDR	*Endpoint Detection and Response*.
ELK	*Elasticsearch, Logstash, Kibana*.
HMM	*Hidden Markov Model*.
IDS	*Intrusion Detection System*.
IoA	*Indicator of Attack*.
IoC	*Indicator of Compromise*.
IP	*Internet Protocol*.
LotL	*Living-off-the-Land*.
MISP	*Malware Information Sharing Platform*.
ML	*Machine Learning*.
PDF	*Portable Document Format*.
RaaS	*Ransomware-as-a-Service*.
RAT	*Remote Access Trojan*.
SIEM	*Security Information and Event Management*.
STIX	*Structured Threat Information eXpression*.
TAXII	*Trusted Automated Exchange of Intelligence Information*.
TIP	*Threat Intelligence Platform*.
TISP	*Threat Intelligence Sharing Platform*.
TTP	*Tactics, Techniques, and Procedures*.
TXT	*Text*.
XDR	*Extended Detection and Response*.

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 [6].

Os ataques cibernéticos evoluíram significativamente ao longo dos anos. No passado, os ataques eram geralmente realizados de maneira direta e utilizavam técnicas relativamente simples. Ferramentas baseadas em assinaturas, conseguiam identificá-los de maneira rápida e eficaz, pois se baseavam em malwares já conhecidos [7]. Contudo, com o surgimento de ameaças mais complexas, como as Ameaças Persistentes Avançadas (*APTs*), os atacantes passaram a empregar técnicas avançadas e encobertas. As *APTs* são ataques cibernéticos sofisticados, realizados de forma direcionada e prolongada, em que invasores se mantêm ocultos por longos períodos dentro de uma rede ou sistema. Geralmente, visam a obtenção de dados sensíveis ou causarem danos de grande impacto [8], [9], empregando técnicas avançadas de evasão e persistência.

As abordagens tradicionais de detecção são baseadas em assinaturas, focando essencialmente em ameaças previamente conhecidas e em *IoCs* (Indicadores de Comprometimento). Embora úteis para identificar variantes já catalogadas, essas estratégias tornam-se insuficientes contra *APTs* que modificam continuamente sua infraestrutura (por exemplo, alterando domínios de comando e controle) e operam por meio de Táticas, Técnicas e Procedimentos (*TTPs*) dinâmicos. Esse tipo de ameaça exige, portanto, uma abordagem que inclua também a análise de comportamento e contexto, em vez de depender somente de assinaturas estáticas.

Em resposta a isso, as plataformas de inteligência de ameaças cibernéticas (*Threat Intelligence Platforms - TIPs*) surgiram, utilizando a inteligência de ameaça cibernética *(Cyber Threat Intelligence - CTI)* para aprimorar a detecção, prevenção e resposta aos ataques. Segundo Huff et al. [10], a *CTI* é um conhecimento acionável e baseado em evidências sobre ameaças cibernéticas, sendo considerado fundamental para a integração de medidas defensivas nas operações de segurança. Essa inteligência pode ser usada para identificar padrões, antecipar ataques e implementar medidas de defesa mais eficazes [11].

Além disso, para que a *CTI* seja eficaz, ela deve atender a vários princípios fundamentais. Deve ser oportuna, fornecida rapidamente para permitir uma resposta eficiente; 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 [12].

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 [4]. Embora existam padrões abertos amplamente utilizados (por exemplo, *STIX* e *TAXII*) para representar e compartilhar dados de ameaças, muitos provedores de inteligência não seguem integralmente essas normas ou não fornecem docu-

mentação adequada. Outro problema está vinculado quanto à análise dos dados feita por parte das pessoas que irão consumi-lo, o qual muitas vezes não é devidamente realizado. Isso acaba gerando inconsistências, dificultando a integração das informações e comprometendo a qualidade e a utilidade da inteligência produzida pelas plataformas de *Threat Intelligence*. Além disso, muitas ferramentas *TIP* concentram-se predominantemente na fase de coleta de dados, negligenciando as etapas subsequentes de análise e disseminação [13]. 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.

Embora as plataformas de inteligência de ameaças cibernéticas sejam fundamentais no compartilhamento de inteligência, muitos sistemas de defesa ainda enfrentam desafios na correlação eficiente dessas informações com os eventos de segurança em tempo real. Além disso, a dependência excessiva de *feeds* de *IoCs*, pode comprometer a detecção de ataques avançados, pelo fato de possuírem um ciclo de vida relativamente curto.

Um dos maiores desafios na aplicação prática da *CTI* está na integração dessas informações em plataformas de monitoramento, como os sistemas *SIEM (Security Information and Event Management)*, de forma que possibilite a correlação automática entre eventos e *TTPs*. Sem essa integração, uma vez que a maioria das abordagens atua de forma reativa, focando somente no uso de *IoCs* ou assinaturas, a inteligência gerada pode não ser aplicada de maneira eficiente para aprimorar a detecção e resposta a incidentes.

Diante desse cenário, torna-se necessário adotar uma abordagem que vá além da simples coleta e análise de dados, permitindo a correlação automática de eventos de segurança com *TTPs* para uma detecção mais eficaz de ameaças avançadas. Assim, este trabalho propõe uma metodologia integrativa que aprimora a detecção e prevenção de ameaças cibernéticas, utilizando a correlação entre eventos de segurança e *TTPs*, baseada no framework *MITRE ATT&CK*. Para validar essa abordagem, será realizado um estudo de caso utilizando amostras reais de malware e ferramentas como *OpenCTI* e *Wazuh*.

Além disso, durante a pesquisa, foi identificada a necessidade de fornecer aos analistas de segurança uma ferramenta que facilitasse a busca e a interpretação de evidências maliciosas no ambiente. Como parte fundamental dessa proposta, desenvolveu-se o "*Toolkit* para Análise e Correlacionamento de *TTPs*", que se destaca como uma solução prática para acelerar o processo de detecção de incidentes e reduzir a sobrecarga manual na investigação de comportamentos suspeitos. Este *Toolkit* é capaz de coletar dados de diferentes fontes de inteligência e correlacioná-los com os logs de segurança, além de mapear as *TTPs* observadas em eventos de segurança, facilitando o processo de identificação de adversários e agilizando a pesquisa de incidentes; ao automatizar grande parte do trabalho de correlação, que frequentemente consome tempo excessivo dos analistas.

Esta dissertação descreve a aplicação prática dessa metodologia, bem como os resultados alcançados na detecção e contenção de amostras de malware reais. Os experimentos apontam que a detecção por *TTPs*, combinada a uma plataforma de monitoramento e a dados robustos de *CTI*, fornece bases mais sólidas para uma possível resposta a incidentes e identificação de um ator malicioso.

1.1 MOTIVAÇÃO

Os desafios na área de segurança cibernética têm se tornado cada vez mais complexos devido à evolução das técnicas de ataque e ao aumento da sofisticação das ameaças. As Ameaças Persistentes Avançadas (*APTs*) representam um risco significativo para organizações, pois empregam métodos furtivos, técnicas avançadas de evasão e ataques prolongados dentro das redes comprometidas. Embora as abordagens convencionais baseadas em assinaturas e Indicadores de Comprometimento sejam eficazes contra ameaças conhecidas, elas se mostram menos eficientes diante de *APTs*, as quais modificam continuamente sua infraestrutura e comportamento. Para lidar com esse cenário dinâmico, torna-se fundamental observar também Táticas, Técnicas e Procedimentos adotados pelos adversários, pois essas informações vão além dos indicadores estáticos e permitem uma detecção mais contextualizada.

Diante desse cenário, as plataformas de inteligência de ameaças cibernéticas (*Threat Intelligence Platforms - TIPs*) foram desenvolvidas para aprimorar a coleta, análise e compartilhamento de inteligência sobre ameaças. No entanto, grande parte dessas plataformas ainda enfrenta dificuldades na integração com sistemas de monitoramento em tempo real, como os *SIEMs*, limitando sua capacidade de fornecer insights acionáveis para a defesa cibernética e um dos desafios críticos enfrentados pelas organizações é a falta de correlação eficiente entre eventos de segurança e os *TTPs* adversários, o que impacta diretamente a capacidade de detecção e resposta a incidentes cibernéticos.

Atualmente, a maioria dos *SIEMs* e ferramentas de monitoramento ainda depende predominantemente de regras baseadas em assinaturas ou *IoCs*, que possuem um ciclo de vida curto e são rapidamente modificados por adversários para evitar detecção. Como consequência, os analistas de segurança enfrentam altos volumes de falsos positivos e dificuldades na identificação de ameaças emergentes, o que compromete a eficiência das operações de defesa cibernética [4]. Para que a inteligência de ameaças seja realmente eficaz, é necessário que ela seja integrada de maneira automatizada aos sistemas de detecção, possibilitando a correlação dinâmica entre eventos monitorados e os padrões de ataque conhecidos. Entretando, é necessário que essa integração seja realizada observando questões específicas, voltada ao modelo de ingestão e consumo de *CTI*, uma vez que o consumo de dados imprecisos, pode nos gerar um *dataset* de baixa qualidade.

Diante disso, a motivação central deste trabalho consiste em desenvolver e validar uma abordagem que, além de integrar dados de *CTI* a um sistema de monitoramento, ofereça um modo ágil de correlacionar *TTPs* e *IoCs*, ampliando a visão do analista sobre potenciais ameaças. Para atender a essa necessidade, propõe-se uma metodologia integrativa que reduz a dependência exclusiva de *IoCs*, melhora a precisão da detecção e minimiza falsos positivos por meio da automação do processo de análise e do enriquecimento da inteligência em plataformas *TIPs* e *SIEMs*. Com base nessa proposta, desenvolveu-se o *Toolkit* para Análise e Correlacionamento de *TTPs*, peça-chave para suprir a falta de ferramentas que, de modo simples e rápido, permitam ao analista localizar no ambiente as evidências mais relevantes de atividade maliciosa. Por fim, para demonstrar a eficácia da metodologia, apresenta-se um estudo de caso prático no qual amostras reais de malware são analisadas em um ambiente de testes que utiliza ferramentas como *OpenCTI* e *Wazuh*.

Dessa forma, este estudo busca contribuir para o aprimoramento da detecção e resposta a incidentes cibernéticos, proporcionando um modelo mais eficiente para a integração de *Cyber Threat Intelligence*

(CTI) em sistemas de monitoramento e defesa.

1.2 OBJETIVOS

Com base no contexto apresentado, o objetivo geral deste trabalho é propor e validar uma metodologia integrativa para aprimorar a detecção e prevenção de ameaças cibernéticas, utilizando *Cyber Threat Intelligence (CTI)* e a correlação automatizada de eventos de segurança com Táticas, Técnicas e Procedimentos, conforme o framework *MITRE ATT&CK*.

Para atingir esse objetivo, os seguintes objetivos específicos são estabelecidos:

- Investigar a integração de fontes de *CTI* em plataformas de monitoramento para aprimorar a detecção de ameaças avançadas.
- Desenvolver um modelo de enriquecimento de inteligência que possibilite a correlação dinâmica entre eventos de segurança e *TTPs*, reduzindo a dependência exclusiva de Indicadores de Comprometimento.
- Avaliar a eficiência da metodologia proposta por meio de um estudo de caso baseado na análise de amostras reais de *malware*.
- Automatizar processos de detecção e correlação, diminuindo a necessidade de intervenção manual e aprimorando a resposta a incidentes.

Dessa forma, este estudo busca responder às seguintes perguntas de pesquisa:

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

PP2. Até que ponto a detecção 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?

Além disso, este trabalho se baseia no processo metodológico proposto por Leite et. al [14], adaptando-o para um contexto mais abrangente, onde múltiplas fontes de inteligência são integradas a plataformas de monitoramento e resposta a incidentes. Essa adaptação busca melhorar a eficácia da correlação de eventos com *TTPs* e a automação do processo de análise de ameaças.

1.3 CONTRIBUIÇÃO DO TRABALHO

Este trabalho contribui para a área de inteligência de ameaça cibernética ao propor uma metodologia integrativa que aprimora a detecção e prevenção de ameaças cibernéticas por meio da correlação estruturada

entre eventos de segurança e TTPs. Suas principais contribuições são:

1. Correlação aprimorada entre *TTPs* e eventos de segurança: Utilização de regras e padrões extraídos do framework *MITRE ATT&CK* para enriquecer os eventos monitorados, melhorando a capacidade de identificação de ameaças.
2. Enriquecimento da *CTI* com fontes de dados diversificadas: Integração de fontes de inteligência de ameaças, incluindo relatórios de segurança, feeds públicos de *IoCs* e informações extraídas de plataformas *OpenCTI* e *SIEM*.
3. Validação prática da metodologia: Aplicação do modelo em um ambiente de testes controlado, utilizando amostras reais de malware para avaliar a eficácia da detecção.
4. Automação do processo de análise de ameaças: Redução da necessidade de intervenção manual na triagem de eventos e alertas, tornando a detecção mais eficiente e escalável.

Com o desenvolvimento deste trabalho, e das contribuições descritas acima, foram gerados dois artigos científicos, sendo um [15] já apresentado e publicado na 11ª Conferência Ibero-Americana Computação Aplicada (CIACA 2024).

- VIEIRA, A. A. de S. e; GONDIM, J. J. C., 2024, "Metodologia Integrativa Para a Detecção e Prevenção de Ameaças Utilizando Inteligência de Ameaça Cibernética e SIEM", Atas das Conferências Ibero-Americanas COMPUTAÇÃO APLICADA e WWW/INTERNET. : Iadis (International Association For Development Of The Information Society), 2024, Vol. 11, pp. 57-65.

E o segundo artigo já aceito, intitulado "*Methodology for Threat Detection and Prevention Integrating Cyber Threat Intelligence and SIEM*", em fase de apresentação e publicação na *13rd World Conference on Information Systems and Technologies (WorldCIST 2025)*.

Para apoio ao processo e correlacionamento de dados em algumas fases da metodologia, foi desenvolvido um programa de computador, intitulado "Toolkit para Análise e Correlacionamento de TTPs", que atualmente se encontra em fase de registro junto à Universidade de Brasília.

1.4 ESTRUTURA DO TRABALHO

Esse trabalho está organizado em 5 capítulos, sendo este de introdução, que apresenta o contexto da pesquisa, incluindo a motivação, os objetivos e as contribuições do trabalho, bem como destacando o desenvolvimento do “Toolkit para Análise e Correlacionamento de TTPs”, o primeiro. O restante está organizado da seguinte forma:

O Capítulo 2 de referencial teórico explora conceitos fundamentais da Inteligência de Ameaças Cibernéticas, Indicadores de Comprometimento, táticas, técnicas e procedimentos, além de abordar os principais desafios enfrentados na detecção e prevenção de ameaças.

O Capítulo 3 descreve a Descreve a estrutura metodológica adotada, incluindo as etapas de coleta, enriquecimento, correlação e resposta, além de elucidar os elementos técnicos do ambiente de testes.

O Capítulo 4 foca no estudo de caso com amostras reais de *malware*, validando a abordagem e destacando o papel do *Toolkit* na correlação de *TTPs*.

O Capítulo 5, resume as principais descobertas, apresenta reflexões sobre as limitações e propõe direções para pesquisas futuras, inclusive sugestões de aperfeiçoamento da ferramenta desenvolvida.

2 REFERENCIAL TEORICO

Neste capítulo, são apresentados os conceitos fundamentais que embasam este estudo, fornecendo uma visão geral dos principais temas relacionados à segurança cibernética e à inteligência de ameaças. Inicialmente, a Seção 2.1 aborda a evolução das ameaças cibernéticas, discutindo tópicos como Indicadores de Comprometimento, inteligência de ameaça cibernética, ameaças persistentes avançadas, entre outros. Em seguida, a Seção 2.2 revisa os principais trabalhos correlatos, destacando metodologias e abordagens utilizadas na literatura para a identificação e mitigação de ameaças cibernéticas. Essa fundamentação teórica é essencial para contextualizar a proposta deste trabalho e evidenciar sua contribuição para a área.

2.1 CONCEITOS RELACIONADOS

Nesta sessão, é apresentada um pouco da história das ameaças cibernéticas, e são explorados alguns conceitos base, que servem como pilares de todo o trabalho desenvolvido.

2.1.1 Evolução do Cenário de Ameaças

De acordo com Ferdous et. al [1], e representado pela Figura 2.1 a história da evolução dos malwares pode ser dividida em cinco estágios, cada um representando avanços importantes em termos de complexidade e impacto. A primeira geração, que abrange os anos 1970 e 1980, foi marcada pelo surgimento dos primeiros exemplos de vírus e *worms* simples, que introduziram o conceito de autorreplicação. Na segunda geração, entre o final dos anos 1980 e meados dos anos 1990, os *malwares* começaram a fazer uso de *scripts* e macros para atacar sistemas.

O período de meados dos anos 1990 até o final da década de 2000, correspondente à terceira geração, e foi marcado pelo surgimento dos chamados *network worms*, que exploravam vulnerabilidades de rede para se disseminar rapidamente, sendo o *'ILOVEYOU'* [16] um dos casos mais emblemáticos do período. Já na quarta geração, ao longo dos anos 2000 e 2010, surgiram ameaças mais complexas, como *trojans, rootkits e ransomwares*. E com a emergência das criptomoedas em 2009, com a disponibilização do Bitcoin, houve um incremento no número desse tipo de ataque devido a facilidade da anonimização na coleta de resgates [17], onde por exemplo o *CryptoLocker* em 2013 foi o primeiro *malware* a requisitar o pagamento em Bitcoin[18].

A quinta e atual geração de malwares, iniciada em 2010, destaca-se pela sofisticação e inovação, empregando técnicas como polimorfismo, exploração de vulnerabilidades, uso avançado de criptografia e estratégias como o *living-off-the-land (LotL)*[19]. Além disso, o ransomware tornou-se central nessa evolução, com avanços desde o *CryptoLocker* em 2013 até ataques devastadores como *WannaCry* e *NotPetya*. Mais recentemente, o surgimento do *Ransomware-as-a-Service (RaaS)*, usado por grupos como *Ryuk, Conti* e *Revil*, ampliou a escala e o impacto das ameaças, combinando táticas de extorsão sofisticadas. A pandemia de Covid-19 também impulsionou ataques massivos contra infraestruturas críticas, como o incidente

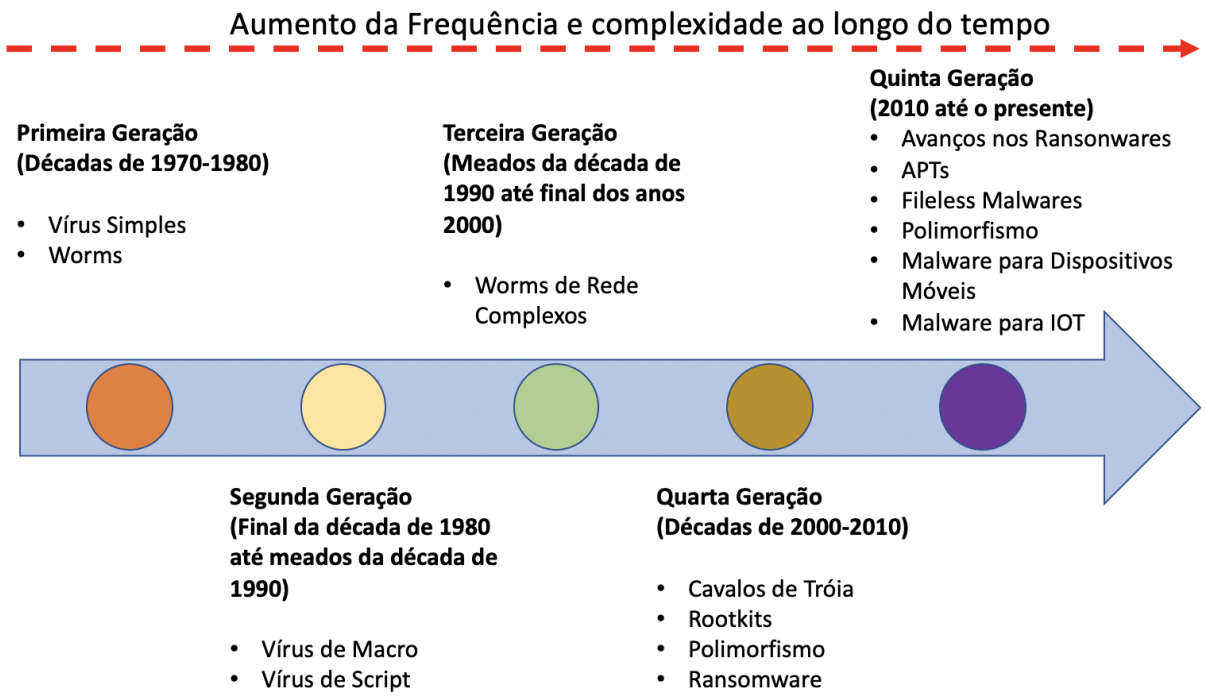


Figura 2.1: Evolução dos Malwares ao longo do Tempo - Adaptado de [1]

da *Colonial Pipeline* [20], onde um ataque de ransomware forçou o desligamento temporário de uma das principais redes de gasodutos dos Estados Unidos, causando escassez de combustível e destacando a vulnerabilidade de sistemas essenciais a ameaças cibernéticas.

Nesse cenário, as Ameaças Persistentes Avançadas (*APTs*) desempenham um papel crítico, com exemplos notáveis como o *Stuxnet* [21], que em 2010 sabotou o programa nuclear iraniano, e a campanha *SolarWinds* [22], conduzida pelo *APT29* em 2020, comprometendo cadeias de suprimentos. O crescimento do uso de dispositivos móveis e de *IoT* também ampliaran a superfície de ataque, com ameaças como *FluBot* e *Mirai botnet* expondo vulnerabilidades nesses ambientes. Avanços recentes, como o malware *BlackMamba*, que utiliza inteligência artificial generativa, sinalizam uma crescente complexidade, exigindo contramedidas inovadoras e eficientes.

2.1.2 Indicadores de Comprometimento

Indicadores de Comprometimento, do inglês *Indicators of Compromise (IoCs)* são evidências digitais que sinalizam a possível ocorrência de uma violação de segurança em sistemas, redes ou dispositivos [23]. Esses artefatos são elementos objetivos que apontam para ações de um invasor, auxiliando tanto na identificação de incidentes em andamento quanto na análise retrospectiva de ataques, e permitem que profissionais de segurança cibernética detectem, investiguem e respondam a atividades maliciosas.

Os *IoCs* podem assumir diferentes formas, dependendo da natureza do incidente. Alguns exemplos são endereços *IP* envolvidos na realização de ataques, hashes de arquivos maliciosos, *URLs* de sites comprometidos, registros de logs que indiquem comportamento anômalo ou suspeito, e até mesmo padrões específicos associados a atividades maliciosas, como strings de texto encontradas em malwares. Esses

indicadores são amplamente utilizados em ferramentas de segurança, como sistemas de monitoramento, soluções de detecção de intrusão (*IDS*) e plataformas de inteligência contra ameaças (*Threat Intelligence Platforms*).

O uso de *IoCs* permite a criação de regras de segurança específicas que ajudam a identificar padrões conhecidos de ameaças. Por exemplo, ao se detectar um hash de arquivo que corresponde a um malware previamente identificado, é possível bloquear a execução desse arquivo antes que cause danos. Além disso, *IoCs* são cruciais na correlação de eventos em sistemas como *SIEMs*, que agregam dados de diferentes fontes para identificar atividades suspeitas.

Apesar de sua utilidade, os *IoCs* enfrentam limitações. Eles são frequentemente reativos, baseando-se em ameaças previamente detectadas e documentadas, o que significa que novas variantes de malware ou técnicas inéditas de ataque podem não ser detectadas se não houver um *IoC* correspondente. Além disso, muitas vezes podem possuir um ciclo de vida curto[24], e adversários sofisticados podem ofuscar ou alterar seus métodos, reduzindo a eficácia de *IoCs* baseados em artefatos estáticos, como endereços *IP* ou *hashes*.

Na tentativa de desenvolver métodos mais proativos, abordagens mais recentes buscam integrar os *IoCs* com outras estratégias, como Indicadores de Ataque (*IoAs*), que também levam em consideração os comportamentos técnicas dos invasores, em vez de artefatos específicos.

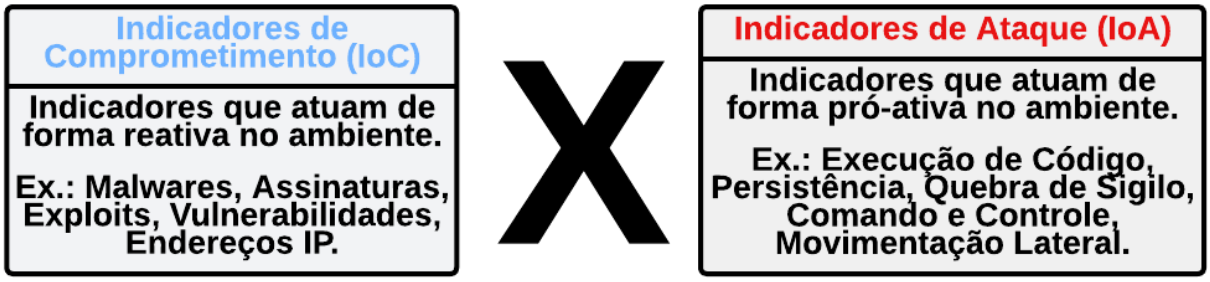


Figura 2.2: IoC versus IoA - Adaptado de [2]

2.1.3 Inteligência de Ameaça Cibernética

O processo de coleta, processamento, análise, implementação e disseminação de informações sobre ameaças, é o que define a inteligência de ameaça cibernética (*Cyber Threat Intelligence)*[25]. A execução desse processo visa transformar dados brutos de segurança em informações acionáveis, permitindo que organizações antecipem, detectem e respondam a ataques com maior eficiência, ao fornecer uma compreensão contextualizada das ameaças, incluindo suas motivações, capacidades e comportamentos.

De acordo com o Centro Nacional de Cybersegurança Britânico[26], a inteligência de ameaça cibernética é geralmente organizada em três níveis principais: estratégico, operacional e tático. Em alguns casos, considera-se um quarto nível, o técnico, embora este seja frequentemente incorporado ao nível tático devido à sua natureza prática. Cada nível segue o ciclo de vida da *CTI* de maneira distinta, atendendo diferentes públicos e objetivos.

A inteligência estratégica foca em fornecer uma visão de alto nível sobre ameaças, ajudando as lideranças a tomar decisões informadas e integrá-las aos processos de gestão de riscos e recursos. Fontes comuns

incluem análises geopolíticas e publicações setoriais. Já a inteligência operacional, ao mapear agentes de ameaça e possíveis ataques, orienta os gestores de segurança na alocação de recursos e melhora a eficácia da resposta a incidentes.

Além do nível operacional, a inteligência tática e técnica atuam diretamente na adaptação das defesas contra ameaças específicas. A inteligência tática aborda as Táticas, Técnicas e Procedimentos utilizados por agentes de ameaça, ajudando equipes de defesa a ajustar suas estratégias com base em práticas recentes, como o uso de ferramentas para extrair e reutilizar credenciais. Por sua vez, a inteligência técnica consiste em dados automatizados, como listas de *IPs* maliciosos e *hashes*, que têm curta validade e precisam ser rapidamente integrados aos sistemas de segurança para bloquear conexões suspeitas.

Dessa forma, a inteligência tática permite ajustar estratégias defensivas com base nas *TTPs* dos adversários, enquanto a inteligência técnica fornece dados acionáveis para mitigar ameaças em tempo real. Ambas desempenham papéis essenciais para uma proteção eficaz.

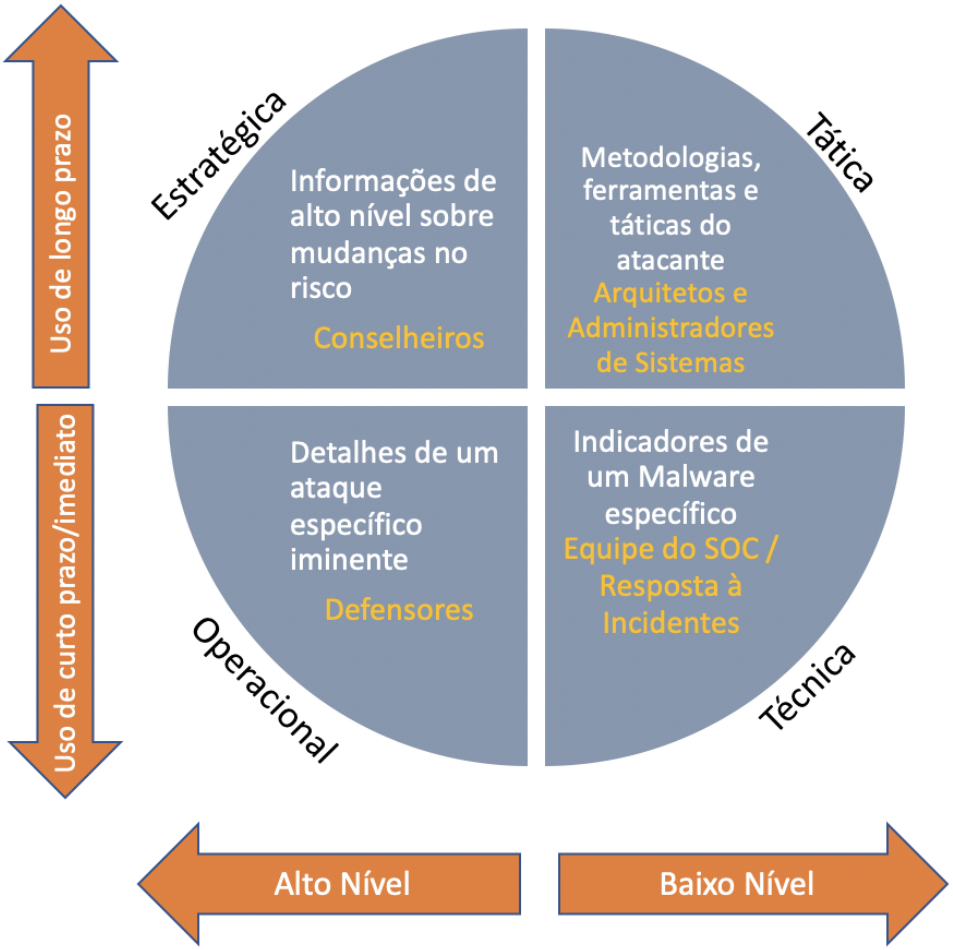


Figura 2.3: Tipos de Inteligência de Ameaça Cibernética - Adaptado de [3]

De acordo com Silva et. al [27], não há uma definição clara do que qualifica uma *CTI*, mas algumas características são amplamente citadas entre a comunidade acadêmica, sendo elas:

- Oportuna: onde têm-se uma correlação entre a origem de um avento e o tempo de reação, ou do uso

de determinada informação, de forma que a interligência deve ser fornecida rapidamente para uma resposta eficaz;

- Relevante: indicando a relação da informação com os serviços da organização e dispositivos da rede, ou seja, contextualizada para o ambiente de uma organização, para que a informação possa ser aplicada de forma prática;
- Abrangente/Completa: descrevendo um incidente de forma extremamente detalhada;
- Clara/Exata: através de informações padronizadas e estruturadas, que melhoram o tempo de resposta a um incidente.

2.1.4 Ciclo de Produção de Inteligência

O ciclo de produção inteligência descreve um conjunto de etapas estruturadas para converter dados brutos em conhecimento acionável, apoiando a tomada de decisões de forma proativa. Embora diversas referências utilizem terminologias ligeiramente diferentes, o presente trabalho adota as cinco etapas a seguir, que se adequam às necessidades específicas da Inteligência de Ameaça Cibernética:

- Coleta - A fase de coleta abrange a extração e junção de dados provenientes de múltiplas fontes, internas ou externas. Do ponto de vista cibernético, exemplos típicos incluem logs de sistemas de detecção de intrusão (*IDS*), repositórios de *malware* e plataformas públicas de *CTI*. Nessa etapa, os elementos obtidos ainda são essencialmente fatos ou indicadores (por exemplo, endereços *IP* maliciosos, *hashes* de arquivos suspeitos, domínios associados a *phishing*). A principal preocupação recai sobre a abrangência e qualidade do conjunto coletado, de modo que ele reflita efetivamente o escopo e os objetivos pré-definidos para a investigação.
- Processamento - Tendo-se um corpo inicial de dados, procede-se à formatação e combinação dos registros de modo a torná-los coerentes e prontos para uso. Esse passo pode incluir a conversão de diferentes formatos (*CSV, JSON, STIX*, entre outros), a remoção de duplicidades e a aplicação de filtros ou técnicas de enriquecimento (por exemplo, consultas de reputação a serviços externos). O objetivo principal é responder a perguntas específicas que orientarão as fases seguintes, convertendo dados dispersos em informações dotadas de estrutura e contexto.
- Análise - Na terceira fase, o enfoque recai sobre a avaliação conjunta desses dados e informações para descobrir padrões, inferir tendências ou relacionar dados a atores de ameaça específicos. Nessa etapa, especialistas em segurança ou algoritmos de correlação comportamental podem identificar Táticas, Técnicas e Procedimentos recorrentes, campanhas ativas e vulnerabilidades mais prováveis de exploração. Além disso, é nessa fase que a informação processada se transforma efetivamente em inteligência acionável, uma vez que as observações são interpretadas de forma a orientar decisões práticas.
- Implantação - De posse da inteligência obtida, pode-se implantá-la diretamente em sistemas de defesa ou políticas de segurança, assegurando uma reação mais proativa contra potenciais ameaças.

Exemplos incluem atualizar listas de bloqueio em *firewalls*, reconfigurar regras de *SIEM* para priorizar certos alertas ou mesmo acionar equipes de resposta a incidentes. O enfoque dessa etapa está na capacidade de aplicar o conhecimento produzido, reduzindo a janela de exposição aos ataques e servindo como contramedida tangível baseada em evidências.

- Disseminação - Por fim, o conhecimento consolidado é expandido por meio do compartilhamento sistemático com as partes interessadas. Em organizações, tal difusão ocorre por meio de relatórios executivos, informes técnicos, treinamentos internos ou mesmo integrações de *feeds* de inteligência com outras plataformas corporativas. Já em comunidades acadêmicas ou de pesquisa, ocorre a publicação de estudos de caso, artigos científicos e relatórios abertos. A disseminação, portanto, garante que a inteligência gerada transcenda o âmbito imediato de um projeto ou setor e promova a colaboração no ecossistema de cibersegurança.

A adoção dessas cinco etapas possibilita uma visão progressiva que vai do dado bruto (coletado em diferentes fontes) à inteligência efetivamente utilizada para proteção proativa e tomada de decisão. Cada uma dessas fases reforça a necessidade de critérios de confiabilidade e relevância ao incorporar novas fontes, bem como a importância de processar e analisar dados de modo consistente antes de se chegar a recomendações práticas. A representação do fluxo do processo de producão de inteligência de ameaças, pode ser observado na Fig. 2.4.

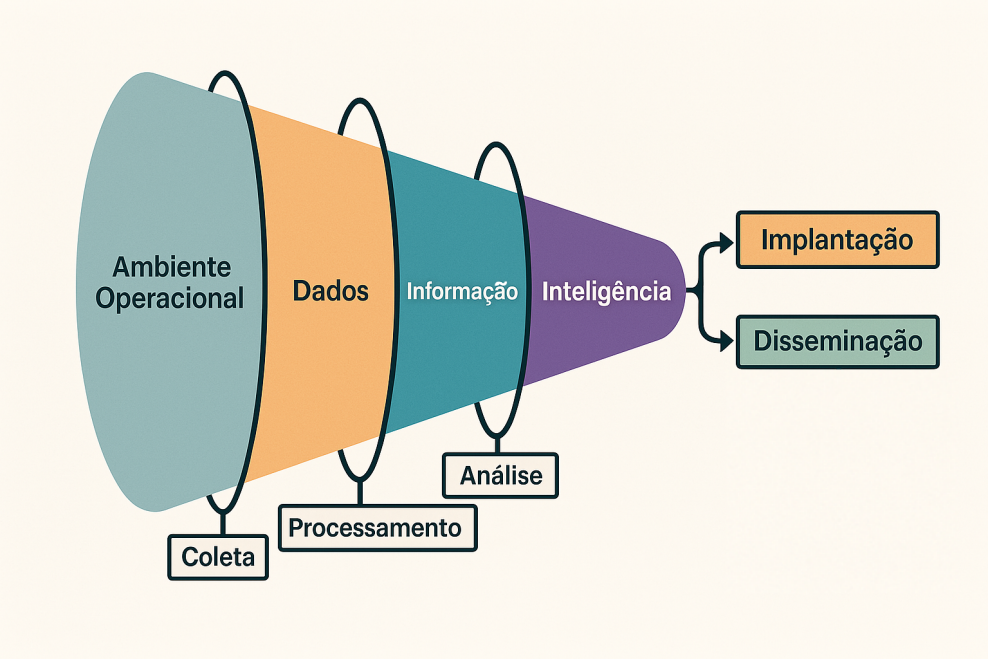


Figura 2.4: Fluxo do Processo de Produção de Inteligência de Ameaças, adaptado de [4]

2.1.5 Plataformas de Compartilhamento de Ameaças

As plataformas de compartilhamento de ameaças, conhecidas como *Threat Intelligence Sharing Platforms (TISPs)*, desempenham um papel crucial na coleta, análise e disseminação de informações sobre ameaças cibernéticas. Essas plataformas integram dados provenientes de múltiplas fontes, como *feeds* de

inteligência, relatórios de segurança e sistemas de monitoramento, enriquecendo essas informações para transformá-las em inteligência acionável. A principal vantagem dessas plataformas é a capacidade de consolidar, processar e compartilhar informações estruturadas sobre ameaças, permitindo uma resposta mais eficaz contra ataques cibernéticos.

Atualmente, apesar da ampla produção de inteligência cibernética em padrões de dados populares como o *CybOX*, *STIX* ou *TAXII*, há ao menos oito padrões distintos utilizados pela comunidade cibernética [4]. Para que os dados obtidos através de compartilhamentos possam auxiliar na detecção, identificação, validação e investigação de potenciais ataques ou ameaças, eles devem ser oriundos de fontes confiáveis [28]. A variabilidade na qualidade das informações compartilhadas e a falta de padronização entre diferentes ferramentas são desafios constantes, dificultando a interoperabilidade entre sistemas e impactando a eficácia da inteligência gerada.

A dissertação de Silva [4] apresenta uma análise comparativa detalhada de diversas plataformas de *CTI (Cyber Threat Intelligence)*, avaliando suas capacidades em termos de arquitetura, compatibilidade com padrões de inteligência, mecanismos de correlação e integração com outros sistemas. Entre as ferramentas analisadas, destacam-se *MISP*, *OpenCTI*, *CRITs*, *CIF* e *Anomali STAXX*, cada uma com abordagens distintas no tratamento de inteligência de ameaças.

O *MISP (Malware Information Sharing Platform)* é amplamente utilizado para coleta, agregação e compartilhamento de indicadores de comprometimento. Ele permite que diferentes entidades colaborem na troca de informações sobre ameaças de forma estruturada, sendo especialmente útil para equipes de resposta a incidentes. Sua compatibilidade com *STIX*, *OpenIOC* e *CSV*, aliada à sua facilidade de integração com *SIEMs* e outras ferramentas de defesa cibernética, torna-o um dos sistemas mais eficientes para a disseminação rápida de indicadores técnicos. No entanto, sua abordagem é fortemente centrada em IoCs, o que limita sua capacidade de modelagem de ameaças mais complexas, dificultando a análise contextual e a correlação de campanhas adversárias.

O *OpenCTI (Open Cyber Threat Intelligence)*, por sua vez, foi desenvolvido com um foco mais abrangente, permitindo não apenas o compartilhamento de inteligência, mas também a modelagem de ameaças e a análise contextual de campanhas maliciosas. Diferente do *MISP*, que se concentra na distribuição de *IoCs*, o *OpenCTI* permite representar adversários, grupos *APT*, campanhas e técnicas do *MITRE ATT&CK*, facilitando uma compreensão mais profunda do comportamento dos atacantes. Além disso, sua interface gráfica avançada possibilita a visualização interativa de ameaças e a correlação entre diferentes eventos e entidades, tornando-se uma ferramenta mais robusta para investigações aprofundadas. Entretanto, seu foco analítico resulta em uma curva de aprendizado mais acentuada, além de ser menos ágil para resposta imediata a incidentes.

Já o *CRITs (Collaborative Research into Threats)*, desenvolvido pela *MITRE*, oferece um modelo baseado em repositórios de ameaças, permitindo a análise de *malwares* e incidentes cibernéticos dentro de um ambiente colaborativo. Ele combina armazenamento e enriquecimento de dados com funcionalidades de investigação, sendo útil para a pesquisa detalhada de ataques. No entanto, sua estrutura não é ideal para o compartilhamento eficiente de inteligência em tempo real, e sua compatibilidade com padrões modernos, como *STIX v2*, é limitada, o que pode prejudicar sua integração com outras ferramentas de inteligência.

O *CIF (Collective Intelligence Framework)*, por sua vez, é voltado para processamento rápido e dis-

tribuição escalável de inteligência, sendo altamente eficiente na normalização e no compartilhamento de dados sobre ameaças. Essa plataforma é amplamente utilizada por organizações que necessitam lidar com grandes volumes de indicadores de ameaças em tempo real, sendo uma das mais escaláveis da categoria. Contudo, sua abordagem prioriza agilidade e automação em detrimento da análise contextual, apresentando limitações quando se trata de modelagem de ameaças e correlação visual de eventos.

Por fim, o *Anomali STAXX* oferece um modelo híbrido, combinando funcionalidades de coleta de inteligência com integração a fontes comerciais de *CTI*, como *FireEye*, *IBM X-Force* e *CrowdStrike*. Ele se destaca pela facilidade de ingestão de feeds de inteligência e pelo suporte nativo aos padrões *STIX/TAXII*, garantindo interoperabilidade com diversas ferramentas de defesa. No entanto, sua estrutura fechada e menos flexível pode limitar a personalização e a integração com sistemas internos, tornando-o menos atrativo para pesquisas e investigações personalizadas.

A análise comparativa dessas plataformas evidencia que *MISP* e *OpenCTI* são as soluções mais completas, pois oferecem melhor suporte ao método *5W3H*, permitindo uma estruturação mais detalhada das ameaças. O método 5W3H, que visa responder às perguntas *What* (O quê?), *Who* (Quem?), *Where* (Onde?), *When* (Quando?), *Why* (Por quê?), *How* (Como?), *How much* (Quanto?) e *How often* (Com que frequência?), se mostra essencial para garantir que os dados coletados sejam contextualizados de maneira clara e objetiva. O *MISP*, por seu foco na distribuição rápida de *IoCs*, utiliza o *5W3H* para padronizar suas informações compartilhadas, enquanto o *OpenCTI* aprofunda essa estrutura ao permitir uma modelagem mais refinada de ameaças e campanhas, tornando-o uma ferramenta mais poderosa para análise avançada. Na Tabela 2.1, temos um resumo de todo o comparativo apresentado.

2.1.6 Ameaças Persistentes Avançadas

Atualmente as Ameaças Persistentes Avançadas (*APTs*, do inglês *Advanced Persistent Threats*) representam um dos maiores desafios para a segurança cibernética moderna. Essas ameaças são caracterizadas por sua sofisticação técnica, alto grau de planejamento e objetivos estratégicos, frequentemente associados a espionagem, sabotagem ou roubo de informações críticas [29]. Ao contrário de ataques cibernéticos oportunistas, como os que buscam ganhos monetários imediatos ou até mesmo provocar uma atividade disruptiva, as APTs são direcionadas, duradouras e executadas por agentes altamente capacitados, que incluem grupos patrocinados por Estados-nação e organizações criminosas avançadas.

De acordo com o estudo conduzido por Krishnapriya et al. [5], a quantidade e a ordem dos estágios em um ataque podem variar conforme o objetivo final do atacante. O adversário pode reorganizar esses estágios e empregar *TTPs* específicas para alcançar sua meta. Na literatura, existem diversas abordagens para representar o ciclo de vida de uma *APT*. Ussath et al. [30] focam na caracterização dos atributos mais relevantes de uma campanha do tipo *APT* e propõem um modelo com três estágios. Já Li et al. [31] propõem um ciclo de vida composto por quatro estágios: preparação, acesso, residência e coleta.

Em outros estudos, Brewer [32] sugere um modelo com cinco estágios, enquanto Vukalović e Delija [33] propõem sete. Apesar dessas diferenças, Abu et al. [34] apontam que a maioria dessas abordagens compartilha essencialmente os mesmos seis estágios fundamentais, conforme definidos por Chen et al. [35]. A seguir, cada um desses seis estágios é descrito em detalhes.

Tabela 2.1: Avaliação das Plataformas *TISP* - Adaptado de [4]

	MISP	**OpenCTI**	**CIF**
Arquitetura Holística			
Aderência ao 5W3H	Muito Alto	Muito Alto	Baixo
Casos de uso	Muito Alto	Muito Alto	Alto
Processo de Produção de Inteligência			
Formato de importação	OpenIOC, STIX, CybOX, JSON, CSV, XML	STIX, CybOX, JSON, CSV, XML	XML, JSON, Zip
Coleta automática	MISP feeds	Utiliza conectores com fontes ou outras plataformas	Sincronização automática com diferentes fontes
Formato de exportação	MISP, OpenIOC, CSV, XML, JSON	CSV, STIX	CSV, JSON, HTML, XLS
Visualização gráfica	Dashboard geral e intuitivo e gráficos de relacionamento	Dashboards diversos e grafos de relacionamento baseados em STIXv2	Interface de linha de comando com possibilidade de integração com ferramenta visual
Correlação	Automática para todos os dados na plataforma	Automática para todos os dados na plataforma	Não convém
Classificação	Baseada no tipo de indicador	Baseada em objetos STIXv2	Baseada no tipo de indicador
Integração	IDS, SIEMs e outras plataformas de CTI	Outras plataformas de Threat Intell	IDSs (Snort, Splunk, Bro, Bind)
Mecanismo de compartilhamento	Grupo de instâncias confiáveis	Instância particular com compartilhamento entre usuários	Grupo de instâncias confiáveis com serviço centralizado
Adicionais			
Documentação	Extensiva e bem elaborada	Extensiva e bem elaborada	Poucos detalhes e descrições sucintas
Modelo de Licença	Open Source (GNU General Public License)	Open Source (Apache License)	Open Source (GNU General Public License)

– Reconhecimento e Armamento: fase onde realiza-se a coleta de informações estratégicas sobre o alvo, utilizando técnicas diversas como engenharia social, scans de rede e exploração de credenciais vazadas. Com base nesses dados, os atacantes desenvolvem ferramentas específicas, como malwares personalizados, adaptando suas táticas ao ambiente do alvo.

– Entrega: após a preparação do ataque, os adversários escolhem um vetor de entrada para entregar o código malicioso. Alguns métodos comumente utilizados incluem campanhas de phishing, anexos infectados, exploração de vulnerabilidades remotas, dispositivos comprometidos ou ataques via serviços expostos na internet. Esse estágio é crítico para garantir que o código malicioso atinja o sistema-alvo, e viabilizar todo o ataque.

– Intrusão Inicial: Uma vez entregue, o malware ou exploit executa seu código malicioso com o objetivo de comprometer um sistema inicial. Os atacantes buscam obter um ponto de apoio dentro da rede, explorando falhas de segurança para evitar detecção e manter acesso contínuo, fazendo o uso

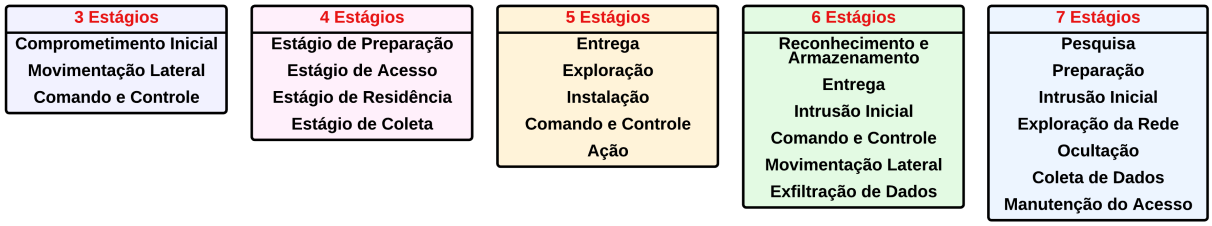


Figura 2.5: Estágios do ciclo de vida de uma *APT* - Adaptado de [5]

de backdoors por exemplo.

– Comando e Controle: Após a intrusão, os atacantes estabelecem comunicação com servidores de comando e controle *(Command and Control – C2)*, o qual permite que o atacante exerça um controle remoto sobre o ambiente comprometido. O *C2* pode ser estruturado de diversas formas, como através da comunicação com domínios maliciosos, canais criptografados, redes peer-to-peer, possibilitando assim a movimentação furtiva dos atacantes dentro do ambiente.

– Movimentação Lateral: Com o acesso estabelecido, os invasores exploram a rede interna para expandir seu controle, elevando privilégios e comprometendo máquinas adicionais. Nessa fase são utilizados entre outros, ataques como o *pass-the-hash* e *kerberoasting*, bem como o uso de ferramentas legítimas (*living-off-the-land*), com o objetivo de acessar sistemas críticos e garantir persistência sem acionar mecanismos de defesa.

– Exfiltração de Dados: por fim, os atacantes atingem seus objetivos estratégicos, que podem incluir a extração de informações confidenciais (*data exfiltration*), espionagem, sabotagem de sistemas, interrupção de serviços, implantação de *ransomware*, entre outros. Muitos desses ataques permanecem indetectáveis por longos períodos, permitindo a coleta contínua de dados sensíveis.

Dada a complexidade e o impacto potencial das *APTs*, sua análise e mitigação permanecem prioridades críticas no campo da segurança cibernética e em várias pesquisas acadêmicas. A mitigação de *APTs* exige uma abordagem mas robusta, sendo um possível meio para atingir esse nível de proteção a combinação de tecnologias, como soluções de Detecção e Resposta de Endpoint (*EDR*) e *SIEM*, com práticas robustas de governança e conscientização.

2.2 TRABALHOS CORRELATOS

Diversas pesquisas recentes têm abordado a detecção de Ameaças Persistentes Avançadas (*APTs*) e o aprimoramento de plataformas de inteligência cibernética, compreendendo modelos estatísticos, técnicas de aprendizado de máquina e análise comportamental. Em [36], por exemplo, os autores utilizam Modelos Ocultos de Markov (HMMs) para correlacionar alertas de segurança ao longo de múltiplas fases de um ataque, buscando prever o próximo estágio das *APTs* e superar a limitação de ferramentas que dependem unicamente de assinaturas. A principal contribuição desse trabalho é o uso de correlação contínua de eventos, permitindo à solução identificar padrões mesmo em cenários complexos, embora ainda seja necessário

um grande esforço manual para manter as regras de correlação atualizadas.

A ênfase em correlação de eventos também é observada em [37], onde Mahboubi et al. discutem a evolução das técnicas de *threat hunting*. Nesse estudo, é realizada uma revisão sistemática sobre como algoritmos de inteligência artificial e métodos heurísticos podem auxiliar na detecção proativa de atividades maliciosas que passam despercebidas por abordagens tradicionais. Além de pontuarem desafios como a complexidade de análise em grandes volumes de dados, os autores enfatizam a necessidade de integrar dados de diferentes fontes, a fim de fornecer uma visão contextualizada das ameaças.

No campo da inteligência de ameaças, o trabalho executado por Jin et al. [38] investiga como o compartilhamento de *Cyber Threat Intelligence* entre organizações tem crescido, mas alerta para problemas de qualidade e profundidade das informações trocadas. O estudo conclui que nem sempre a simples disponibilização de *feeds* de *IoCs* ou relatórios genéricos resulta em benefício prático — em muitos casos, a ausência de contexto ou de detalhes sobre Táticas, Técnicas e Procedimentos prejudica a ação efetiva das equipes de segurança. Já o estudo conduzido por Ainslie et al. [3] reforça que Plataformas de Inteligência de Ameaças não devem se restringir a servir de repositórios: o ideal é que forneçam recursos analíticos e automações que impulsionem a tomada de decisão em tempo real. Nesse ponto, o artigo destaca a carência de integração entre *TIPs* e sistemas de defesa ágeis, como ferramentas *SIEM*, que poderia reduzir a janela de exposição a ataques.

No estudo conduzido por Gonzáles-Granadillo et al. [39], o enfoque dos autores recai sobre Sistemas de Gerenciamento de Informações e Eventos de Segurança. Após analisarem ferramentas comerciais e de código aberto, os autores mostram que, embora sejam indispensáveis para reunir e correlacionar grandes quantidades de eventos, muitos *SIEMs* ainda apresentam limitações na análise comportamental e na resposta imediata. Tais lacunas tornam-se críticas em cenários de infraestruturas essenciais, onde a rapidez na contenção de incidentes é determinante para prevenir interrupções de serviços ou impactos financeiros.

Buscando aprimorar a detecção baseada em padrões de ataque, Leite et al. [14] propõe uma abordagem para mapear automaticamente *TTPs*, utilizando um esquema de extração de indicadores e correlação em sistemas de monitoramento de rede. Esse processo viabiliza a criação de "assinaturas de comportamento" que, segundo os autores, podem ser aplicadas de forma independente ao ambiente alvo, facilitando a escalabilidade. Em contrapartida, [40] utiliza grafos persistentes para unificar as perspectivas de atacante e de defensor, permitindo correlacionar múltiplos estágios de um ataque. O modelo proposto constrói um histórico dos eventos e da progressão das técnicas empregadas, auxiliando no *threat hunting* em tempo real.

Uma alternativa com foco em inteligência artificial surge em [41], onde Spyros et. al apresenta um *framework* holístico para gerenciamento de *CTI*, integrando soluções como *MISP* e *Wazuh*. A proposta se destaca por utilizar algoritmos de *Machine Learning* no enriquecimento de dados, fornecendo insights acionáveis com mínima intervenção humana. Ao combinar dados internos (sensores) e externos (relatórios de ameaças), o sistema filtra falsos positivos e prioriza alertas com base na criticidade.

Em seguida, Çakmakçı et al. [42] introduz um método incremental de correlação de alertas em plataformas *SIEM*, onde eventos dispersos são correlacionados de forma contínua para reconstruir potenciais cenários de *APT* ao longo do tempo. Isso permite identificar atividade adversária dividida em múltiplas fases, algo comum em ataques sofisticados que não se manifestam em um único pico de atividade. Já Mah-

moud et al.[43] destaca uma outra perspectiva, tentando detectar os estágios iniciais de *APT* a partir de registros de baixo nível no *kernel* do sistema operacional. O uso de grafos de proveniência visa mapear o encadeamento de processos suspeitos, antecipando a descoberta de movimentações laterais ou exfiltrações de dados antes de se tornarem irreversíveis.

No contexto de revisões sistemáticas, Buchta et al. [44] classifica, de modo abrangente, uma série de abordagens dedicadas à identificação de *APTs*, discutindo pontos como escassez de *datasets* públicos, padronização de avaliações e necessidades futuras de pesquisa. Em paralelo, Ali et al. [45] apresenta o *TTPMapper*, que aprofunda o problema de traduzir relatórios de *CTI* não estruturados em mapeamentos de *TTPs* do *framework MITRE ATT&CK*, utilizando modelos de linguagem capazes de automatizar a extração e classificação dos artefatos descritos. Para a nossa proposta, uma possível adoção do *TTPMapper* seria estratégica, ao possibilitar que o processo de análise dos relatórios de inteligência fosse acelerado e enriquecido. Dessa forma, as Táticas, Técnicas e Procedimentos seriam identificadas com maior precisão, integrando-se diretamente ao mapeamento realizado no "*Toolkit* para Análise e Correlacionamento de *TTPs*" e fornecendo uma base mais consistente para a correlação de eventos no *SIEM* e para a resposta a incidentes.

Em [46], Sachidananda et al. traz uma abordagem focada na predição de etapas futuras do adversário, com uso de aprendizado de máquina para correlacionar comportamentos observados e atribuir ataques a grupos específicos, baseando-se em padrões repetitivos de exploração de vulnerabilidades (*CVEs*). Esse método pode, inclusive, orientar equipes de segurança sobre quais medidas preventivas tomar com antecedência, elevando o nível de proteção em ambientes alvo de APTs reincidentes.

Complementando essas abordagens, Kern et al. [47] propõe o modelo *D3TECT*, que permite às organizações priorizar estrategicamente as melhores fontes de dados para a detecção de ataques cibernéticos. O estudo enfatiza que nem todas as fontes de dados possuem o mesmo valor para identificação de ameaças e que uma escolha inadequada pode resultar em desperdício de recursos e baixa eficácia. Utilizando o *MITRE ATT&CK Framework* e bases de dados públicas de *CTI*, o modelo ranqueia fontes de dados conforme sua relevância na detecção de *TTPs*, considerando também restrições organizacionais, como privacidade de dados e limitações técnicas. Embora o modelo tenha sido validado com dados públicos de ameaças reais, ele ainda carece de testes em ambientes simulados e de integração com *SIEMs*.

Em conjunto, esses estudos reforçam tendências como a integração de *CTI*, a combinação de algoritmos de detecção baseados em anomalia e comportamentos (incluindo *IA*) e o foco no monitoramento contínuo de *TTPs*. Apesar das contribuições relevantes, grande parte dos trabalhos ainda carece de estratégias de automação robustas e não demonstra uma integração profunda entre *TIPs* e sistemas de monitoramento ou resposta em tempo real. Além disso, surge a necessidade de garantir a qualidade, relevância e tempestividade das informações trocadas, algo que permanece como um desafio. Essas lacunas motivaram o desenvolvimento da metodologia proposta neste trabalho, que visa agregar inteligência de ameaças à detecção e correlação de eventos, bem como automatizar ações defensivas de forma mais ágil e confiável.

Para fornecer uma visão consolidada das abordagens presentes nos trabalhos mencionados, a Tabela 2.2 apresenta uma síntese de estudos relevantes, destacando seu foco, a abordagem adotada e o método empregado. Para sua produção, foram selecionados artigos levando-se em conta a atualidade, publicados nos últimos três anos, e relacionados diretamente com os temas *SIEM, APT, CTI, TIP* e *Threat Detection*.

Tabela 2.2: Síntese dos trabalhos correlatos mais relevantes

Foco	Abordagem	Método	Referência
Revisão sistemática sobre evolução de técnicas de *Threat Hunting*	Avaliação de abordagens baseadas em *AI*, aprendizado de máquina e métodos heurísticos	Revisão de literatura, análise de metodologias e categorização de desafios e tendências	[37]
Tornar a inteligência de ameaças mais acionável para resposta a incidentes	Automação da correlação entre eventos de rede e *CTI*	Mapeamento de *TTPs* em eventos de rede para construção de padrões de ataque	[14]
Modelagem de ataques cibernéticos e *Threat Hunting*	Construção de grafos persistentes para correlacionar a visão do atacante e do defensor	Simulação da campanha do *APT29* com *MITRE ATT&CK, Sysmon e SIEM*	[40]
Gestão de inteligência de ameaças cibernéticas	*Framework* baseado em *IA* para coleta, análise e compartilhamento de *CTI*	Integração entre *MISP, Wazuh, honeypots e ML*	[41]
Detecção de *APTs* via correlação de alertas SIEM	Correlação incremental de alertas gerados por regras	Regras de correlação e *SIEM (ELK Stack)*	[42]
Detecção de *APTs* nas fases iniciais	Análise de logs do kernel e rastreamento de eventos	Construção de um grafo de proveniência para correlacionar atividades suspeitas	[43]
Revisão de Sistemas de Detecção de *APTs* e Identificação de Desafios	Análise sistemática da literatura sobre *APT Detection*	Proposta de uma arquitetura de referência para detecção de *APTs*, categorização de métodos de detecção e avaliação de desafios científicos	[44]
Mapeamento preciso de *TTPs* a partir de relatórios de inteligência de ameaças não estruturados	Uso de aprendizado de máquina para classificar e mapear técnicas do *MITRE ATT&CK* a partir de dados extraídos de relatórios	Implementação do TTPMapper, que combina modelos baseados em *CyBERT* e *GPT-4o* para aprimorar a identificação de *TTPs*	[45]
Correlação, predição e atribuição de ataques *APTs*	Uso de aprendizado de máquina e correlação de eventos de segurança	Desenvolvimento do APTer, que correlaciona e prevê estágios de APTs e os atribui a grupos específicos usando *MITRE ATT&CK*	[46]
Seleção estratégica de fontes de dados para detecção de ataques cibernéticos	Modelo *D3TECT*, que classifica e prioriza fontes de dados para identificar *TTPs*	Análise de técnicas do *MITRE ATT&CK* e uso de dados públicos de *CTI* para validar o modelo	[47]

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*.

Em seguida, a Tabela 2.3 expõe uma comparação entre as principais características dessas investigações correlatas e a metodologia aqui proposta. Observa-se que nosso modelo se sobressai ao integrar, de forma abrangente, a detecção de *TTPs* com o processo de enriquecimento automático de inteligência, garantindo não apenas correlações mais confiáveis, mas também respostas mais ágeis e contextualizadas frente a

ameaças complexas como as *APTs*.

Tabela 2.3: Comparação da metodologia proposta com trabalhos correlatos

Artigo	**[37]**	**[42]**	**[43]**	**[41]**	**[14]**	**[45]**	**[47]**	**[46]**	**[40]**	**Metodologia Proposta**
Possibilita a identificação de *TTPs*	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Integração com *TIPs*	Sim	Não	Não	Sim	Sim	Não	Não	Não	Não	Sim
Enriquecimento de Dados/Inteligência	Sim	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Integra com *SIEM*	Sim	Sim	Não	Sim	Não	Não	Não	Sim	Sim	Sim
Validação com Amostras Reais de *Malware*	Não	Sim	Sim	Não	Sim	Não	Não	Sim	Não	Sim

3 METODOLOGIA PROPOSTA

Com base nos conceitos e trabalhos correlatos apresentados no Capítulo 2, este capítulo descreve a metodologia proposta para aprimorar a detecção e resposta a ameaças cibernéticas por meio da integração de inteligência de ameaças (*Cyber Threat Intelligence*) em plataformas de monitoramento e resposta a incidentes. O objetivo central é permitir a correlação automatizada de eventos de segurança com Táticas, Técnicas e Procedimentos adversários, melhorando a precisão da detecção e reduzindo falsos positivos.

Para alcançar esse objetivo, a metodologia segue um ciclo estruturado, dividido em quatro fases principais:

1. **Coleta de Indicadores e Inteligência** – agregação de dados de fontes internas e externas, incluindo *feeds* de *IoCs*, relatórios de ameaças e eventos de segurança em tempo real.
2. **Enriquecimento de Dados e Inteligência** – normalização e correlação das informações coletadas, utilizando frameworks como *MITRE ATT&CK* para mapear comportamentos adversários.
3. **Correlação e Análise** – identificação de padrões de ataque e cruzamento de dados com eventos históricos para determinar a criticidade das ameaças.
4. **Resposta e Prevenção a Incidentes** – aplicação de contramedidas, geração de alertas e automatização de ações defensivas.

O processo metodológico adotado é inspirado na abordagem proposta por Leite et al. em *"Actionable Cyber Threat Intelligence for Automated Incident Response"* [14], mas é adaptado para um contexto mais amplo, abrangendo diferentes fontes de inteligência e integrando-se a ferramentas como *OpenCTI, Wazuh e Sysmon*.

A Figura 3.1 ilustra a estrutura geral do fluxo metodológico, que será detalhado nas Seções 3.1 a 3.4, cada um correspondendo às fases citadas acima.

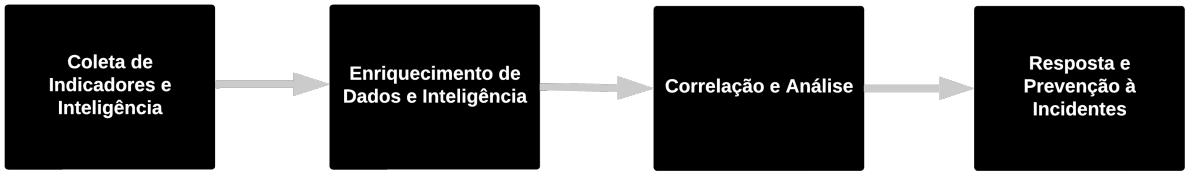


Figura 3.1: Descrição da Estrutura

3.1 COLETA DE INDICADORES E INTELIGÊNCIA

A primeira etapa da metodologia consiste em coletar dados brutos de diferentes origens, tanto internas quanto externas, com o objetivo de fornecer uma base robusta para a detecção de ameaças. No âmbito das fontes internas, são utilizadas soluções de monitoramento instaladas nos endpoints – por exemplo, sensores – os quais capturam logs de sistema operacional, eventos de segurança e alterações em arquivos críticos. Esses dados de log são então enviados em tempo real para um servidor centralizado de gerenciamento de logs, onde serão posteriormente analisados.

Para as fontes externas, utiliza-se fontes de inteligência pública, responsáveis por fornecer relatórios estruturados de segurança que contêm, entre outros fatores, Indicadores de Comprometimento, endereços *IP* maliciosos, hashes de arquivos suspeitos e nomes de domínio potencialmente perigosos. Essa coleta ocorre de forma contínua ou em intervalos configurados, possibilitando que a ferramenta de inteligência de ameaça cibernética (por exemplo, *OpenCTI* ou *MISP*) seja populada com dados relevantes sobre novas campanhas e *TTPs* observadas no meio externo. Entretando, é necessário pontuarmos a dificuldade na obtenção de dados de fontes que sejam consideradas de alta qualidade, uma vez que não há critérios de avaliação bem definidos, para a devida mensuração e avaliação da qualidade.

Após a aquisição inicial dos dados externos, executa-se uma etapa de pré-processamento para filtrar duplicidades e padronizar campos-chave, como endereços *IP* e *hashes*. Essa padronização garante uma estrutura uniforme dos registros, facilitando a correlação posterior e reduzindo o risco de armazenar o mesmo indicador diversas vezes.

Dada a brevidade do ciclo de vida de alguns *IoCs*, a atualização contínua da plataforma de inteligência assegura que a base permaneça atualizada, refletindo ameaças emergentes de forma ágil. Assim, todo o conjunto de informações coletadas nesta fase – dados internos e externos – serve de alicerce para o enriquecimento (Seção 3.2), onde serão empregadas outras fontes de inteligência, e para a subsequente correlação (Seção 3.3) e resposta a incidentes (Seção 3.4).

3.2 ENRIQUECIMENTO DE DADOS E INTELIGÊNCIA

3.2.1 Enriquecimento de Dados

Em relação aos dados obtidos através dos sensores instalados nos endpoints, realiza-se o mapeamento dos dados obtidos em relação às *TTPs* conhecidas usando o framework *MITRE ATT&CK* como referência [48]. O processo faz uso de 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 de ameaças, correlacionando os indicadores observados com táticas conhecidas de adversários. Dessa forma, qualquer menção a técnicas específicas (por exemplo, roubo de credenciais ou exfiltração de dados) é associada diretamente ao dado obtido, permitindo uma compreensão mais rápida do comportamento adversário e orientando os analistas na priorização de incidentes.

3.2.2 Enriquecimento de Inteligência

Após a fase de coleta, a metodologia visa adicionar contexto às informações obtidas nos relatórios de segurança e aos indicadores de comprometimento neles contidos. Essa etapa de enriquecimento abrange, portanto, não apenas hashes, endereços *IP* ou domínios, mas também as descrições mais amplas, como características de grupos adversários, ferramentas maliciosas e possíveis campanhas vinculadas. Por meio desse processo, dados antes fragmentados tornam-se mais úteis e consistentes para a identificação e resposta a ameaças.

Uma prática essencial para alcançar a qualidade esperada é recorrer a bases confiáveis de inteligência, capazes de fornecer evidências adicionais sobre atores maliciosos, métodos de ataque, histórico de uso de determinadas Táticas, Técnicas e Procedimentos ou até mesmo o grau de severidade vinculado a cada indicador. Fontes de relatórios pouco confiáveis podem gerar resultados equivocados quando enriquecidos, pois acabam associando *IoCs* legítimos a comportamentos maliciosos ou ignorando indicadores realmente perigosos, desse modo, recomenda-se a utilização de *feeds* verificados ou de alta qualidade, como *VirusTotal* [49] e *Hybrid Analysis* [50]. De modo geral, o processo de enriquecimento pode ser dividido em quatro etapas:

3.2.2.1 Identificação de Conteúdos no Relatório

Os relatórios importados na fase de coleta são analisados para localizar tanto seus *IoCs* (por exemplo, endereços *IP* e *hashes*) quanto métodos de ataque e adversários específicos. Com isso, obtém-se um mapeamento inicial do que pode ser enriquecido.

3.2.2.2 Consulta a fontes de inteligência

Nesta etapa, ocorrem requisições a diferentes bancos de dados ou plataformas de conhecimento, feitas por meio de conectores especialmente desenvolvidos para integrar o sistema a feeds e serviços de análise de ameaças. Esse mecanismo verifica, por exemplo, se um *IoC* já foi relatado em incidentes anteriores, se apresenta elevado índice de detecção em ferramentas de análise de malware ou se está ligado a campanhas recentes de *phishing* ou *ransomware*.

3.2.2.3 Validação e Padronização

À medida que as informações retornam dos conectores, ocorre a filtragem do que é relevante, incluindo a exclusão de dados redundantes. Em seguida, tudo é armazenado com formato e nomenclatura padronizados, de modo a facilitar a correlação posterior e garantir integridade nos registros.

3.2.2.4 Atualização do Repositório

Por fim, o relatório e seus indicadores voltam para o repositório central, agora enriquecidos com detalhes adicionais. Esse enriquecimento pode incluir referências a *TTPs* conhecidas, metadados sobre a

probabilidade de ameaça ou até mesmo as campanhas às quais cada *IoC* se relaciona.

Concluída essa etapa, os relatórios passam a conter detalhes mais abrangentes sobre cada indicador ou tática reportada, bem como uma visão consolidada dos modos de operação de potenciais adversários. Esses relatórios enriquecidos são então utilizados na fase seguinte de correlação e análise, viabilizando a detecção de ameaças e a definição de respostas mais efetivas aos incidentes.

3.3 CORRELAÇÃO E ANÁLISE

Nesta etapa, as *TTPs* que foram correlacionados a um indicador são comparados com a base de informações de ataques e ameaças cibernéticas obtida dos relatórios de segurança, e presente na ferramenta de inteligência de ameaça cibernética. Caso observe-se a presença dessa *TTP* vinculada a indicadores, em um dos relatórios, realiza-se então um segundo nível de verificação, onde o indicador suspeito é comparado a uma lista de indicadores relacionadas a todos os *TTPs* identificados. Em caso afirmativo de correlacionamento, confirma-se então a presença de um ator malicioso no ambiente.

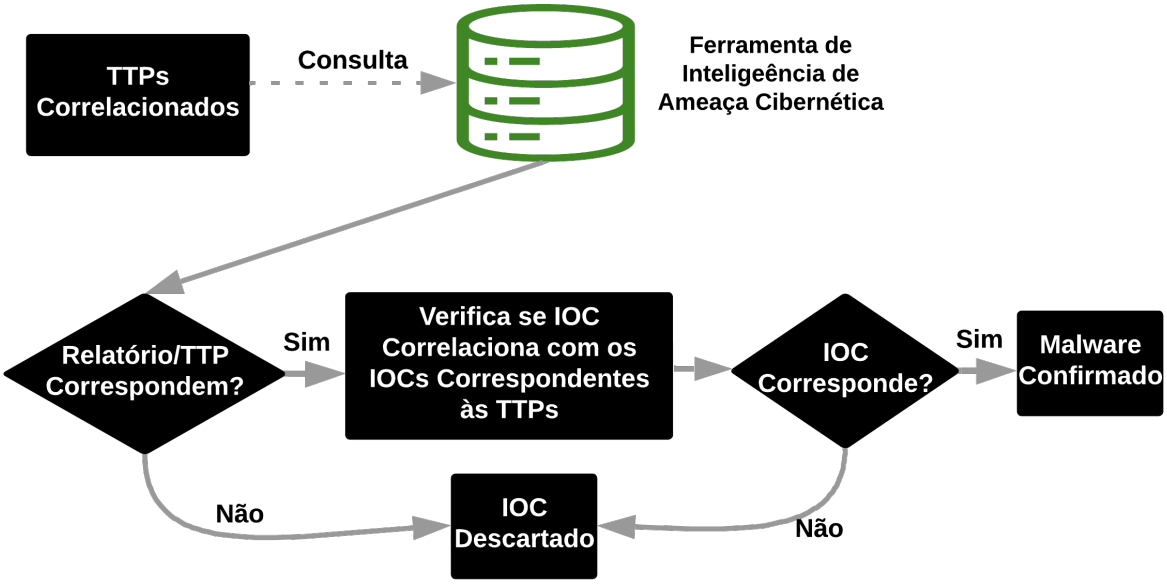


Figura 3.2: Processo de Correlação

3.4 RESPOSTA E PREVENÇÃO A INCIDENTES

A etapa final da metodologia consiste em tomar ações concretas para conter, mitigar e prevenir incidentes, fundamentadas nas correlações e análises realizadas anteriormente (Seções 3.2 e 3.3). Uma vez que se identifica comportamentos suspeitos ou confirma a presença de atividades maliciosas, inicia-se um processo de resposta cujo escopo varia conforme o grau de criticidade e o potencial impacto no ambiente.

Quando um incidente é considerado relevante, as ações de contenção e prevenção são disparadas no Wazuh por meio de *Active Response* e ações de resposta do *File Integrity Monitoring*. No ambiente de testes, a maior parte dessas respostas ocorre após a disponibilização do *hash* malicioso em uma lista *CDB*. Outras ações de resposta também podem ser empregados como:

– Bloqueio ou Isolamento: Interromper conexões com endereços *IP* suspeitos, bloquear domínios maliciosos e restringir o acesso de sistemas infectados à rede corporativa, de modo a impedir movimentação lateral ou exfiltração de dados.

– Quarentena de Arquivos: Remover ou confinar arquivos identificados como maliciosos, evitando que se propaguem ou comprometam ainda mais o sistema.

– Encerramento de Processos: Finalizar execuções de malware ativo ou serviços indevidos detectados no ambiente.

– Regras de Prevenção: Inserir assinaturas ou regras em sistemas de detecção e prevenção de intrusão, firewalls, bem como ajustar políticas de segurança para barrar tentativas futuras semelhantes.

A priorização de incidentes poderia ser determinada pela severidade das táticas ou técnicas empregadas pelos adversários, bem como pela criticidade dos ativos potencialmente afetados. Por exemplo, um incidente que envolva acesso a dados sensíveis ou interrupção de serviços críticos receberia tratamento urgente, enquanto eventos de menor impacto poderiam ser escalonados de maneira mais gradual. Essas decisões seriam baseadas nos indicadores e *TTPs* mapeados, que nortearam a equipe de segurança sobre a probabilidade de evolução do ataque e possíveis danos associados.

3.5 LABORATÓRIO DE TESTES

Para materializar o fluxo metodológico, e validar a metodologia proposta, foi desenvolvido um laboratório de testes representado na Figura 3.3, composto pelos seguintes elementos:

- *OpenCTI*: Plataforma de *Threat Intelligence* responsável por receber relatórios de segurança (por exemplo, do *AlienVault OTX*) e armazenar indicadores de comprometimento.
- *Wazuh*: Ferramenta que cumpre o papel de *SIEM/XDR*, realizando a coleta centralizada de logs, a análise de eventos em tempo real e a correlação com indicadores enriquecidos.
- *AlienVault OTX*: Ferramenta utilizada para obtenção dos *feeds* de *CTI.*
- *Hybrid Analisys e VirusTotal*: Ferramenta utilizadas para enriquecimento de inteligência.
- Máquinas Clientes: Sistemas *Windows*, cada um equipado com um sensor *Wazuh* e o *Sysmon* (para coleta de logs detalhados do sistema operacional).
- Rede Controlada: Todo o tráfego de dados é direcionado e monitorado de forma segura, garantindo isolamento e minimizando riscos de contaminação externa.

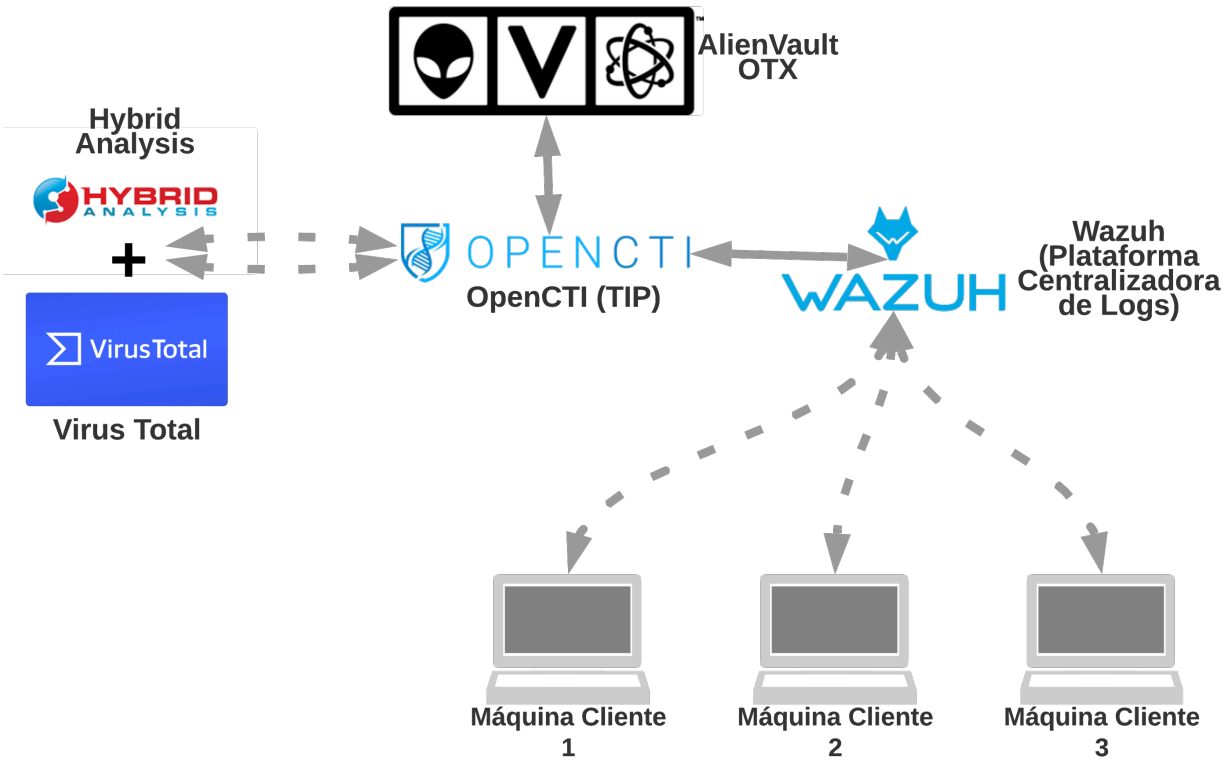


Figura 3.3: Ambiente de Laboratório Utilizado

Como premissa para validacão da metodologia, temos que cada máquina cliente envie seus registros de sistema e eventos de segurança para a plataforma centralizadora de logs, e de forma simultânea, a *TIP* se mantenha atualizada com relatórios e *IoCs*, a fim de fornecer subsídios ao processo de enriquecimento e correlação de incidentes. As especificações técnicas das máquinas utilizadas estão dispostas na Tabela 3.1.

Tabela 3.1: Especificações Técnicas

	Servidor de Inteligência	**Plat. Centralizadora de Logs**	**Máquina Cliente 1, 2 e 3**
Sistema Operacional	Ububtu 24.04.1 LTS	Ububtu 22.04.4 LTS	Windows 10
CPU	2 Cores	2 Cores	2 Cores
RAM	9 GB	8 GB	8 GB
Armazenamento	60 GB	40 GB	40 GB

3.5.1 Justificativa Para Ferramentas Empregadas

A arquitetura desenvolvida neste trabalho faz uso de quatro componentes-chave – *Wazuh*, *OpenCTI*, *Azure* e o *Framework MITRE ATT&CK* – que, em conjunto, oferecem suporte à metodologia integrativa de detecção e resposta a ameaças cibernéticas. A escolha dessas ferramentas baseou-se em fatores como robustez, facilidade de integração, escalabilidade e aderência aos objetivos de correlação de Táticas, Técnicas e Procedimentos (*TTPs*).

O *Wazuh*, ferramenta de código aberto que se apresenta como uma evolução do *OSSEC*, foi selecionado

para atuar como plataforma de monitoramento e correlação de eventos por ser um *SIEM* e *XDR* (Detecção e Resposta Estendidas) [51] reconhecido, com recursos abrangentes para análise de logs, detecção de intrusões e resposta automatizada a incidentes. Em especial, sua capacidade de integrar sensores instalados em diferentes sistemas operacionais (inclusive *Windows* e *Linux*) possibilita a coleta unificada de dados e a aplicação de regras de correlação em tempo real. Essa característica é fundamental para o presente estudo, pois a metodologia proposta demanda o cruzamento de eventos de segurança com as informações provenientes da ferramenta de inteligência. Além disso, o *Wazuh* fornece um módulo de *Active Response* e outro de *File Integrity Monitoring (FIM)*, essenciais para bloquear ou isolar ameaças automaticamente, bem como monitorar alterações não autorizadas em arquivos críticos.

Com base no comparativo realizado na Subseção 2.1.5, a plataforma *open source OpenCTI* [52] foi adotada como *Threat Intelligence Sharing Platform (TISP)* responsável pela ingestão, enriquecimento e modelagem de dados de ameaças, incluindo *IoCs*, relatórios de segurança e mapeamento de *TTPs* segundo o *framework MITRE ATT&CK*. A escolha do *OpenCTI* se justifica por sua arquitetura baseada em *STIX 2.1*, que permite associar indicadores a grupos adversários, campanhas e técnicas específicas, criando uma visão contextualizada das ameaças, bem como a integração com diversas fontes de dados e suporte aprimorado ao método *5W3H*. Sua abordagem analítica oferece uma visão mais completa do ciclo de vida das ameaças, permitindo uma investigação mais eficiente e aprofundada. Outro ponto determinante foi a facilidade de integração com fontes públicas e privadas de *STIX 2.1*, bem como a capacidade de estabelecer conectores para ferramentas de análise de *malware* (por exemplo, *VirusTotal*), enriquecendo a informação de forma automática. Dessa forma, ele se estabelece como a plataforma mais robusta para correlação, análise e compartilhamento de inteligência de ameaças cibernéticas, alinhando-se aos objetivos desta pesquisa.

Já a adoção do *Azure* como plataforma de hospedagem justifica-se principalmente pelos requisitos de escalabilidade e segurança do ambiente de testes. O estudo demandou a criação de diversas máquinas virtuais, capazes de executar amostras de *malware* em um contexto controlado, além de servidores para o *Wazuh* e para o *OpenCTI*. A infraestrutura em nuvem do *Azure* permitiu alocar recursos sob demanda, garantindo a disponibilidade de ambientes isolados para testes sem impactar sistemas locais. A escolha do *Azure* também levou em consideração suas ferramentas nativas de gerenciamento e monitoramento, agregando camadas extras de confiabilidade e viabilizando o rápido provisionamento de instâncias. Dessa forma, o ambiente pôde ser dimensionado para suportar picos de coleta e processamento de *logs* sem comprometer o desempenho do laboratório, além de facilitar a reprodução do cenário de testes em outras fases do projeto.

O *Framework MITRE ATT&CK* foi selecionado para embasar a definição e a correlação das Táticas, Técnicas e Procedimentos que caracterizam os comportamentos adversários. Ao representar de modo sistemático as fases de ataque e as ações executadas pelos atacantes, esse *framework* que é amplamente reconhecido na comunidade de cibersegurança, facilita a análise comportamental e a compreensão das motivações, vetores e métodos utilizados em diferentes campanhas maliciosas. No contexto deste trabalho, o *MITRE ATT&CK* é fundamental para categorizar os eventos capturados pelo *Wazuh* e relacioná-los às informações do *OpenCTI*, atribuindo às ameaças dados mais precisos e possibilitando uma resposta mais efetiva aos incidentes.

Em conjunto, essas soluções embasam a metodologia aqui proposta, permitindo coletar, enriquecer e

correlacionar dados de ameaças em escala, além de suportar a ferramenta "*Toolkit* para Análise e Correlacionamento de *TTPs*" desenvolvida ao longo do trabalho. O resultado é um ecossistema unificado, onde as informações de *CTI* fluem para o *Wazuh* em tempo real, e onde eventuais ameaças detectadas recebem ações de bloqueio e contenção de forma ágil, reforçando a efetividade da abordagem em cenários com *malwares* sofisticados.

3.5.2 Adaptação Metodológica

Inicialmente, a metodologia proposta previa que, na etapa de Correlação e Análise, os *malwares* fossem identificados de forma dinâmica, à medida que novas *TTPs* surgissem na plataforma centralizadora de *logs*.

O processo iniciaria-se com a detecção de uma *TTP* inicial, denominada TTP_1. Assim que essa *TTP* fosse identificada, ela seria disponibilizada para a *Toolkit*, que realizaria uma consulta na base de dados da plataforma *TISP*, identificando todos os relatórios que contivessem essa *TTP* específica. Formalmente, a lista de relatórios obtidos poderia ser representada como:

$$l_{Rep1} = \{R_i \in TISP \mid TTP_1 \in R_i\} \tag{3.1}$$

Ou seja, l_{Rep1} corresponderia ao conjunto de todos os relatórios R_i presentes no *TISP* que mencionassem a TTP_1.

A partir dessa lista de relatórios, todas as *TTPs* associadas seriam extraídas para formar uma nova lista contendo as *TTPs* esperadas, ou seja, aquelas que poderiam ocorrer em conjunto com TTP_1. Esse conjunto de *TTPs* seria dado por:

$$l_{TTPs1} = \bigcup_{R_i \in l_{Rep1}} TTP(R_i) \tag{3.2}$$

Aqui, $TTP(R_i)$ representa o conjunto de TTPs mencionadas em um relatório R_i. O operador de união ($\bigcup$) indica que estamos coletando todas as TTPs de cada relatório em l_{Rep1} e combinando-as em um único conjunto. Isso significa que se uma TTP aparecer em múltiplos relatórios, ela será considerada apenas uma vez em l_{TTPs1}.

De forma análoga, os *malwares* mencionados nos relatórios de l_{Rep1} seriam coletados, formando a lista de *malwares possíveis*:

$$l_{Malwares1} = \bigcup_{R_i \in l_{Rep1}} Malware(R_i) \tag{3.3}$$

Nessa equação, $Malware(R_i)$ representa o conjunto de malwares descritos no relatório R_i. Assim como na equação anterior, o operador de união ($\bigcup$) está agregando todos os malwares citados nos relatórios de l_{Rep1} e consolidando-os em um único conjunto $l_{Malwares1}$, sem duplicatas. Isso permitiria identificar os malwares que, com base no *TISP*, estariam associados à TTP_1.

Em posse da l_{TTPs1} e $l_{Malwares1}$, seria disponibilizado ao usuário na *Toolkit* quais seriam as próximas *TTPs* possíveis, bem como quais *malwares* poderiam estar associados. Quando uma nova TTP, denominada TTP_2, surgisse na plataforma centralizadora de logs, ela também seria enviada para a *Toolkit*. Neste estágio, ocorreria um refinamento da lista de relatórios relevantes, considerando apenas aqueles que contivessem tanto TTP_1 quanto TTP_2. Esse refinamento poderia ser expresso matematicamente como:

$$l_{Rep2} = l_{Rep1} \cap \{R_i \in TISP \mid TTP_2 \in R_i\} \tag{3.4}$$

A interseção ($\cap$) indica que agora a nova lista de relatórios l_{Rep2} conteria apenas os relatórios que fossem previamente identificados em l_{Rep1} e que também mencionassem a nova TTP_2. Essa filtragem refinaria a busca, reduzindo o conjunto de relatórios relevantes.

Consequentemente, a lista de *TTPs* esperadas e a lista de *malwares* possíveis seriam refinadas com base nesses novos relatórios:

$$l_{TTPs2} = \bigcup_{R_i \in l_{Rep2}} TTP(R_i) \tag{3.5}$$

$$l_{Malwares2} = \bigcup_{R_i \in l_{Rep2}} Malware(R_i) \tag{3.6}$$

Nesse caso, as novas listas de *TTPs* e *malwares* possíveis seriam reavaliadas apenas com base nos relatórios restantes em l_{Rep2}, tornando-as mais específicas para a investigação em curso.

Esse processo de refinamento iterativo continuaria até que a lista de *malwares* possíveis contivesse um único elemento, permitindo a atribuição precisa de um *malware* específico ao comportamento observado. Assim, o critério de parada do processo poderia ser expresso como:

$$\exists M \in l_{Malwares_n}, \text{ tal que } l_{Malwares_n} = \{M\} \tag{3.7}$$

Dessa forma, a metodologia garantiria que a correlação entre as TTPs identificadas nos logs e os relatórios armazenados no *TISP* permitisse, progressivamente, restringir a busca até que fosse possível inferir qual *malware* específico estaria envolvido na atividade maliciosa observada.

Entretanto, ao serem realizados alguns testes com essa metodologia, foi detectada uma inconsistência, a qual forçou a sua evolução para a atualmente descrita na Fig. 3.4. A metodologia tinha um ponto de falha, no momento da disponibilização das *TTPs* ao *Toolkit*. Caso o analista responsável pelo fornecimento desses dados, deixasse de disponibilizar uma *TTP*, ou até mesmo, fornecesse uma *TTP* na ordem errada, toda a cadeia de detecção poderia ser comprometida, uma vez que são realizadas eliminações de relatórios, a cada iteração.

Desse modo, pode-se concluir que apesar de conseguirmos identificar as *TTPs* envolvidas na execução de uma provável ameaça, alguns fatores poderiam impedir que chegássemos na fase de identificação do ator malicioso. Ou seja, a utilização da identificação de *TTPs* é um processo útil e válido, mas esse processo

atuando de forma isolada, não é o suficiente. Desse modo, como parte do refinamento para melhoria e adaptacão do processo metodológico, partiu-se para o processo de adicionarmos inteligência em conjunto às *TTPs*, o qual foi obtido através do enriquecimento de relatórios, e descrito nos casos subsequentes.

3.6 ARQUITETURA FINAL

Reunindo todos os componentes descritos anteriormente, bem como a necessidade de evolução metodológica, a Figura 3.4 ilustra, de forma consolidada, como cada elemento interage ao longo das fases da metodologia (coleta, enriquecimento, correlação e resposta). Como pode ser observado na figura, cada módulo cumpre um papel essencial para completar o ciclo de detecção e resposta a ameaças. A coleta de dados e a geração de eventos nos endpoints alimenta, em tempo real, o servidor de logs, que aplica regras de correlação e, se necessário, solicita dados adicionais à plataforma de inteligência. Por fim, as conclusões do sistema de monitoramento fornecem subsídios para que a equipe de segurança decida sobre contramedidas estratégicas.

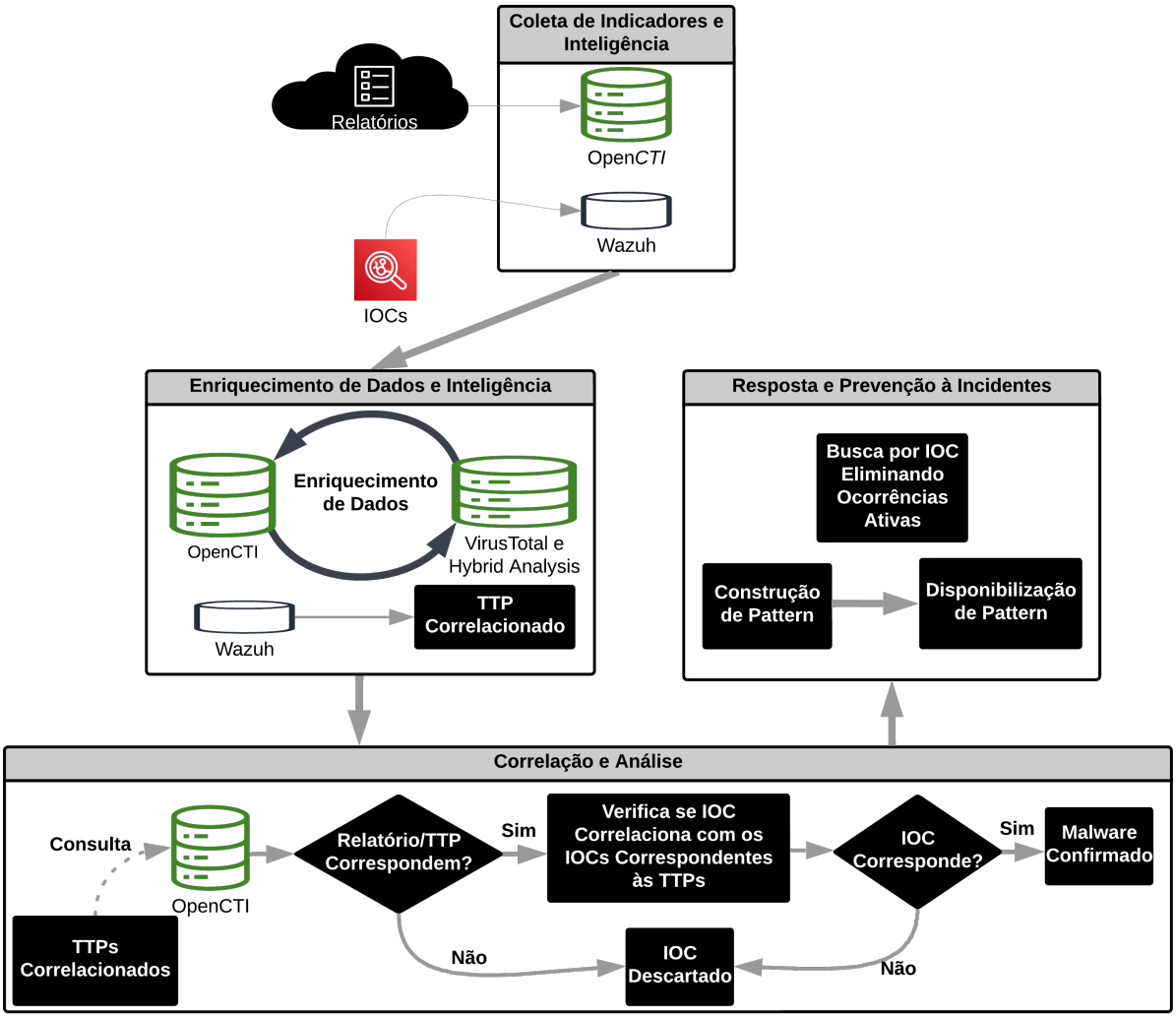


Figura 3.4: Fluxo final da Metologogia Proposta

4 RESULTADOS EXPERIMENTAIS

Este capítulo descreve a aplicação prática da metodologia proposta anteriormente, a fim de validar a eficácia das etapas de coleta, enriquecimento, correlação e resposta a incidentes em um ambiente realista. A seguir, são apresentados os principais componentes da arquitetura, a forma como o *OpenCTI* foi configurado para compartilhar inteligência de ameaças, a configuração do *Wazuh* como plataforma centralizada de logs, o processo de coleta e análise de amostras de malware e, por fim, a discussão dos resultados obtidos.

4.1 CONFIGURACÃO DA FERRAMENTA DE COMPARTILHAMENTO DE AMEAÇAS

Durante este estudo, o *OpenCTI* foi instalado em um servidor Linux dedicado, com conectores de Inteligência habilitados para o *AlienVault OTX* (serviço que publica *IoCs* e relatórios sobre ameaças recentes). Como o *OpenCTI* é uma ferramenta aberta, em que qualquer integrante pode disbonibilizar dados a serem consumidos por outras partes, a qualidade e confiabilidade entre as fontes de dados pode variar bastante. Por conta disso, a fonte de relatórios utilizada como fonte de dados na ferramenta *OTX*, foi a disponibilizada e mantida pela própria *AlienVault*. A cada intervalo de 30 minutos, o *OpenCTI* consultava o *OTX*, importando novos relatórios com entradas de *IPs*, hashes, domínios e possíveis menções a grupos adversários. Durante a condução desse estudo de caso, aproximadamente 1.840 (Figura 4.1) relatórios foram importados para a ferramenta.

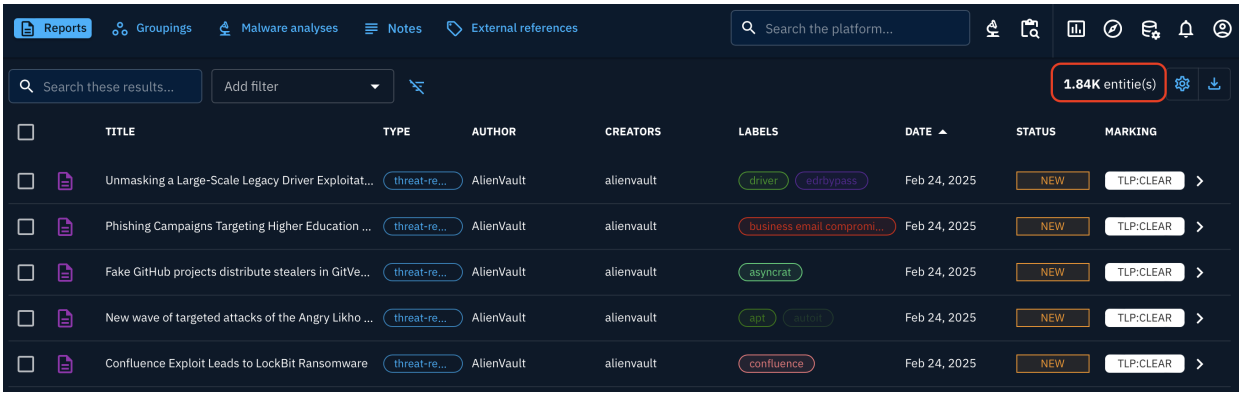


Figura 4.1: OpenCTI populado com Relatórios

Como fontes adicionais de informação para enriquecer e prover contexto aos relatórios de *CTI* (Figura 4.2), também foi configurada via conectores a integração entre o *OpenCTI* com o *VirusTotal* [49] e *Hybrid Analysis* [50]. Diferentemente da integraçção do *AlientVault OTX*, 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.

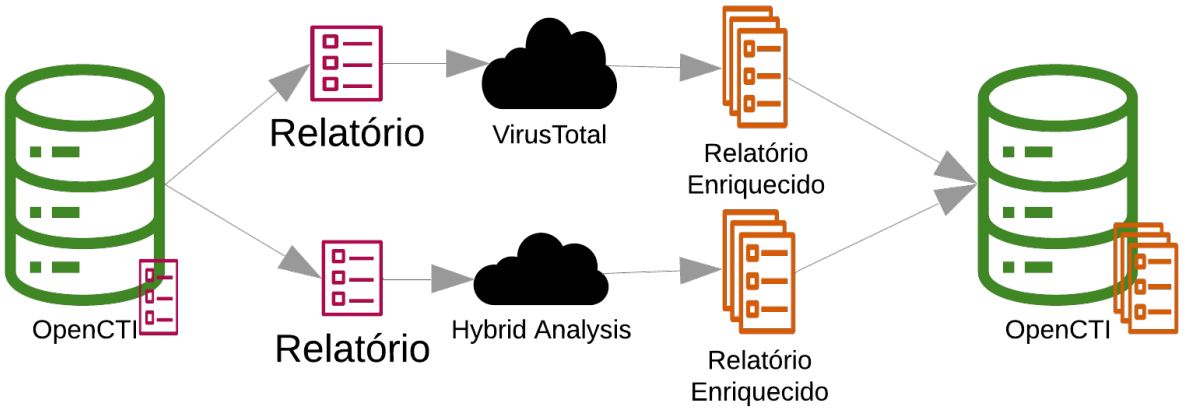


Figura 4.2: Processo de Enriquecimento

4.2 INSTALAÇÃO E CONFIGURAÇÃO DA PLATAFORMA DE *LOGS*

O *Wazuh* foi instalado em um servidor Linux executando o sistema operacional *Ubuntu* dedicado. Sua função principal é coletar, correlacionar e analisar logs de endpoints, proporcionando uma visão consolidada e em tempo real da segurança da rede. Para que o *Wazuh* pudesse receber os logs e eventos dos endpoints, sensores foram instalados em máquinas virtuais configuradas com *Windows* 10, utilizadas para a execução dos malwares. Para aprimorar a coleta de dados, o *Sysmon* foi configurado conforme as recomendações em Hartong [53], o que permitiu a coleta de logs detalhados do sistema.

4.3 AUTOMAÇÃO DA CORRELAÇÃO E ANÁLISE

Visando otimizar o tempo de aplicação da metodologia, seguindo uma das premissas que ela busca implementar (otimização de tempo por parte de um analista), foi desenvolvida a ferramenta chamada "*Toolkit* para Análise e Correlacionamento de *TTPs*". A ferramenta está modularizada em 5 etapas, a seguir descritas:

- **1ª Etapa - Buscar Relatórios com *TTP* X**: o usuário fornece ao programa desenvolvido uma *TTP* que tenha sido observada em uma ferramenta de monitoramento, para que seja buscada em uma Plataforma de Compartilhamento de Inteligência Cibernética, todos os relatórios que fazem referência a essa *TTP*.

  À medida que novas *TTPs* são observadas, elas também são fornecidas ao programa. Os relatórios são então listados (Figs. 4.3 e 4.4), e o resutado final é gravado em um arquivo *TXT*, para caso seja necessária uma revisão posterior.

  Conforme exemplos presentes, na Fig. 4.3, realiza-se a busca pela Técnica 1569, que corresponde de forma geral à técnica Serviços de Sistema, e já na Fig. 4.4), realiza-se a busca pela Técnica 1021, que corresponde de forma geral à técnica de Serviços Remotos. É importante elencar que a Toolkit também recebe e processa a entrada de subtécnicas que tenham sido disponibilizadas.

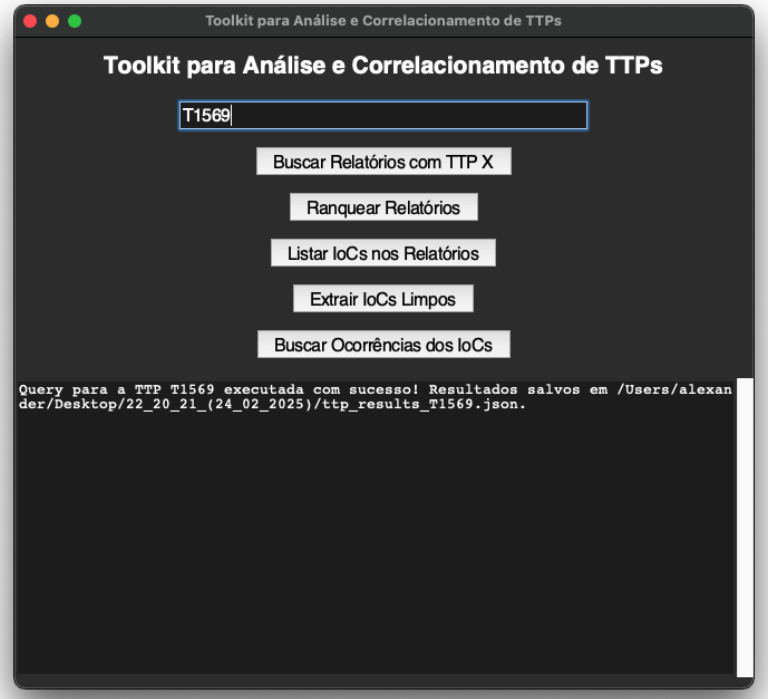


Figura 4.3: Busca pela Técnica 1569

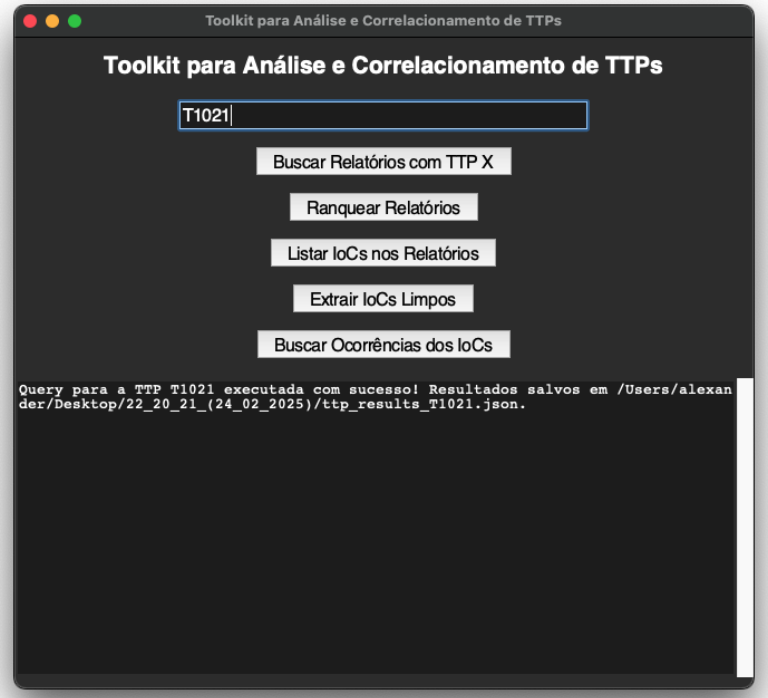


Figura 4.4: Busca pela Técnica 1021

- **2ª Etapa - Ranquear Relatórios**: em posse de todos os títulos de relatórios, que contenham aquelas *TTPs* listadas anteriormente, é realizado um levantamento onde se verifica todas as *TTPs* presentes nos relatórios listados. A partir desse momento, realiza-se um ranqueamento dos relatórios, onde o critério utilizado é a quantidade de *TTPs* presentes naquele relatório.

  A ferramenta então nos traz os cinco relatórios que mais possuem *TTPs* em seu conteúdo, para obtenção dos relatórios mais relevantes. Novamente, o resutado é gravado em um arquivo *TXT*, para caso seja necessária uma revisão posterior. A ação correspondente pode ser verificada na Fig. 4.5.

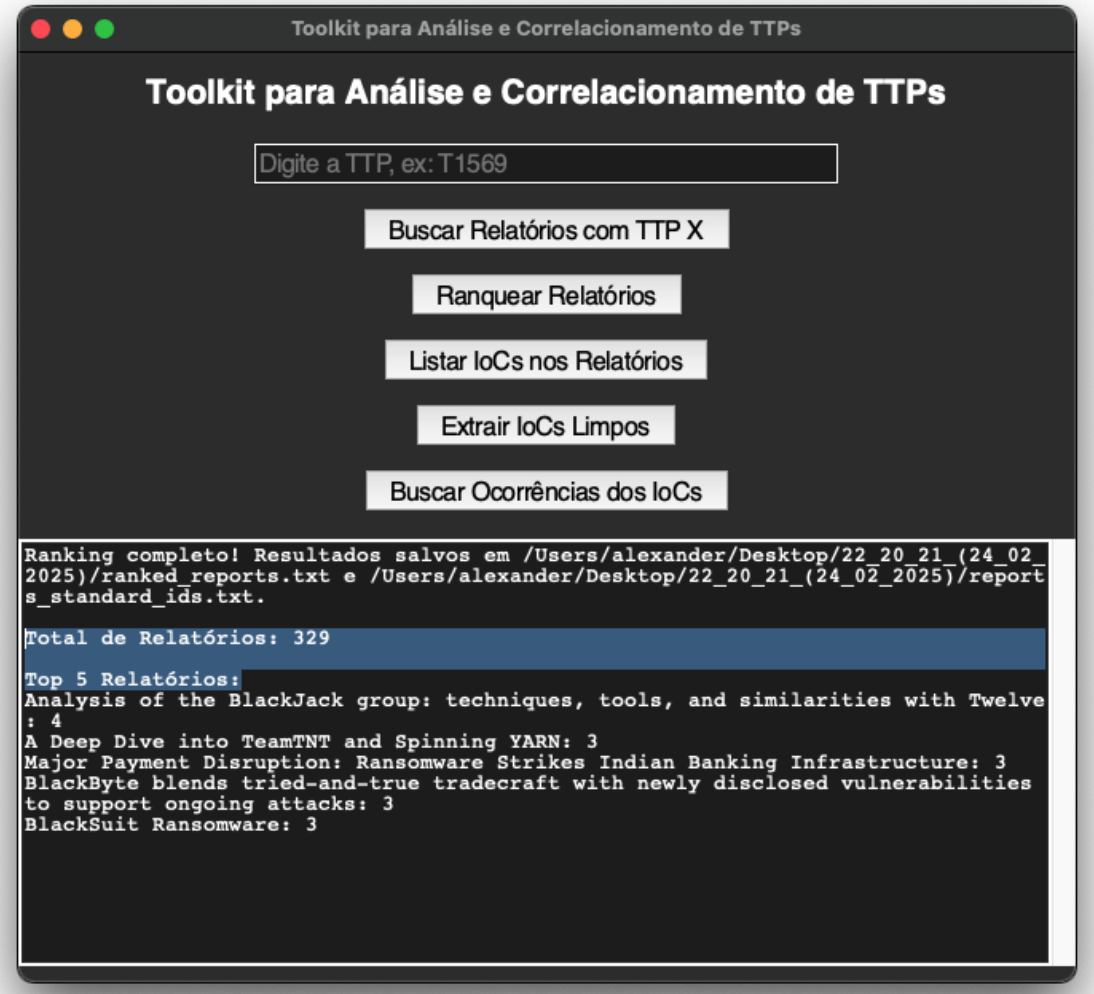
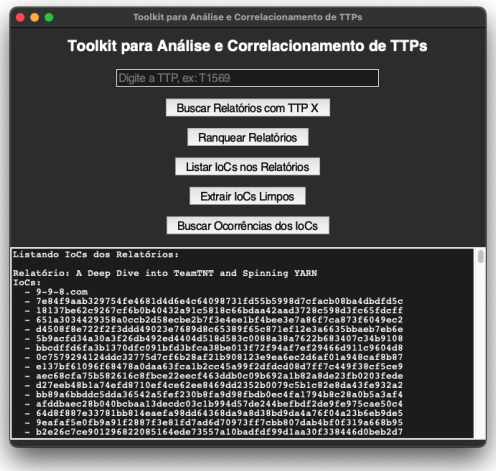


Figura 4.5: Listagem e Ranquemaneto dos Relatórios

- **3ª Etapa - Listar *IoCs* nos Relatórios**: são listados, e informados em tela, todos os Indicadores de Comprometimento presentes em cada um dos relatórios, bem como salvos os resultados em arquivos *TXT*. Na Figura 4.6 (a), temos a listagem inicial dos *IoCs* contidos no relatório *"A Deep Dive into TeamTNT and Spinning YARN"*. Já na Figura 4.6 (b), temos o processo de extração de todos os *IoCs* completo.



(a) *IoCs* Relatório - *A Deep Dive into TeamTNT and Spinning YARN*

(b) Extração Completa

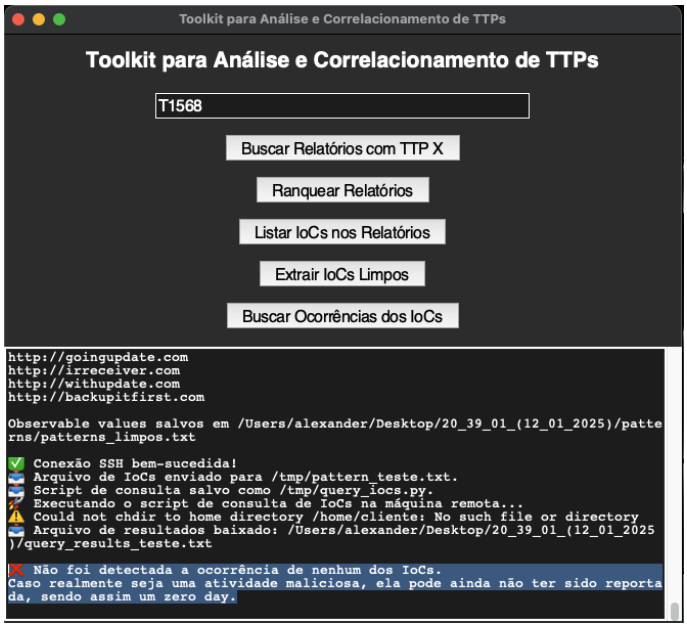
Figura 4.6: Extração de *IoCs* de todos os Relatórios Listados

- **4ª Etapa - Extrair *IoCs* Limpos**: os *IoCs* de todos os relatórios citados são extraídos e disponibilizados na forma de uma lista simples, para facilitar a correlação com a ferramenta centralizadora de logs (Fig. 4.7).

Figura 4.7: Lista simples de todos os *IoCs* Presentes

- **5ª Etapa - Buscar Ocorrências dos *IoCs***: realiza-se a busca da ocorrência desses IoCs no ambiente em uma ferramenta centralizadora de logs, como um *SIEM* por exemplo. Caso seja detectada presença de algum dos *IoCs*, a ferramenta nos trás o *IoC* e o relatório correspondente, conforme podemos ver na Fig. 4.8(a), de modo que assim podemos correlacionar a sequência de execução das *TTPs* a um determinado Ator Malicioso. Caso não ocorra a presença de um dos *IoCs*, a ferramenta nos trás a visualização disponível na Fig 4.8(b), indicando a presença de um possível *Zero Day* no ambiente.

(a) Output quando uma ameaça é detectada



(b) Output indicando possível zero day

Figura 4.8: Resultados possíveis na busca por *IoCs*.

É importante ressaltarmos que o programa desenvolvido foi integrado a um conjunto de ferramentas específico, utilizados no desenvolvimento dessa tese de mestrado, mas pode trabalhar de forma agnóstica, de forma que com os devidos ajustes, ele pode realizar o levantamento de relatórios em várias ferramentas de Compartilhamento de Inteligência Cibernética; bem como, buscar pela ocorrência dos *IoCs*, em várias ferramentas centralizadoras de logs. Com a utilização do mesmo, analistas de segurança de uma organização podem otimizar o tempo de detecção e resposta a uma possível ameaça no ambiente.

4.4 COLETA E ANÁLISE DE AMOSTRAS DE *MALWARE*

Para a obtenção de amostras de malware, foi utilizado o repositório *Malware Bazaar* (Fig. 4.9), mantido pela comunidade "*abuse.ch*". Esse repositório é uma fonte valiosa de amostras de *malware* que são compartilhadas com a comunidade de segurança da informação [54], e em sua base temos mais de 863 mil amostras catalogadas, disponibilizando *hashes*, nomes de arquivos, família de *malware*, entre outras informações. As amostras obtidas foram usadas para testar a eficácia da metodologia proposta na identificação de ameaças. Os malwares utilizados para validar a metodologia foram o *Agent Tesla* e o *Smoke Loader*.

Cada amostra foi executada manualmente em uma máquina virtual *Windows*, com o *Sysmon* registrando todo o comportamento interno (criação de processos, conexões de rede, manipulação de arquivos etc.). Enquanto isso, o agente *Wazuh* encaminhava esses logs ao servidor central, que automaticamente os interpretava e fornecia os *TTPs* associados aos eventos ocorridos durante a execução do *malware*.

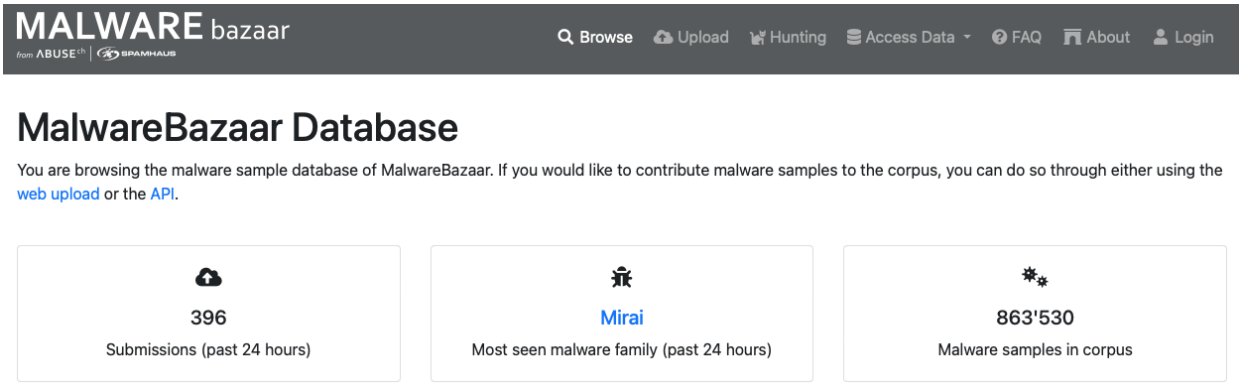


Figura 4.9: Malware Bazaar

4.5 ESTUDO DE CASO E RESULTADOS

4.5.1 Caso 1 - *Malware Agent Tesla*

O *Agent Tesla* é um malware do tipo *keylogger* e *RAT (Remote Access Trojan)*, amplamente utilizado por cibercriminosos para furtar credenciais, capturar pressionamentos de teclas, monitorar a atividade do sistema e exfiltrar dados [55] [56]. Lançado em 2014, ele se popularizou por sua interface fácil de usar e por ser comercializado como um "*malware-as-a-service*"em fóruns clandestinos, permitindo que mesmo

criminosos sem conhecimento técnico avançado o utilizem [57].

Esse *malware* é frequentemente distribuído por campanhas de *phishing*, anexado a documentos maliciosos do Microsoft Office, PDFs ou arquivos executáveis, e continua sendo uma ameaça ativa, evoluindo constantemente para contornar novas proteções de segurança. Após a infecção, o *Agent Tesla* coleta credenciais armazenadas em navegadores, clientes de e-mail e aplicativos FTP/VPN, além de registrar atividades do sistema. Os dados roubados são exfiltrados via SMTP, FTP e HTTP/S para servidores de Comando e Controle controlados pelos atacantes.

O *Agent Tesla* evoluiu significativamente ao longo dos anos, incorporando técnicas avançadas de evasão, como execução em memória, criptografia de comunicações e ofuscação de código, dificultando sua detecção por soluções de segurança tradicionais. Ele continua sendo uma das ameaças mais prevalentes, aparecendo regularmente em relatórios de malware globais, destacando sua relevância no cenário de ameaças cibernéticas atual.

Durante a execução de uma amostra aleatória do *Agent Tesla*, os logs gerados nas estações clientes foram enviados, por meio dos sensores, para a plataforma centralizadora de logs. 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 na base de dados da plataforma *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, de 1.840 disponíveis. Após a criação da lista l_{Rep}, os relatórios nela contidos foram ranqueados com base no número de TTPs associados, produzindo o ranking R_1:

$$R_1 = f(L_{Rep}) \tag{4.1}$$

$$f(i) = |TTP_i \cap L_{TTPs}| \tag{4.2}$$

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:

$$A_1 = \{r \in R_1 : r \text{ menciona } \textit{Malware}\} = \emptyset \tag{4.3}$$

A segunda abordagem envolveu a verificação dos Indicadores de Comprometimento 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 [58], 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:

$$C_1 = \{i \in I_1 : i \text{ corresponde aos Logs}\} = \emptyset \tag{4.4}$$

Essa falta de correlação levantou questões sobre a atualidade e relevância dos relatórios analisados.

4.5.2 Caso 2 - *Agent Tesla* (Amostra de Referência Documentada)

Finalmente, foi realizada uma segunda validação com uma versão diferente do *Agent Tesla*, cuja presença já havia sido identificada na base de relatórios do *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:

$$R_2 = f(L_{Rep2}) \tag{4.5}$$

$$A_2 = \{r \in R_2 : r \text{ menciona } \textit{Malware2}\} \neq \emptyset \tag{4.6}$$

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:

$$C_2 = \{i \in I_2 : i \text{ corresponde aos Logs}\} \neq \emptyset \tag{4.7}$$

Uma vez em posse dos Indicadores de Comprometimento que confirmaram a presença do malware na estação de testes, uma lista de Banco de Dados Constante (*CDB*) é populada no *Wazuh*, com os respectivos *IoCs* no formato 'Chave:Valor', indicando o *malware* em questão. Essa lista pode ser preenchida com diversos indicadores, como hashes de arquivos, endereços *IP*, nomes de domínios, entre outros, e possui o seguinte formato:

$$
\begin{aligned}
&Key : Value \\
&i_1 : Malware \\
&i_2 : Malware \\
&\vdots \\
&i_n : Malware
\end{aligned}
\tag{4.8}
$$

Desse modo, para a execução do Malware2, a seguinte lista CDB foi gerada:

$$
\begin{aligned}
&Key : Value \\
&ab9cd59d789e6c7841b9d28689.....1606f184889cc7e6acadcc : AgentTesla
\end{aligned}
\tag{4.9}
$$

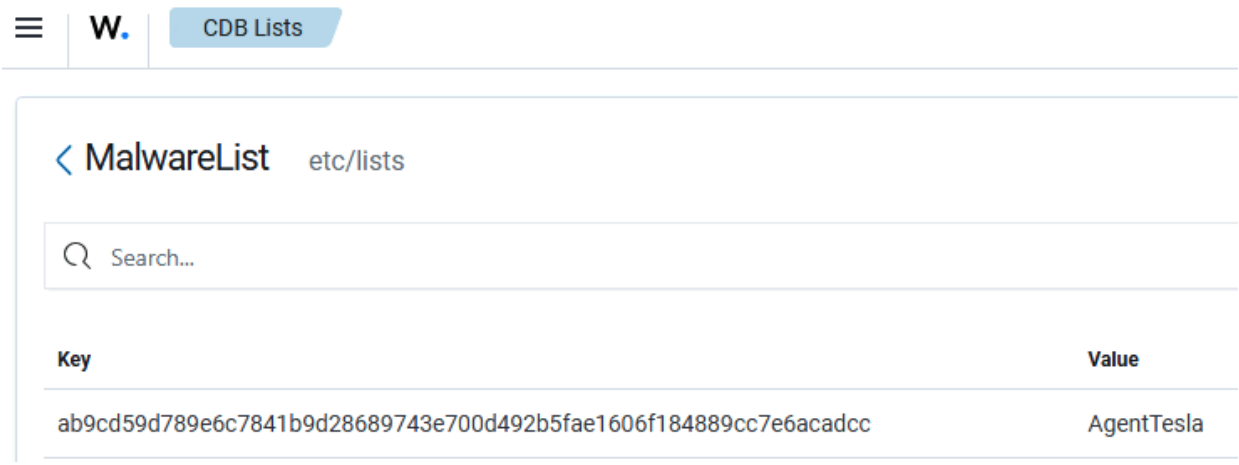


Figura 4.10: Lista CDB - Hash Agent Tesla

Uma vez configurada essa lista, qualquer conjunto de ações que envolva o manuseio desse hash, como a criação ou modificação de arquivos, passa a ser monitorado no ambiente por meio do módulo de Monitoramento de Arquivos e Integridade (*FIM - File Integrity Monitoring*), prevenindo execuções futuras. Assim que os sensores nas estações verificaram a presença dessa nova configuração, as propriedades dos arquivos foram recuperadas e comparadas com a lista *CDB* gerada, onde ocorreu uma equivalência no hash dos arquivos. Em conjunto com o módulo de Resposta Ativa (*Active Response*), o arquivo correspondente ao malware foi excluído, completando assim, todo o ciclo da metodologia proposta.

- ***FIM - Agent Tesla***: logs correspondentes ao módulo de *File Integrity Monitoring*, acusando a adição do arquivo no sistema, e logo em seguida, a sua deleção.

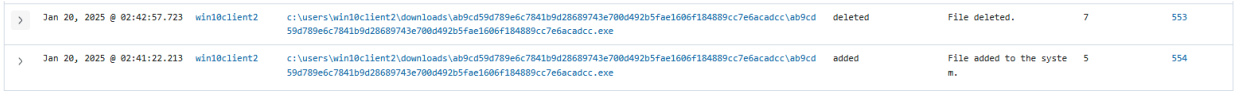


Figura 4.11: Detecção e Exclusão Agent Tesla - FIM

- ***Active Response - Agent Tesla***: na Figura 4.12, temos o log correspondente ao módulo de Active Response realizando a deleção do arquivo correspondente, e na Figura 4.13, temos o mesmo log mas de maneira completa, com informações como caminho, *hash*, atributos do arquivo, ação tomada, etc.

Figura 4.12: Exclusão Arquivo Agent Tesla - Active Response

Figura 4.13: Log Completo de Remoção Agent Tesla - Active Response

4.5.3 Caso 3 - *Malware Smoke Loader*

O *Smoke Loader* é um malware do tipo *bot* que atua principalmente como um carregador de outras ameaças, permitindo que atacantes instalem softwares maliciosos adicionais em sistemas comprometidos. Ativo desde 2011, o *Smoke Loader* é comercializado em mercados clandestinos e frequentemente utilizado para distribuir diversos tipos de malware, incluindo trojans bancários, ransomwares e mineradores de criptomoedas[59]. Além de sua função principal de carregamento, esse *malware* possui módulos próprios que permitem a execução de uma variedade de ações maliciosas sem a necessidade de componentes externos. Para evitar a detecção por soluções de segurança, ele emprega técnicas avançadas de evasão, como a criação de cópias temporárias de bibliotecas do sistema e a utilização de métodos anti-análise. A constante atualização e adaptação de suas funcionalidades o tornam o uma ameaça persistente no cenário de segurança cibernética.

Para realizarmos a validação da metodologia com um terceiro *malware*, obteve-se uma amostra aleatória do *Smoke Loader* no repositório do *Malware Bazaar*. O *malware* novamente foi executado em um ambiente de testes controlado, em uma das máquinas virtuais, e os logs correspondentes à execução foram recebidos na plataforma centralizadora de logs. Seguindo o mesmo processo, 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_{TTPs3}. Com a lista l_{TTPs3} em mãos, buscamos através do *Toolkit* desenvolvido, todos os relatórios que continham pelo menos uma das *TTPs* mencionadas anteriormente (Fig. 4.14). Todos os resultados das buscas foram gravados, em caso de necessidade de validações posteriores.

Como resultado dessa busca aos relatórios, gerou-se a lista l_{Rep3}, contendo 533 relatórios, de um conjunto de 1.840. Após a criação da lista l_{Rep3}, os relatórios nela contidos foram ranqueados com base no

(a) T1055 (b) T1070

Figura 4.14: Busca por *TTPs* do *Smoke Loader*.

número de TTPs associados, produzindo o ranking R_3. Novamente, nos 5 principais relatórios de R_3, não havia nenhuma menção específica ao Smoke Loader (Fig 4.15). Entretanto, ao revisar a lista de relatórios, havia 4 relatórios na lista, que faziam menções diretas ao *Smoke Loader*.

Figura 4.15: Ranking com 533 Relatórios

$$R_3 = f(L_{Rep3})$$

$$f(i) = |TTP_i \cap L_{TTPs3}|$$

O próximo passo do *Toolkit* seria a listagem dos *IoCs* nos relatórios. Desse modo, o *Toolkit* realiza conexões no *OpenCTI*, e realiza o levantamento de todos os *IoCs* presentes nos relatórios especificados. Essa ação gerou uma lista limpa contendo aproximadamente 8.100 indicadores de comprometimento, conforme presente na Fig. 4.16. A lista é gerada dessa maneira por questões de arquitetura, para viabilizar a utilização em seguida pela própria ferramenta.

Figura 4.16: Levantamento de *IoCs*

Ao realizarmos o correlacionamento desses indicadores de comprometimento com o *Wazuh*, houve uma correspondência positiva para um dos *IoCs* listados, que estava reportado em um dos relatórios do *Smoke Loader*. O relatório em questão era o *"SmokeLoader Evolution Through The Years"*, conforme podemos validar através da Fig. 4.17.

Figura 4.17: Identificação *malware Smoke Loader*

Partimos então para a fase de remediação da ameaça, onde adicioamos o *IoC* correspondente à lista *CDB*, já criada previamente para o *Agent Tesla* (Fig. 4.18).

$$\begin{gathered} Key : Value \\ ab9cd59d789e6c7841b9d28689.....1606f184889cc7e6acadcc : AgentTesla \\ 070a94ee0cd9ac1b1ed467353f.....447c04f53bc52d4fe3f8cc : SmokeLoader \end{gathered} \tag{4.10}$$

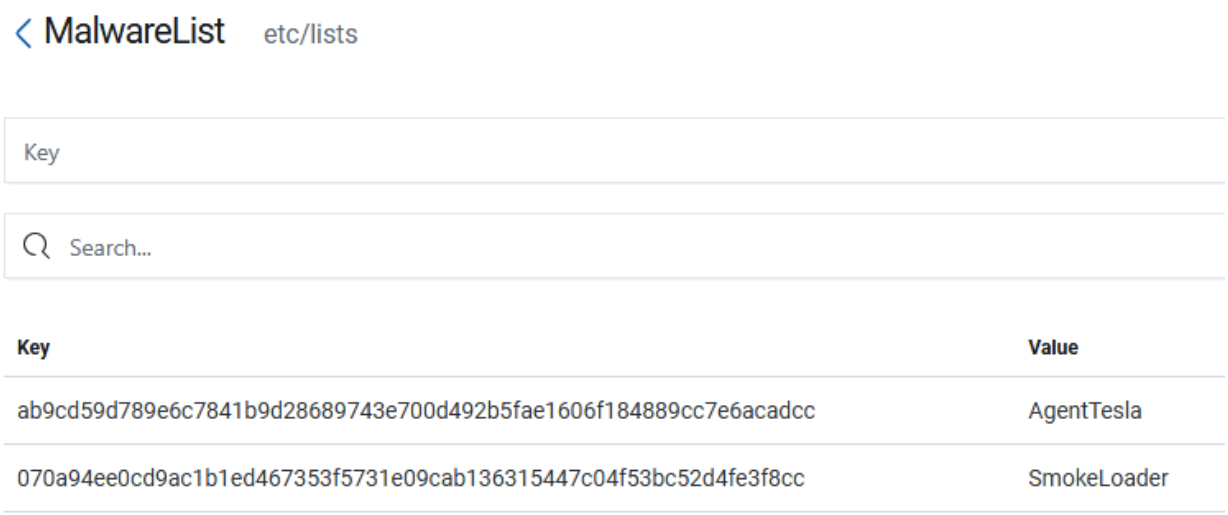


Figura 4.18: Lista CDB - Hash Smoke Loader

De modo análogo a como ocorreu no *Agent Tesla*, a partir do momento que os sensores dispostos nas máquinas receberam a configuracão imposta pela lista *CDB*, os arquivos passaram a ser monitorados em busca de uma correspondëncia, e ao achar o arquivo correspondente, o mesmo foi deletado.

4.6 DISCUSSÃO

Os experimentos realizados demonstraram a eficácia da metodologia proposta na detecção e identificação de ameaças cibernéticas, destacando a importância da correlação entre eventos de segurança e inteligência de ameaças. A separação dos estudos de caso em diferentes subseções (4.5.1 a 4.5.3) permitiu uma análise mais detalhada dos desafios enfrentados e das melhorias obtidas ao longo do processo. Além disso, a evolução metodológica ao longo dos experimentos foi essencial para refinar a abordagem, garantindo maior precisão e confiabilidade nos resultados.

Na subseção de Adaptação Metodológica (3.5.2), a primeira tentativa de implementação da metodologia revelou limitações significativas, especialmente relacionadas à dependência da ordem das *TTPs* fornecidas pelo analista. O fluxo original previa que, conforme novas *TTPs* fossem identificadas, elas seriam correlacionadas dinamicamente com malwares conhecidos. No entanto, se uma TTP fosse disponibilizada fora da sequência esperada ou omitida, a metodologia eliminava relatórios potencialmente relevantes, com-

prometendo a precisão da detecção. Esse problema evidenciou a necessidade de refinamento no critério de eliminação de relatórios e maior flexibilidade no processamento das *TTPs*.

Outra limitação identificada foi a incapacidade da correlação dinâmica de malwares fornecer uma identificação confiável do ator malicioso. A metodologia inicialmente dependia apenas da presença de *TTPs* para inferir a presença de um malware específico, sem levar em conta outros fatores, como a riqueza dos relatórios utilizados na análise. Como resultado, a abordagem original apresentou dificuldades em restringir a busca para identificar um único agente malicioso.

Para solucionar essas limitações, a metodologia evoluiu ao integrar enriquecimento de dados na plataforma de inteligência de ameaças. No Caso 1 (4.5.2), a incorporação de informações mais robustas nos relatórios, incluindo detalhes sobre os *malwares* e suas campanhas associadas, permitiu uma melhoria significativa na precisão da detecção e identificação. Essa nova abordagem garantiu que a correlação entre eventos e *TTPs* fosse mais confiável, reduzindo falsos positivos e acelerando a convergência das investigações. Dessa forma, conseguimos avançar para um modelo que não apenas identifica padrões de ataque, mas também permite a identificação precisa de um agente de ameaça específico, conectando as evidências coletadas a um adversário conhecido.

No Caso 2 (4.5.3), realizamos uma segunda validação utilizando uma amostra previamente conhecida do *Agent Tesla*. Diferente do Caso 1, aqui partimos de um malware cuja presença já estava documentada na base de relatórios da *TIP*, permitindo uma análise mais precisa do processo de identificação. Os testes demonstraram que, ao utilizarmos amostras bem documentadas e relatórios de maior qualidade, foi possível refinar a correlação entre *TTPs* e *IoCs*, resultando em uma identificação mais confiável do *malware*. Esse estudo confirmou que a disponibilidade de relatórios ricos em detalhes e atualizados tem um impacto direto na capacidade da metodologia de realizar uma identificação precisa.

Reconhece-se, contudo, que na prática organizacional, raramente se dispõe de amostras tão bem documentadas ou relatórios de alta qualidade em tempo hábil. Esse fato representa uma limitação importante: quanto mais completas as informações (mapeando *TTPs* e descrevendo *IoCs* confiáveis), mais eficiente se torna o processo de correlação. Em ambientes reais, muitas fontes podem ser incompletas, o que reforça a necessidade de metodologias robustas e processos de validação capazes de lidar com dados parciais ou inconsistentes.

No Caso 3 (4.5.3), validamos a aplicação da metodologia para um malware diferente, coletado do repositório *Malware Bazaar*. A execução do *Smoke Loader* em um ambiente de testes controlado permitiu analisar sua interação com o sistema, registrando os logs correspondentes. A busca por *TTPs* resultou em 533 relatórios, onde inicialmente não houve uma referência direta ao *Smoke Loader* nos primeiros relatórios ranqueados. No entanto, uma análise mais aprofundada revelou quatro relatórios com menção direta ao *malware*, permitindo correlacionar os *TTPs* e *IoCs* observados com uma base documentada de ameaças. Essa validação reforça a robustez da metodologia em diferentes cenários e contra diferentes agentes maliciosos.

Outro aspecto fundamental identificado nos experimentos foi a dependência da metodologia na qualidade dos relatórios carregados na plataforma de inteligência de ameaças. A precisão da identificação das ameaças está diretamente relacionada ao nível de detalhe dos dados disponíveis. Relatórios superficiais ou inconsistentes podem comprometer a eficácia da detecção, resultando em identificações imprecisas ou na

necessidade de intervenções manuais adicionais para validação dos eventos. Dessa forma, é essencial que a curadoria dos dados de inteligência seja realizada com rigor, garantindo que as fontes utilizadas possuam informações confiáveis e bem estruturadas.

Por fim, os resultados obtidos reforçam o potencial da metodologia proposta em otimizar a detecção e identificação de ameaças cibernéticas. A integração de inteligência de ameaças ao processo de correlação de eventos demonstrou ser uma estratégia eficiente para reduzir o tempo de resposta a incidentes e aprimorar a visibilidade sobre ataques em andamento. No entanto, a eficácia da abordagem depende da qualidade, estruturação e evolução contínua da metodologia, destacando a necessidade de aprimoramentos constantes para garantir sua aplicabilidade em cenários dinâmicos e ambientes corporativos complexos.

4.6.1 Respostas às Perguntas de Pesquisa

Nesta subseção, revisitam-se as perguntas de pesquisa definidas no Capítulo 1, avaliando em que medida foram respondidas pelos resultados obtidos nos estudos de caso (Seção 4.5).

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

As análises realizadas nos Casos 2 (Seção 4.5.2) 3 (Seção 4.5.3) demonstraram que a correlação de dados de fontes externas de *CTI* (por exemplo, *AlienVaultOTX*) com os eventos coletados pelo *Wazuh*, aliada ao *OpenCTI*, viabilizou uma detecção mais ágil e eficaz de *malwares* como o *Agent Tesla* e o *Smoke Loader*. Observou-se que, quando existiam *IoCs* confiáveis e relatórios detalhados, o sistema de monitoramento pôde identificar comportamentos suspeitos de forma mais direcionada, reduzindo falsos positivos e facilitando a triagem dos alertas mais críticos. Dessa forma, a PP1 foi amplamente atendida, pois os experimentos mostraram que a integração de *CTI* enriquece significativamente o processo de detecção de ameaças avançadas, conferindo às equipes de segurança maior capacidade de resposta.

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

No Caso 2 (*Agent Tesla*), ao mapear as atividades suspeitas no *framework MITRE ATT&CK* e correlacioná-las com os relatórios de fontes externas, tornou-se parcialmente factível detectar comportamentos maliciosos, uma vez que os indicadores de comprometimento não estavam previamente catalogados. Já no Caso 3 (*Smoke Loader*), ao associar *TTPs* juntamente aos indicadores de comprometimento, a detecção pôde ser estabelecida. Assim, a PP2 foi parcialmente respondida, pois, embora o uso de *TTPs* em conjunto à inteligência de ameaça cibernética tenha se mostrado eficaz para identificar comportamentos avançados, a eficácia da detecção depende fortemente da qualidade e da atualização frequente dos relatórios de CTI. Portanto, há espaço para investigações adicionais em cenários mais amplos e com maior variedade de *malwares*.

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

Os testes evidenciaram que a simples adição de *IoCs* em um *SIEM* não é suficiente para lidar com *APTs* que se adaptam facilmente aos ambientes, e atualizam os seus métodos de ataque de forma dinâmica. Quando os *IoCs* eram complementados por dados contextuais – tais como a frequência de uso, associação a campanhas ativas ou mesmo vínculo com *TTPs* – a plataforma de monitoramento foi capaz de produzir alertas mais coerentes e descartar falsos positivos recorrentes. Pode-se então concluir que a PP3 foi amplamente atendida, pois ao enriquecermos os dados com fontes adicionais de *CTI*, foi produzida inteligência acionável, que auxiliou no processo de detecção de ameaças.

5 CONCLUSÃO

A integração de fontes de inteligência cibernética no contexto de sistemas de Gerenciamento de Informações e Eventos de Segurança demonstrou ser uma abordagem eficaz para melhorar a detecção e prevenção de ameaças cibernéticas avançadas. A pesquisa demonstrou que a combinação de diferentes camadas de *CTI*, incluindo relatórios detalhados (com *TTPs*) e *IoCs* atualizados, proporcionou uma detecção e resposta mais ágil. Ressalta-se que os *IoCs* fazem parte da inteligência de ameaças, mas seu uso isolado pode ser complementado pela análise de Táticas, Técnicas e Procedimentos, aumentando a eficácia geral das defesas. 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 de ameaças, especialmente ao correlacionar Táticas, Técnicas e Procedimentos com ameaças. A pesquisa demonstrou que, ao adicionar camadas adicionais de contexto aos *TTPs* e *IoCs* conhecidos, foi possível melhorar significativamente a precisão da detecção e acelerar as respostas a incidentes.

Além disso, a análise dos *IoCs* mostrou-se eficaz na detecção de *malwares* avançados, como o *Agent Tesla* e o *Smoke Loader*, 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.

5.1 TRABALHOS FUTUROS

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 geral 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, especialmente se os modelos forem explicáveis ou interpretáveis. 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 identificação.

REFERÊNCIAS BIBLIOGRÁFICAS

1 FERDOUS, J.; ISLAM, R.; MAHBOUBI, A.; ISLAM, M. Z. A review of state-of-the-art malware attack trends and defense mechanisms. *IEEE Access*, v. 11, p. 121118–121141, 2023.

2 CROWDSTRIKE. *Indicators of Attack (IOA) vs. Indicators of Compromise (IOC)*. 2025. Accessed on: February 15, 2025. Disponível em: <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/ioa-vs-ioc/>.

3 AINSLIE, S.; THOMPSON, D.; MAYNARD, S.; AHMAD, A. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers Security*, v. 132, p. 103352, 2023. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404823002626>.

4 Silva, A. Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto. In: *Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília*. [s.n.], 2020. Disponível em: <https://repositorio.unb.br/handle/10482/40541>.

5 KRISHNAPRIYA, S.; SINGH, S. A comprehensive survey on advanced persistent threat (apt) detection techniques. *Computers, Materials and Continua*, v. 80, n. 2, p. 2675–2719, 2024. ISSN 1546-2218. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1546221824005952>.

6 Abu, M.; Selamat, S.; Ariffin, A.; Yusof, R. Cyber threat intelligence – issue and challenges. In: *Indonesian Journal of Electrical Engineering and Computer Science 10*. [s.n.], 2018. p. 371–379. Disponível em: <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>.

7 ASLAN, A.; SAMET, R. A comprehensive review on malware detection approaches. *IEEE Access*, v. 8, p. 6249–6271, 2020.

8 Wu, J. New approaches to cyber defense. in: Cyberspace mimic defense. In: *[S.l.]: Springer*. [S.l.: s.n.], 2020. p. 113–157. ISBN 978-3-030-29844-9.

9 Imperva. Advanced persistent threat (apt). In: *Advanced persistent threat (APT)*. [s.n.], 2024. Acessed on: August 21, 2024. Disponível em: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>.

10 HUFF, P.; MASSENGALE, S.; PHUONG, T. V. X.; GOURISETTI, S. N. G. A privacy-preserving cyber threat intelligence sharing system. In: *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. [S.l.: s.n.], 2024. p. 49–58.

11 Sagar, S. Developing proactive cyber threat intelligence from the online hacker community: A computational design science approach. In: *The University of Arizona.* [s.n.], 2018. Disponível em: <http://hdl.handle.net/10150/628454>.

12 Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. In: *Computers Security, Elsevier BV*. [s.n.], 2018. v. 72, p. 212–233. ISSN 0167-4048. Disponível em: <https://doi.org/10.1016/j.cose.2017.09.001>.

13 Sauerwein, C.; Sillaber, C.; Mussmann, A.; Breu, R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In: *The 13th International Conference on Wirtschaftsinformatik*. [s.n.], 2017. p. 837–851. Disponível em: <https://wi2017.ch/images/wi2017-0188.pdf>.

14 Leite, C.; Hartog, J. den; Santos, D. R. dos; Constante, E. Actionable cyber threat intelligence for automated incident response. In: *Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30–December 2, 2022, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2023. p. 368–385. ISBN 978-3-031-22294-8. Disponível em: <https://doi.org/10.1007/978-3-031-22295-5_20>.

15 VIEIRA, A. A. d. S. e.; GONDIM, J. J. C. Metodologia integrativa para a detecção e prevenção de ameaças utilizando inteligência de ameaça cibernética e siem. In: *Atas das Conferências Ibero-Americanas COMPUTAÇÃO APLICADA e WWW/INTERNET*. [S.l.]: IADIS (International Association For Development Of The Information Society), 2024. v. 11, p. 57–65.

16 Rahul Awati. Iloveyou virus. In: *Tech Target*. [s.n.], 2021. Accessed on: January 10, 2025. Disponível em: <https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus>.

17 HUANG, D. Y.; ALIAPOULIOS, M. M.; LI, V. G.; INVERNIZZI, L.; BURSZTEIN, E.; MCROBERTS, K.; LEVIN, J.; LEVCHENKO, K.; SNOEREN, A. C.; MCCOY, D. Tracking ransomware end-to-end. In: *2018 IEEE Symposium on Security and Privacy (SP)*. [S.l.: s.n.], 2018. p. 618–631.

18 Actual Media. The history of ransomware. In: *The History of Ransomware*. [s.n.]. Accessed on: January 12, 2025. Disponível em: <https://ransomware.org/what-is-ransomware/the-history-of-ransomware/>.

19 BARR-SMITH, F.; UGARTE-PEDRERO, X.; GRAZIANO, M.; SPOLAOR, R.; MARTINOVIC, I. Survivalism: Systematic analysis of windows malware living-off-the-land. In: *2021 IEEE Symposium on Security and Privacy (SP)*. [S.l.: s.n.], 2021. p. 1557–1574.

20 BEERMAN, J.; BERENT, D.; FALTER, Z.; BHUNIA, S. A review of colonial pipeline ransomware attack. In: *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. [S.l.: s.n.], 2023. p. 8–15.

21 AL-RABIAAH, S. The "stuxnet" virus of 2010 as an example of a "apt" and its "recent" variances. In: *2018 21st Saudi Computer Society National Computer Conference (NCC)*. [S.l.: s.n.], 2018. p. 1–5.

22 MITRE ATTCK. Solarwinds compromise. In: *Campaigns*. [s.n.], 2024. Accessed on: January 10, 2025. Disponível em: <https://attack.mitre.org/campaigns/C0024/>.

23 NOVAK, P.; OUJEZSKY, V. Heuristic malware detection method based on structured cti data: A research study and proposal. In: *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. [S.l.: s.n.], 2024. p. 1–6.

24 BIJMANS, H.; LEUKEN, M. van. No time to choose: Leveraging internet scans to determine ioc lifetimes. In: *2024 IEEE International Conference on Big Data (BigData)*. [S.l.: s.n.], 2024. p. 2586–2595.

25 MAVROEIDIS, V.; BROMANDER, S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: *2017 European Intelligence and Security Informatics Conference (EISIC)*. [S.l.: s.n.], 2017. p. 91–98.

26 UK Cyber Security Program. In: *Cyber Threat Intelligence in Government: A Guide for Decision Makers Analysts*. [s.n.], 2019. Accessed on: January 20, 2025. Disponível em: <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf>.

27 SILVA, R.; GONDIM, J.; ALBUQUERQUE, R. Methodology to improve the quality of cyber threat intelligence production through open source platforms. In: ____. [S.l.: s.n.], 2023. p. 86–98. ISBN 978-3-031-30591-7.

28 SONWANI, H.; DIVYA, M.; DHAWAN, A.; MANTRI, A.; G, D.; KUMAR, H. A comprehensive study on threat intelligence platform. In: *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. [S.l.: s.n.], 2022. p. 1–5.

29 MANSUR, A. A.; ZAMAN, T. User behavior analytics in advanced persistent threats: A comprehensive review of detection and mitigation strategies. In: *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*. [S.l.: s.n.], 2023. p. 1–6.

30 USSATH, M.; JAEGER, D.; CHENG, F.; MEINEL, C. Advanced persistent threats: Behind the scenes. In: *2016 Annual Conference on Information Science and Systems (CISS)*. [S.l.: s.n.], 2016. p. 181–186.

31 LI, M.; HUANG, W.; WANG, Y.; FAN, W.; LI, J. The study of apt attack stage model. In: *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. [S.l.: s.n.], 2016. p. 1–5.

32 BREWER, R. Advanced persistent threats: minimising the damage. *Network Security*, v. 2014, n. 4, p. 5–9, 2014. ISSN 1353-4858. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1353485814700406>.

33 VUKALOVIć, J.; DELIJA, D. Advanced persistent threats - detection and defense. In: *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. [S.l.: s.n.], 2015. p. 1324–1330.

34 Abu Talib, M.; NASIR, Q.; Bou Nassif, A.; MOKHAMED, T.; AHMED, N.; MAHFOOD, B. Apt beaconing detection: A systematic review. *Computers Security*, v. 122, p. 102875, 2022. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404822002693>.

35 CHEN, P.; DESMET, L.; HUYGENS, C. A study on advanced persistent threats. In: DECKER, B. D.; ZÚQUETE, A. (Ed.). *Communications and Multimedia Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. p. 63–72. ISBN 978-3-662-44885-4.

36 GHAFIR, I.; KYRIAKOPOULOS, K. G.; LAMBOTHARAN, S.; APARICIO-NAVARRO, F. J.; ASSADHAN, B.; BINSALLEEH, H.; DIAB, D. M. Hidden markov models and alert correlations for the prediction of advanced persistent threats. *IEEE Access*, v. 7, p. 99508–99520, 2019.

37 MAHBOUBI, A.; LUONG, K.; ABOUTORAB, H.; BUI, H. T.; JARRAD, G.; BAHUTAIR, M.; CAMTEPE, S.; POGREBNA, G.; AHMED, E.; BARRY, B.; GATELY, H. Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, v. 232, p. 104004, 2024. ISSN 1084-8045. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804524001814>.

38 JIN, B.; KIM, E.; LEE, H.; BERTINO, E.; KIM, D.; KIM, H. Sharing cyber threat intelligence: Does it really help? *Proceedings 2024 Network and Distributed System Security Symposium*, 2024. Disponível em: <https://api.semanticscholar.org/CorpusID:267625726>.

39 GONZáLEZ-GRANADILLO, G.; GONZáLEZ-ZARZOSA, S.; DIAZ, R. Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, v. 21, n. 14, 2021. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/21/14/4759>.

40 BERADY, A.; JAUME, M.; TONG, V. V. T.; GUETTE, G. From ttp to ioc: Advanced persistent graphs for threat hunting. *IEEE Transactions on Network and Service Management*, v. 18, n. 2, p. 1321–1333, 2021.

41 SPYROS, A.; KORITSAS, I.; PAPOUTSIS, A.; PANAGIOTOU, P.; CHATZAKOU, D.; KAVALLIEROS, D.; TSIKRIKA, T.; VROCHIDIS, S.; KOMPATSIARIS, I. Ai-based holistic framework for cyber threat intelligence management. *IEEE Access*, v. 13, p. 20820–20846, 2025.

42 ÇAKMAKçı, S. D.; GKOKTSIS, G.; BUCHTA, R.; DETKEN, K. O.; HEINE, F.; KLEINER, C. Apt detection: An incremental correlation approach. In: *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. [S.l.: s.n.], 2023. v. 1, p. 151–156.

43 MAHMOUD, M.; MANNAN, M.; YOUSSEF, A. Apthunter: Detecting advanced persistent threats in early stages. *Digital Threats*, Association for Computing Machinery, New York, NY, USA, v. 4, n. 1, mar. 2023. Disponível em: <https://doi-org.ez54.periodicos.capes.gov.br/10.1145/3559768>.

44 BUCHTA, R.; GKOKTSIS, G.; HEINE, F.; KLEINER, C. Advanced persistent threat attack detection systems: A review of approaches, challenges, and trends. *Digital Threats*, Association for Computing Machinery, New York, NY, USA, v. 5, n. 4, dez. 2024. Disponível em: <https://doi-org.ez54.periodicos.capes.gov.br/10.1145/3696014>.

45 ALI, A.; PENG, M.-C. Ttpmapper: Accurate mapping of ttps from unstructured cti reports. In: *2024 IEEE International Conference on Future Machine Learning and Data Science (FMLDS)*. [S.l.: s.n.], 2024. p. 558–563.

46 SACHIDANANDA, V.; PATIL, R.; SACHDEVA, A.; LAM, K.-Y.; YANG, L. Apter: Towards the investigation of apt attribution. In: *2023 IEEE Conference on Dependable and Secure Computing (DSC)*. [S.l.: s.n.], 2023. p. 1–10.

47 KERN, M.; SKOPIK, F.; LANDAUER, M.; WEIPPL, E. Strategic selection of data sources for cyber attack detection in enterprise networks: a survey and approach. In: *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2022. (SAC '22), p. 1656–1665. ISBN 9781450387132. Disponível em: <https://doi-org.ez54.periodicos.capes.gov.br/10.1145/3477314.3507022>.

48 MITRE ATT&CK. Matrix - enterprise. In: *Enterprise Matrix*. [s.n.], 2024. Accessed on: September 9, 2024. Disponível em: <https://attack.mitre.org/matrices/enterprise/>.

49 VirusTotal. Reports. In: *VTDoc*. [s.n.], 2024. Accessed on: October 5, 2024. Disponível em: <https://docs.virustotal.com/docs/results-reports>.

50 Hybrid Analysis. Public knowledge base. In: *Free Automated Malware Analysis*. [s.n.], 2024. Accessed on: October 5, 2024. Disponível em: <https://www.hybrid-analysis.com/knowledge-base>.

51 Wazuh. The open source security platform. In: . [s.n.], 2024. Accessed on: August 25, 2024. Disponível em: <https://wazuh.com>.

52 Filigran. Opencti documentation space. In: *OpenCTI Documentation*. [s.n.], 2024. Accessed on: August 24, 2024. Disponível em: <https://docs.opencti.io/latest/>.

53 Hartong, O. A sysmon configuration repository for everybody to customise. In: *sysmon-modular*. [s.n.], 2023. Accessed on: Semptember 1, 2024. Disponível em: <https://github.com/olafhartong/sysmon-modular>.

54 MalwareBazaar. Malwarebazaar database. In: *MalwareBazaar by Abuse*. [s.n.], 2024. Accessed on: August 24, 2024. Disponível em: <https://bazaar.abuse.ch>.

55 WIDIYASONO, N.; SELAMAT, S. R.; RIZAL, R.; FIDAYAN, A.; MULYANI, S. R.; RISNANTO, S. Advanced malware analysis methods: Behaviour-based detection and reverse engineering. In: *2024 18th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*. [S.l.: s.n.], 2024. p. 1–5.

56 TECHNOLOGIES, C. P. S. *Agent Tesla Malware*. 2025. Accessed on: February 23, 2025. Disponível em: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware/>.

57 AWASTHI, K. *Decoding Agent Tesla: The Spyware Stealing Data Silently!* 2024. Accessed on: February 24, 2025. Disponível em: <https://fidelissecurity.com/threatgeek/threat-intelligence/agent-tesla/>.

58 PREUVENEERS, D.; JOOSEN, W. Sharing machine learning models as indicators of compromise for cyber threat intelligence. *Journal of Cybersecurity and Privacy*, v. 1, n. 1, p. 140–163, 2021. ISSN 2624-800X. Disponível em: <https://www.mdpi.com/2624-800X/1/1/8>.

59 GUBI, I. *The 2019 Resurgence of Smokeloader*. 2019. Accessed on: February 25, 2025. Disponível em: <https://research.checkpoint.com/2019/2019-resurgence-of-smokeloader/>.